UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO STRICTU SENSU

SÍLVIA LEVENFUS

DISSERTAÇÃO DE MESTRADO

O RECONHECIMENTO FACIAL COMO GARANTIA DA PREVENÇÃO À FRAUDE E DA SEGURANÇA DO TITULAR (ART. 11, g, da LGPD)

O RECONHECIMENTO FACIAL COMO GARANTIA DA PREVENÇÃO À FRAUDE E DA SEGURANÇA DO TITULAR (ART. 11, g, da LGPD)

Dissertação de Mestrado apresentada como requisito parcial à aprovação junto ao Programa de Pós-Graduação da Universidade Federal do Rio Grande do Sul, em nível de Mestrado, sob orientação do Prof. Dr. Fabiano Menke.

Porto Alegre

2021

banca

Agradecimentos

Aos meus pais, David e Rosane, pelo apoio incansável nesta

jornada.

Ao meu orientador , Prof. Dr. Fabiano Menke, por todos os ensinamentos e compartilhamentos de ideias.

À Universidade Federal do Rio Grande do Sul – UFRGS, por permitir meu

crescimento pessoal e acadêmico.

Por fim, a todos que, de alguma forma, contribuíram na minha trajetória,

tornando possível a elaboração deste trabalho.

Resumo

O presente estudo tem por objeto analisar a temática do reconhecimento facial (dado pessoal sensível); refletindo sobre os seus benefícios, desafios e como o mundo jurídico brasileiro deve compreender e regular. Com base em uma abordagem hipotético-dedutiva, busca-se contextualizar biometria, o funcionamento da tecnologia de reconhecimento facial e refletir sobre a sua acurácia em diferentes contextos. Com a publicação da Lei Geral de Proteção de Dados brasileira (LGPD), pretende-se compreender o significado pretendido pelo legislador com o art. 11, II, alínea g e, a partir disso, verificar a sua aplicação no campo prático e ético. Expõem-se alternativas substitutivas e metodológicas para tema tão complexo. Entende-se pela insuficiência, *a priori*, do ordenamento brasileiro – em específico, a LGPD; para lidar com o reconhecimento facial. Sugere-se a alternativas principiológicas e orientativas, e um exercício cauteloso de ponderação, sob pena de a inovação afrontar a privacidade e os direitos individuais.

Palavras-chave: Reconhecimento facial. LGPD. Privacidade.

Abstract

The present study aims to analyze the topic of facial recognition (sensitive personal data); reflecting on its benefits, challenges and how the Brazilian legal world should understand and regulate. Based on a hypothetical-deductive approach, we seek to contextualize biometrics, the functioning of facial recognition technology and reflect on its accuracy in different contexts. With the publication of the Brazilian General Data Protection Law (LGPD), we seek to understand the meaning intended by the legislator with art. 11, II, point g and, from there, verify its application in the practical and ethical fields. Substitute and methodological alternatives are exposed for such a complex topic. It is understood by the insufficiency, a priori, of the Brazilian legal system - specifically, the LGPD; to handle facial recognition. We suggest alternative principles and guidelines, and a cautious exercise of weighting, otherwise the innovation will affront privacy and individual rights.

Keywords: Facial recognition. LGPD. Privacy.

"Assim, ganha relevância, de maneira nova, o corpo, que se torna fonte direta de informações, objeto de um contínuo data mining, efetivamente uma mina a céu aberto da qual é possível extrair dados ininterruptamente. Repetimos: o corpo, em si, está se tornando uma password".

Stefano Rodotá, em "A vida na sociedade de vigilância",p. 265

SUMÁRIO

INTRODUÇÃO

Sistemas de identificação digital onipresentes não são mais o reino da fantasia futurista ou distópica[1], como previsto por George Orwell, Aldous Huxley, Margaret Atwood. A tecnologia, especificamente a de reconhecimento facial, pode ser encontrada em aeroportos, elevadores, instituições privadas e na palma da mão (celulares).

O que se entendeu por público e privado não mais representa a sociedade atual. O conceito de privacidade igualmente vem contornando de forma maleável a sociedade, para que se possa adaptar aos novos tempos.

Na Roma antiga, denominava-se *pessoa* a máscara utilizada por atores. A palavra *persona,* de origem latina, não significava sujeito de direitos (até porque os escravos romanos eram considerados coisas), mas sim, *máscara*[2]. Assim como o termo pessoa, que hoje possui relação com sujeito de direito, a privacidade nem sempre possuiu o mesmo significado. Pelo contrário, molda-se constantemente para acompanhar o dinamismo da sociedade.

Em relação ao domínio público e privado, a nomenclatura "privado" advém do *privativo*[3]: "viver uma vida inteiramente privada significa, acima de tudo, estar privado de coisas essenciais a uma vida verdadeiramente humana".[4] E, em se tratando da privatividade, poder-se-ia equivaler domínio público e privado como "o que deve ser exibido e o que deve ser ocultado". Posteriormente, criado o entendimento de que o domínio do oculto pode ser vasto e amplo no que tange à intimidade (e não privatividade)[5].

E, portanto, embora domínio público e privado não sejam traduzidos como publicizar e ocultar, compreende-se que o seu significado intrínseco foi transposto: "há coisas que devem ser ocultadas e outras que necessitam ser expostas em público para

---

[1] ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ . Acesso em 03 mar. 2022, p. 1

[2] MOREIRA ALVES, Jose Carlos. Direito Romano 16 ed. Rio de Janeiro: Forense,2014, p. 97

[3] Nesse sentido: "A privatividade era como que o outro lado escuro e oculto do domínio público, e como ser político significava atingir a mais alta possibilidade da existência humana, não possuir um lugar privado próprio (como no caso do escravo) significava deixar de ser humano. ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020, p. 79

[4] ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020, p. 72.

[5] ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020, p. 88-89

que possam adquirir alguma forma de existência".[6] Nesse sentido, o que resta da privatividade na esfera moderna é justamente a de abrigar o que é íntimo[7].

Em relação ao debate sobre intimidade e nascimento da privacidade, merece relevância o século XIX. A substituição de um perfil rural, por uma sociedade urbana, com avanços tecnológicos, como jornais, rádio e televisão, exigia também uma alteração nos direitos individuais. Questões atinentes à *propriedade privada* eram debatidas nos tribunais, mas passou-se a vislumbrar a *necessidade de uma proteção mais ampla* em relação *a* outras questões que surgiram em decorrência do tema: "fotografias instantâneas e as empresas jornalísticas invadiram os recintos da vida privada e doméstica, [...] a fofoca [...] tornou-se um comércio"[8].

Exemplifica-se com o caso Pollard *versus* Photographic Co 40 Ch. Div. 345 (1888), em que um fotógrafo tirou uma foto de uma senhora e foi proibido de exibir e vender as cópias das fotos, sob o argumento de descumprimento implícito de termo contratual e *quebra de confiança*[9].

Para tanto, naquele momento o termo "propriedade" significava tanto posse tangível quanto intangível[10] . Outras questões além do campo físico, como as emoções, pensamentos e sensações estavam requerendo também reconhecimento legal e proteção. Assim, o próximo passo para a proteção da pessoa em uma esfera mais intangível, seria o que o Juiz Cooley denominou como *"direito de ser deixado só"*[11]. Portanto, surgido na Common Law e não em âmbito legislativo, a necessidade de uma proteção mais ampla do direito proprietário fez com que dois juristas, Samuel Warren e Louis Brandeis publicasem o artigo "The right to privacy". O texto ficou conhecido como o pioneiro a abordar o tema da privacidade[12].

---

[6] ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020, p. 90.

[7] ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020, p. 47

[8] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890 – p.195-196.

[9] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890 – p.208

[10] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890, p. 193. Um dos argumentos utilizados pelo advogado do fotógrafo no caso Pollard *versus* Photographic Co 40 Ch. Div. 345 (1888), foi o de que uma pessoa não tem a posse de suas caracterísitcas, não sendo cabível a restrição no uso da imagem pelo fotógrafo. WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890, p. 208-209

[11] Trazução livre do autor. Original; "the right to be let alone". WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890, p. 195.

[12] Assim: "a moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o célebre artigo de Brandeis e Warren, The right do Privacy, apresenta uma clara liha evolutiva".

Já no século XX, grandes mudanças ocorreram. Ao final da 2ª Guerra Mundial, o resultado do extermínio de milhões de pessoas gerou a enorme necessidade de proteção da esfera humana. Nesse sentido, a publicação da Declaração Universal dos Direitos Humanos pela ONU, em 1948[13]. O seu artigo 12 assim refere: "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais inferências ou ataques".

Merece destaque também o cenário alemão, posto que o país apresenta o maior desenvolvimento doutrinário e valorização sobre a temática de proteção de dados. Inclusive, o tema é tratado como instituto autônomo no país (*Datenschutz*)[14]. Em 1949, publicada a Lei Fundamental da República Federal da Alemanha. O artigo art. 2º, §1º, relativo ao livre desenvolvimento da personalidade assim referia: "Todos têm o direito ao livre desenvolvimento de sua personalidade, desde que não violem direitos de outrem e não se choquem contra a ordem constitucional ou a lei moral"[15]. Cumpre ressaltar que a sua aplicação foi controversa, principalmente no que tange à sua interpretação de forma mais ampla ou restrita[16].

A Corte alemã reconheceu que a norma do art. 2º, §1º não abrigava somente um direito de liberdade geral de ação (Caso Elfes), mas também um direito ao respeito à esfera privada (decisões do microcenso BVerGE 27, 1 (6) e dos autos de divórcio (BVerGE 27, 344 (352)) de 1969 e 1970, respectivamente[17]. O direito geral de personalidade alemão é fruto do artigo 1º, §1º (dignidade da pessoa) com o art. 2º, §1º (liberdade) da Lei Fundamental.

Em 1970, na Alemanha, o Estado de Hesse editou a primeira normativa mundial sobre proteção de dados. E, em 1977, foi aprovada pelo Parlamento alemão a Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*). Entretanto, foi em 1983 com

---

DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.30.

[13] UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em 02 fev. 2022.

[14] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coords). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015, p. 205- 230, p. 205

[15] SCHWABE, J. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. MARTINS, Leonardo; HENNIG, Beatriz et al (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005, p. 187

[16] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020, p. 2.

[17] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020, p. 4

a Lei do Censo (*Volkszählungsgesetz*) que ocorreu o ápice do reconhecimento da proteção de dados[18], conforme se verá a seguir.

A referida lei objetivava realizar um novo censo populacional, no qual haveria também uma coleta de inúmeros dados pessoais dos cidadãos como: nome, endereço, telefone, estado civil, religião, fonte principal de sustento, ocupação profissional, formação profissional, função desempenhada no emprego.[19] Ressalta-se a possibilidade de que os dados coletados pudessem acabar vinculando indivíduos, posto que eram mais de 160 perguntas a serem respondidas. Além disso, o objetivo não era apenas para fins estatísticos, mas igualmente para comparação e correção de registros. Este contexto fez surgir um grande receio na população, com uma percepção geral contra o aumento da vigilância e do processamento de dados[20].

Várias Reclamações Constitucionais foram ajuizadas contra a lei, referindo que violava alguns direitos fundamentais, como o direito ao livre desenvolvimento da personalidade derivado do Art. 2º, §1º da Lei Fundamental. No mérito, o Tribunal Constitucional alemão (TCF) julgou as Reclamações Constitucionais parcialmente procedentes, confirmando a constitucionalidade da lei. Entretanto, declarou a nulidade dos dispositivos que falavam sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa[21]. Portanto, em que pese tenha sido considerada constitucional, vários pontos foram modificados para que fosse possível observar a proteção dos dados dos cidadãos, como a transferência destes dados a outros órgãos governamentais[22].

Ademais, diferentemente de outras decisões anteriores da Corte, esta deixou claro que " não mais importava se as informações coletadas dos cidadãos eram íntimas,

[18] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coords). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015, p. 205

[19] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coords). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015, p. 206-207.

[20] HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law And Security Review*, Kassel, n. 25, p. 84-88, 2009, p.85

[21] SCHWABE, J. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. MARTINS, Leonardo; HENNIG, Beatriz et al (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005, p. 233-234

[22] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coords). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015, p. 207

privadas ou públicas, tratava-se, antes, dos riscos para a personalidade que poderiam surgir do processamento eletrônico dos dados"[23]. Isso porque, este processamento poderia ameaçar o poder do indivíduo de decidir se e como gostaria fornecer a outros os seus dados pessoais, tendo em vista a possibilidade de "elaboração de um perfil completo da personalidade por meio de sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização".[24]

Assim, a presente decisão reconheceu constitucionalmente, pela primeira vez, a autodeterminação informativa, em que pese o seu desenvolvimento tenha ocorrido ao longo de vários julgados do Tribunal Constitucional da Alemanha. Para tanto, o surgimento do direito à autodeterminação informativa[25] é instrínseco à proteção da personalidade como direito fundamental, posto ser um desdobramento do direito ao livre desenvolvimento da personalidade[26]. De acordo com Gerrit Hornung e Christoph Schnabel, a autodeterminação informativa é a âncora legal para a proteção de dados na Constituição alemã, sendo a decisão mais importante na história de proteção de dados do país[27]. Ademais, ainda que na época da decisão sobre o censo a vigilância era muito menos intensa, a população criou uma consciência sobre os efeitos negativos que a vigilância poderia trazer à democracia[28].

Após a decisão do censo de 1983, a autodeterminação informativa foi elevada como fundamento da disciplina de proteção de dados pessoais[29], influenciando com que outros países buscassem criar normativas e proteção aos dados pessoais.

Mas, como refere Stefano Rodotá, a privacidade não pode mais ser analisada sob o prisma: "entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus

---

[23] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020, p. 11

[24] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020, p. 11

[25] Ou autodeterminação informacional.

[26] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020, p. 2

[27] HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law And Security Review*, Kassel, n. 25, p. 84-88, 2009, p.85

[28] HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law And Security Review*, Kassel, n. 25, p. 84-88, 2009, p.90.

[29] Nesse sentido, o reconhecimento pela Lei Geral de Proteção de Dados brasileira da autodeterminação informativa como fundamento da disciplina de proteção de dados pessoais: Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa. BRASIL. BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 fev 2022.

segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais[..]". [30] Nesse sentido, em que pese ainda possa ser utilizada em situações específicas, o "direito a ser só" não mais representa uma definição propriamente dita de privacidade.

A esfera privada sofreu uma ampliação progressiva, abrangendo situações mais diversas: "conjunto de ações, comportamentos, opiniões, preferências, informações pessoais,sobre os quais o interessado pretende manter um controle exclusivo"[31]. É por isso a transformação de *"pessoa-informação-sigilo*" para "*pessoa-informação-circulação*"[32]. Para tanto, a sociedade de informação requer definições funcionais de privacidade – o que se permite alcançar maior aproximação com o *direito de manter o controle sobre as próprias informações*[33]. Assim sendo, a proteção de dados pessoais "torna-se um valor em si, sintetiza as prerrogativas da pessoa, contribui para construir a nova cidadania e definir as características de um sistema político-constitucional"[34].

Pode-se dizer que "o big data transforma a maneira como entendemos e exploramos o mundo"[35]. Nesta era, é possível dizer que "todos os dados serão considerados valiosos"[36], sendo que "o valor imediato da maioria dos dados é evidente para os que o coletam. Na verdade, eles provavelmente os reúnem com um propósito específico em mente." Ainda, a coleta dos dados se tornou mais fácil e menos custosa, permitindo maior circulação da informação[37]. Esta transformação e dispersão dos dados pessoais ocasiona dificuldades na proteção da privacidade, bem como traz riscos ao

[30] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 25.
[31] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 92.
[32] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 93
[33] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 92.
[34] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 292
[35] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p. 48
[36] Para os autores o "o segredo do valor dos dados está na aparente ilimitada reutilização em potencial: o custo/benefício. Coletar dados é essencial, mas não o bastante, já que a maior parte do valor dos dados está no uso, não na detenção". MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p. 85
[37] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p. 70-71

criar previsões (desafio na esfera da justiça e do livre-arbítrio).[38] A posse do conhecimento agora significa a capacidade de prever o futuro[39]. Pontua-se que a utilização irresponsável do big data é capaz de transformá-la em um "instrumento de poderosos", trazendo desafios[40] e podendo gerar repressão[41].

Nesse sentido, a importância de analisar formas as novas formas de vigilâncias, a partir de tecnologias biométricas. A tradição europeia de proteção de dados influenciou na Lei Geral de Proteção de Dados brasileira (LGPD), e ambas trouxeram desafios à proteção da privacidade, conforme se abordará nesta pesquisa[42].

É primordial o destaque de Danilo Doneda[43]

> **a utilização de dados pessoais não é, em si, um problema.** Na verdade, ela torna possíveis várias atividades, desde o planejamento administrativo até a ação humanitária, passando pela pesquisa de mercado e por mais um número infindável de áreas. Ocorre que a atividade do tratamento de dados pessoais **requer instrumentos** que a harmonize com os parâmetros de proteção da pessoa humana presentes nos direitos fundamentais e funcionalizados por instrumentos regulatórios que possibilitem aos cidadãos um **efetivo controle em relação aos seus dados pessoais** [...] (grifo nosso)

Para tanto, o cerne do estudo é abordar a temática do reconhecimento facial (dado pessoal sensível), refletindo sobre os seus benefícios, desafios e como o mundo jurídico nacional deve compreender e regular. Portanto, a privacidade relacionada à

[38] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p. 105

[39] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p.132d

[40] Ver sobre a temática: O'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Abraham, Rafael (trad.). 1. Ed. São Paulo: Editora Rua do Sabão, 2020.

[41] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013, p. 106

[42] O enfoque dado especificamente à legislação europeia é por ter influenciado na LGPD.

[43] DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.24

informação e dados informáticos não é a mesma de outros tipos de privacidade[44]. Justamente por isso, o surgimento de novas abordagens sociológicas e jurídicas[45].

Utiliza-se a abordagem hipotético-dedutiva. Esta é a mais adequada ao presente trabalho, pois consiste na observância de lacunas nos conhecimentos, a partir disso formula hipóteses e testa a predição da ocorrência de fenômenos abrangidos pela hipótese, por meio da inferência dedutiva [46]. Assim, esta proposta é a mais adequada na medida em que se analisarão as normativas e princípios jurídicos e se procurará verificar a insuficiência de seus dispositivos no reconhecimento facial.

O estudo é dividido em duas partes.

A primeira aborda, de forma dogmática, a tecnologia do reconhecimento facial, na qual são trazidos os temas da vigilância e monitoramento; tecnologias biométricas; como funciona um sistema de reconhecimento facial; acurácia deste; e desafios correlatos.

Na segunda parte, traz-se a temática de forma mais pragmática, aprofundando nos cenários europeu e brasileiro. Aborda-se como a legislação americana e europeia vislumbra a temática da biometria e do reconhecimento facial e como esta pode ser compreendida na LGPD. Para tanto, expõe-se o consentimento na normativa de proteção de dados brasileira e quais as hipóteses do tratamento de dados pessoais sensíveis, quando o consentimento é indispensável ou não. Após, especifica-se o tema quando da análise do art. 11, II, alínea g, da LGPD:

> Art. 11. O tratamento de **dados pessoais sensíve**is somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> **II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:**
> **g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.**

[44] Nesse sentido, o conceito de privacidade não é suficiente para incluir o tema daa vigilância comtemporânea. LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 196.
[45] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 187
[46] MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 6 ed. São Paulo: Atlas, 2007.

A partir disso, é destrinchado o significado buscado pela alínea: tratamento de dados sensíveis sem consentimento do titular; garantia de prevenção à fraude; garantia à segurança do titular; processos de identificação e autenticação de cadastro; sistemas eletrônicos. Por fim, busca-se mesmo sendo legal o dispositivo, se pode ser compreendido como ético e razoável quando do tratamento de dados. Assim, são analisados os princípios da lei, bem como outras normativas brasileiras. Pretende-se verificar a suficiência do ordenamento brasileiro – em específico, a LGPD; para lidar com o tema do art. 11, II, alínea G, de forma prática, sem que viole a privacidade e os direitos individuais.

Ao final, propõe-se alternativas possíveis para lidar com a temática, sugerindo-se teste de bases legais, outras opções de tecnologias biométricas e a criação de autorregulação sobre o tema.

Defende-se pela insuficiência, *a priori*, do ordenamento jurídico brasileiro para lidar com a matéria do reconhecimento facial no tema proposto.

1 RECONHECIMENTO FACIAL: FUNDAMENTOS DOGMÁTICOS DESTA TECNOLOGIA BIOMÉTRICA

> O corpo está se tornando uma senha, o seu caráter físico toma o lugar das palavras-chaves abstratas, através de impressões digitais, íris, traços da face, DNA: recorre-se com frequência sempre maior a estes dados biométricos não somente para fins de identificação ou como chave para acessar diversos sistemas, mas também como elementos de classificação, para realizar controles posteriores ao momento da identificação. E o corpo pode também ser predisposto para ser seguido e localizado permanentemente. RODOTÁ, p. 248

Este capítulo tem como escopo apresentar um entendimento inicial sobre vigilância, biometria e reconhecimento facial. Para tanto, "defendendo a pessoa e o seu corpo, defendem-se valores fundamentais dos sistemas democráticos, que não podem

ser militados ou sacrificados sem que caia em perigosas tentações de caráter totalitárias"[47].

1.1 Compreensões iniciais sobre vigilância e monitoramento

É preciso destacar que a temática da vigilância, em que pese possa ser associada ao monitoramento, não necessariamente possui o mesmo significado ou objetivo. Normalmente quando se menciona vigilância, o pensamento é remetido à força policial, por isso a escolha de autores pela palavra monitoramento em substituição[48]. Assim, nem sempre estará associada à segurança: casos em que se vislumbra outros tipos de vigilância relativos desde a fazer compras na internet e ingressar em edifícios[49].

De acordo com Roger Clarke, pode-se conceituar vigilância (*surveillance*) como

> investigação sistemática ou monitoramento das ações ou comunicações de uma ou mais pessoas. O seu objetivo principal é geralmente coletar informações sobre eles, suas atividades ou associados. Pode haver uma intenção secundária de dissuadir toda a população ou realizar algum tipo de atividade[50].

De igual sorte, a temática não é recente. As civilizações antigas, como a egípcia, possuíam registros populacionais, como para fins tributários e de prestação de serviços. Mas também havia a associação com a busca de segurança: a importância de um vigilante na guarda de castelos, por exemplo. Entendia-se a preservação da segurança como uma racionalização para se desenvolver uma atenção cuidadosa e diferenciar amigos de adversários: "vigiar para cuidar"[51].

---

[47] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 266

[48] Helen Nissenbaum optou pela substituição do termo vigilância (surveillance) por monitoramento (monitoring and tracking), posto que a vigilância usualmente é associada à força policial. NISSENBAUM, Helen. Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press: California, 2010, p. 22

[49] LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 9

[50] Tradução livre do autor. Original: *Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates. There may be a secondary intention to deter a whole population from undertaking some kinds of activity.* CLARKE, Roger. Information Technology and Dataveillance. DUNLOP, C; KLING, R (Eds). Controversies in Computing. Academic Press. 1991. Disponível em: http://www.rogerclarke.com/DV/CACM88.html. Acesso em: 02 fev. 2022. Online.

[51] BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 95

O advento tecnológico do século XIX permitiu novos tipos de vigilância, na medida em que o registro poderia tanto ser escrito como impresso[52]. Como pontua David Lyon, o avançar da vigilância é paradoxal: é fruto da busca por cidadania e também de maior controle estatal[53]. Ao mesmo tempo que passa a estar presente na esfera pública e democrática, diminui a atenção sob a esfera privada[54] da família e da religião, por exemplo[55].

No capitalismo, Karl Marx entendia que a vigilância estava entre as relações das classes (trabalhadores e empresa) – embora os primeiros fossem livres, trabalhando sem coação, o dono ainda haveria de manter o controle do trabalhador para que produzisse mais em menos tempo e com menos custo[56]. Já Max Weber acreditava que a vigilância não estava apenas sob o teto da fábrica, mas também ligada às instituições burocráticas (a empresa capitalista estaria dentro deste guarda-chuva). Portanto, a vigilância estaria inserida na necessidade de uma *organização disciplinada*, com regras, procedimentos, divisão de responsabilidades, tudo visando *racionalidade* e eficiência.[57]

Foi no século XX que Foucalt, em Vigiar e Punir (1975) posiciona a presença da vigilância não só em organizações, como prisões, fábricas, exército, mas inserida na própria sociedade: "*sociedade disciplinar*"[58]. Nesta, há técnicas e estratégias de poder onipresentes, cujo objetivo é vigiar os indivíduos, documentar comportamentos e classificar grupos que seguem as normas sociais[59]. Assim, em meados de 1990, um novo mundo digital e eletrônico trouxe mais reflexões sobre o tema da vigilância. Resta

[52] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 22-24
[53] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 38
[54] "Há uma gratidão pela proteção e aquisição de direitos possibilitados pela vigilância, ao passo que sente-se intromissão quando há a invasão do espaço privado e ameaça à autonomia. Tradução livre do autor. Original: "We are both grateful for protection or the procurement of rights which it affords, and simultaneously irritated and defensive when meddlesome bureaucracy invades what we see as our private space, or angered at the threats posed to our autonomy.". LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 38
[55] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 24
[56] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 25
[57] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 25
[58] Tradução livre do autor. Original: "discipline in society-at-large". LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 26
[59] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 26

analisar se houve grandes mudanças com a substituição da "*vigilância do papel*" para a "*vigilância eletrônica*"[60].

David Lyon refere que as novas tecnologias, como a tecnologia da informação, implicaram em grandes modificações – trazendo reflexos na política, economia e cultura[61]. Este avanço tecnológico permitiu com que fosse possível coletar, armazenar e divulgar dados em grande escala e com menor custo. E, ainda, transformou informações de indivíduos que circulavam fora do mercado, como preferências consumeristas, em valor - *commodities*[62].

Assim, embora a vigilância tenha se originado em instituições governamentais, como exército e repartições, espalhou-se para todas as áreas da vida[63].Ações ordinárias, como retirar dinheiro de um caixa eletrônico, votar, receber benefícios governamentais, usar um cartão de crédito e cruzar fronteiras ao viajar são exemplos disso. Em cada qual mencionada, há uma análise e registro computacional sobre o sujeito.[64]

Como refere David Lyon, "participar da sociedade moderna é estar sob vigilância eletrônica"[65]. Merece destaque também o termo cunhado por Shoshana Zuboff: *capitalismo de vigilância*[66]*:*

> **o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais.** Embora alguns desses dados sejam aplicados para o **aprimoramento de produtos e serviços**, o restante é declarado como superávit comportamental do proprietário, alimentado avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições

[60] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 41-42. Tradução livre do autor. Original: "paper to eletronic surveillance".
[61] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 44
[62] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 45
[63] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 5.
[64] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 4
[65] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 4. Tradução livre do autor. Original: "to participate in modern society is to be under electronic surveillance"
[66] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 18-19

> comportamentais que chamo de **mercados de comportamentos futuros** (grifo nosso)[67]

Vale ressaltar que o *capitalismo de vigilância* não se caracteriza por ser uma tecnologia, mas "uma lógica que permeia a tecnologia e a direciona numa ação"[68]. Um dos exemplos é o caso do *Pokémon Go*[69], um jogo de caça a *Pokemons* baseado em realidade aumentada. O jogo conseguia modular comportamentos dos participantes, ao estipular regras, recompensar e punir formas de agir[70]. A autora refere ser o Google o pioneiro, principal praticante e centro de difusão do capitalismo de vigilância[71]. A empresa descobriu que "nós somos menos valiosos que as apostas alheias no nosso comportamento futuro"[72].

Shoshana Zuboff critica esta nova sociedade do capitalismo de vigilância[73], no qual este seria uma "força nefasta comandada por novos imperativos econômicos que desconsideram normas sociais e anulam direitos básicos associados à autonomia individual e os quais são essenciais para a própria possibilidade de uma sociedade democrática"[74]. Mas isso não significa que há necessariamente uma tendência negativa à vigilância: não necessariamente é boa ou ruim[75]. Nesse sentido, Roger Clarke discorda que "a vigilância é, por si só, má ou indesejável; sua natureza deve ser compreendida, e

---

[67] Nesse sentido, a autora questiona: "Se o Google é uma empresa de busca, por que está investindo em dispositivos de smart home, dispositivos inteligentes feitos para serem vestidos e carrros autodirigidos? Se o Facebook é uma rede social, por que está desenvolvendo drones e realidade aumentada? Essa diversidade às vezes confunde quem olha de fora, mas costuma ser apludida como um investimento visionário: apostas excêntricas no futuro". ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 154

[67] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 80

[68] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 26

[69] Ver mais em: O que é o Pokémon Go e por que está causando tanto furor no mundo dos games? BBC. 2016. Disponível em: https://www.bbc.com/portuguese/geral-36802725. Acesso em 02 fev. 2022; https://pokemongolive.com/pt_br/

[70] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 357-358

[71] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 80

[72] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 113

[73] "Uma explicação para os muitos triunfos do capitalismo de vigilância paira sobre todas as outras: ele não tem precedentes". ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 23

[74] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020, p. 23

[75] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 5. Tradução livre do autor. Original: "is not unambiguously good or bad".

a sociedade deve decidir as circunstâncias em que deve ser usada e as salvaguardas que devem ser aplicadas a ela"[76].

Nesse sentido, merece destaque um estudo publicado em 1999 por Clive Norris e Gary Armstrong, no qual buscou verificar se o circuito fechado de televisão (CFTV)[77] utilizado nas ruas britânicas para prevenir crimes também poderia ser discriminatório: se existiam alvos específicos da vigilância – e como os operadores selecionavam os alvos (ex: idade e gênero)[78]. A motivação veio por uma onda de pesquisas anteriores que buscavam responder sobre a eficácia das CFTVs para redução da criminalidade como causa isolada, sem analisar outros fatores[79]. Para Norris e Armstrong CFTV "não é apenas voltada para a redução do crime, mas muito mais. É sobre um poder de assistir e intervir em inúmeras situações, podendo estas ser sobre criminalidade ou não"[80].

Foram observadas 592 horas de monitoramento[81], gerando 888 vigilâncias direcionadas (quando o monitoramento do indivíduo na imagem dura mais de um minuto). O resultado tem relação com idade, raça e gênero, apontando que os alvos eram majoritariamente homens (93%)[82]; adolescentes (39%)[83] e negros (31%). Para

---

[76] Tradução livre do autor. Original: *I explicitly reject the notion that surveillance is, of itself, evil or undesirable; its nature must be understood, and society' must decide the circumstances in which it should be used, and the safeguards that should he applied to it.* CLARKE, Roger. Information Technology and Dataveillance. DUNLOP, C; KLING, R (Eds). Controversies in Computing. Academic Press. 1991. Disponível em: http://www.rogerclarke.com/DV/CACM88.html. Acesso em: 02 fev. 2022. Online.

[77] Circuito fechado de televisão ou circuito fechado, mais conhecido como câmeras de vigilância, é um sistema de câmeras em locais específicos que transmitem para uma TV monitorada os sinais captados. Costuma ser utilizado para vigilância e segurança, presente tanto em ambientes públicos como privados. Em inglês, o termo "*Closed Circuit Television Camreas – CCTV*" é utilizado. Será utilizado o termo CFTV neste trabalho.

[78] NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 157 - 178

[79] NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 157 - 158

[80] Tradução livre do autor. Original: "is about far more than just the reduction of crime. It is about the power to watch and potentially intervene in a variety situations, whether or not they be criminal". NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 158.

[81] [81] As descobertas foram fruto de uma pesquisa de 02 anos. Foram realizadas observações em três locais: no centro comercial de uma grande cidade metropolitana (população superior a 500.000 habitantes); praça do mercado de uma cidade do condado (cerca de 200.000 habitantes); e um bairro pobre do centro da cidade (cerca de 250.000 habitantes com população etnicamente diversificada). As anotações foram separadas em subdivisões: (1) dados de turno; (2)dados de suspeita (motivo da suspeita, tipo de suspeita, como foi realizada a vigilância, quantas câmeras foram usadas); (3)dados pessoais (ex: idade, raça, sexo, aparência); (4)Dados sobre como o sistema de vigilância foi usado durante as observações. NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.160-161

[82] Praticamente o início de uma vigilância ou uma vigilância direcionada em mulheres eram por razões voyeurísticas, descaracterizando o propósito do monitoramento. Clive; ARMSTRONG, Gary. CCTV and

avaliar se os alvos também eram focados com base no comportamento, dividiu-se em categorias: (a)relacionada ao crime; (b) relacionada à ordem; (c) nenhuma razão óbvia[84]; ou (d) outra. O maior percentual de indivíduos vigiados foi categorizado como "nenhuma razão óbvia" (36%).

FIGURA 1 – MOTIVOS PARA VIGILÂNCIA: IDADE, RAÇA E IDADE

Table 3: Reason for Surveillance by Age, Race and Gender in Numbers and Percentages

Age						
	Teenagers		In their twenties		Thirties plus	
Crime Related	59	(22%)	80	(26%)	17	(17%)
Public Order	30	(11%)	83	(27%)	46	(45%)
No Obvious	173	(65%)	115	(38%)	21	(21%)
Other	4	(2%)	29	(9%)	18	(18%)
Total	266	(100%)	307	(100%)	102	(101%)
Gender						
	Male		Female			
Crime Related	138	(22%)	19	(43%)		
Public Order	150	(24%)	12	(27%)		
No Obvious	302	(47%)	7	(16%)		
Other	49	(8%)	6	(14%)		
Total	639	(101%)	44	(100%)		
Race						
	White		Black			
Crime Related	115	(25%)	42	(20%)		
Public Order	148	(32%)	13	(6%)		
No Obvious	163	(35%)	141	(68%)		
Other	41	(9%)	12	(6%)		
Total	467	(101%)	208	(100%)		

Fonte: NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.164

Curiosamente, embora os adolescentes fossem os mais vigiados, apenas 18% deles eram presos (23% mobilizados), diferentemente dos adultos que, embora fossem menos vigiados, representaram 82% das prisões. No mesmo sentido os negros:

---

the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 174.

[83] Em virtude do traje, localização ou linguagem corporal. Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.164.

[84] A vigilância seria registrada como "nenhuma razão óbvia" se não houvessem sinais do comportamento do indivíduo ou não fosse um criminoso já conhecido. NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.163

representaram 32% da vigilância direcionada, mas apenas 9% dos presos[85].Assim, entendeu-se que, *não haveria uma discriminação "real",* na medida em que a vigilância direcionada, ainda que focasse mais tempo em monitorar determinados indivíduos, não necessariamente acarretava consequencias "reais" para estes[86].

Por fim, entendeu-se que os *operadores das CFTVs eram extremamente discricionários*, possibilitando escolhas de quem e por quanto tempo será vigiado. Portanto, a atitude destes seria discriminatória, ao consturir um padrão de segmentação (a) homens; (b) adolescentes e (c)negros[87]. Os pesquisadores concluíram que o fato dos operadores das CTFTVs terem focado em grupos específicos, *per si*, já os caracteriza como suposta ameaça: "essa interação social tecnologicamente mediada e distanciada é,então, *carregada de significado*"[88]. Ainda:

> [...] para literalmente milhares de negros e jovens da classe trabalhadora, por mais cumpridores da lei, transmite uma mensagem negativa sobre sua posição na sociedade. Mas tem mais amplo consequências do que apenas seu impacto na psicologia individual. O princípio central do policiamento por consentimento – que o policiamento é visto como legítimo por aqueles que o vivenciam – é minado. **Se os grupos sociais vivenciam a vigilância CCTV como uma extensão de discriminação e policiamento injusto, a consequente perda de legitimidade pode ter consequências desastrosas para a ordem social.**"[89]

Portanto, a vigilância por vídeo (*video surveillance*) é problemática, seja ela em âmbito público ou privado: a vigilância limita a liberdade, torna o comportamento mais

---

[85] NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 172.

[86] NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 172.

[87] NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.175.

[88] Tradução livre do autor. Original: "This technologically mediated and distanced social interaction is, then, loaded with meaning". NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.176.

[89] Tradução livre do autor. Original: "...for literally thousands of black and working-class youths, however law-abiding, it transmits a wholly negative message about their position in society. But it has wider consequences than just its impact on individual psychology. The central tenet of policing by consent — that policing is viewed as legitimate by those who experience it — is undermined. If social groups experience CCTV surveillance as an extension of discriminatory and unjust policing, the consequential loss of legitimacy may have disastrous consequences for social order". NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p.176.

autoconsciente[90]. Nesse sentido, Rodotà refere que o aumento da vigilância dos espaços públicos também tem efeito sobre os comportamentos tanto individuais como coletivos, como a redução da espontaneidade e da liberdade[91]. Para tanto, a vigilância concede poder aos observadores, reduzindo a falta de controle de quem está sendo vigiado[92]

Interessante pontuar a metáfora "eu não tenho nada a esconder" *("i have nothing to hide"),* abordada por Daniel Solove e utilizada antigamente pelo governo britânico quando da instalação de câmeras de vigilância nas cidades (CCTVs)[93]. O autor refere que este argumento traz a ideia errônea de que a privacidade é sobre "esconder" coisas ruins – privacidade como forma de sigilo (*secrecy*), tendo um aspecto mais particular. Mas, o problema do argumento não é apenas isso: a privacidade traz uma ideia mais geral, não só voltada ao particular[94]. Exemplos trazidos por Solove são: *agregação* (*aggregation*) – fusão de dados *a priori* inócuos, mas quando combinados, podem trazer informações sensiveis; *exclusão* (*exclusion*) – quando o governo usa base de dados de indivíduos sem o seu conhecimento, não permitindo, portanto, que tenham ciência sobre essas informações, como são usadas e a possibilidade de acessar e corrigir informações; uso secundário (*secundary use*) – utilização de dados para propósito diferente da finalidade e sem o consentimento do sujeito; *distorção* (*distortion*) – as informações obtidas podem traçar um perfil do sujeito, mas que possa não refletir a totalidade da situação, contexto, dado[95].

Na sociedade moderna, a vigilância não é mais excepcional. Para Rodotà, torna-se cotidiana[96]:

> [...]das classes de cidadãos perigosos passa para a generalidade das pessoas. A multidão não é mais solitária e anônima. A digitalização das imagens, as técnicas de reconhecimento facial permitem extrair o indivíduo da massa, individuá-lo e segui-lo. O *data mining*, a incessante busca de informações sobre os comportamentos de cada um, proporciona uma contínua produção

[90] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 178-179
[91] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 258.
[92] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 179
[93] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011.
[94] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 26-27
[95] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 27-29
[96] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 258.

> de perfis individuais, familiares, de grupo. **A vigilância não conhece limites**. *(grifo nosso)*

A *informação* também é uma forma de monitoramento, haja vista que interações e transações podem ser monitoradas e rastreadas[97]. Para o uso sistemático de dados pessoais em investigação ou monitoramento de ações, comunicações ou pessoas, é possível a utilização do termo *dataveillance* (vigilância de dados)[98]. O *dataveillance* pode ser de dois tipos. A vigilância pessoal (*personal dataveillance*) ocorre quando há um motivo específico para investigar ou monitorar. Já a vigilância em massa (*mass dataveillance*) se manifesta com alvo em grupos de pessoas e costuma ter o objetivo de identificar determinados indivíduos. Ambas possuem tanto benefícios quanto riscos. Pontos positivos seriam permitir a segurança física de pessoas e de patrimônio (como fraudes e furtos), tanto no âmbito público, quanto privado. Mas, dentre os perigos, exemplifica o risco de identificação errada, interpretação errônea ao usar os dados fora do contexto original, utilização de dados sem o consentimento do titular[99].

Ademais, impende mencionar que o *monitoramento*[100] pode ser direto ou indireto. O primeiro utiliza a chamada vigilância por vídeo (CCTV) em ambientes públicos e privados[101]. Já o segundo, constitui-se de gravações, escutas telefônicas, sistemas de rastreamento computadorizados (que podem integrar detecção de movimento, luz e calor)[102]. No mundo moderno, as câmeras de vigilância são usuais no controle de viajantes em aeroportos, bem como escâneres corporais e aparelhos biométricos, proliferados desde o 11 de setembro de 2001[103].

---

[97] NISSENBAUM, Helen. Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press: California, 2010, p. 23

[98] CLARKE, Roger. Information Technology and Dataveillance. DUNLOP, C; KLING, R (Eds). Controversies in Computing. Academic Press. 1991. Disponível em: http://www.rogerclarke.com/DV/CACM88.html. Acesso em: 02 fev. 2022. *Online*.

[99] CLARKE, Roger. Information Technology and Dataveillance. DUNLOP, C; KLING, R (Eds). Controversies in Computing. Academic Press. 1991. Online.

[100] Nomenclatura utilizada por Helen Nissenbaum em substituição do termo vigilância (surveillance). NISSENBAUM, Helen. Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press: California, 2010, p. 22

[101] Sobre o uso de câmeras no ambiente empresarial, especificamente no âmbito da Lei Geral de Proteção de Dados brasileira (LGPD), ver: COSTA, Guilherme Spillari; LEVENFUS, Silvia. O uso de câmeras no ambiente empresarial e a LGPD. Revista digital ESA/OAB. V. 10. 2021. N.2. Porto Alegre. Disponível em: https://www.oabrs.org.br/arquivos/file_611ac48b0587d.pdf. Acesso em: 03 mar. 2022.

[102] NISSENBAUM, Helen. Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press: California, 2010, p. 22-23

[103] A partir de 11 de setembro de 2001, aumentou 1.600% a quantidade de informações acumulada pela tecnologia de ponta do Exército americano LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 9 e 85

É paradoxal o fato de que novas técnicas e tecnologias que visam a trazer mais segurança ao mesmo tempo também aumentam a *insegurança*: "não é possível saber quando as categorias de risco podem "acidentalmente" nos incluir, ou, mais precisamente, nos excluir de participação, ingresso ou direitos"[104]. Nesse sentido, "pessoas categorizados como inocentes agora correm risco e estão amedrontadas"[105].

E, na *modernidade líquida*, a *vigilância líquida* assume outros papeis que vão além do monitoramento: também abrange *rastreamento, localização, classificação* e *observação sistemática*[106]. Este cenário multifacetado apresenta desafios[107]:

> [...] as novas práticas de vigilância [...] permitem uma nova transparência, em que não somente os cidadãos, mas todos nós, por todo o espectro dos papéis que desempenhamos na vida cotidiana, **somos permanentemente checados, monitorados, testados, avaliados, apreciados e julgados. (**grifo nosso)

Ao mesmo tempo em que a vida se torna mais transparente às organizações de vigilância, "suas próprias atividades são cada vez mais difíceis de discernir. À proporção que o poder se move à velocidade dos sinais eletrônicos na fluidez da modernidade líquida, a transparência simultaneamente aumenta para uns e diminui para outros"[108]. É nesse cenário que se apresenta o desafio de compreender e estudar sobre tecnologias: por um lado benéficas, e por outro, podem ter consequências indesejáveis.

2.2.Biometria e tipos de tecnologias biométricas

Não é recente a utilização de traços biológicos para confirmar a identidade de uma pessoa. O primeiro sistema biométrico foi criado em 1883 por Alphonse Bertillon, chefe da divisão criminal do Departamento de Polícia de Paris. Utilizavam-se

[104] BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 96
[105] BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 97
[106] LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 16-19. A partir de
[107] LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 19
[108] LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013, p. 19

características antopométricas[109], como altura e largura da cabeça com outros atributos como cor do olho, tatuagens e cicatrizes, com o objetivo de identificação de uma pessoa no âmbito penal[110]. Cumpre referir que as medidas eram manuais e, em que pese pudessem gerar algumas variações, eram suficientes para uma identificação razoavelmente precisa[111].

FIGURA 2- SISTEMA BERTILLONAGE

Fig. 1.18 The Bertillonage system, so named after its inventor Alphonse Bertillon, relied on the precise measurement of various attributes of the body for identifying recidivists. These measurements included the height of the individual, the length of the arm, geometry of the head, and the length of the foot. The process was tedious to administer and did not guarantee uniqueness across individuals.

Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 46

As medições eram registradas em cartões e indexadas, o que facilitava o trabalho policial em caso de reincidência. Entretanto, o sistema era muito suscetível a erros, haja vista que determinadas características poderiam ser similares em mais de um indivíduo[112]. A ideia de Bertillon começou a ganhar bastante prestigio até ser

[109] Entende-se antropometria como o estudo das medidas e dimensões das partes do corpo. São analisados aspectos genéticos e biológicos e utilizadas várias técnicas de medição. SIGNIFICADOS. Significado de Antropometria. Disponível em: https://www.significados.com.br/antropometria/. Acesso em 18 jan. 2022
[110] Estes atributos são considerados "*soft biometrics*", como se explicará ao longo do capítulo.
[111] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015, p. 1426.
[112] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 45

ultrapassada por uma grande descoberta ao final do Século XIX: a unicidade das impressões digitais humanas[113].

A partir daquele momento, os departamentos policiais começaram a coletar as impressões digitais de criminosos e armazená-las em arquivos. Somente após que se descobriu a possibilidade de coletar as impressões digitais em cenas de crime e, assim, verificar a identidade do criminoso ao combinar com outras impressões presentes no banco de dados[114].

Na sociedade informacional, é cada vez mais conveniente identificar uma pessoa, como para permitir o ingresso em outro país ou identificar um funcionário de uma empresa[115]. Tecnicamente, a nomenclatura *identificação pessoal* ocorre quando se procede a associação de uma identidade a um indivíduo[116]. Há algumas formas de identificar uma pessoa, associando dados a ela[117]. *Biometria* é o termo utilizado para referir algumas técnicas possíveis de identificação de uma pessoa[118].

A título ilustrativo abrangem as técnicas biométricas de identificação pessoal[119]:

(i) Aparência. Exemplo: gênero sexual, raça, altura, peso, cor da pele;
(ii) Comportamento social. Exemplo: estilo de fala, sinais corporais, modo de falar
(iii) Biodinâmica. Exemplo: modo de assinar, análise da voz
(iv) Fisiografia natural. Exemplo: medida craniana, impressão digital, geometria das mãos, retina, padrões capilares, padrão de DNA.
(v) Características físicas impostas. Exemplo:se utiliza pulseira, microchip, tornozeleira.

[113] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 39
[114] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 39
[115] JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.02.
[116] JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.01-02.
[117] CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.4. Disponível em: https://openresearch-repository.anu.edu.au/bitstream/1885/46248/27/03Paper02.pdf . Acesso em 24 dez, 2021.
[118] CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.4.
[119] CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.4-8.

Portanto, características fisiológicas e comportamentais podem ser consideradas *características biométricas*[120].

De acordo com a *International Organization for Standardization* (ISO)[121], *característica biométrica* (*biometric charactristic – deprecated noun*) é um conjunto único e repetível de características (i) biológicas e (ii)comportamentais; capazes de alcançar um *reconhecimento biométrico* (*biometric recognition*). Exemplos de características biométricas: estrutura da íris, dinâmica de assinatura manuscrita, topografia facial e topografia da mão[122]. Cabe referir a impossibilidade de separação entre as características biológicas e comportamentais. Explica-se: a impressão digital é resultado de (i) característica biológica: padrões da crista do dedo; e (ii) comportamental: ato de apresentar o dedo[123].

Impende referir que a utilização de cada *característica biométrica* dependerá da aplicação a que for submetida, haja vista prós e contras a depender do caso. É possível utilizar *sete fatores de adequação* para verificar se uma característica biológica ou comportamental é conveniente para uma aplicação biométrica[124]. São eles: universalidade (*universality)*, unicidade (*uniqueness*), permanência (*permanence*), mensurabilidade (*measurability)*, desempenho (*performance*), aceitabilidade (*acceptability*) e evasão/ofuscação (*cirumvention*)[125]. Exemplica-se a seguir[126]: universalidade: cada indivíduo que acessa a aplicação deve ter a característica; unicidade: a característica deve ser suficientemente singular em relação aos outros indivíduos comparados; e permanência: a característica deve durar determinado período de tempo, caso contrário, poderá gerar falsas correspondências.

---

[120] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 33

[121] International Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online

[122] International Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online

[123] International Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online

[124] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 29

[125] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 29- 30

[126] Tradução livre do autor. JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 29- 30

De forma ilustrativa, as características biométricas mais comuns são:[127]

Impressão digital (*Fingerprint*): Impressão digital é o padrão de sulcos e vales na superfície de um dedo[128], *a priori* permanentes e únicos, até mesmo para gêmeos idênticos[129]. É possível que o padrão seja danificado temporariamente, em caso de lesões superficiais na área ou, excepcionalmente, de forma definitiva, em danos mais profundos[130]. Desde o final do século XIX, a impressão digital era utilizada para reconhecimento em aplicações forenses, sendo coletada de forma manual e gravada em papel (*the ink-on-paper technique)*[131]. A técnica de reconhecimento da impressão digital popularizou-se devido ao surgimento de sensores convenientes (independentemente de intervenção humana), rápidos e acessíveis, disseminando-se em outras áreas que não só a forense[132]. Por exemplo, na segurança nacional e em combate à fraude no âmbito consumerista[133]. A utilização da impressão digital em sistemas biométricos ficou tão popularizada que os indivíduos compreendiam como sinônimos o termo reconhecimento biométrico e impressão digital[134]. Vale ressaltar que uma boa qualidade da imagem obtida da impressão digital é essencial para possibilitar uma correspondência correta. Exemplo de fatores que influenciam a qualidade: resolução da imagem e área do dedo[135].

Impressão da palma (*Palmprint):* É possível dividir em palma da mão e sola do pé - ambas impressões são únicas, permanentes e podem ser utilizadas para identificação[136]. A impressão da palma[137] é similar ao da impressão digital, mas possui

---

[127] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 30

[128] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 30

[129] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 51-52,54

[130] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 52

[131] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 60

[132] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 30;60

[133] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 52

[134] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 53

[135] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 62-63

[136] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 85

[137] Ver mais sobre o tema em: STOIMCHEV, Marjan; IVANOVSKA, Marija; STRUC, Vitomir. Learning to Combine Local and Global Image Information for Contactless Palmprint Recognition. *Sensors*, 2022

mais distinção, como linhas e rugas[138]. Entretanto, em virtude da área maior a ser capturada e, consequentemente, tamanho e custo maiores dos scanners[139], acaba não sendo muito conveniente o seu uso ao comparar com a impressão digital[140]. Um exemplo comum de aplicação com a impressão da palma do pé (*sole prints*) é para o registro de recém-nascidos em hospital. Utiliza-se a palma do pé, pois estes costumam manter os punhos fechados, dificultando a captura da impressão digital ou da impressão da palma da mão[141].

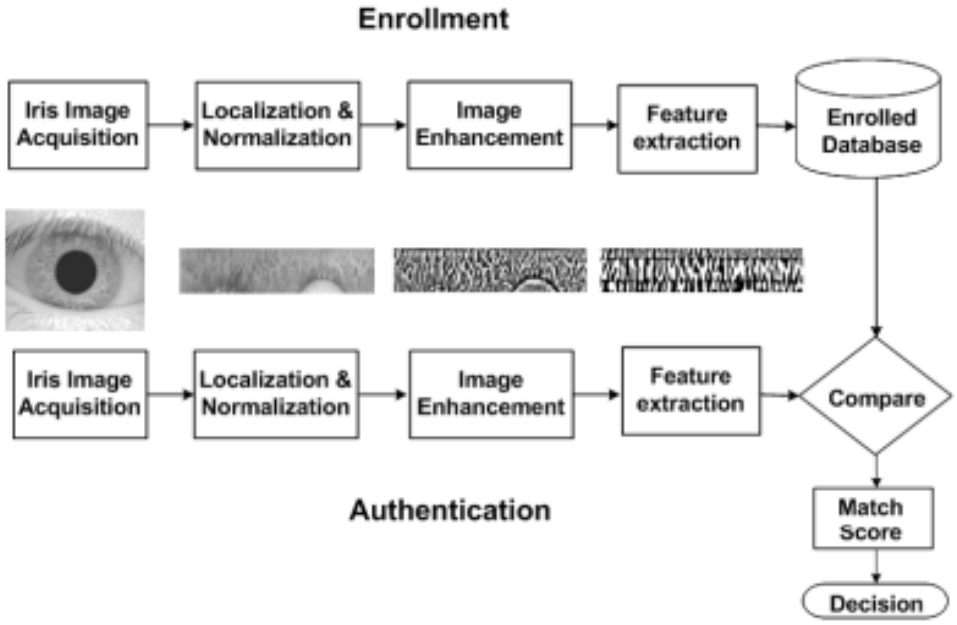
Íris (Iris): Corresponde a região branca dos olhos, que também é formada durante o desenvolvimento do feto[142]. Cada iris possui uma distinção, sendo que até mesmo gêmeos possuem diferença em sua textura. É justamente a textura dela que permite o reconhecimento biométrico[143]. Normalmente, o sistema de reconhecimento da íris funciona por meio de comparação de duas íris e análise de sua correspondência. Funciona da seguinte forma: (1)Aquisição de imagem da íris: obtenção de imagem 2D do olho; (2)Segmentação: isola a imagem da íris de outras capturadas junto, como a pupila, pálpebras e cílios, identificando os limites internos e externos da íris. Esta fase é fundamental, pois qualquer imprecisão na localização da íris pode influenciar na correspondência posteriormente; (3)Normalização: sistema transforma a textura da íris de coordenadas cartesianas para coordenadas pseudo-polares. O resultado é uma imagem retangular que possui informações sobre o ângulo da íris e direção radial; (4) Codificação e correspondência: a codificação é o processo de extração de conjuntos numéricos da íris (codifica a textura da íris). Os números obtidos são o código da íris respectiva[144]. As imagem abaixo representam as etapas descritas.

[138] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 31
[139] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 31
[140] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 85
[141] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 85
[142] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 31
[143] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 143
[144] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 141-145

FIGURA 3 – ETAPA DE AQUISIÇÃO DA IMAGEM DA ÍRIS

Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 147

FIGURA 4– SISTEMA TÍPICO DE RECONHECIMENTO DE ÍRIS COM QUATRO MÓDULOS: AQUISIÇÃO, SEGMENTAÇÃO, NORMALIZAÇÃO E CODIFICAÇÃO/CORRESPONDÊNCIA



Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 144

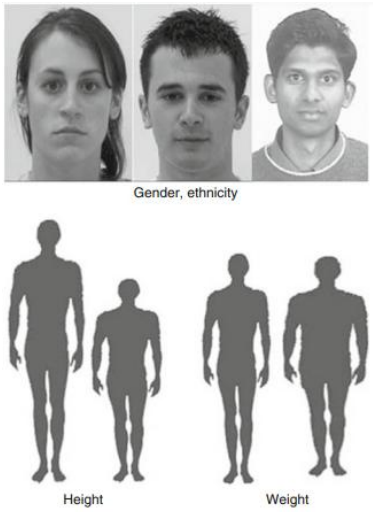
Rosto (Face): É uma forma de reconhecimento não intrusiva, pois pode ocorrer em ambiente não controlado (ex: rua)[145]. Reflexões mais aprofundadas serão abordadas no próximo capítulo.

Em virtude das muitas variações possíveis de traços biométricos, destaca-se mais quatro traços biométricos sob finalidade exemplificativa: *soft biometrics*, orelha (*ear*), marcha (*gait*) e geometria da mão (*hand geometry*)[146]. *Soft Biometrics*: nem sempre uma característica biométrica possibilitará a identificação de um indivíduo, mas auxiliará neste processo. Os atributos como gênero, etnia, idade, cicatrizes, tatuagens poderão complementar as biometrias supramencionadas. Denomina-se *soft biometric* ou *light biometric* as informações que complementam a os identificadores biométricos

[145] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 32
[146] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 176.

tradicionais[147]. Por exemplo, a idade, gênero e etnia podem ser estimados por meio da imagem da face, já extraída por uma aplicação biométrica[148].

FIGURA 5 – EXEMPLOS DE SOFT BIOMETRICS: gênero, etnia, altura e peso.

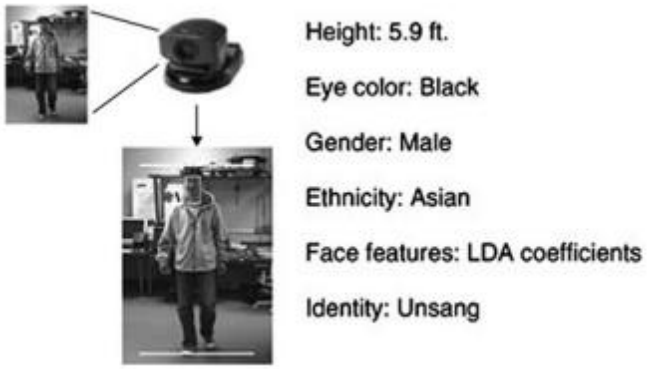


Fonte: Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015, p. 1427

A imagem abaixo ilustra a utilização de *soft biometrics* para identificação correta do sujeito.

[147] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015, p. 1425.
[148] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015, p. 1427..

FIGURA 6 – SOFT BIOMETRICS

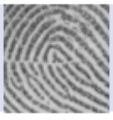
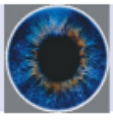


Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015, p. 1426

Cada característica biométrica pode ser utilizada em diferentes aplicações, sendo mais benéfica ou prejudicial a depender do caso. Ressalta-se que inexiste biometria que seja, por si só, efetivamente ideal: "*none is "optimal*""[149]. Cada qual possui características diferentes e que se prestam para determinada aplicação.

FIGURA 7 – COMPARAÇÃO DE TECNOLOGIAS BIOMÉTRICAS COM REQUISITOS

Table 1. Comparison of several biometric technologies (assessments based on authors' perceptions).

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectibility	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

[149] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 36

Fonte: JAIN, PANKANTI, S; PRABHAKAR, 2003, p. 36

Em se tratando de sistemas informáticos, a identificação pessoal é a associação de dados com um ser humano. Aplicável, por exemplo, a bancos de dados, a arquivos e a documentos[150]. Entende-se como *reconhecimento biométrico* o *reconhecimento automatizado* de indivíduos baseado em suas características biológicas e comportamentais[151]. Assim, é imprescindível a presença de um sistema biométrico capaz de reconhecer uma pessoa levando-se em consideração características fisiológicas ou comportamentais[152].Para que o *reconhecimento automatizado* ocorra, utiliza-se um sistema baseado em máquina que realiza o reconhecimento[153]. Neste caso, pode ocorrer o acompanhamento por um humano, mas é prescindível.[154]

Denomina-se sistema biométrico aquele sistema capaz de reconhecer uma pessoa levando-se em consideração características fisiológicas ou comportamentais. É usual que este sistema tenha duas finalidades: (i)*verificação* ou (ii) *identificação*[155]. A identificação também pode ser chamada de *reconhecimento*[156].

A *verificação* trata de confirmar uma afirmação biométrica ao comparar com outra biometria[157]. De forma simplificada: afirmar ou negar a identidade de um indivíduo: "Eu sou quem eu digo que sou?"[158][159]. Para que isso seja possível, o sistema

[150] CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.3
[151] Tradução livre pelo autor.
[152] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 33
[153] Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online
[154] Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online
[154] Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online
[155] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 33
[156] JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.01-02.
[157] Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. online
[158] Tradução livre do autor de: "*Am i Who I clam I am*?".JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.02

validará a identidade do indivíduo comparando a sua característica biométrica capturada com o modelo biométrico, normalmente presente em um banco de dados. O nome desta comparação é *one-to-one comparision*[160] (comparação um-para-um), haja vista que haverá apenas um sujeito envolvido[161].

Já a *identificação* é uma pesquisa biométrica em um banco de dados, com o objetivo de encontrar uma biometria identificadora de referência atribuível a um indivíduo[162]. De forma simplificada, o sistema visa reconhecer um sujeito ao pesquisar por modelos em um banco de dados[163]. O reconhecimento objetiva estabelecer a identidade de um sujeito: "Quem sou eu?"[164][165], "Quem é essa pessoa?"[166]. O nome desta comparação é *one-to-many comparision*[167] (comparação um-para-vários)[168].

As aplicações biométricas podem ser divididas em quatro categorias genéricas[169]: (a) *controle de acesso a dados*. Exemplo: *login* em dispositivo ou rede; (b) *controle de acesso a materiais ou áreas*. Exemplo: entrada física em local; (c) *validar uma identidade com outra credencial existente*. Exemplo: controle de fronteira; (d) *registrar ou identificar indivíduos cujas identidades necessitam ser determinadas biometricamente.* Exemplo: banco de dados centralizados[170].

---

[159] JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.01-02.

[160] Ver mais sobre em: "3.5.10". Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017

[161] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 33-34

[162] ". Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017

[163] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 34

[164] Tradução livre do autor de: "*Who am I*?". JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identification in Network Society. New York: Springer, 1996, p. 01-40, p.03

[165] JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40, p.02-03.

[166] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 34

[167] Ver mais sobre em: "3.5.11". Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017

[168] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 34

[169] Os autores JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 36 subdividem em três aplicações principais: comercial, governamental e forense.

[170] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 169-170.

Entretanto, para ilustrar todas as possíveis aplicações biométricas, aumentam-se as categorias[171]:

Aplicação forense: A biometria nesta aplicação visa uma identificação segura de supostos criminosos, ao utilizar a impressão digital para confirmar ou identificar a identidade em uma base de dados. Cumpre referir que o FBI possui um dos maiores bancos de dados biométricos, com impressões digitais tanto criminais quanto civis[172].

Verificação de antecedentes:Tecnologias biométricas têm sido usadas para realizar a verificação de antecedentes (*background checks*) para ingresso em emprego ou também ocupações governamentais[173].

Vigilância: Os sistemas biométricos automatizam e agilizam a vigilância: localizam, rastreiam e identificam sujeitos em determinado espaço ou área[174].

Controle de fronteira:As tecnologias biométricas, como a impressão digital, íris e reconhecimento facial, são facilitadoras para automatizar e agilizar o processo de cruzamento de fronteiras. É utilizado o processo de confirmação de identidade 1:1[175]. Este processo para controle de fronteira segue padrões internacionais para utilização de passaportes com biometria[176].

Prevenção de fraude:Para prevenir fraudes no setor público, como a reinvidicação de benefícios em dobro, sistemas biométricos têm sido utilizados[177]. Exemplo de prevenção à fraude é o sistema de verificação biométrica utilizado pelo Walt Disney World Resort, em Orlando (Flórida). O objetivo é evitar fraudes na utilização dos ingressos, como vender o ingresso já utilizado para outra pessoa. Para tanto, ao ingressar no parque de diversões, o visitante fornece a sua impressão digital e esta é vinculada ao ingresso específico, não sendo possível utilizar por outra pessoa ou, pela mesma pessoa, em dias diferentes (salvo se o bilhete for de entrada múltipla). O sistema consegue captar impressões digitais com ótima qualidade, e também é seguro

[171] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.
[172] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.
[173] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.
[174] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.
[175] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 172.
[176] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.
[177] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.

para a privacidade do visitante, na medida em que os seus dados pessoais não ficam associados aos dados da impressão digital do banco de dados e este é limpo regularmente[178].

Tempo e presença: A utilização de tecnologia biométrica pode auxiliar na gestão de funcionários, como a verificação do comparecimento ao trabalho[179]. Muitas organizações utilizam a geometria da mão e a impressão digital como forma de garantir a presença e, portanto, possibilitar um correto pagamento de acordo com as horas trabalhadas[180];

Reconhecimento do consumidor: Neste caso, a biometria tem como escopo confirmar a identidade do consumidor para que se execute uma transação comercial. A utilização da impressão digital tem sido utilizada para substituir *tokens* e senhas e, consequentemente, gerar maior segurança na relação consumerista[181]. Em algumas renomadas instituições financeiras japonesas foram instalados sistemas biométricos de autenticação com leitura da veia da palma da mão (*palm-vein authentication*)[182].

Controle de acesso físico (*Physical Acess Control* - PAC): Esta aplicação é bem comum no mercado[183], sendo comercializada atrás apenas das aplicações forenses[184]. Ao fazer uso das tecnologias biométricas, é possível identificar ou verificar a identidade de um sujeito antes de permitir a sua entrada a determinada área[185]. É preciso diferenciar autenticação e autorização. A primeira visa a identificação da identidade do indivíduo. Já a segunda, permite com que este acesse ou não determinada área a partir da resposta do sistema biométrico[186]. Essa separação entre autenticação e autorização é essencial, pois se um usuário não for mais autorizado a ingressar em determinada área

---

[178] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011, p. 41

[179] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171

[180] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

[181] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

[182] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 40-41.

[183] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 172.

[184] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 06.

[185] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 170.

[186] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 06.

(autorização), ainda poderá acessar uma área mais ampla (autenticação)[187]. Vale ressaltar que é corriqueira a utilização do controle de acesso físico de funcionários a áreas seguras ou protegidas[188]. Assim, para que o controle de acesso físico ocorra da melhor forma possível, é preciso que o sistema biométrico seja pensado para comunicar-se adequadamente com as estruturas existentes de acesso de controle, bem como interoperáveis com sistemas de acesso de controle lógico[189]. As biometrias mais utilizadas nesta aplicação são a impressão digital, a geometria da mão, face e íris[190]. Inicialmente utilizava-se a impressão digital e a geometria da mão. Entretanto, com o avanço dos sistemas de reconhecimento facial e de íris, estes passaram a ser utilizados também nesta aplicação[191];

Controle de acesso lógico (*Logical Acess Control*): Para esta aplicação, é utilizada a autenticação biométrica para o controle de acesso a sistemas e/ou dispositivos hardware[192], como computadores, redes e celulares[193]; Fatores levaram a uma necessidade de utilizar um sistema biométrico. Em resumo: (i)senhas são fáceis de quebrar; senhas complexas são difíceis de lembrar; (iii) a quebra de senhas é escalonável; (iv) senhas e *tokens* podem ser compartilhadas por usuários sem que o sistema consiga identificar se é o usuário original[194]. A partir disso, a utilização da biometria permite manter a segurança do usuário, sem que este precise lembrar de senhas[195]. A impressão digital é a mais usada, em virtude da sua confiabilidade, facilidade e acurácia[196], além de ter atingido o tamanho, preço e desempenho

[187] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 07.
[188] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 172.
[189] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 06.
[190] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 05.
[191] SOUTAR, Colin. Physical Acess Control. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.05-09. New York: Springer, 2015, p. 08.
[192] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.
[193] BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015, p.01
[194] BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015, p.02-03
[195] BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015, p.03
[196] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

necessários para integração com dispositivos de acesso, como notebooks[197]. Basta apenas que o usuário realize uma ação definitiva para permitir a autenticação, como um toque digital ou deslize para realizar a leitura da impressão digital.[198]

Proteção de Ativos: Nesta aplicação, sistemas biométricos objetivam proteger informações digitais e materiais sensíveis de usuários não autorizados. Exemplo comum é a utilização da impressão digital para acesso a cofres com arquivos sensíveis[199].

Autenticação remota: A utilização da biometria neste caso permite um método seguro de autenticação, mesmo à distância[200]. Desta forma, a relação é mais ágil, confiável, e menos custosa. Por exemplo, para a ativação de uma conta bancária, a utilização de tecnologia biométrica de voz (confiável) já seria suficiente, poupando o percurso do sujeito até a agência bancária (aumenta a agilidade e diminui o custo). Outro exemplo é o caso da comprovação de vida de idosos aposentados para ganhar o benefício da pensão. Com a utilização de uma tecnologia biométrica, o processo se torna mais facilitado[201]. Ainda, a possibilidade de que eleitores autenticados possam votar utilizando um aplicativo oficial com acesso à voz como senha única e imutável. Desta forma, o processo de votação seria confiável e robusto, bem como evitaria eventuais votos e registros duplicados[202].

As aplicações acima referidas tendem a empregar tecnologias biométricas para aumentar a (i) segurança; (ii) eficiência e (iii)conveniência[203].

Buscou-se trazer conceitos iniciais sobre biometria, bem como os tipos e suas aplicações[204].

---

[197]BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015, p.03

[198] BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015, p.03

[199] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

[200] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

[201] KRISH, Ashok. Biometrics: **The Benefits and Challenges of Remote Authentication Systems**. Forbes Business Council. 2020. Disponível em: https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/07/biometrics-the-benefits-and-challenges-of-remote-authentication-systems/?sh=794390397bbc. Acesso em: 21. dez. 2021.

[202] KRISH, Ashok. Biometrics: **The Benefits and Challenges of Remote Authentication Systems**. Forbes Business Council. 2020. Disponível em: https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/07/biometrics-the-benefits-and-challenges-of-remote-authentication-systems/?sh=794390397bbc. Acesso em: 21. dez. 2021.

[203] DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 171.

[204] Ver mais sobre biometria em: JAIN, Anil Kumar; NANDAKUMAR, Karthik; ROSS, Arun. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letter*. Elsevier, 2016; DANTCHEVA, Antitza; ELIA, Petros; ROSS, Arun. What Else Does Your Biometric

2.4. Como funciona um sistema de reconhecimento facial

O reconhecimento facial é uma das principais tecnologias biométricas. A sua importância se deu com os avanços dos aparelhos de captura de imagem - como câmeras de vigilância e de aparelhos telefônicos; com o aumento no número de imagens de rostos circulando na internet, e também com demandas para garantir maior segurança[205].

Em comparação a outras biometrias já tratadas anteriormente, o reconhecimento facial possui muitas vantagens, como a possibilidade de captura à distância e de forma encoberta[206], o que facilita a sua utilização em aplicações de vigilância[207]. Nesse sentido, caracteriza-se por ser um método não intrusivo[208]. Além disso, a face também pode demonstrar emoções e informações biográficas[209], o que permite maior interação e personalização de dispositivos e programas[210]. Ainda, observa-se que as pessoas estão mais dispostas a compartilharem a sua face, como em redes sociais.[211]

Como se verá a seguir, o reconhecimento facial seria a única tecnologia biométrica capaz de obter inúmeras informações, não "só " capazes de identificar ou verificar um sujeito, mas também de desvendar informações como gênero, idade, emoção, extração de características únicas.

É possível a utilização tanto do termo reconhecimento da face (*face recognition*), como reconhecimento facial (*facial recognition*)[212]. O mais importante

---

Data Reveal? A survey on Soft Biometrics. IEEE Transactions on Information Forensics and Security, 2015; WENG, John J; SWETS, Daniel L. Face Recognition. In: JAIN, Anil; BOLLE, Ruud; PANKANTI, Sharath (Eds). Biometrics. Personal Identification in Networked Society. Nova Iorque: Springer, 2006, p.65-86

[205] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 1.

[206] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 1; JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[207] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[208] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 32

[209] Como gênero, etnia e idade. JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[210] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[211] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[212] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p5

não é tanto o seu termo, mas o que significa: "é o processamento automático de imagens digitais[213] de rostos com o objetivo de identificar, autenticar/verificar ou categorizar indivíduos"[214]. Ademais, os sistemas de reconhecimento facial estão inseridos nos tipos de tecnologias com inteligência artificial capazes de identificar indivíduos em imagem e vídeo ao analisar as suas características faciais. Salienta-se que os sistemas de reconhecimento facial possuem deep learning, um tipo de inteligência artificial que permite um aprendizado de máquina, fazendo com que o modelo utilizado aprenda a identificar corretamente os dados.[215]

É possível definir Tecnologia de Reconhecimento Facial (*Facial Recognition Technologies – FRTs*) como uma coleção de ferramentais digitais que objetivam realizar tarefas em imagens ou vídeos de rostos *humanos* para responder basicamente a três questionamentos: (1) Há um rosto na imagem?; (2) Que tipo de rosto é mostrado na imagem?; (3) De quem é o rosto mostrado na imagem?[216]

Para responder a primeira pergunta – há um rosto na imagem?; utiliza-se a detecção facial (*face detection*): processo de localizar rostos em uma imagem ou vídeo. Neste momento não se está falando de identificar um sujeito ou os seus atributos, gênero, idade, mas apenas encontrar rostos de indivíduos em determinada circunstância[217]. A detecção facial também permite o reconhecimento e localização de características faciais; obtenção dos contornos dos atributos da face (ex: olhos, boca e nariz); reconhecimento da expressão facial e rastreio de rostos em vídeo, por exemplo. Isso permite com que seja possível embelezar selfies, gerar avatares a partir da foto e usar em aplicativos de jogos que respondem às expressões do jogador[218].

---

[213] Entende-se como imagem digital a representação de imagem bidimensional ou tridimensional. EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 1.

[214] EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 2. Tradução livre do autor.

[215] CRUMPLER, William. How accurate are facial recognition systems – and why does it matter? Center for Strategic & International Studies. 2020. Disponível em: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter . Acesso em: 25 fev. 2022

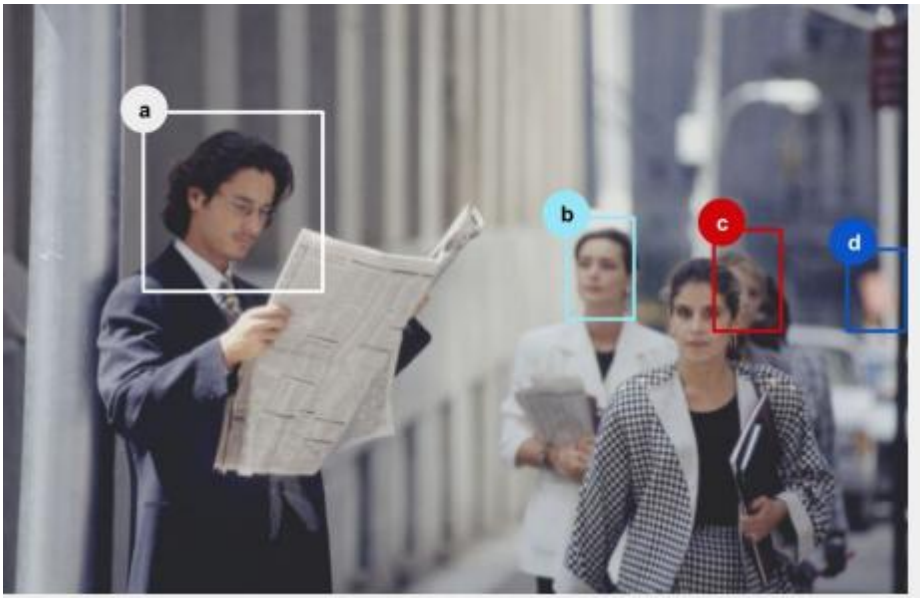
[216] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020. Disponível em: https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf . Acesso em: 03 jan, 2021, p. 2

[217] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.2-3

[218] Estas são as aplicações possíveis com o Machine Learning (ML) Kit's face detection API do Google. GOOGLE DEVELOPERS. Face Detection. Disponível em: https://developers.google.com/ml-kit/vision/face-detection. Acesso em: 03 fev. 2022.

Na detecção facial, é possível dois erros pelo software: (a) Falso negativo: não encontra um rosto que esteja presente e (b)Falso positivo: identifica como rosto algo que não é.[219] A figura abaixo expõe exemplos de detecção facial, também apresentando falsos negativos e falsos positivos.

FIGURA 8– DETECÇÃO FACIAL



Fonte: BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.3

Em relação à segunda pergunta – que tipo de rosto é mostrado na imagem?; é possível dividir em categorias[220]:

(a) Classificação de atributo da face (*face attribute classification*):): quando se trata de sexo, raça ou etnia denomina-se atributo de face;
(b) Estimativa de atributo da face (*face attribute estimation*): já quando se trata de número, como idade, utiliza-se o termo estimativa de atributo de face.
(c) Detecção de atributo da face (*face attribute detection*): enquanto que a detecção de acessórios, óculos, barbas e bigodes é chamada de detecção de atributo da face.

[219] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.3
[220] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.4

(d) Classificação de emoções, afeto e expressões faciais (*emotion, affect and facial expression classification*): a tecnologia de reconhecimento facial pode classificar as expressões, como "sorriso" e também estado emocional, como "feliz" e "raiva"[221].

No que tange ao terceiro questionamento – de quem é o rosto mostrado na imagem?; trata-se de verificar ou identificar um sujeito. Esta etapa pode ocorrer de duas formas: por meio da verificação da face (*face verification*) ou identificação da face (*face identification*)[222]. Denomina-se imagem de consulta (*query image*) ou apenas consulta (*query*) a imagem do rosto do sujeito que se objetiva reconhecer[223].

A verificação da face (*face verification*) ou também autenticação da face (*face authentication*)[224] envolve comparar a imagem de consulta que está se buscando a identidade, com a identidade que está sendo reinvidicada [225]. Em síntese: "a primeira pessoa é a mesma que a segunda?"[226]. Uma aplicação corriqueira é a utilização do reconhecimento facial para o controle de acesso – seja físico ou virtual; como desbloqueio de telefone, acesso à conta bancária[227], serviços de imigração (como o *E-passport)*[228]. A verificação ou autenticação da face também pode ser chamada de one-to-one match[229], *1-to-1 matching* ou *1-to-1 comparision*[230].

[221] Ver exemplos de aplicação em: LEO, Marco et AL. Automatic Emotion Recognition in Robot-Children Interaction for ASD treatment. IEEE Internacional Conference on Computer Vision Workshop (ICCVW). 2015, p-537-545; SATI; Vishwani et AL. Face Detection and Recognition, Face Emotion Recognition Trough NVIDIA Jetson Nano. In: Ambient Intelligence – Software and Applications. Internacional Symposium on Ambient Intelligence. 11. 2020, p. 177-185

[222] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.5

[223] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.5

[224] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 2.

[225] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 2-3

[226] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.6. Tradução livre do autor.

[227] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.5

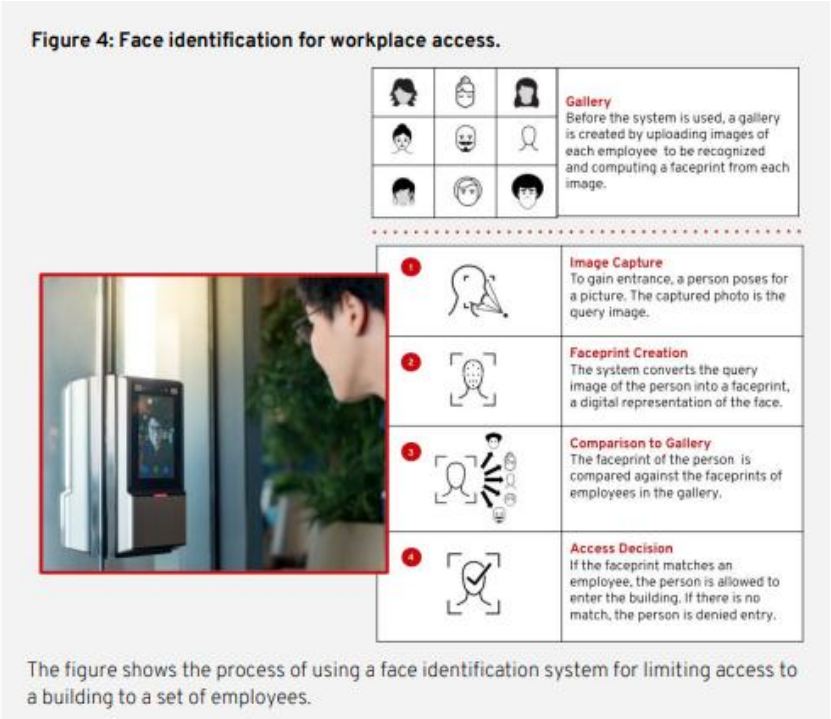
[228] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 2-3

[229] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 2-3

[230] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.6.

Já a identificação da face (face identification) ou reconhecimento da face (*face recognition*)[231] compara a imagem de consulta que está se buscando a identidade com várias imagens de rostos de bancos de dados (*gallery*)[232], buscando encontrar uma correspondência[233]. Basicamente, busca-se responder: "De quem é este rosto?"[234]. Exemplifica-se com uma rede social virtual (*social network service – SNS*) que consegue identificar uma pessoa e sugerir a sua marcação em uma foto ou vídeo[235], e com a identificação/reconhecimento de sujeitos em câmeras de segurança[236]. A identificação ou reconhecimento da face também pode ser referida como *1-to-many comparision*, *1-to-many matching*, 1-to-many identification ou *1-to-N identification*[237].

FIGURA 9 – IDENTIFICAÇÃO DA FACE PARA CONTROLE DE ACESSO EM LOCAL DE TRABALHO



[231] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p. 2.
[232] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.6
[233] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3.
[234] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.6 Tradução livre do autor.
[235] EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 3
[236] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3.
[237] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.6

Fonte: BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p. 9

Cumpre referir que a identificação é mais problemática do que a verificação. Isso porque, o sistema de identificação requer uma análise de várias comparações[238]. Mas, ainda há o desafio das identificações remotas e também em tempo real (ex: em um sistema de vigilância público). A *1-to-many comparision* de forma remota costuma ter menor acurácia, na medida em que é mais difícil para as câmeras obterem imagens consistentes e de boa qualidade enquanto da movimentação do indivíduo[239].

De forma mais técnica, explica-se como funciona um sistema de reconhecimento facial. Normalmente, ocorrem quatro etapas: (i)Detecção do rosto (*face detection*); (ii) normalização da face (face normalization); (iii)extração de recursos da face (face feature extraction) e (iv)correspondência da face (face matching)[240].

Detecção do rosto (*face detection*): rastreamento do rosto, no qual é segmentada a face do restante da área detectada. É fornecida uma aproximação da localização e escala do rosto. Já a **marcação da face** (*face landmarking*), localiza pontos faciais, como olhos, nariz, boca.[241]

Normalização da face (face normalization): normaliza a face geometricamente e fotometricamente para que seja possível o reconhecimento independentemente da iluminação ou pose[242]. Por exemplo, converte-se a imagem para um tamanho padrão e ajustam-se as distribuições de cores[243].

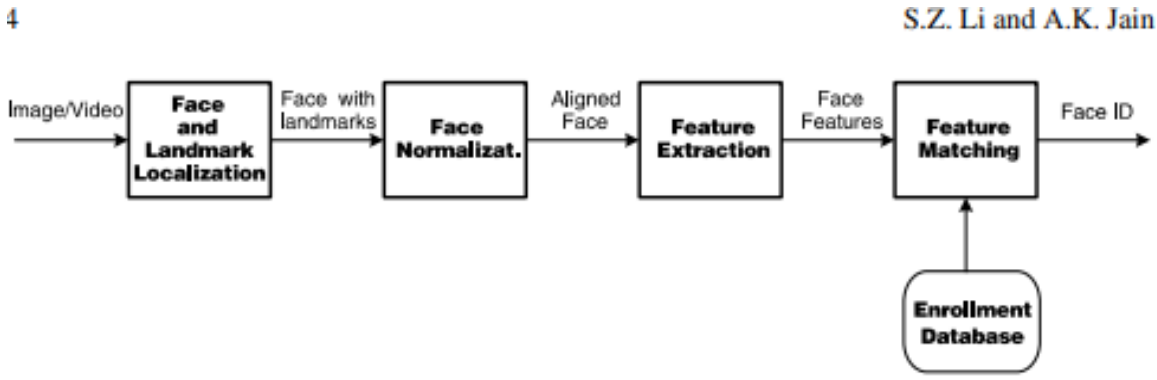
---

[238] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 40.
[239] CRUMPLER, William. How accurate are facial recognition systems – and why does it matter? Center for Strategic & International Studies. 2020. Disponível em: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter . Acesso em: 25 fev. 2022.
[240] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3.
[241] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.4.
[242] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.4.
[243] EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 2.

Extração de recursos da face (face feature extraction): na imagem normalizada do rosto, ocorre a extração de recursos úteis da face capazes de distinguir outros rostos[244].

Correspondência da face *(face matching):*é nesse momento em que os recursos extraídos da face são comparados com uma ou várias faces do banco de dados (*enrolled database*). Se o objetivo é a verificação/autenticação da face (*face verification or authenticatio*) – 1:1; o sistema de correspondência dirá "sim" (*yes*) ou "não" (*no)*. No caso da identificação/reconhecimento facial (*face identification or recognition)* – 1:N; o sistema de correspondência aponta "correspondente" (*match found*) quando há uma confiança suficiente com base na pontuação atingida, ou "desconhecido" (*unknown*) quando a pontuação de correspondência está abaixo da pontuação determinada[245]. Há ainda um terceiro objetivo ao comparar duas imagens de rosto.

FIGURA 10 – REPRESENTAÇÃO DO FLUXO DE PROCESSAMENTO DO RECONHECIMENTO FACIAL:detecção, normalização, extração e correspondência



Fonte: LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.4.

[244] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.4.
[245] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.4.

Importante referir que o sistema também pode objetivar extrair características de um sujeito para classificá-lo em uma ou mais categorias, como **idade** e **sexo**[246]. Tanto a idade como o gênero é considerada *soft biometrics*[247].

Em relação à **classificação de idade**, exemplifica-se: um sistema de jogos online que utiliza classificação de idade para permitir ou negar acesso a conteúdos do jogo. Ainda, um jogo que funciona com câmeras e controle de gestos e movimentos pode prever a idade provável, sexo e humor, podendo ser utilizados para aprimorar a experiência do usuário[248].

Uma lei chinesa, introduzida em 2019[249], proíbe que menores de idade (menores de 18 anos) joguem videogame entre 22h-08h e, e estabelece o limite de no máximo noventa minutos por dia. Após, foram permitidas apenas sessões de até uma hora, das 20h-21h, aos finais de semana e feriados. A partir do dia 01 de junho de 2021, foi determinado que os jogos deveriam incluir um sistema de autenticação de identidade nacional chinesa, com o objetivo de prevenir que as crianças chinesas menores de idade acessassem os games[250]. Esta normativa fez com que a empresa chinesa Tencent[251] implementasse reconhecimento facial nos jogos para cumprir a legislação. A medida vale apenas para a China e em jogos de celular. O sistema denomina-se "*Midnight Patrol*"[252] e funciona da seguinte maneira: quando o usuário joga além do limite previsto, é solicitada uma varredura facial (*facial scan*). Quem recusar é identificado automaticamente como menor e expulso do jogo[253].

Uma pesquisa realizada buscou analisar o desempenho de um sistema de aprendizagem de reconhecimento facial (*deep learning face recognition*) em crianças

---

[246]EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 2.

[247] GUO, Guodong. Gender Classification. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p834

[248] EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012, p. 3.

[249] TUNHOLI, Murilo. China proíbe menores de 18 anos de jogar videogame por mais de 3h semanais. Tecnoblog. Disponível em: https://tecnoblog.net/noticias/2021/08/30/china-proibe-menores-de-18-anos-de-jogar-videogame-por-mais-de-3h-semanais/. Acesso em: 02 fev. 2022

[250] HOLLISTER, Sean. How Tencent's sweeping new facial scans Will atch Chinese kids playing past curfew. The Verge. Disponível em: https://www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace. Acesso em 02 fev. 2022.

[251] Empresa líder mundial em internet e tecnologia. Desenvolve produtos e serviços, como videogames e computação em nuvem. Ver mais em: https://www-tencent-com.translate.goog/en-us/about.html?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc#about-con-1

[252] Em tradução livre do autor: Patrulha da Meia-Noite.

[253] HOLLISTER, Sean. How Tencent's sweeping new facial scans Will atch Chinese kids playing past curfew. The Verge. Disponível em: https://www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace. Acesso em 02 fev. 2022.

versus adultos. O resultado foi a existência de um viés claro quando da comparação das faces infantis e adultas. O estudo referiu a necessidade de maior aprofundamento na temática e que há carência de estudos sobre o tema[254].

Em relação à **classificação de gênero**, o objetivo é determinar, com base na análise biométrica, se o sujeito é do gênero feminino ou masculino. Usualmente este processo costuma ocorrer após a **extração de recursos da face**, quando é aplicado o classificador de gênero[255].

FIGURA 11 – MODELO TÍPICO DE CLASSIFICAÇÃO DE GÊNERO

Fonte: GUO, Guodong. Gender Classification. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 834

Ilustram-se as **aplicações** da classificação de gênero[256]: (a) controle de acesso (*acess control*) de determinada área – como evitar que homens ingressem em banheiros femininos prevenindo situações de assédio; (b)*businnes intelligence*: para segmentação de publicidade e melhoria na experiência do cliente e; (c) Filtragem de imagem (*image filtering*) para auxiliar na organização de bases de dados de imagens e vídeos[257].

[254] NISHA, Srinivas; KARL, Ricanek; MICHALSKI, Danai; BOLME, David; MICHAEL, King. Face Recognition Algoritm Bias: Performance Differences on Images of Children and Adults. United States . 2019. Disponível em: https://www.osti.gov/biblio/1559665. Acesso em 05 fev.2022

[255] GUO, Guodong. Gender Classification. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 833

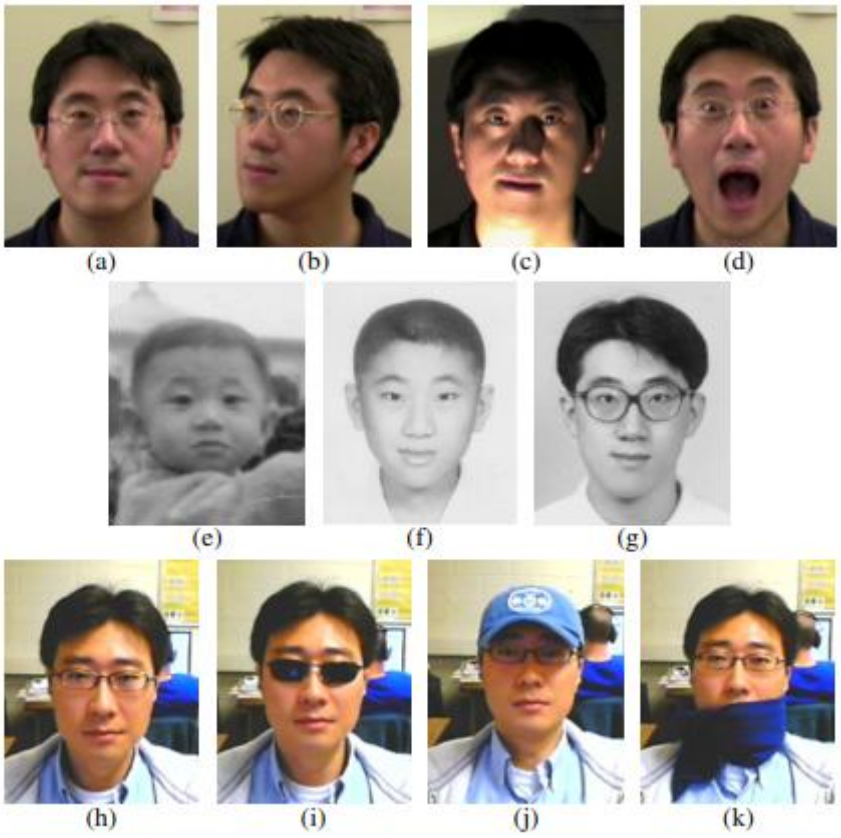
[256] No mesmo sentido: NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p.1

[257] GUO, Guodong. Gender Classification. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 834

2.5 Acurácia dos sistemas de reconhecimento facial

Quando se aborda o tema da acurácia, primeiro é necessário definir o que esta significa. É possível compreender esta como: "grau de exatidão ou precisão demonstrado por uma tabela ou operação"[258]. A partir disso, é imprescindível que se observe a acurácia dos sistemas de reconhecimento facial. Há vários fatores que desafiam o reconhecimento automatizado de rostos, como *variações de pose, iluminação, idade, expressão facial, aparência* (ex: maquiagem, pelos faciais, acessórios)[259].

FIGURA 12 – IMAGENS FACIAIS E SUAS VARIAÇÕES (adaptado)



Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 99

[258] DICIO. Dicionário Online de Portugês. Acurácia. Disponível em: https://www.dicio.com.br/acuracia/. Acexso em: 10 fev. 2022

[259] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

A variação de *pose* é um dos pricipais fatores que prejudica o desempenho de reconhecimento. Imagens de um mesmo sujeito em diferentes poses (variação intra-usuário) podem sofrer maior variação do que imagens de dois sujeitos em uma mesma posição (variação entre usuários)[260].

Em que pese não tão abordado pela academia em relação aos outros fatores que influenciam na acurácia, a *oclusão* na totalidade da imagem ou em parte dela também deve ser mencionada[261]. A oclusão facial ocorre quando acessórios[262] ou objetos estão presentes na face[263]. A iluminação ou a falta dela e a variação da pose também podem gerar oclusão - a aparência facial muda consideravelmente com a oclusão[264].

FIGURA 13 – DIFERENTES CENÁRIOS DE FACES OCLUÍDAS E LIVRES DE OCLUSÃO (imagem adaptada)

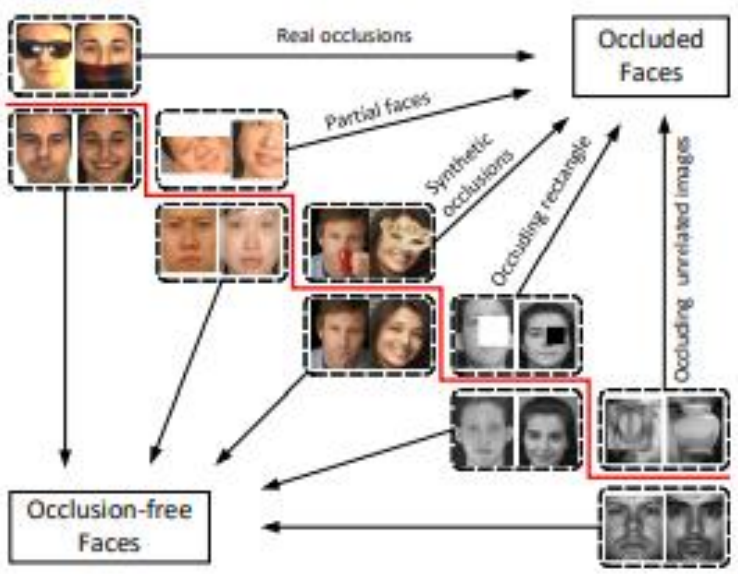


Fig. 2. Different occluded face recognition testing scenarios involved in OFR.

[260] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 129

[261] ZENG, Dan; VELDHUIS, Raymond; SPREEUWERS, Luuk. A survey of face recognition techniques under oclusion. University of Twente,Netherlands,2020. Disponível em: https://arxiv.org/pdf/2006.11366.pdf. Acesso em: 20 fev. 2022, p. 1

[262] Tal situação é recorrente em vídeos de vigilância, no qual o sujeito pode estar com acessórios que intencionalmente dificultam a identificação. Outro exemplo é em sistemas de autenticação facial, em que o mecanismo rejeita a imagem quando os olhos não são detectados (sujeito está utilizando óculos escuros) .JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 130

[263] Ver mais sobre o tema da oclusão parcial da face em: EKENEL, Hazm Kemal; STIEFELHAGEN, Rainer. Why is facial occlusion a challenging problem? In: TISTARELLI, Massimo; NIXON, Mark (Eds.). Advances in Biometrics. Third Internacional Conference ICB. Springer: Itália, 2009, p. 299- 308.

[264] ZENG, Dan; VELDHUIS, Raymond; SPREEUWERS, Luuk. A survey of face recognition techniques under oclusion. University of Twente,Netherlands,2020, p. 1

Fonte: ZENG, Dan; VELDHUIS, Raymond; SPREEUWERS, Luuk. A survey of face recognition techniques under oclusion. University of Twente,Netherlands,2020, p. 2

Um dos grandes desafios da oclusão no reconhecimento facial são as inúmeras possibilidades de se ocluir um rosto (*occlusion diversity*). Esta diversidade na possibildade de oclusão dificulta a alimentação do sistema de reconhecimento. Além disso, as bases de dados utilizadas para estudos deste tipo com imagens ocluídas são ínfimas. Portanto, são necessários conjuntos de dados em larga escala com diversidades de imagens ocluídas. Isso permitirá um melhor treinamento nos sistemas de reconhecimento, bem como criação de protocolos para melhor identificar ou autenticar faces ocluídas[265].

Ainda em relação à oclusão, pesquisadores do National Institute of Standards and Technology (NIST) publicaram dois estudos em 2020[266] sobre o desempenho de algoritmos de reconhecimento facial em rostos ocluídos por máscaras para prevenir o COVID-19.

O primeiro estudo[267], dentre outras conclusões, apontou o que já se esperava: as imagens em que as máscaras mais ocluem a face apresentam maior taxa de falsas não correspondências; as máscaras mais largas (que ocluem mais a face) dão 2x mais taxas de falsos negativos que as menores (redondas). Além disso, em comparação com máscaras azul-claras e pretas, as pretas tem maior taxas de erro – a razão é desconhecida[268]. O segundo estudo[269]observou notáveis reduções de taxas de erro em imagens com máscaras faciais. Quanto à cor da máscara, adicionou-se as cores branca e

[265] ZENG, Dan; VELDHUIS, Raymond; SPREEUWERS, Luuk. A survey of face recognition techniques under oclusion. University of Twente,Netherlands,2020, p. 14

[266] NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. United States Department of Commerce. 2020. Disponível em: https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report_6b.pdf. Acesso em: 01 fev. 2022; NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6A: Face Recognition accuracy with masks using pré-COVID-19 algorithms. . United States Department of Commerce. 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf. Acesso em: 01 fev. 2022.

[267] A base de dados utilizada foi apenas one-to-one (1:1) e os algoritmos fornecidos ao NIST foram anteriores à pandemia de COVID-19. NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6A: Face Recognition accuracy with masks using pré-COVID-19 algorithms. . United States Department of Commerce. 2020, s.n

[268] NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6A: Face Recognition accuracy with masks using pré-COVID-19 algorithms. . United States Department of Commerce. 2020, s.n.

[269] A base de dados também era de onte-to-one (1:1) e os algoritmos fornecidos ao NIST foram desde meados de março de 2020. NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. United States Department of Commerce. 2020, s.n.

vermelhas: os algoritmos tiveram maiores taxas de erro nas máscaras pretas e vermelhas do que nas azuis e brancas – o motivo segue desconhecido[270].

Ainda, o reconhecimento da face é dificultado por semelhanças em rostos, como em gêmeos e parentes, podendo confundir sujeitos distintos[271]. No Face ID da Apple é possível ocorrer tal situação e a empresa indica a utilização de senha se o cliente estiver preocupado com a segurança do aparelho em termos de desbloqueio. A empresa refere que a probabilidade de erro também é maior em crianças abaixo de 13 anos, pois as suas características faciais ainda não estão completamente desenvolvidas[272].

FIGURA 14– SEMELHANÇA NA FACE DE GÊMEOS E PARENTES
(imagem adaptada)

(a) Twin[1] (b) Family[2]

[1] www.marykateandashley.com.
[2] news.bbc.co.uk/hi/english/in_depth/americas/2000/us_elections.

Fig. 3.2 The problem of inter-class similarity. The face images of some people (e.g., twins or families) exhibit similarities in appearance that can confound an automated face recognition system.

Fonte: JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 100

[270] NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. United States Department of Commerce. 2020, s.n.

[271] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 98

[272] "The probability that a random person in the population could look at your iPhone or iPad Pro and unlock it using Face ID is approximately 1 in 1,000,000 with a single enrolled appearance. As an additional protection, Face ID allows only five unsuccessful match attempts before a passcode is required. **The statistical probability is different for twins and siblings that look like you and among children under the age of 13**, because their distinct facial features may not have fully developed. **If you're concerned about this, we recommend using a passcode to authenticate.**" APPLE. About Face ID advanced technology. Disponível em: https://support.apple.com/en-us/HT208108. Acesso em: 20 fev. 2022.

Primeiramente, os sistemas poderão dar resultados diferentes de acordo com uma *captura da face (mugshot) estática* e em *ambiente controlado*; para uma *captura da face dinâmic*a e em *local descontrolado* (cluttered background)[273].

Em ambientes descontrolados há maior complexidade: podem ter vários rostos na imagem ou vídeo, com expressões faciais e posições diferentes. Isso pode implicar em, além de diferentes características de cada sujeito, como maquiagem, acessórios, diferentes idades, também fatores como oclusão e variações na iluminação[274].

Em relação ao ambiente controlado, ressalta-se que o desempenho melhor exige imagens faciais capturadas com fundo fixo e simples e com *iluminação controlada*. Além da iluminação, o sistema também tem maior dificuldade de comparar imagens obtidas de ângulos e momentos diferentes[275].

Ainda, a **acurácia na classificação de gênero** poderá depender do tipo de tecnologia empregada, bem como do ambiente em que há a coleta da imagem da face[276]. Há um impacto negativo na precisão quando a imagem é coletada em ambiente descontrolado (*in the wild),* no qual há variação de pose, iluminação, expressão facial e plano de fundo. Ao contrário, há maior precisão na classificação em ambientes controlados (*constrained)*[277].

Em relação à precisão, é possível dividir em (a)cenários de usuários cooperativos (*cooperative user scenarios*) e, (b) cenários de usuários não cooperativos (*noncooperative user scenarios*)[278].

O primeiro se dá quando o usuário está disposto a apresentar o rosto de forma propícia para que seja dado o acesso ou privilégio, como pose frontal, olhos abertos. Nesses casos, além de uma postura pró ativa do usuário, o seu rosto costuma estar mais próximo do sistema, o que facilita o trabalho de reconhecimento para sistema.

---

[273] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 32

[274] WENG, John J; SWETS, Daniel L. Face Recognition. In: JAIN, Anil; BOLLE, Ruud; PANKANTI, Sharath (Eds). Biometrics. Personal Identification in Networked Society. Nova Iorque: Springer, 2006, p.66

[275] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biometrics**. New York:Springer, 2011, p. 32

[276] Nesse mesmo sentido: LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3; HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020,p. 22

[277] NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p.4-5.

[278] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3

Exemplos de cenários de usuários cooperativos é o controle de acesso físico, *login* de computador e passaporte eletrônico[279].

Já o segundo ocorre quando o usuário não sabe que está tentando ser identificado, como em aplicações de vigilância. O cenário do usuário não cooperativo é o mais desafiador, pois, além da distância, a iluminação, movimento, posição da face e outros fatores influenciam na dificuldade[280].

Em relação à acurácia na classificação de gênero, uma pesquisa publicada *pelo National Institute of Standars and Technology* (NIST)[281] concluiu que esta classificação é mais precisa em homens do que em mulheres. Esta resposta foi fruto de uma análise de banco de dados com 240 mil imagens de vistos[282].

Em um dos estudos do NIST, observou-se que a **idade** também influencia na classificação de gênero. Há maior precisão em jovens adultas (21-30 anos). Entretanto, todos os algoritmos analisados demonstraram uma queda na precisão da classificação em mulheres com o avançar da idade, decrescente principalmente com mais de 50 anos. O que significa que, acima desta idade, é alta a probabilidade de que o sistema classifique erroneamente (*misclassifying*) mulheres como homens[283].

FIGURA 15 – EXEMPLOS DE CLASSIFICAÇÃO ERRÔNEA (misclassification) COMO MASCULINO EM MULHERES ACIMA DE 50 ANOS

[279] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3.
[280] LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15, p.3.
[281] NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015. Online. Disponível em: https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification. Acesso em: 05 fev. 2022.
[282] A principal base de dados utilizada era composta de imagens coletadas em ambiente controlado (controlled), com iluminação, pose e expressões faciais também em condições controladas. NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 5
[283] NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 8

Fonte: NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 9

Diferentemente, a maior precisão na classificação do gênero masculino se dá na faixa de idade dos 31-60 anos[284]. As únicas hipóteses referidas na pesquisa de identificação errônea de homens – como mulheres; ocorreu em sujeitos de Taiwan e Japão. Acredita-se que a classificação errada tenha ocorrido pelo fato de homens asiáticos serem mais propensos a ter o formato do rosto mais fino, ausência de pelos faciais e penteados de cabelos mais compridos[285]. As pesquisas publicadas pelo NIST supramencionadas não foram as únicas a apontar vieses (bias) de gênero e raça.

Em 2018, estudo realizado por Joy Boulamwini (Instituto de Tecnologia de Massachusetts- MIT) e Timnit Gebru (Microsoft)[286] analisou os classificadores comerciais de gênero da Microsoft, IBM e Face++ e, para permitir uma análise completa, optou por dividir em 04 subgrupos separados por **gênero** *e* **tipo de pele**: **homens mais claros** (lighter males), **mulheres mais claras** (lighter females), **homens mais escuros** (darker males) e **mulheres mais escuras** (darker females)[287].

Foi criada uma **base de dados** denominada *Pilot Parliaments Benchmark* (PPB). Esta foi composta de 1.270 imagens de mulheres e homens membros dos Parlamentos dos países europeus (Islândia, Finlândia e Suécia) e africanos (Senegal, África do Sul e Ruanda). A escolha das fotos de parlamentares deu-se em virtude de serem imagens públicas e, portanto, disponíveis abertamente (sem necessidade de licença para uso) e com pouca variação de pose. A escolha desses países específicos deu-se pela paridade

[284] NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 9

[285] NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 11

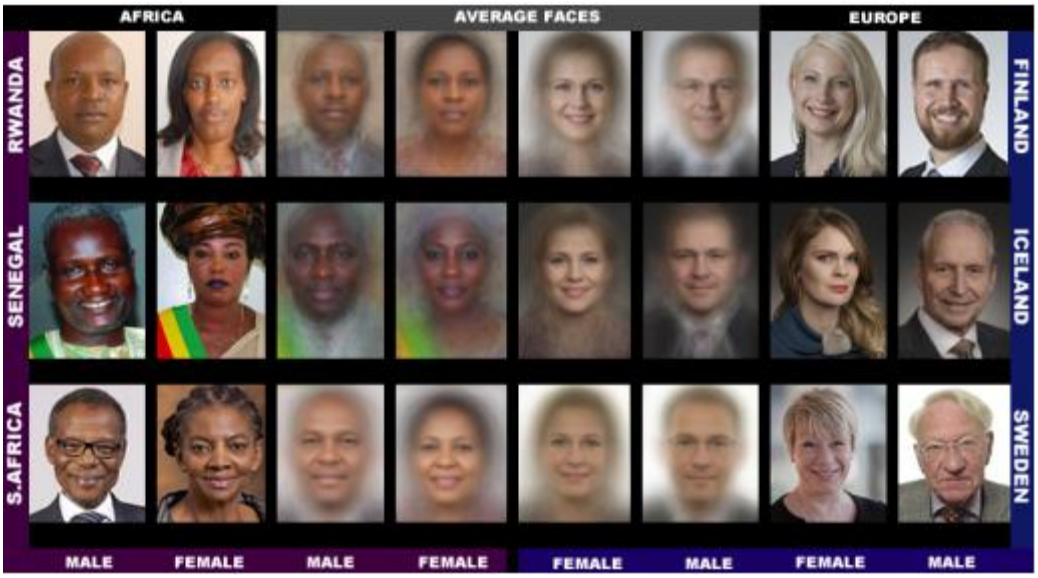
[286] Timnit Gebru foi demitida principalmente após controvérsias relativas ao artigo escrito. EPOCA NEÓCIOS. Quem é a funcionária do Google demitida após acusar empresa de racismo e censura. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2020/12/quem-e-funcionaria-do-google-demitida-apos-acusar-empresa-de-racismo-e-censura.html. Acesso em: 05 fev. 2022.

[287] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018. Disponível em: https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf. Acesso em 05 fev. 2022

de gênero em seus parlamentos e também pela prevalência de indivíduos de pele mais clara nos europeus e de pele mais escura nos africanos[288].

A figura abaixo representa um exemplo do *Pilot Parliaments Benchmark* (PPB), retratando esta situação. Observa-se que há parlamentares que não foram identificados em relação ao país (*average faces*). Apesar de ter sido possível a identificação do gênero, optou-se por não agregar a raça ou etnia para determinar o local de origem.

FIGURA 16 – AVERAGE FACES



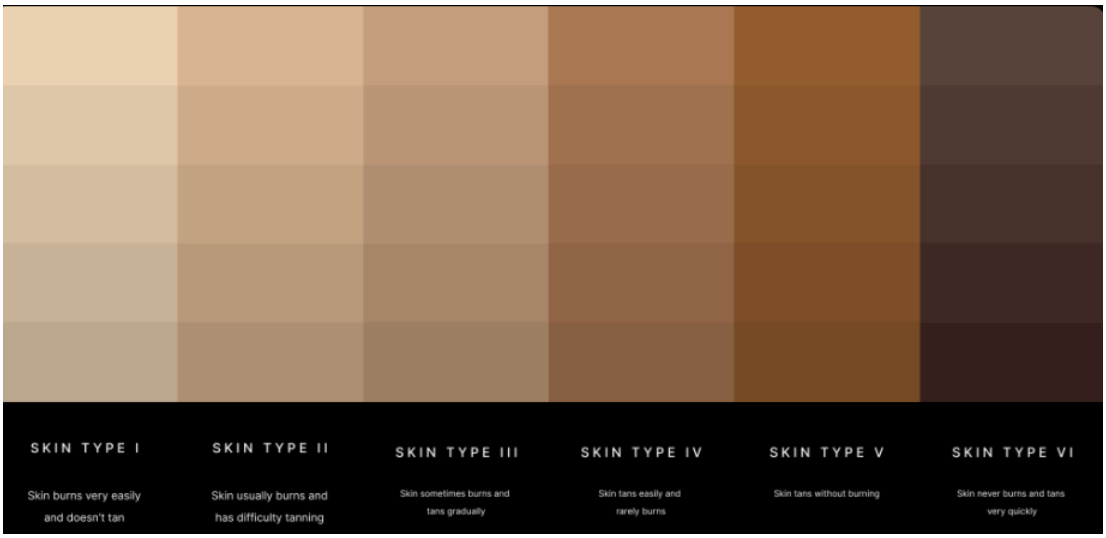
Fonte: BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 4

Assim, optou-se pelo **tipo de pele**, ao invés de raça ou etnia. Isso porque, embora estas possam ser utilizada para avaliar algumas formas de discriminações algorítmicas, enfrentam duas limitações quando da análise em imagens: as características fenotípicas podem sofrer alterações dentro de uma mesma raça ou etnia

[288] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 5-6.

e, dentro de uma região demográfica, também são possíveis essas modificações. Assim, entendeu-se que o tipo de pele seria um atributo fenotípico mais objetivo para utilizar nos classificadores e observar a existência ou não de vieses, independente do local de origem[289]. Para possibilitar a análise do tipo de pele, escolheu-se a marcação de seis pontos Fitzpatrick (*Fitzpatrick six-point labeling*)[290]. Esta classificação rotula a pele de Tipo I a Tipo VI. Veja-se:

FIGURA 17- MARCAÇÃO DE SEIS PONTOS FITZPATRICK (*FITZPATRICK SIX-POINT LABELING*) – CLASSIFICAÇÃO DO TIPO DE PELE I-VI



Fonte: SCALE. Scale AI and Research Partner MIT Media Lab Analyse Bias in Dermatological Datasets to improve diagnoses. Disponível em: https://scale.com/blog/clinical-dermatology. Acesso em: 08 fev. 2022

As autoras dividiram em duas categorias os **tipos de pele**: (a)**assuntos mais claros** (lighter subjects): tipos de pele na **escala Fitzpatrick I, II ou III**; (b) **assuntos mais escuros** (darker subjects): tipos de pele na escala **Fitzpatrick IV, V ou VI**. Esta

[289] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 4
[290] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 6

separação foi realizada para distinguir melhor a dicotomia pele clara *versus* pele escura[291].

Após a criação do banco de dados *Pilot Parliaments Benchmark* (PPB), com a separação por gênero e tipos de pele, foi possível dar início à análise dos **classificadores comerciais de gênero**. Escolheu-se os classificadores de gênero disponibilizados por *API bundles*[292] da **Microsoft** e **IBM,** como o *Microsof't Cognitive Services Face API*[293] e o *IBM's Watson Visual Recognition API*[294].. Também foi escolhida a **Face++,** empresa de visão computacional com sede na China, que possui tecnologia de análise facial,[295] inclusive adotada em alguns computadores da Lenovo. Destaca-se que as companhias foram escolhidas posto que utilizavam classificação de gênero *e* análise da face em seus *API bundles*; haviam realizado demonstrações públicas de classificações de gênero (Face++) e análise da face (Microsoft e IBM), e não informaram detalhes sobre a metodologia de classificação de gênero[296] e dos dados de treinamento utilizados[297].

Os resultados encontrados foram[298]:

(i) Todos os classificadores **desempenharam melhor em assuntos mais claros** (*lighter subjects*) do que em assuntos mais escuros (*darker subjects*);

(ii) Todos os classificadores **desempenharam melhor em homens do que em mulheres** (diferença da taxa de erro – 8,1% - 20,6%)

(iii) Todos os classificadores **desempenharam pior em mulheres mais escuras** (taxa de erro entre 20,8% - 34,7%);

---

[291] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 7

[292] Entende-se como *API bundles* um pacote de produtos monetizáveis, podendo ser aplicativos ou serviços. É uma classificação utilizada por desenvolvedores.

[293] Ver mais em: MICROSOFT. Azure. API de Detecção Facial. Um serviço de IA que analisa rostos e imagens. Disponível em: https://azure.microsoft.com/pt-br/services/cognitive-services/face/#overview. Acesso em: 08 fev. 2022

[294]Ver mais em: IBM. Watson Visual Recognition. Disponível em: https://www.ibm.com/fi-en/cloud/watson-visual-recognition. Acesso em: 08 fev. 2022

[295] Ver mais em: FACEPLUSPLUS. Disponível em: https://www.faceplusplus.com/. Acesso em 08 fev. 2022

[296] Ressalta-se que os APIs da Microsoft e Face++ indicam na classificação apenas se o rosto é feminino ou masculino. O API da IBM fornece um percentual de confiança sobre a classificação realizada. BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 11

[297] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 8

[298] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 8-10

(iv) Microsoft: alcançou menores taxas de erro (12,9% em assuntos mais escuros e 0,7% em assuntos mais claros)

(v) IBM: obteve o pior desempenho na precisão de classificação em assuntos mais escuros (taxa de erro de 22,4%), e o melhor desempenho em mulheres mais claras (taxa de erro de 0,0%).

(vi) Para Microsoft e IBM, homens mais escuros são piores classificados que homens mais claros;

(vii) Face++: obteve excelente desempenho em assuntos mais claros (mulheres e homens), com taxa de erro de 0% e a menor taxa de erro na classificação de homens mais escuros (taxa de erro de 0,7%)

Em resumo, descobriu-se que os classificadores desempenharam melhor em **homens mais claros** (ligher males), ao passo que as **mulheres mais escuras**[299] (darker females) têm as maiores taxas de erro em todos os classificadores[300].

Outra pesquisa realizada no mesmo ano (2018) merece destaque. Impulsionados pelos resultados obtidos na pesquisa de Boulamnwi e Gebru, pesquisadores da IBM e da Universidade da Califórnia (Berkeley) buscaram testar se as mulheres mais escuras foram classificadas erroneamente em virtude do padrão de cabelo (observou-se visualmente que a maioria das mulheres mais escuras possuíam cabelos curtos)[301].

Por fim, cumpre referir a existência de críticas posteriores à publicação do estudo no que tange à utilização da escala Fitzapatrick Skin Type (*Fitzpatrick six-point labeling)* . Entende-se que existiriam muitas variações de tons de pele em um mesmo sujeito, a depender da iluminação, horário e sistema. Ocorre uma variação de mais de 2x nestas circunstâncias, o que se observa na diferença da maior variação para a menor variação (vide imagem, resultando em ambos os casos uma diferença de 48)[302]. A

[299] Não foi trazido na pesquisa o motivo pelo qual os homens desempenharam melhor papel em relação às mulheres.

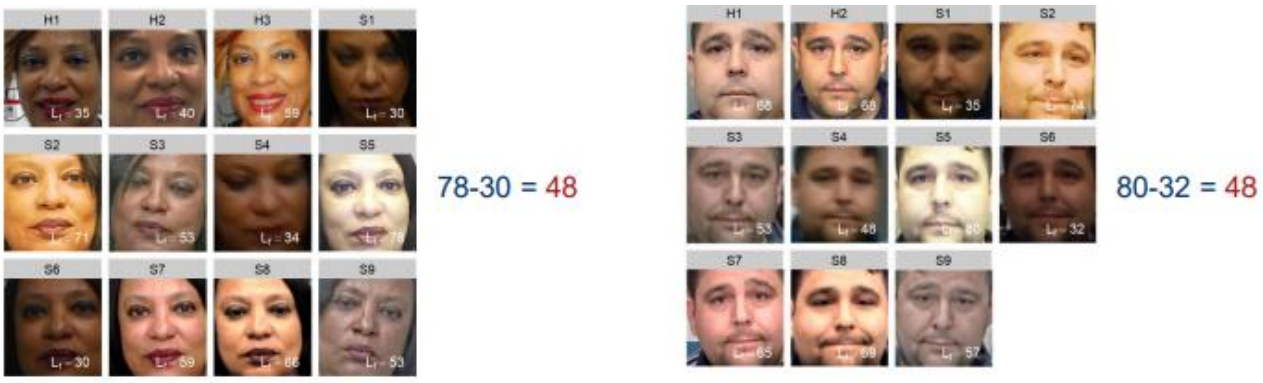
[300] BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018, p. 12

[301] MUTHUKUMAR, Vidya; PEDAPATI, Tejaswini; RATHA, Nalini; SATTIGERI, Prasanna; WU; Chai-Wah; KINGSBURY, Brian; KUMAR, Abhishek; THOMAS, Samuel; MOJSILIVIC, Aleksandra; VARSHNEY, Kush. Understanding Unequal Gender Classification Accuracy from face Images. 2018. Disponível em: https://arxiv.org/pdf/1812.00099.pdf. Acesso em 08 fev. 2022., p. 2

[302] HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020. Disponível em:

variação de uma única pessoa (48) normalmente é maior do que as diferenças entre os grupos demográficos[303].

FIGURA 18- VARIAÇÕES NA MEDIÇÃO DE LUMINOSIDADE DA ÁREA DO ROSTO



Fonte: HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020, p. 14

Ainda, os críticos referem que a *Fitzapatrick Skin Type* (*Fitzpatrick six-point labeling)* não seria confiável na utilização de classificadores como na pesquisa de Boulamnwi e Gebru, posto que não visa identificar nem medir a cor da pele, mas sim, a medição da sensibilidade da luz UV em cada tom de pele[304].

Ainda, cumpre referir que o sistema de reconhecimento facial pode ocasionar dois tipos de erros: (a)Correspondência Falsa (*false match or false accept - FMR*): ocorre quando o sistema confunde medidas biométricas de duas pessoas e entende como sendo de um indivíduo. (b) Falsa Não Correspondência (*false nonmatch or false reject* -

https://pages.nist.gov/ifpc/2020/presentations/36_Fitzpatrick_IFPC2020_Final.pdf. Acesso em: 08 fev. 2022, p. 14-15

[303] HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020, p. 15

[304] HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020, p. 21.

FNMR): acontece quando o sistema confunde medidas biométricas da mesma pessoa e entende como sendo de dois indivíduos distintos[305].

A acurácia do sistema biométrico será relativa à sua aplicação. Em situações forenses, a Falsa Não Correspondência *(FNMR)* é mais crítica[306], haja vista que um inocente poderá ser apreendido, ao mesmo tempo em que um delinquente poderá ser inocentado. Em relação ao controle de acesso, a Correspondência Falsa (FMR) seria mais segura, na medida em que poderia impedir o acesso de pessoas não autorizadas[307].

Em se tratando de aplicações civis, dependerá muito do tipo de aplicação, sendo necessário analisar ambos FMR e FNMR Por exemplo, uma Combinação Falsa em uma situação de retirada de valores em totem bancário (*ATM card verification*), poderia gerar perdas milionárias na conta do outro indivíduo. Já a Falsa Não Correspondência nessa mesma situação, poderia ocasionar a dificuldade de identificar um cliente, a sua saída da empresa, pela consequente falta de confiança deste na organização[308].

Quanto à acurácia nas atividades de identificação e precisão, Rodotá assevera[309] ser

> indispensável assegurar-se da sua precisão, já que as técnicas utilizadas podem revelar elevados percentuais de erros, positivos e negativos. Isto ocorre pelo caráter ainda experimental de algumas técnicas ou então pela situação particular em que estas são empregadas (como as condições de luz ou o ângulo da imagem, no caso da identificação facial)

Para tanto, observa-se a diferença na acurácia em relação a gêneros, idade e variação do ambiente, o que é desafiador justamente pelo fato da tecnologia já estar em utilização no mercado.

---

[305] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 34-35

[306] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 34-35

[307] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 35

[308] JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 36

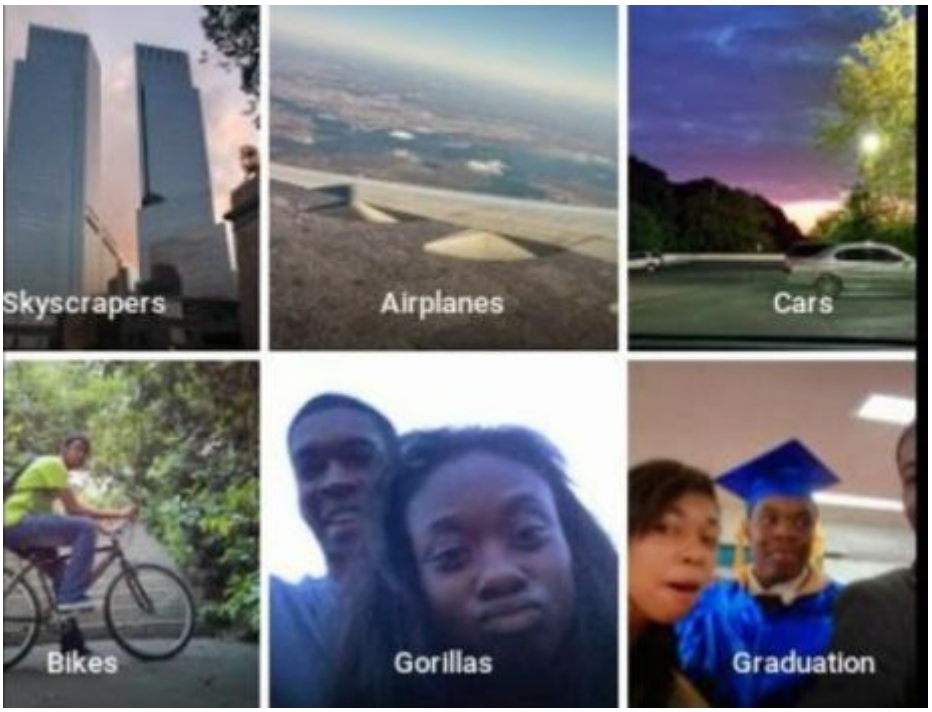
[309] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 266

2.6 Desafios correlatos

Além das questões relativas à acurácia do sistema de reconhecimento facial, também existem desafios que tangem a esfera da privacidade dos indivíduos e necessitam ser apontados.

Em 2015, o Google Fotos reconheceu erroneamente um casal negro como sendo "gorilas". O aplicativo já havia reconhecido equivocadamente cães como cavalos. Estas situações foram automáticas e realizadas pelo software de inteligência artificial. O Google pediu desculpas para o casal, e demonstrou bastante preocupação com o caso[310].

FIGURA 19 – CASAL É IDENTIFICADO COMO GORILA (IMAGEM ADAPTADA)



Fonte: BBC. Google apologises for Photos app's racist blunder. Disponível em: https://www.bbc.com/news/technology-33347866. Acesso em: 08 fev. 2022

Já foi visto que os sistemas de reconhecimento facial podem errar. Em que pese algumas taxas de erro possam ser pequenas em comparação com as taxas de acerto, o

[310]BBC. Google apologises for Photos app's racist blunder. Disponível em: https://www.bbc.com/news/technology-33347866. Acesso em: 08 fev. 2022

impacto negativo capaz de gerar em determinados indivíduos não é pequeno. Supõe-se um sistema com falsa correspondência (*false match*) de 1 indivíduo a cada 500. Se este for utilizado para controle de acesso em locais da cidade, de uma população de 2milhões de pessoas, seriam 4.000 correspondências falas. Soma-se o fato de que nestas correspondências falsas há maior chance de que ocorra em segmentos específicos , aumentando a possibilidade de discriminação. Tal situação possibilita questionamentos sobre implantação desta tecnologia em áreas maiores e população-alvo[311].

O que se pretende apontar é que, mesmo que o percentual seja baixo, pode custar a privação da liberdade de inocentes. São inúmeros casos de prisões injustas de homens negros em virtude de erros de identificação (*misidentification*) dos sistemas de reconhecimento facial. Veja-se a seguir alguns.

Em 2019, o Departamento de Polícia de Woodbridge (Nova Jersey) prendeu Nijeer Parks por uma análise equivocada de reconhecimento facial. Houve a comparação da carteira de motorista falsa do suspeito foragido com um banco de dados de rostos que constava a face de Parks. O sistema entendeu incorretamente que havia uma combinação[312].

No mesmo ano, o Departamento de Polícia de Detroit acusou erroneamente dois homens de crimes que não cometeram[313]. O primeiro caso foi de Robert Williams, tendo ocorrido devido a uma correspondência incorreta de reconhecimento facial, quando da comparação de imagens de segurança com uma foto antiga da sua carteira de motorista que estava em um banco de dados[314]. Já Michael Oliver foi acusado de um crime pelo sistema de reconhecimento facial da Polícia de Detroit[315]. Depois de uma análise e revisão humana das fotos do suspeito e de Oliver, a justiça entendeu que este foi identificado erroneamente e o caso foi arquivado[316].

---

[311] BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020, p.15-16.

[312] CNN. EUA: Polícia prende inocente a partir de sistema de reconhecimento facial. Disponível em: https://www.cnnbrasil.com.br/internacional/sistema-de-reconhecimento-facial-enviou-este-homem-inocente-para-a-prisao/. Acesso em: 05 fev. 2022

[313] Informações mais detalhadas sobre os casos podem ser conferidas em: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MICHIGAN SOUTHERN DIVISION. Dsiponível em: https://www.aclumich.org/profiles/aclu_affiliates/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclumich.org%2Fsites%2Fdefault%2Ffiles%2Ffield_documents%2F001_complaint_1.pdf#page=1&zoom=auto,-12,798. Acesso em 05 fev. 2022.

[314] THE VERGE. Detroit man sues Police for wrongfully arresting him based on facial recognition. Disponível em: https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest. Acesso em: 05 fev. 2022

[315] O software é utilizado em Detroit como ferramenta de investigação desde 2017.

[316] DETROIT FREE PRESS. Controversial Detroit facial recognition got him arrested for a crime He didn't commit. Disponível em:

Todos os casos são de homens negros.

Desde 2019, várias cidades americanas baniram a utilização do reconhecimento facial para uso policial[317], como São Franscisco[318] (primeira cidade a banir), Oakland[319], New Orleans[320], Boston[321], Virginia[322] e Portland[323].

Em 2021, a Uber[324] também entrou na mira. Dois sindicatos[325] tomaram medidas judiciais contra a empresa por suposta discriminação na verificação facial do aplicativo em pessoas de pele mais escura, o que pode acarretar o bloqueio ou encerramento da conta. O objetivo da verificação facial é aumentar a segurança do passageiro, impedindo que motoristas compartilhem contas, haja vista uma verificação de antecedentes criminais para obtenção da licença para dirigir no aplicativo. Antes de iniciar o turno de trabalho, a empresa solicita uma *selfie*[326] em tempo real do motorista, momento me que o sistema realiza a correspondência com a foto da conta registrada[327]. É possível a escolha se a verificação é realizada pela Microsoft ou por humano. No caso de não correspondência automática, há revisão humana. Se também não houver

---

https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/. Acesso em: 05 fev. 2022.

[317] É possível encontrar as cidades americanas onde foi banido o reconhecimento facial no mapa interativo: FIGHT FOR THE FUTURE. Ban Facial Recognition. Disponível em: https://www.banfacialrecognition.com/map/ Acesso em: 05 fev. 2022

[318] THE NEW YORK TIMES. San Fransciso Bans Facial Recognition Technology. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 05 fev. 2022

[319] CNET. Facial recognition banned in another city. Oakland, California, hás followed San Francisco as the second Bay Area city to vote down the use os the technology. Disponível em: https://www.cnet.com/tech/mobile/facial-recognition-banned-in-another-city/. Acesso em: 05 fev. 2022

[320] THE LENS. New Orleans Ciry Council bans facial recognition, predictive policing and other surveillance tech. Disponível em: https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech/. Acesso em: 05 fev. 2022

[321] BOSTON GLOBE MEDIA PARTNERS. Boston City Council unanimously passes ban on facial recognition technology. Disponível em: https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban/. Acesso em: 05 fev. 2022

[322]GOVERNMENT TECHNOLOGY. Virginia Bill to put de facto ban on facial recognition tech. Disponível em: https://www.govtech.com/policy/virginia-bill-to-put-de-facto-ban-on-facial-recognition-tech.html. Acesso em: 05 fev. 2022.

[323] GOVERNMENT TECHNOLOGY. Portland, Maine, councilors ban facial recognition tech. Disponível em: https://www.govtech.com/public-safety/portland-maine-councilors-ban-facial-recognition-tech.html. Acesso em: 05 fev. 2022.

[324] Empresa de aplicativo de transporte privado urbano

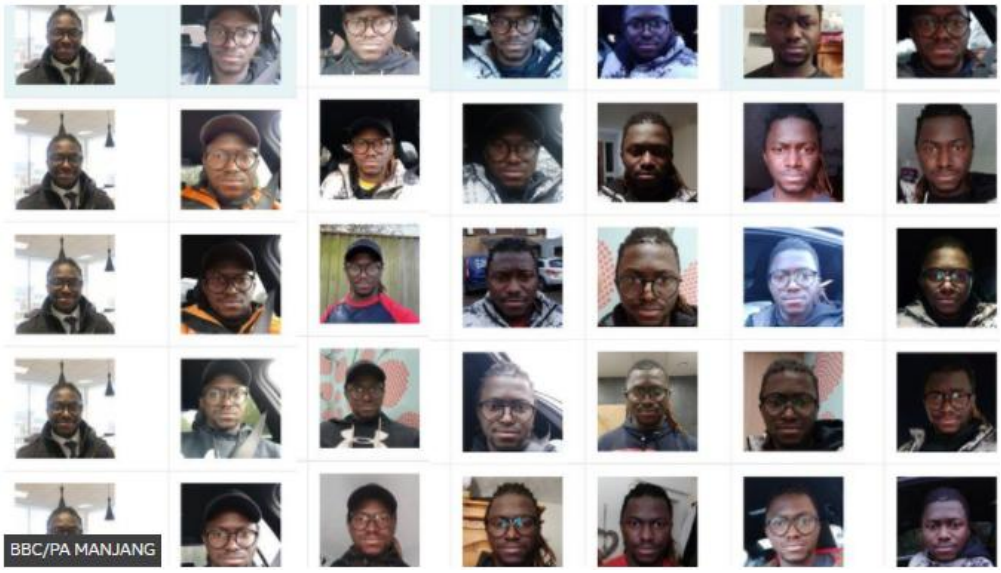
[325] Sindicato de Motoristas de Aplicativos e Correios (*App Drivers & Couriers Union* – ADCU) e Sindicato dos Trabalhadores Independentes da Grã-Bretanha (Independent Workers' Union of reat Britain – IWGB)

[326]Termo inglês comumente usado. Significa fotografia da face, retirada pelo próprio sujeito normalmente pelo seu dispositivo telefônico.

[327] Para entender melhor o funcionamento, ver: UBER. Engineering Safety with Uber's real-Time ID Check. Disponível em: https://eng.uber.com/real-time-id-check/. Acesso em: 05 fev. 2022; UBER. Por que preciso tirar uma foto minha?. Disponível em: https://help.uber.com/driving-and-delivering/article/por-que-preciso-tirar-uma-foto-minha--?nodeId=7fa8a60d-cf6f-49ac-9a50-b4bf6a3978ef. Acesso em: 05 fev. 2022

correspondência analisada por um humano, o motorista ficará 24h em uma "lista de espera" (com a conta bloqueada. Após este prazo, será requisitada nova verificação. Em caso de negativa de correspondência, a conta será desativada. O Secretário-Geral do Sindicato de Motoristas de Aplicativos e Correios (*App Drivers & Couriers Union* – ADCU) referiu a existência de falhas inaceitáveis, que ocorrem principalmente contra a força de trabalho de pessoas de cor[328].

FIGURA 20- SELFIES DO MOTORISTA PA EDRISSA MANJANG, QUE FORAM CONSIDERADAS "INCOMPREENSÍVEIS" (*MINDBOGGLING*) PELO UBER EATS. O SUJEITO ESTÁ COM MEDIDAS JUDICIAIS CONTRA A EMPRESA.



Fonte: BBC. Legal action over alleged Uber facial verification bias. Disponível em: https://www.bbc.com/news/technology-58831373 Acesso em 05 fev. 2022.

Esta situação remete a outro desafio relacionado à acurácia: como fazer com que os indivíduos tenham *confiança* no sistema sabendo que há possibilidade de erros.

[328] BBC. Legal action over alleged Uber facial verification bias. Disponível em: https://www.bbc.com/news/technology-58831373 Acesso em 05 fev. 2022.

Os casos mencionados refletiram situações em que houve problemas no sistema, gerando identificações errôneas ou, até mesmo, não identificando o sujeito. Entretanto, outra questão deve ser pontuada. Questiona-se: e se o sistema identificar corretamente, com alto índice de acurácia, *poderá*, mesmo assim, ser utilizado? Aqui são inseridas questões éticas e legais. Dependerá não só do ambiente em que será implementada a tecnologia, bem como do consentimento e aceitação dos indivíduos.

. Como refere Rodotá: " Os escopos de identificação, vigilância, segurança das transações, podem realmente justificar qualquer utilização do corpo humano que se torne possível pela inovação tecnológica?"[329].

Merece destaque a fala de Rodotá: "Se o corpo, explorado intimamente em sua estrutura genética, nos abre inquietantes perspectivas, novas preocupações nascem da difusão das técnicas de localização de pessoas". Este tema da "localização e da possibilidade de mapear cada movimento das pessoas aponta assim para uma dimensão na qual a proteção dos dados pode se cruzar com outros direitos fundamentais,invioláveis e indisponíveis". O que se pontua é que, mesmo que o sujeito tenha consentido, poderá não ser legítima a sua localização através do telefone e recurso de produto que possa controlar o seu comportamento, por exemplo[330]. Para tanto, Rodotá defende o *direito de não ser localizado* quando da "utilização lesiva à dignidade ou que interfira flagrantemente na esfera privada alheia", sendo mantidas as regras sobre o consentimento"[331].

Em 2021, nove escolas em *North Ayrshire* (Reino Unido) começaram a utilizar a tecnologia de reconhecimento facial na fila do pagamento do almoço da cantina escolar, alegando tornar mais célere e eficiente o processo de reconhecimento dos educandos. Um porta –voz do Conselho de North Ayrshire relatou que um dos objetivos também seria diminuir o contato para identificação (*contactless identification*), em virtude do Covid-19. A empresa que instalou a tecnologia, *CRB Cunninghams Education Solutions*, referiu que os pais tiveram que dar consentimento explícito. Já o Conselho de

[329] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 248
[330] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 252-253
[331] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 253

North Ayrshire referiu que 97% das crianças **ou** dos pais deram consentimento para o novo sistema[332].

Dias após o anúncio da introdução da tecnologia e depois de inúmeras preocupações sobre privacidade ao adotar tecnologia intrusiva em menores, e questionamentos de organizações, como a autoridade britânica de proteção de dados independente – *Information Commissioner Office* (ICO); o Conselho de *North Ayrshire* decidiu pausar temporariamente o seu uso e continuar usando o sistema anterior (número de identificação PIN) enquanto analisa os questionamentos e apontamentos[333].

Este caso – apenas pincelado um exemplo de utilização em escolas; traz à luz reflexões sobre alguns princípios aplicáveis ao caso: como os princípios da necessidade, finalidade, pertinência, proporcionalidade e dignidade. Em relação ao princípio da necessidade: "a difusão do recurso à biometria para além de situações de estrita necessidade ameaça tolher progressivamente aos cidadãos a sensibilidade necessária para dar-se conta dos riscos à sua liberdade pessoal [...] perda do controle exclusivo sobre o próprio corpo"[334].

Em decorrência das crescentes discussões sobre a temática da ética utilização do reconhecimento facial, muitas empresas passaram a anunciar que não vão mais utilizar sistemas de reconhecimento facial. É o caso do Facebook. No final de 2021, a empresa referiu que não irá mais usar um software de reconhecimento facial para identificar rostos em imagens e vídeos[335].

A Meta[336] anunciou que será excluído o modelo usado para a identificação dos usuários da rede social *Facebook*.A decisão impactará o sistema (*Automatic Alt Text-AAT*) que descreve imagens para pessoas com deficiência visual. Entretanto, a empresa mencionou que é necessário sopesar os benefícios e as preocupações da sociedade com o reconhecimento facial, e aguarda regras claras de reguladores. Enquanto isso, direciona o futuro da utilização desta tecnologia a empresa para formas mais restritas de

---

[332] THE GUARDIAN. ICO to step in after schools use facial recogntion speed up lunch queue. 2021. Disponível em: https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk. Acesso em 05 fev. 2022

[333] BBBC. Schools pause facial recognition lunch plans. Disponível em: https://www.bbc.com/news/technology-59037346. Acesso em: 05 fev. 2022.

[334] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 266-270

[335]BBC. Facebook to end use of facial recognition software. Disponível em: https://www.bbc.com/news/business-59143323. Acesso em: 05 fev. 2022

[336] Novo nome dado à empresa controladora de tecnologias, como Facebook, Instagram e WhatsApp. Ver mais sobre em: https://about.facebook.com/.

autenticação pessoal - como nos próprios dispositivos de um indivíduo; pois entende que permite maior privacidade, controle e transparência[337].

Ainda, pontua-se uma pesquisa realizada pelo *Ada Lovelace Institute*[338], buscou questionar pessoas sobre o uso da tecnologia de reconhecimento facial no Reino Unido[339]. Dentre os resultados:

- 90% dos entrevistados tinham ciência da utilização da tecnologia, mas apenas 53% souberam falar sobre, o que se depreendeu que a maioria das pessoas não tinha condições de desenvolver uma opinião formada sobre – a consciência é alta, mas o conhecimento é baixo;
- 46% entende que deveria ter a oportunidade de consentir ou recusar o uso da tecnologia (dentre os grupos minoritários que responderam a pesquisa – mais sujeitos à discriminação; composto por negros, asiáticos e minorias étnicas, foi 56% em relação aos outros);
- 70% entende que a tecnologia deve ser permitida pela polícia em investigações criminais, 54% concorda com o uso desbloqueio de celulares (locking sostems), e 50% em aeroportos para substituir o uso de passaportes.
- 67% dos entrevistados não se sentem confortáveis com a ideia de utilização do reconhecimento facial em escolas e 61% em relação ao transporte público, sob pena de normalizar a vigilância (64% e 61% respectivamente)[340].
- Em relação ao setor privado, cerca de 77% não se sente confortável com o uso da tecnologia por lojas para rastreamento de clientes ou recrutamento de candidatos para vagas – o motivo é a falta de confiança de que as empresas utilizem a tecnologia de forma ética

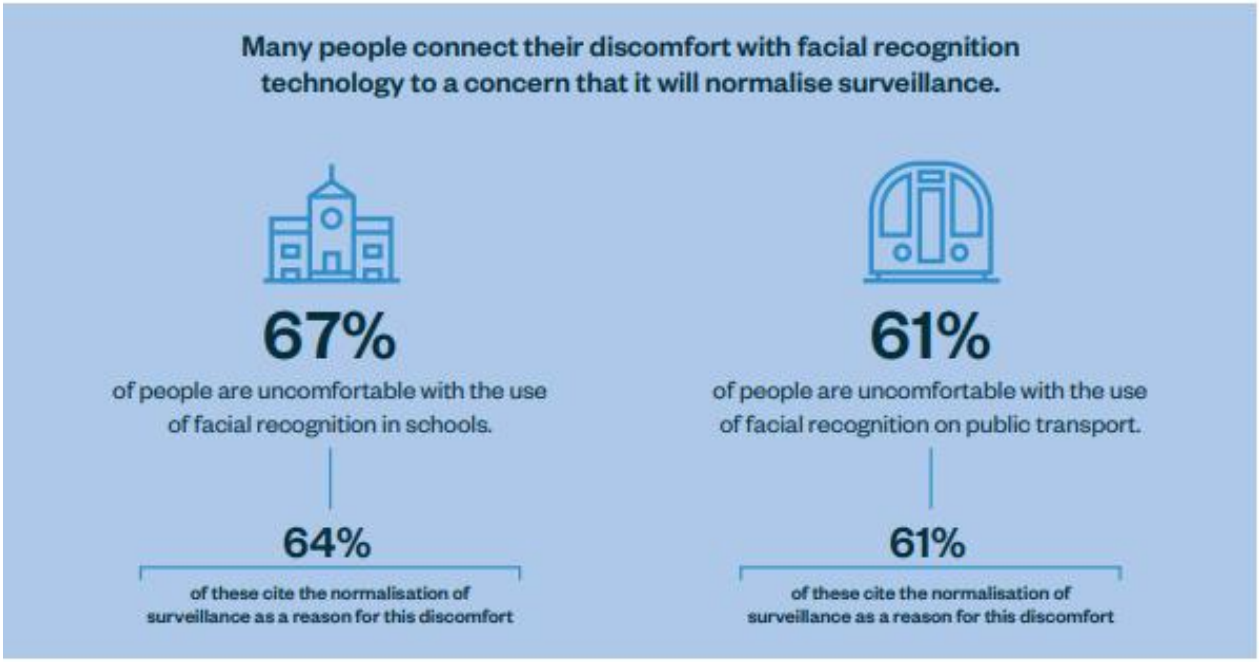
[337] META. Na update on our use of face recognition. 2021. Disponível em: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ . Acesso em: 05 fev. 2022

[338] ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ . Acesso em 03 mar. 2022

[339] O Instituto Ada Lovelace encomendou a pesquisa da YouGov, sendo a primeira pesquisa deste tipo para entender a opinião do público britânico sobre a utilização do reconhecimento facial no setor privado. Foram entrevistados 4.109 adultos em todo o Reino Unido. ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019, p. 2

[340] ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ . Acesso em 03 mar. 2022, p. 9

FIGURA 21 – DESCONFORTO NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL SOB PENA DE NORMALIZAR A VIGILÂNCIA



Fonte: ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ . Acesso em 03 mar. 2022, p. 9

Assim, denota-se que os indivíduos ainda não estão receptivos e seguros suficientemente com a utilização do reconhecimento facial. Entretanto, em que pese a privacidade e a segurança possam entrar em conflito, há formas de conciliá-las. Exemplifica-se: supervisionando programas de segurança, garantindo com que esses funcionem de forma equilibrada e controlada[341]. Portanto, há a necessidade de avaliações rigorosas nas medidas de segurança, gerando além de melhor proteção da privacidade, também segurança ponderada e eficaz[342].

[341] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 207
[342] SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 209

Como refere Lyon, quando se traz à discussão a palavra *vigilância*, é alta a chance de o assunto se tornar *privacidade*[343]. E, se o assunto então for *vigilância eletrônica*, dirão que há uma *invasão na sua privacidade*[344]. Para isso, é preciso que se analise:

> Quais são os problemas que certas medidas de segurança causam à privacidade e às liberdades civis? Como esses problemas podem ser amenizados? Que tipo de supervisão devemos ter sobre a medida de segurança? Podemos proteger a privacidade de maneira que não reduza substancialmente a eficácia da medida de segurança?[345]

Entretanto, há que se destacar duas situações dentro da esfera das tecnologias e privacidade. De uma forma positiva, a privacidade é protegida quando o sistema biométrico previne que sujeito sem autorização ingresse em local físico ou lógico, saque dinheiro em caixa eletrônico de outrem, por exemplo. Por outro lado, determinadas aplicações biométricas – como o reconhecimento facial; podem ser obtidas sem o conhecimento do sujeito. Assim "aqueles que desejam permanecer anônimos em qualquer situação particular podem ser negados de sua privacidade pelo reconhecimento biométrico"[346].

Por ora, o que se pontua é que a utilização de dados biométricos "exige uma abordagem tecnicamente prudente, se os entusiasmos e as certezas definitivas que com frequência são proclamadas, sobretudo por aqueles que têm interesse em colocar no mercado estas tecnologias"[347].

---

[343] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 170

[344] LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994, p. 180

[345] Tradução livre do autor. Original: "What are the problems certain security measures cause for privacy and civil liberties? How can these problems be ameliorated? What kind of oversight should we have over the security measure? How effective will the security measure be? Can we protect privacy in ways that won't substantially reduce the effectiveness of the security measure?". SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 207-208

[346] Tradução livre do autor. Original: "Consequently, those who desire to remain anonymous in any particular situation could be denied their privacy by biometric recognition." JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003, p. 42

[347] RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008, p. 266

2 RECONHECIMENTO FACIAL: DESAFIOS PRAGMÁTICOS NO DIREITO BRASILEIRO

> When figuring out whether to regulate something, I believe it is best to begin by looking at the problems and then crafting regulation to address them.SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011, p. 179-180

Para que seja possível o aprofundamento em matéria brasileira, é necessário antes expor o cenário normativo global sobre biometria e reconhecimento facial. Após, brevemente a evolução da proteção de dados pessoais no Brasil, advento da Lei Geral de Proteção de Dados brasileira (LGPD) e aprofundamento na temática do tratamento de dados pessoais sensíveis (art. 11, II, g), focado no reconhecimento facial.

2.1 Panorama internacional sobre biometria e reconhecimento facial

Diante da amplitude do quadro internacional, será dado recorte em âmbito americano e europeu, bem como será brevemente apresentada a matéria no contexto latino americano. O específico delineamento deu-se em virtude de serem dois cenários muito distintos, que possuem abordagens e desdobramentos sobre biometria e reconhecimento facial que merecem a devida atenção. Ainda, vale dizer que podem trazer lições "a serem aprendidas por legisladores e gestores públicos no Brasil"[348].

De igual sorte, em geral, as "regulações sobre o uso de sistemas de reconhecimento facial ainda se encontram em estágio experimental. Para serem eficientes, as futuras abordagens precisam considerar as rápidas mudanças nas tecnologias de monitoramento de dados biométricos [..]"[349].

[348] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy BR. 2020, p. 1. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

[349] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy BR. 2020, p. 1. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

Em contexto americano, inexiste uma lei geral, mas legislação fragmentada. Em se tratando de normativas para proteção à privacidade, destaca-se a Lei de Privacidade de Comunicação Eletrônica (ECPA[350]), de 1986, a Lei de Proteção da Privacidade de Crianças (COPPA)[351], de 2000, a Lei de Portabilidade e Transparência de Seguros de Saúde[352], de 1996, e a Lei de Privacidade e Proteção de Dados dos Consumidores da Califórnia[353], de 2021[354].

Quanto à biometria, a primeira lei a regular a coleta e tratamento de dados biométricos nos Estados Unidos[355] foi em 2008, em Illinois (*âmbito estadual*): *Biometric Information Privacy Act* (BIPA)[356], que garante com que os consumidores tenham o controle de seus dados biométricos, bem como proíbe *organizações privadas* de coletá-los sem que: informe quais dados estão sendo coletados ou armazenados; informe a finalidade específica e o tempo de armazenamento e retenção; obtenha o consentimento por escrito. Ainda, é proibida a venda ou que ocorra lucro com as informações biométricas dos indivíduos vulneráveis[357].

[350] Bane a interceptação de mensagens telefônicas ou eletrônicas, bem como garantir a segurança de informações. VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[351] Prevê regras para responsáveis por websites e serviços online objetivando proteger a privacidade de crianças e adolescentes (até 13 anos) no meio digital . VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[352] Traz obrigações como a notificação de órgãos públicos (secretarias de saúde), padrões de segurança para dados médicos, vedação para uso ou compartilhamento de dados sem consentimento, em regra. VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[353] Aplica-se para empresas que fazem negócios na Califórnia e objetiva garantir os direitos e proteger os dados de quem vive na Califórnia, com foco no consumidor.

[354] VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[355] BIONI, Bruno Ricardo. LUCIANO, Maria. Princípio da precaução como vetor de regulação de Inteligências Artificial: seriam as leis de proteção de dados pessoais o seu portal de entrada? In Inteligências Artificial (Organizadores Caitlin Sampaio et al). Rio de Janeiro, 2019, p. 207-231, p. 223.

[356] Ver: UNITED STATES. ILLINOIS GENERAL ASSEMBLY. (740 ILCS 14/) Biometric Information Privacy Act. Disponível em: 740 ILCS 14/ Biometric Information Privacy Act. (ilga.gov). Acesso em: 10 jun. 2022.

[357] . UNITED STATES. BIOMETRIC INFORMATION PRIVACY ACT (BIPA). ACLU. Disponível em: https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa. Acesso em: 10 jun. 2022.

Em 2020, o BIPA foi reformulado e introduzido em *âmbito nacional*: National Biometric Information Privacy Act of 2020 (NBIPA)[358]. No BIPA (2008), identificador biométrico (*biometric identifier*) estava previsto como: " escaneamento de Iris ou retina, impressão digital, impressão de voz, geometria da mão ou face (*face geometry).* Os identificadores biométricos não incluem amostras de escrita, assinaturas, fotografias [..]"[359]. Já na nova versão, foi atualizada a definição, passando a incluir como identificador biométrico (*biometric identifier*): " impressão facial (*faceprint*), incluindo qualquer impressão facial derivada de uma fotografia (*including any faceprint derived from a photograph*)"[360].

[358] UNITED STATES. NATIONAL BIOMETRIC INFORMATION PRIVACY ACT OF 2020. 2.4400. Disponível em: Text - S.4400 - 116th Congress (2019-2020): National Biometric Information Privacy Act of 2020 | Congress.gov | Library of Congress. Acesso em: 14 jun. 2022.

[359] Artigo completo: "Seg. 10. Definições. Nesta Lei: "Identificador biométrico" significa uma varredura de retina ou íris, impressão digital, impressão de voz ou varredura da geometria da mão ou do rosto. Os identificadores biométricos não incluem amostras de escrita, assinaturas escritas, fotografias, amostras biológicas humanas usadas para testes ou triagem científica válida, dados demográficos, descrições de tatuagens ou descrições físicas, como altura, peso, cor do cabelo ou cor dos olhos. Os identificadores biométricos não incluem órgãos, tecidos ou partes doados conforme definido no Illinois Anatomical Gift Act ou sangue ou soro armazenados em nome de receptores ou potenciais receptores de transplantes vivos ou cadavéricos e obtidos ou armazenados por uma agência de aquisição de órgãos designada pelo governo federal. Os identificadores biométricos não incluem materiais biológicos regulamentados pela Lei de Privacidade de Informações Genéticas. Os identificadores biométricos não incluem informações capturadas de um paciente em um ambiente de saúde ou informações coletadas, usadas ou armazenadas para tratamento de saúde, pagamento ou operações sob a Lei federal de Portabilidade e Responsabilidade de Seguros de Saúde de 1996. Os identificadores biométricos não incluem um Raio-X, processo roentgen, tomografia computadorizada, ressonância magnética, PET scan, mamografia ou outra imagem ou filme da anatomia humana usada para diagnosticar, prognosticar ou tratar uma doença ou outra condição médica ou para validar ainda mais testes ou triagem científica."Tradução livre pelo autor. BIOMETRIC INFORMATION PRIVACY ACT (BIPA). ACLU. Disponível em: https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa. Acesso em: 10 jun. 2022.

[360] Artigo completo: 1) IDENTIFICADOR BIOMÉTRICO.—O termo "identificador biométrico"(A) inclui (i) uma varredura de retina ou íris; (ii) uma impressão de voz; (iii) uma impressão facial (incluindo qualquer impressão facial derivada de uma fotografia); (iv) impressões digitais ou palmares; e (v) qualquer outra informação de identificação única com base nas características da marcha de um indivíduo ou outra característica imutável de um indivíduo; (B) não inclui amostras de escrita, assinaturas escritas, fotografias, amostras biológicas humanas usadas para testes ou triagem científica válida, dados demográficos, descrições de tatuagens ou descrições físicas, como altura, peso, cor do cabelo ou cor dos olhos; (C) não inclui órgãos, tecidos ou partes doados ou sangue ou soro armazenados em nome de receptores ou potenciais receptores de transplantes vivos ou cadavéricos e obtidos ou armazenados por uma agência de aquisição de órgãos designada pelo governo federal; (D) não inclui informações capturadas de um paciente em um ambiente de saúde para fins médicos ou informações coletadas, usadas ou armazenadas para tratamento de saúde, pagamento ou operações sob a Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (Lei Pública 104-191); e (E) não inclui um raio-x, processo de roentgen, tomografia computadorizada, ressonância magnética, PET scan, mamografia ou outra imagem ou filme da anatomia humana usada para diagnosticar, prognosticar ou tratar uma doença ou outra condição médica ou para validar ainda mais testes científicos ou triagem. (2) INFORMAÇÕES CONFIDENCIAIS E SENSÍVEIS.—O termo "informações confidenciais e sensíveis"— (A) significa informações pessoais que podem ser usadas para identificar exclusivamente um indivíduo ou a conta ou propriedade de um indivíduo; e (B) inclui marcadores genéticos, informações de testes genéticos, números identificadores exclusivos para localizar contas ou propriedades, números de contas, números de identificação pessoal, códigos de acesso, números de carteira de motorista ou números de Previdência Social.". Tradução livre pelo autor. UNITED STATES. NATIONAL BIOMETRIC INFORMATION

Outras legislações americanas também merecem relevo: *Texas Business and Commerce Code §503.001, Capture or use of biometric identifier* (Texas, USA)[361] – Texas é o segundo estado americano após Illinois a ter uma lei de privacidade biométrica. No mesmo sentido do BIPA, identificador biométrico (*biometric identifier*) está definido como "escaneamento de Iris ou retina, impressão digital, impressão de voz, geometria da mão ou face (*face geometry*[362]*)"*[363].

Washington é o terceiro estado americano a ter uma legislação de privacidade biométrica: HB 1493 Whashington EUA (2017)[364] – estabelece requisitos para empresa coletarem e usarem identificadores biométricos para fins comerciais[365]. Curiosamente, inexiste previsão expressa sobre o reconhecimento facial quando da definição de identificador biométrico (*biometric identifier*): "dados gerados por medições automáticas das características biológicas de um indivíduo, como impressão digital, impressão de voz, retinas ou íris dos olhos ou *outras características biológicas únicas*, que são usadas pela pessoa ou licenciado para autenticar exclusivamente a identidade de um indivíduo quando o indivíduo acessa um sistema ou conta"[366]. Em que pese poderia se entender que o reconhecimento da face estaria incluso na "outras características biológicas únicas", estranha-se o fato de a legislação ter suprimido o reconhecimento da face (já estava previsto em legislação anteiror).

PRIVACY ACT OF 2020. 2.4400. Disponível em: Text - S.4400 - 116th Congress (2019-2020): National Biometric Information Privacy Act of 2020 | Congress.gov | Library of Congress. Acesso em: 14 jun. 2022.

[361] UNITED STATES. TEXAS. Texas Business and Commerce Code §503.001, Capture or use of biometric identifier. Disponível em: https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001. Acesso em: 15 jun. 2022.

[362] Traduzido pelo autor. Original: "(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.". UNITED STATES. TEXAS. Texas Business and Commerce Code §503.001, Capture or use of biometric identifier. Disponível em: https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001. Acesso em: 15 jun. 2022.

[363] UNITED STATES. TEXAS. Texas Business and Commerce Code §503.001, Capture or use of biometric identifier. Disponível em: https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001. Acesso em: 15 jun. 2022

[364] UNITED STATES. STATE OF WASHINGTON. HOUSE BILL 1493. Disponível em: https://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Bills/1493.pdf#page=1. Acesso em: 10 jun. 2022

[365] WASHINGTON BECOMES THIRD STATE TO ENACT BIOMETRIC PRIVACY LAW. Privacy & Information Securtity Law blog. Disponível em: https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/. Acesso em: 10 jun. 2022.

[366] Tradução livre do autor. Original: "(1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas or irises, or other unique biological characteristic, which are used by the person or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account." UNITED STATES. STATE OF WASHINGTON. HOUSE BILL 1493. Disponível em: https://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Bills/1493.pdf#page=1. Acesso em: 10 jun. 2022

Em relação ao reconhecimento facial, inexiste uma legislação federal americana que regule o tema[367]. Mas, a US Federal Trade Comission (US FTC) [368] emitiu algumas diretrizes referindo que as empresas não podem enganar os seus consumidores sobre como elas usam os algoritmos de reconhecimento facial (transparência)[369]. Salienta-se que, em 2012, a US FTC já havia publicado um estudo sobre boas práticas na utilização da tecnologia te reconhecimento facial[370].

Ainda, a utilização de sistema de reconhecimento facial nos EUA não segue uma abordagem única, mas há várias iniciativas legislativas municipais e estaduais que vem adotando uma postura pelo banimento da tecnologia[371]: a justificativa é a proteção de direitos e garantias individuais.[372]

Diferentemente, na Europa a matéria é mais centralizada. Ressalta-se a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção do processamento e circulação de dados pessoais e à livre circulação desses dados[373], que foi revogada pelo Regulamento Geral de Proteção de Dados (EU – 2016/679). Com o RGPD,a proteção de dados ficou unificada para os indivíduos na União Europeia (EU).

Em relação aos dados biométricos, o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) assim os define:

---

[367] MADIEGA, Tambiama; MILDEBRATH, Hendrik. EUROPEAN PARLIAMENT. Regulating facial recognition in the EU. 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Acesso em: 10 jun. 2022. P. 32

[368] Comissão Federal de Comércio dos EUA, cujo objetivo é a proteção do consumidor americano.

[369] JILLSON, Elisa. Aiming for truth, fairness, and equity in your company'suse of AI. Federal rade Commission. FTC. 2021. Disponível em: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Acesso em: 10 jun. 2022.

[370] FEDERAL TRADE COMMISSION. Best Practices for Common Uses of Facial Recognition Technologies. 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf. Acesso em: 10 jun. 2022.

[371] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy BR. 2020, p. 9. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

[372] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy BR. 2020, p. 17. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

[373] PARLAMENTO EUROPEU. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 10 jun. 2022.

> 14) «Dados biométricos», dados pessoais **resultantes de um tratamento técnico específico** relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que **permitam ou confirmem a identificação única dessa pessoa singular**, nomeadamente **imagens faciais** ou **dados dactiloscópicos** (grifo nosso).[374]

Denota-se que o RGPD pontua a necessidade de haver um *tratamento técnico específico* que permita ou confirme a identidade[375]. Exemplifica-se com um sistema eletrônico de impressão digital em entrada de academias: os usuários, para terem acesso ao ambiente precisam de alguma condição de validade que permita o seu ingresso: são membros? Estão com a mensalidade em dia? Existe alguma restrição de acesso para aquele sujeito?[376].

Em relação à definição trazida pelo Article 4 (14), a ICO menciona que a imagem da face (*face imaging*) e a impressão digital são categorias não exaustivas[377], podendo incluir outras, como o reconhecimento facial, escaneamento da Iris e reconhecimento de voz.

Conforme o Art. 9º do regulamento, os dados biométricos estão dentro de uma categoria especial de dados pessoais (*special categories of personal data). A priori*, o tratamento deste tipo de dado é proibido, *exceto se a hipótese se enquadrar nos casos descritos taxativamente na legislação,* como através do consentimento explícito do titular, ou necessário à proteção dos interesses vitais do titular[378].

---

[374] Art. 4º. Definições. 4). REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Acesso em: 10 mai. 2022.

[375] Até o presente momento, não há uma definição clara na doutrina sobre se o processamento de fotogafias digitais serem consideradas dados biométricos automaticamente e, por consequência, dados pessoais sensíveis. Para a ICO, em que pese a imagem digital permita identificar um indivíduo, somente será dado biométrico se for realizado um "processamento técnico específico", utilizando por base correspondência ou identificação de imagem automatizada (automated imagem matching and identification). ICO - Information Comissioner's Office. What is special category data?. Disponível em: What is special category data? | ICO. Acesso em: 10 mai 2022. Online.

[376] ICO - Information Comissioner's Office. What is special category data?. Disponível em: What is special category data? | ICO. Acesso em: 10 mai 2022. Online.

[377] A autoridade britânica esclarece que dados dactiloscópicos (dactyloscopic data) significam dados da impressão digital (fingerprint data). ICO - Information Comissioner's Office. What is special category data?. Disponível em: What is special category data? | ICO. Acesso em: 10 mai 2022. Online.

[378] Vide: Artigo 9.o Tratamento de categorias especiais de dados pessoais 1. **É proibido o tratamento de dados pessoais** que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filo sóficas, ou a filiação sindical, bem como o tratamento de dados gené ticos, **dados biométricos** para identificar uma pessoa de forma inequí voca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. **2. O disposto no n.o 1 não se aplica se se verificar um dos seguintes caso:** a) Se o titular dos dados tiver dado o seu **consentimento explícito** para o tratamento desses dados pessoais para uma ou mais finalidades espe cíficas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.o 1 não pode ser anulada pelo titular dos dados; **b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos**

Para tanto, no RGPD são utilizadas as nomenclaturas *special categories of personal data* ("*sensitive data"):* tipos de dados que merecem proteção específica no processamento de dados, haja vista que possuem significantes riscos em relação a direitos e a liberdades fundamentais[379]. O rol é amplo. Exemplifica-se: liberdades de pensamento, expressão, religião, discriminatória; direito à integridade corporal, direito ao respeito à vida privada e familiar[380].

Cumpre referir a liberdade concedida aos Estados-Membros na fixação de regras para tratamento de dados biométricos:

---

específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados; c) Se o tratamento for necessário **para proteger os interesses vitais do titular dos dados ou de outra pessoa singular,** no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento; d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, **por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais**, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares; e) Se o tratamento se referir a **dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;** f) Se o tratamento for necessário à **declaração, ao exercício ou à defesa de um direito num processo judicial** ou sempre que os tribunais atuem no exercício da suas função jurisdicional; g) Se o tratamento for necessário por motivos de **interesse público importante**, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados; h) Se o tratamento for necessário para efeitos de **medicina preventiva ou do trabalho,** para a avaliação da capacidade de trabalho do em pregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.o 3; i) Se o tratamento for necessário por motivos de **interesse público no domínio da saúde pública,** tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional; j**) Se o tratamento for necessário para fins de arquivo de interesse público,** para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o , n.o 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados. (grifo nosso).REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Acesso em: 10 mai. 2022. Nesse sentido, ver também o Recital (51) e (52). GDPR

[379] Vide Recital (10). GDPR. Não estão inclusos na categoria especial de dados aqueles relacionados à condenações criminais penais e infrações (vide art. 10º), posto que o regulamento possui regras separadas para o tratamento destes.

[380] ICO - Information Comissioner's Office. What is special category data?. Disponível em: What is special category data? | ICO. Acesso em: 10 mai 2022. Online.

> 4. Os Estados-Membros **podem manter ou impor novas condições, incluindo limitações**, no que respeita ao tratamento de dados genéticos, **dados biométricos** ou dados relativos à saúde: (grifo nosso)[381].

Em janeiro de 2021, foi publicado o documento intitulado "Diretrizes do Conselho da Europa para o reconhecimento facial no âmbito da convenção para a proteção de pessoas quanto ao processamento automático de dados pessoais (Convenção 108)"[382] . A publicação visa os setores público e privado, bem como

> fornece um conjunto de medidas de referência para governos, desenvolvedores, fabricantes, prestadores de serviços e demais entidades que usam ferramentas de reconhecimento facial, com o intuito de garantir que a referida tecnologia não afete adversamente a dignidade humana, os direitos humanos e as liberdades fundamentais das pessoas[383]

Merece relevo que o documento fala sobre a utilização do reconhecimento facial em relação ao setor público e privado. Destaca-se:

(i)setor público: em regra, o consentimento não deve ser utilizado como fundamento jurídico para a utilização do reconhecimento facial por autoridades públicas – o uso da tecnologia já deve estar previsto em lei ou a sua utilização pensada com propósitos legítimos;

(ii) setor privado[384]: há a exigência do consentimento (explícito,específico, livre e informado) dos titulares e, considerando a indispensabilidade deste, a utilização do reconhecimento facial somente poderá ocorrer em ambientes controlados (*controlled environments*), independentemente se for para autenticação ou verificação. De forma a garantir que a obtenção do consentimento foi dada livremente, é direito do titular

[381] Artigo 9. 4. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Acesso em: 10 mai. 2022.

[382] COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022.

[383] GUEDES, Paula. 7 Recomendações para a regulação do Reconhecimento Facial. Instituto de Tecnologia e Sociedade do RIO – ITS RIO. Disponível em: https://itsrio.org/pt/artigos/7-recomendacoes-para-a-regulacao-do-reconhecimento-facial/. Acesso em: 03 jun. 2022.

[384] Exceto entidades privadas autorizadas a exerxer tarefas semelhantes às das autoridades públicas. COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022, p. 7.

escolher soluções alternativas ao reconhecimento facial, como utilizar uma senha ou crachá de identificação. Em relação ao ambiente, o documento refere que o setor privado não deverá utilizar o reconhecimento facial em ambientes descontrolados (*uncontrolled environments*), como shoppings, em que há um interesse por trás – como traçar um perfil do consumidor para fins de marketing[385].

Em abril de 2021, foi publicada a Proposta de Regulamento de Inteligência Artificial da União Europeia[386], cujo objetivo é "regular a Inteligência Artificial na União Europeia, a partir de uma abordagem baseada no risco". Uma das principais preocupações elencadas são os sistemas de identificação biométrica à distância, o que inclui o reconhecimento facial. Isso porque, a depender do grau de risco, esta tecnologia poderia ser classificada como "risco inaceitável/elevado", ou seja, proibida, ou sujeita a obrigações, como a realização de relatórios de impacto[387].

O Comitê Europeu de Proteção de Dados (EDPB) e a Autoridade Europeia para a Proteção de Dados (EDPS), da União Europeia, apresentaram um parecer sobre a Proposta de Regulamento supramencionada, opinando pela proibição geral da utilização de qualquer inteligência artificial para reconhecimento automatizado de indivíduos de forma remota em espaços públicos, como o reconhecimento de rostos[388]. Para tanto, quando da análise da Proposta de Regulamento, Dora Kaufman refere que "apesar da expressa intenção de estimular o desenvolvimento e a implementação da IA na Europa, a rigidez das regras e o custo associado para atendê-las apontam na direção oposta".[389]

Merece relevo que a Autoridade Europeia para a Proteção de Dados (EDPS) acima referida, em 2010 já havia publicado o documento "The EDPS Video-

---

[385] COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022, p. 7.

[386] EUROPEAN COMMISSION. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. Brussels, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206. Acesso em: 10 jun. 2022.

[387] GUEDES, Paula. 7 Recomendações para a regulação do Reconhecimento Facial. Instituto de Tecnologia e Sociedade do RIO – ITS RIO. Disponível em: https://itsrio.org/pt/artigos/7-recomendacoes-para-a-regulacao-do-reconhecimento-facial/. Acesso em: 03 jun. 2022.

[388] EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses os AI that can lead to unfair discrimination. European Data Protection Supervisor – EDPS. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en. Acesso em: 20 jun. 2022.

[389] KAUFMAN, Dora. Proposta Europeia de Regulamentação da IA: impressões preliminares. EPOCA NEGÓCIOS. 2021. Disponível em: https://epocanegocios.globo.com/colunas/IAgora/noticia/2021/04/proposta-europeia-de-regulamentacao-da-ia-impressoes-preliminares.html. Acesso em: 15 jun. 2022.

Surveillance Guidelines"[390], cujo objetivo era conceder recomendações para instituições e órgãos europeus em como desenvolver e operar o seus sistemas de câmeras (*video-surveillance*).

Por fim, salienta-se a atuação de algumas das autoridades europeias de proteção de dados que vem desenvolvendo trabalhos de relevo e publicando material orientativo sobre a matéria, como a Information Comissioner's *Office* – ICO[391] (autoridade britânica) e a Agencia Espanõla de Proteccion de Datos[392] – AEPD (autoridade espanhola).

Em relação à América Latina, vários países já possuem legislações de proteção de dados, como o Chile, Argentina, Uruguai e Colômbia[393]. Merece destaque o Chile, primeiro país LATAM a aprovar uma Lei de Proteção de Dados, em 1999: Lei nº19.628. Por exemplo, a lei chilena, de 1999, foi a primeira a traçar limites para o uso de dados e garante direitos aos titulares, como o direito de acesso, correção e eliminação, por exemplo. Na Argentina, a Ley de Protección de lós Datos Personales, de 2000, regula bases de dados públicas e privadas.[394] Desde 2016, foram criados outros projetos de lei para reformar e atualizar a lei vigente[395] e, desde 2019, Buenos Aires conta com um sistema de reconhecimento facial[396] para identificar pessoas foragidas – nos três primeiros meses após a instalação do sistema, pelo menos 170 pessoas foram presas com o auxílio da tecnologia. Mas, no mesmo período, um homem passou seis

[390] THE EDPS VIDEO-SURVEILLANCE GUIDELINES. European Data Protection Supervisor. EDPS.Brussels: 2010. Disponível em: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf. Acesso em: 20 jun. 2022.

[391] ICO. The use of live facial tecognition technology in public places. Information Commissioners Opinion. 2021. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 20 jun. 2022.

[392] AEPD. Guía sobre El uso de videocâmaras para seguridad y otras finalidades. Agencia Espanõla de Protección de Datos. 2021. Disponível em: https://www.aepd.es/sites/default/files/2019-12/guia-videovigilancia.pdf. Acesso em: 20 jun. 2022.

[393] VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[394] VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

[395] Ver sobre em: ARGENTINA.GOB.AR. Proyecto de Ley de Protección de Datos Personales. Disponível em: https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales. Acesso em: 04 jun. 2022.

[396] Ver mais sobre o tema do reconhecimento facial na Argentina: ConMiCaraNo. El reconocimiento facial se expande em Argentina. ADC. Disponível em: https://conmicarano.adc.org.ar/. Acesso em: 15 jun. 2022.

dias preso por ter sido erroneamente identificado (as autoridades negaram que o erro tenha sido devido à utilização desta tecnologia)[397].

Ademais, um ponto que merece ser questionado e que abrange o âmbito internacional é se fotografias podem ser consideradas identificadores biométricos (*biometric identifier*), como previsto no BIPA, ou dado pessoal sensível (*special type of data),* como no RGPD[398].

Em relação ao BIPA, a normativa prevê "identificadores biométricos" e "informações biométricas", sendo que o estatuto afirma claramente que as fotografias (*photographs*) não podem ser um "identificador biométrico", bem como exclui informações ("informação biométrica") que possam ser derivadas de "identificador biométrico". Para tanto, no caso de uma foto não puder ser considerada como um "identificador biométrico", qualquer informação retirada dela também, na teoria, não poderia ser considerada "informação biométrica". Entretanto, na prática, os tribunais decidiram o contrário: embora tenham reconhecido que as informações obtidas por fotografia não podem ser consideradas como "informações biométricas" – por exclusão expressa do BIPA; questionaram se a informação em si pode ser um "identificador biométrico" .[399] A própria atualização do BIPA (NBIPA) vem em sentido dos tribunais. O entendimento ainda não está consolidado.

O RGPD, em seu considerando (51), dispõe que:

> [...] o **tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais**, uma vez que não são 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.[400] (grifo nosso).

[397] PAIVA, Letícia. Reconhecimento facial para segurança avança na América Latina mesmo sem normas claras. JOTA. Disponível em: https://www.jota.info/justica/reconhecimento-facial-seguranca-publica-03052021. Acesso em: 05 jun. 2022.

[398]Para mas aprofundamento na temática, ver: IAPP. Ask the privacy expert. Disponível em: https://iapp.org/news/a/ask-the-privacy-expert/#:~:text=When%20photographs%20disclose%20race%2C%20ethnic,consent%20requirement%20in%20any%20case.. Acesso em: 20 jun. 2022. A análise sobre o tema no âmbito nacional, será dada em tópico seguinte.

[399] GARAVAGLIA, Aaron. Data extracted from photographs: covered under BIPA? National Law Review, v. XI, n. 84. 2022. Disponível em: https://www.natlawreview.com/article/data-extracted-photographs-covered-under-bipa. Acesso em: 22 jun. 2022.

[400] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Acesso em: 10 mai. 2022.

Nessa direção, é o que refere a ICO: "embora uma imagem digital possa permitir a identificação por meio de características físicas, ela só se torna um dado biométrico se você realizar "*processamento técnico específico*"". Para que isso ocorra, "normalmente, isso envolve o uso dos dados da imagem para criar um modelo ou perfil digital individual, que, por sua vez, você usa para correspondência e identificação automatizadas de imagens"[401].

Entende-se que o tema ainda é recente e todas as hipóteses possíveis de discriminação ou afronta ao direito de imagem devem ser elencadas antes de optar por determinada posição.

2.2 Brasil: LGPD e as hipóteses de tratamento de dados pessoais sensíveis (art. 11)

Sob influência mais direta do RGPD, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) inaugura um regime geral de proteção de dados pessoais nacional, complementando e atualizando normas esparsas já existentes – Lei de Acesso à Informação (Lei n. 12.527/2011), Marco Civil da Internet, Código de Defesa do Consumidor[402], somando-se à proteção da privacidade e da imagem previstas na Constituição Federal e no Código Civil. Ainda, a LGPD vem com o objetivo de "proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor"[403].

A LGPD dispõe sobre "o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[404].

[401] ICO. What is special type of data? Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/. Acesso em: 15 jun. 2022.
[402] DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da Nova Lei Geral de Proteção de Dados brasileira. In: CAVALLI, Olga; BELLI, Luca. Governança e regulações da internet na América Latina:. p. 309 – 325, 2019. Disponível em: . Acesso em: 18 mai. 2022.P. 336
[403] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, v. 120. São Paulo: Ed. RT, nov.-dez. 2018, p. 469-483, p. 470.
[404] Vide art. 1º. BRASIL. LGPD.

Antes de adentrar no tema dos dados pessoais, é preciso aclarar a sua diferença do termo informação. Em que pese *dados* e *informação* sejam corriqueiramente confundidos, há diferenças que precisam ser pontuadas. Como refere Danilo Doneda:

> **O dado, assim, estaria associado a uma espécie de "pré-informação"**, anterior à interpretação e a um processo de elaboração. A **informação**, por sua vez, alude a algo além da representação contida no dado, chegando no limiar da cognição. Mesmo sem aludir ao seu significado, na informação, **já se pressupõe a depuração de seu conteúdo** – daí que a informação carrega em si também um sentido instrumental, no sentido da redução do estado de incerteza.[405]

Ademais, a Lei de Acesso à Informação (Lei nº12. 527/2011) dispõe, em seu art. 3º, IV, que "informação pessoa é aquela relacionada à pessoa natural identificada ou identificável". E, em seu art. 31, preconiza que "o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais"[406].

Ainda, no Glossário de Segurança da Informação (Portaria nº 93 de 26 de setembro de 2019)[407], define-se como informação "dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato". Já a informação pessoal, é aquela " informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;"[408]. É nesse sentido a lei de proteção de dados brasileira: "I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;[409]".

A LGPD indica quais são as hipóteses taxativas em que o tratamento de dados é legítimo. O conceito de tratamento é disposto no art. 5º, X, da referida normativa:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da

[405] DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.140

[406] BRASIL. LEI N. 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 jun. 2022.

[407] BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 07 jun. 2022.

[408] [408] BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021

[409] Vide art. 5º, I. BRASIL. LGPD.

> informação, modificação, comunicação, transferência, difusão ou extração;[410]

Faz-se uma ressalva. Quando o propósito do tratamento for realizado exclusivamente com determinados propósitos, como segurança nacional, defesa nacional, segurança do Estado; ou atividades de investigação e repressão de infrações penais; a LGPD não se aplica. Neste caso, a normativa prevê a necessidade de criação de legislação específica para abordar o tema, em que deverão ser previstas medidas proporcionais e estritamente necessárias ao atendimento do interesse público, princípios e direitos do titular[411].

Desde já, vale ressaltar a inexistência de hierarquia[412] entre as bases legais. No artigo. 7º encontram-se as hipóteses para tratamento de dados pessoais, quais sejam:

> I - mediante o fornecimento de **consentimento** pelo titular;
> II - para o **cumprimento de obrigação legal ou regulatória pelo controlador;**
> III - pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de **políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício **regular de direitos** em **processo judicial, administrativo ou arbitral**, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a **proteção da vida ou da incolumidade física do titular ou de terceiro;**
> VIII - para a **tutela da saúde**, em procedimento realizado por **profissionais da área da saúde ou por entidades sanitárias**;
> VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por **profissionais de saúde, serviços de saúde ou autoridade sanitária**; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos **interesses legítimos do controlador ou de terceiro,** exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.(grifo nosso)[413]

[410] BRASIL. LGPD.
[411] BRASIL. LGPD. Vide Art 4º, III, ; §1º.
[412] Em que pese a disposição horizontal iniciando pela base legal do consentimento optada pelo legislador.

A legislação apresenta como a primeira hipótese de tratamento – não sendo esta necessariamente prioritária, haja vista que poderá haver outras bases legais mais propícias no caso; o consentimento. Este se caracteriza pela "manifestação livre, informada e inequívoca pela qual o *titular concorda com o tratamento de seus dados pessoais* para uma finalidade determinada"[414], devendo este ser fornecido por escrito *ou outro meio que demonstre a manifestação de vontade* do titular[415].

Para tanto, caso o consentimento[416] seja dado por escrito, deverá este "constar de cláusula destacada das demais cláusulas contratuais"[417]. Não sendo este obtido por escrito, assim enquadrando-se na hipótese "outro meio que demonstre a manifestação de vontade", caberá "ao controlador o ônus da prova de que o consentimento foi obtido" conforme preconiza a LGPD [418], sendo vedado o tratamento de dados pessoais em que houver vício de consentimento[419].

Cumpre ressaltar que "a informação pessoal pode ser agrupada em subcategorias, ligadas a determinados aspectos da vida de uma pessoa". Isso permite a adoção de normas específicas a depender do tipo de informação e contexto. Assim sendo, pensar em uma setorização facilita o planejamento da abordagem a ser dada ao tipo da informação. É justamente o exemplo dos *dados pessoais sensíveis*: determinadas informações que, quando do tratamento, podem levar a resultados discriminatórios ou lesivos, apresentando maior risco potencial do que outras informações.[420].

Há uma variação sobre a disposição da temática dos dados sensíveis a depender da concepção de cada ordenamento jurídico global,[421]mas, o que se visa em comum é

---

[413] BRASI. LGPD. Art. 7º;
[414] BRASIL. LGPD. Vide art. Art. 5º, XII.
[415] BRASIL. LGPD. Vide Art. 8º.. Ver também os §§2º , 3º e 4º deste artigo: "§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei; § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.; § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.";
[416] Para aprofundamento na matéria: BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. Ed. Rio de Janeiro: Forense, 2020
[417] BRASIL. LGPD. Vide. Art. 8º, §1º.
[418] BRASIL. LGPD. Vide Art.8º, §2º
[419] BRASIL, LGPD. Vide art. 8º, §3º;
[420] DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.146-147. Nesse sentido: "A vedação ao tratamento discriminatório e abusivo é o ponto essencial para identificar os limites ao uso de dados semsíveis".MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 122.
[421] DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.148

garantir maior proteção a esta categoria, permitindo com que sejam *freadas práticas discriminatórias* e garantindo com que o titular dos dados pessoais sensíveis possa se realizar e relacionar na sociedade – *desdobrando a sua personalidade livremente*[422].

Compreender dado sensível é mais do que entender a sua natureza ou identificar o seu conteúdo, mas sim, verificar a potencialidade discriminatória que o seu tratamento pode gerar – e, ao identificar este fator, proibir ou limitar o seu tratamento[423].

Entretanto, não se pode olvidar que "há situações nas quais a discriminação pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos"[424]. A LGPD define dados pessoais sensíveis como:

> 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;[425]

Vale dizer que o tema dados pessoais sensíveis na legislação nacional não é novo, já sendo proibido o seu uso em bancos de dados de análise de crédito na Lei do Cadastro Positivo (Lei nº12.414/11)[426]:

> Art. 3º **Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.**
> § 1º Para a formação do banco de dados, somente poderão ser armazenadas **informações objetivas**, claras, verdadeiras e de fácil compreensão, que sejam **necessárias** para avaliar a situação econômica do cadastrado.
> [...]
> § 3º Ficam proibidas as anotações de:
> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> **II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à**

[422] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. Ed. Rio de Janeiro: Forense, 2020, p. 85.
[423] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 122-123
[424] DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021, p.148
[425] BRASIL. LGPD. Vide art. 5º, I, II, III.
[426] Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

> **orientação sexual e às convicções políticas, religiosas e filosóficas** (grifo nosso)[427].

Portanto, ao analisar conceder ou não o crédito e, levando-se em consideração a vedação da inclusão de informações que sejam personalíssimas à finalidade que se almeja, está se observando os princípios da finalidade e não discriminação – foco exclusivo na análise da concessão de crédito e evitar o tratamento discriminatório, respectivamente.[428] É justamente o princípio da não discriminação que norteia a proteção dos dados pessoais sensíveis, "constituindo-se a justificativa basilar para a sua tutela rigorosa" e, por consequência, de sua aplicação com limitações. Assim, quando a se estiver diante de dados potencialmente lesivos – pelo potencial discriminatório; restará a aplicação de regras para o seu tratamento[429].

Também merece pontuar a discussão no âmbito nacional se fotografias podem ser consideradas como dados pessoais sensíveis. Para Aline Fachinetti, uma fotografia ou filmagem pode revelar dados de origem étnica, racial, informações de saúde ou religiosa ou filiações partidárias, o que se poderia defender o seu enquadramento como dado pessoal sensível – *mesmo que indiretamente*[430]. Nesse sentido, a autora refere que dados inicialmente pessoais poderiam se tornar sensíveis, de acordo com o seu tratamento. Assim, exemplifica:

> Um exemplo hipotético poderia abranger até o consumo de energia elétrica, já que, analisando este consumo, pode ser possível prever questões inclusive religiosas (por exemplo, a análise poderia levar à inferência de que determinada pessoa é judia, de acordo com um padrão de consumo de energia menor durante o Sabbath).[431]

Ademais, Fachinetti assevera que, na prática, "o impacto e o risco ao titular para definir sensibilidade do dado deveriam ser levados em consideração", já que a matéria

[427] BRASIL. Lei do cadastro Positivo....
[428] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 122.
[429] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 122.
[430]FACHINETTI. Aline Fuke. LGPD: fotos, inferências e a sensibilidade de dados pessoais. JOTA. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-fotos-inferencias-e-a-sensibilidade-de-dados-pessoais-03092019#sdfootnote1sym. Acesso em: 20 jun. 2022.
[431] FACHINETTI. Aline Fuke. LGPD: fotos, inferências e a sensibilidade de dados pessoais. JOTA. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-fotos-inferencias-e-a-sensibilidade-de-dados-pessoais-03092019#sdfootnote1sym. Acesso em: 20 jun. 2022.

ainda é discutida, inclusive em âmbito internacional[432]. Para Rodrigo Pironti e Mariana Keppen, referem que "em não sendo a imagem captada para fins de tratamento específico de reconhecimento facial, não deve o dado ser classificado como sensível"[433].

Em se tratando de dados pessoais sensíveis, em que pese haja similaridade nas hipóteses de tratamento, é necessário pontuar algumas diferenças. O rol também é taxativo, mas mais limitador haja vista a sensibilidade envolvida no conteúdo dos dados. Veja-se o que dispõe o Art. 11 da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis **somente poderá ocorrer** nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal **consentir,** de forma **específica e destacada, para finalidades específicas**;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que **for indispensável** para:
> a) **cumprimento de obrigação legal ou regulatória pelo controlador;**
> b) tratamento compartilhado de dados necessários à execução, pela **administração pública,** de **políticas públicas** previstas em leis ou regulamentos;
> c) realização de estudos **por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) **exercício regular de direitos**, inclusive em contrato e em **processo judicial, administrativo e arbitral**, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e**) proteção da vida ou da incolumidade física do titular ou de terceiro;**
> f) **tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias**; ou
> f) **tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;** ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) **garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais**.(grifo nosso)[434]

Nesse sentido, o art. 11 apresenta duas hipóteses autorizativas de tratamento de dados sensíveis: (a) quando se enquadrar na base legal do consentimento – devendo este

[432] FACHINETTI. Aline Fuke. LGPD: fotos, inferências e a sensibilidade de dados pessoais. JOTA. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-fotos-inferencias-e-a-sensibilidade-de-dados-pessoais-03092019#sdfootnote1sym. Acesso em: 20 jun. 2022
[433]PIRONTI, Rodrigo; KEPPEN, Mariana Tomasi. As fotografias, as câmeras de segurança e os dados sensíveis na LGPD. CONJUR. 2021. Disponível em: https://www.conjur.com.br/2021-ago-23/opiniao-fotografias-cameras-seguranca-dados-sensiveis#author. Acesso em: 21 jun. 2022.
[434] BRASIL. LGPD. Art. 11.

ser específico, destacado, e com finalidade determinada; (b) quando da dispensa excepcional de consentimento[435].

Breves considerações sobre os incisos do art. 11 da LGPD a seguir:

> I - quando o titular ou seu responsável legal **consentir,** de forma **específica e destacada, para finalidades específicas**;

Denota-se tanto no artigo 7º quanto no art. 11 a necessidade de consentimento – quando for o caso de sua utilização; ou, enquadramento em outra base legal. Em resumo, o que se verifica é a dispensa de consentimento quando indispensável para o tratamento de dados relacionados a interesses públicos ou ao próprio titular de dados[436].

> II - sem fornecimento de consentimento do titular, nas hipóteses em que **for indispensável** para:

As exceções previstas no inciso II, do art. 11 são fruto de uma ponderação de interesses realizada pelo legislador, priorizando interesses de natureza pública frente aos do titular, naquelas circunstâncias e contextos determinados[437]. Assim sendo, a natureza da norma é permissiva – autorizativa do tratamento de dados pessoais sensíveis; ao contrário da GDPR, em que, a priori, é proibido o tratamento da categoria especial de dados (*special type of data)*[438].

> **a) cumprimento de obrigação legal ou regulatória pelo controlador;** (grifo nosso);

[435] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 137

[436] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 128

[437] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 138- 139. A autora critia o posicionamento do legislador nesse sentido: "[...] críticas podem ser feitas a este posicionamento legislativo, especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de direitos fundamentais de seu titular, tais como os da igualdade, liberdade e privacidade [...].

[438] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 137

Dispensa de consentimento pelo legislador, fazendo referência ao princípio da legalidade – permissão para que o controlador atue em estrito cumprimento de dever legal[439].

> b) **tratamento compartilhado** de dados necessários à execução, pela **administração pública,** de **políticas públicas** previstas em leis ou regulamentos; (grifo nosso)

. Entende-se este por "uso de dados pessoais por agentes de tratamento (controlador ou operador) que foram obtidos indiretamente, isto é, pela disponibilização difusa destes dados originalmente tratados por outro agente"[440]. Já a LGPD conceitua uso compartilhado de dados, no qual abarca o tratamento compartilhado de dados, como:

> XVI - **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou **tratamento compartilhado** de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; (grifo nosso)[441]

Nessa hipótese, observam-se os elementos qualificadores autorizativos: (a) tratamento compartilhado; (b) execução pela administração pública de políticas previstas em leis ou regulamentos. Novamente presente a efetivação do princípio da legalidade e, desta vez, o da publicidade[442], consoante preconiza o art. 23, I, da LGPD[443].

---

[439] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 139

[440] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 139

[441] BRASIL. LGPD. Art. 5º, XVI.

[442] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 140-141

[443] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;. BRASIL. LGPD.

> c) realização de estudos **por órgão de pesquisa**, garantida, **sempre que possível**, a **anonimização** dos dados pessoais sensíveis; (grifo nosso)

Vale destacar que a normativa não especifica sobre a natureza pública ou privada do órgão de pesquisa, o que se entende por abarcar ambos[444]. A anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"[445]. Esta prática é uma forma de garantir a segurança dos dados do titular, haja vista que o dado anonimizado não é considerado dado pessoal, pois, a priori, impossível a identificação do titular[446].

> d) **exercício regular de direitos**, inclusive em **contrato** e em **processo judicial, administrativo e arbitral**, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; (grifo nosso)

Será considerado, por exemplo, "legítimo, regular e não abusivo o tratamento de dados pessoais sensíveis em casos em que é exigido do agente de tratamento, em processo civil, por ordem judicial, informações sobre determinado titular de dados para fins de realização da função jurisdicional"[447].

> e) **proteção da vida** ou da **incolumidade física** do **titular ou** de **terceiro;** (grifo nosso)
>
> f) **tutela da saúde, exclusivamente,** em procedimento realizado por **profissionais de saúde, serviços de saúde** ou **autoridade sanitária;** ou (Redação dada pela Lei nº 13.853, de 2019) Vigência (grifo nosso)

Ambas as hipóteses retratam situações relacionadas à saúde do titular de dados. Exemplifica-se com atendimento médico de urgência, no qual o interesse preponderante é a vida, "sobrepondo-se essa proteção ao exercício de sua autonomia, por meio da dispensa da manifestação do consentimento"[448].

---

[444] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 142
[445] BRASIL. LGPD. Vide art. 5º, XI.
[446] Vide arts.5º, III; 12 da LGPD.
[447] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 146
[448] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 146

O inciso g) será pormenorizadamente abordado nos próximos tópicos.

Por fim, importante adicionar também que a LGPD possui um artigo específico para o tratamento de dados pessoais de crianças e adolescentes:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o **consentimento específico e em destaque** dado por pelo menos um dos pais ou pelo responsável legal.
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para **contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção**, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao **fornecimento de informações pessoais além das estritamente necessárias à atividade.**
> § 5º O controlador deve realizar todos os **esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança,** consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de **maneira simples, clara e acessível**, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (grifo nosso)[449].

Vale ressaltar que os dados de crianças e adolescentes podem ser tanto dados pessoais como dados pessoais sensíveis, sendo somados ao artigo 14 os cuidados de sua aplicação.

.3 Reconhecimento facial como dado pessoal sensível com ilustração de casos

A LGPD não aborda especificamente o tópico reconhecimento facial. Como referido anteriormente, a normativa, em seu artigo 5º, II, insere dado biométrico como

[449] BRASIL. LGPD. Art. 14.

dado pessoal sensível, mas não traz a definição de dado biométrico, nem biometria[450]. Inclusive, uma das primeiras versões da LGPD (Projeto de Lei nº4060/12, que regulamenta o tratamento de dados pessoais no Brasil[451]) não falava sobre dados biométricos. Segundo o PL, dados sensíveis seriam:

> Art. 7º. Para os fins da presente lei, entende-se como
> [...]
> IV - **dados sensíveis: informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular;** (grifo nosso)[452]

Após é que ocorreu a inclusão presente na versão atual da legislação:

> 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;[453]

Em que pese ausentes maiores aprofundamentos acerca desta temática na LGPD, é possível encontrar um conceito de biometria no Glossário de Segurança da Informação, instituído pelo Departamento de Segurança da Informação (GSI) do Governo Federal:

> BIOMETRIA - verificação da identidade de um indivíduo por meio de uma característica física[454]

[450] Nesse sentido: "Embora não exista uma definição de dados biométricos na legislação brasileira, a Lei Geral de Proteção de Dados considera dados biométricos como dados sensíveis. Este tipo de dado está sujeito a condições específicas de tratamento. "..INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p.34. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em: 15 jun. 2022.

[451] BRASIL. PL N. 4060/2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0ju06izhj6peecftv2zrqmw5o11591812.node0?codteor=1001750&filename=PL+4060/2012. Acesso em: 06 jun. 2022.

[452] BRASIL. BRASIL. PL N. 4060/2012.

[453] BRASIL. LGPD. Vide art. 5º, I, II, III.

[454] BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 06 jun. 2022.

Ainda, previsto que um sistema biométrico é um "conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca". No documento, vale referir que também há a definição de dado pessoal sensível, nos iguais termos da LGPD[455].

Vale mencionar que o Decreto n. 10.046/2019, que instituiu o Cadastro Base do Cidadão refere como "atributo biométrico": " 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".[456]

A utilização de biometria no Brasil não é tema recente[457]. Por exemplo, a Lei nº 13.444/2017, que dispõe sobre a Identificação Civil Nacional (ICN)[458] e, de acordo com o art. 1º, tem o objetivo de " identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.", sendo utilizada, dentre outras bases de dados, a base de dados biométricos da Justiça Eleitoral[459]. Em 2018 foi

[455] **DADO PESSOAL SENSÍVEL** - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 06 jun. 2022.

[456] BRASIL. DECRETO. N. 10,046, DE 09 DE OUTUBRO DE 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração federal e institui o cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Vide art. 2º, II. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 jun. 2022.

[457] Os casos abordados neste tópico não dirão respeito ao âmbito penal. Ver mais sobre em: BRASIL. BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. 2019.Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf . Acesso em: 15 jun, 2022; GOVERNO DO ESTADO DA BAHIA. Reconhecimento Facial impede entrada de homicida em circuito. Secretaria da Segurança Pública. SSP/BA. 2019. Disponível em: http://www.bahia.ba.gov.br/2019/03/noticias/carnaval/reconhecimento-facial-impede-entrada-de-homicida-em-circuito/. Acesso em: 06 jun. 2022; GOVERNO DO ESTADO DO CEARÁ. Chefe de organização criminosa é preso após ser identificado por reconhecimento facial. 2021. Disponível em:https://www.policiacivil.ce.gov.br/2021/05/01/chefe-de-organizacao-criminosa-e-preso-apos-ser-identificado-por-reconhecimento-facial/. Acesso em: 20 jun. 2022;

[458] BRASIL. Lei N. 13.444, DE 11 DE MAIO DE 2017. Disponível em: L13444 (planalto.gov.br). Acesso em: 15 jun. 2022.

[459]BRASIL. Lei N. 13.444, DE 11 DE MAIO DE 2017. Disponível em: L13444 (planalto.gov.br). Acesso em: 15 jun. 2022. Art. 1º É criada a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.

Art. 2º A ICN utilizará: I – a base de dados biométricos da Justiça Eleitoral;

II – a base de dados do Sistema Nacional de Informações de Registro Civil (Sirc), criado pelo Poder Executivo federal, e da Central Nacional de Informações do Registro Civil (CRC Nacional), instituída

publicada a Pòrtaria n.248, do Ministério da Saúde, que obriga a identificação biométrica da palma da mão dos recém-nascidos do Brasil, bem como a identificação biométrica da mãe[460]. A publicação da portaria foi uma solicitação do Conselho Nacional de Justiça (CNJ), para iniciar a coleta de dados para a Identificação Civil Nacional (ICN)[461], cujo objetivo ter um banco de dados nacional, bem como a prevenção do desaparecimento de crianças e tráfico de pessoas.[462].

Ainda, a Resolução nº306, de 17 de dezembro de 2019 do Conselho Nacional de Justiça (CNJ), Estabelece diretrizes e parâmetros para a emissão de documentação civil e para a identificação civil biométrica das pessoas privadas de liberdade[463]. De acordo com o seu Art. 1º, § único: "A identificação biométrica compreende a coleta de assinatura, fotografia frontal e coleta datiloscópica". Ademais, o dado biométrico está inserido na categoria de dados pessoais sensíveis, como bem refere o art. 5º da referida resolução. Por fim, o mesmo dispositivo ainda prevê, no contexto da sua redação, que o tratamento destes dados necessita ser "proporcional, não discriminatório e em cumprimento à finalidade [...]"[464].

É preciso ressaltar alguns exemplos no campo prático. Incluem-se situações para facilitar o exercício da cidadania – política pública; como obter o benefício de aposentadoria do Instituto Nacional do Seguro Social (INSS). Lançado pelo Governo Federal, o reconhecimento facial do aplicativo Meu gov.br será a primeira etapa da prova de vida dos aposentados do INSS, sem a exigência de deslocamento até às agências. A validação ocorre por meio da comparação das fotos tiradas pelo sistema de

---

pelo Conselho Nacional de Justiça, em cumprimento ao disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009 ; III – outras informações, não disponíveis no Sirc, contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizadas por outros órgãos, conforme definido pelo Comitê Gestor da ICN.

[460] BRASIL. PORTARIA N. 248, DE 2 DE FEVEREIRO DE 2018. MINISTÉRIO DA SAÚDE. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2018/prt0248_05_02_2018.html. Acesso em 15 jun. 2022.

[461] BRASIL. LEI N. 13.444, DE 11 DE MAIO DE 2017. Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm#:~:text=L13444&text=LEI%20N%C2%BA%2013.444%2C%20DE%2011%20DE%20MAIO%20DE%202017.&text=Disp%C3%B5e%20sobre%20a%20Identifica%C3%A7%C3%A3o%20Civil%20Nacional%20(ICN).. Acesso em: 15 jun. 2022.

[462] INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p.34-35. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em: 15 jun. 2022.

[463] CONSELHO NACIONAL DE JUSTIÇA. RESOLUÇÃO N. 306 DE 17 DE DEZEMBRO DE 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3146. Acesso em: 15 jun, 2022.

[464] CONSELHO NACIONAL DE JUSTIÇA. RESOLUÇÃO N. 306 DE 17 DE DEZEMBRO DE 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3146. Acesso em: 15 jun, 2022.

reconhecimento facial com a base de dados do TSE ou da CNH (número do documento respectivo é solicitado ao cidadão)[465]. O principal objetivo é dar mais confiabilidade ao benefício da prova de vida e também permitir com que outros serviços sejam solicitados sem que o beneficiário precise sair de casa[466].

Há pelo menos 06 (seis) meses[467], a tecnologia de reconhecimento facial vem sendo usada em 27 escolas públicas de Mata de São João (município baiano): mais de 7 (sete) mil estudantes são monitorados em tempo real. Ao entrar na escola, cada aluno é identificado pelo sistema. Os dados obtidos são registrados com o objetivo de acompanhar a frequência escolar do estudante e substituir a chamada tradicional. Os pais são comunicados automaticamente em caso de ausência na escola, servindo também para um controle da própria escola – se deve acionar o Conselho Tutelar, Conselho Municipal da Criança e do Adolescente, Secretaria de Educação. Além de combater a evasão escolar, o sistema tem contribuído para gerar economia: as cantinas passaram a produzir a quantidade exata de refeições baseada no número de alunos presentes (já foi registrada 30%-40% de economia)[468].

Em outubro de 2021, foi lançado o Programa de Gestão Tecnológica – Conecte Educação, pela Secretaria Municipal de Educação da Prefeitura de Goiânia (GO), que traz soluções para inovar nas gestões das unidades das redes municipais. O sistema de software conta com reconhecimento facial e com 22 módulos de integração, como serviço de frequência escolar com reconhecimento facial (o pai será informado quando o filho ingressar na escola), conexão com Conselho Tutelar, serviços de saúde, biblioteca virtual, gestão pedagógica, alimentação, entre outros[469].

Em fevereiro de 2022, a Prefeitura de Betim (Minas Gerais instalou a tecnologia de reconhecimento facial em escolas da rede municipal. Na entrada da escola, os estudantes passarão por dispositivo que identificará cada um e registrará a sua presença.

---

[465] Veja o funcionamento em: PASSO A PASSO DA PROVA DE VIDA POR BIOMETRIA FACIAL. INSS OFICIAL. YOUTUBE. Disponível em: https://www.youtube.com/watch?v=2ieYg06OHjc. Acesso em 15 jun. 2022.

[466] RECONHECIMENTO FACIAL PELO APLICATIVO MEU GOV.BR É A PRIMEIRA ETAPA DA PROVA DE VIDA DOS APOSENTADOS. GOVERNO FEDERAL. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/agosto/reconhecimento-facial-pelo-aplicativo-meu-gov-br-e-a-primeira-etapa-da-prova-de-vida-dos-aposentados. Acesso em: 15 jun. 2022.

[467] Notícia publicada em fevereiro de 2022.

[468] ESCOLAS PÚBLICAS DE MUNICÍPIO BAIANO USAM RECONHECIMENTO FACIAL PARA CONTROLAR FREQUENCIA DOS ALUNOS. Globo notícias. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2022/02/09/escolas-publicas-de-municipio-baiano-usam-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml. Acesso em: 10 jun. 2022.

[469] PREFEITURA LANÇA SISTEMA DE RECONHECIMENTO FACIAL NAS ESCOLAS E CMEIS DE GOIÂNIA. PREFEITURA DE GOIÂNIA. Disponível em: https://www.goiania.go.gov.br/prefeitura-lanca-sistema-de-reconhecimento-facial-nas-escolas-e-cmeis-de-goiania/. Acesso em: 15 jun. 2022;

O sistema visa otimizar o tempo ao substituir a chamada tradicional, e também ter mais economia, evitando desperdício de merenda escolar ao saber exatamente o número de alunos presentes[470]. Os casos acima não foram os únicos[471].

Sobre a implantação de tecnologias de reconhecimento facial na educação pública - por motivos de (i)segurança; (ii) checagem de presença mais simples; e (iii) evitar o desperdício de alimentos; bem como a utilização de reconhecimento biométrico em provas de ingresso ao ensino superior, merece menção o Relatório elaborado pelo Instituto Alana em parceira com a InternetLab.[472] Vale referir que, o uso de tecnologia biométrica pode ser benéfico, a depender do caso: se implementado em consonância com a privacidade de dados e o melhor interesse das crianças. Assim sendo:

> o processamento de dados pessoais sensíveis de crianças deve ser legal, transparente, deve mitigar riscos, prever direitos e salvaguardas. Os objetivos específicos devem ser explícitos, determinados e alinhados com o melhor interesse da criança - e não podem ser razoavelmente alcançados por outros meios; os dados devem ser adequados, relevantes e limitados ao absolutamente necessário. A segurança e a confidencialidade dos dados devem ser garantidas e o acesso não autorizado, evitado[473].

[470] PREFEITURA DE BETIM INSTALA RECONHECIMENTO FACIAL NAS ESCOLAS DA REDE MUNICIPAL. PREFEITURA DE BETIM. Disponível em: https://www.betim.mg.gov.br/portal/noticias/0/3/11327/prefeitura-de-betim-instala-reconhecimento-facial-nas-escolas-da-rede-municipal/. Acesso em: 17 jun. 2022.

[471] Ver mais sobre em: ESCOLA MUNICIPAL DE MATÃO ADOTA RECONHECIMENTO FACIAL PARA CONTROLAR FREQUENCIA DOS ALUNOS. G1. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/sp/sao-carlos-regiao/noticia/2019/12/11/escola-municipal-de-matao-adota-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml. Acesso em: 15 jun. 2022. PROFESSORES DO IFES REALIZAM CHAMADAS POR RECONHECIMENTO FACIAL. A GAZETA. Disponível em: https://www.agazeta.com.br/es/gv/professores-do-ifes-realizam-chamadas-por-reconhecimento-facial-1019?utm_medium=redacao&utm_source=twitter&origin_r=leiaag. Acesso em 10 jun 2022; PARANAVAÍ É PREMIADA POR SISTEMA DE RECONHECIMENTO FACIAL NAS ESCOLAS. PORTAL DA CIDADE. Disponível em: https://paranavai.portaldacidade.com/noticias/cidade/paranavai-e-premiada-por-sistema-de-reconhecimento-facial-nas-escolas-0654. Acesso em: 15 jun. 2022; SISTEMA DE RECONHECIMENTO FACIAL JÁ FUNCIONA NAS ESCOLAS DE IPATINGA. DIÁRIO DO AÇO. Disponível em: https://www.diariodoaco.com.br/noticia/0075842-sistema-de-reconhecimento-facial-ja-funciona-nas-escolas-de-ipatinga. Acesso em: 15 jun. 2022.

[472] INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p.38-42.

[473] INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p.10.

Exemplo de aplicação benéfica é a utilização da tecnologia de reconhecimento facial para tornar o embarque de passageiros no aeroporto mais ágil e seguro: Programa Embarque + Seguro 100% Digital do Governo Federal. O primeiro aeroporto a testar a tecnologia foi o terminal de Florianópolis (SC). O projeto também já passou por Salvador (BA), Brasília (DF), Confins (BH) e ponte aérea Rio de Janeiro-São Paulo (RJ/SP). O embarque é liberado, utilizando o ponto de controle biométrico, sem a necessidade de apresentar documento e bilhete aéreo[474]. A medida, já testada com passageiros, foi ampliada para pilotos e comissários[475]. De acordo com o presidente do Serviço Federal de Processamento de Dados - Serpro, Gileno Barreto, o programa atende aos preceitos da LGPD: "os dados que precisam ser utilizados para o embarque com o reconhecimento facial não são compartilhados com terceiros e o passageiro precisa assinar um termo de consentimento para o uso" da tecnologia[476]. No setor público, há outros casos[477].

Entretanto, também há casos em que a utilização do reconhecimento facial repercutiu de forma negativa, adentrando na esfera legal. Veja-se.

A Hering[478] foi a primeira empresa brasileira a ser condenada por violações decorrentes do uso de tecnologias de reconhecimento facial. A empresa implementou a tecnologia em sua loja Hering *Experience* no Shopping Morumbi (São Paulo), sem o consentimento dos consumidores, o que foi considerado prática abusiva, de acordo com o Código de Defesa do Consumidor (CDC). De acordo com a Secretaria Nacional do Consumidor (SENACON), por meio da tecnologia de detecção facial, a Hering conseguia captar as *reações d*os consumidores e, assim, traçar um perfil dos visitantes, personalizando as ofertas de produtos de acordo com as reações dos potenciais clientes. O objetivo seria proporcionar uma melhor experiência de compra ao consumidor. A partir disso, constatou-se que a empresa aproveitou-se da vulnerabilidade do

[474] AEROPORTO DE BRASILIA TESTA EMBARQUE DE PASSAGEIROS FEITO POR RECONHECIMENTO FACIAL. GOVERNO FEDERAL. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/aeroporto-de-brasilia-testa-embarque-de-passageiros-feito-por-reconhecimento-facial. Acesso em: 15 jun. 2022.

[475] AEROPORTO DE CONGONHAS TESTA EMBARQUE POR RECONHECIMENTO FACIAL COM TRIPULANTES. GOVERNO FEDERAL. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/aeroporto-de-congonhas-testa-embarque-por-reconhecimento-facial-com-tripulantes. Acesso em: 15 jun. 2022.

[476] AEROPORTO DA CAPITAL DO PAÍS TESTA EMBARQUE COM RECONHECIMENTO FACIAL. GOVERNO FEDERAL. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/noticias/2021/8/aeroporto-da-capital-do-pais-testa-embarque-com-reconhecimento-facial. Acesso em: 15 jun. 2022.

[477] Ver em: RECONHECIMENTO FACIAL NO BRASIL. INSTITUTO IGARAPÉ. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em 15 jun. 2022

[478] Franquia de vestuário brasileiro

consumidor, ocorrendo ainda a violação do direito à informação (captação sem consentimento) e aos direitos de personalidade. A Hering foi condenada ao pagamento de multa de R$58.767,00, ao Fundo de Defesa de Direitos Difusos (FDDD)[479].

Nesse mesmo sentido da detecção facial e da captação sem o consentimento do usuário, foi o caso da Via4quatro.

Em 2018, a empresa Concessionária da Linha 4 do Metrô de São Paulo S.A.(ViaQuatro) instalou Portas Interativas Digitais, com sensores colocado acima de propagandas publicitárias. Esta instalação captava, sem o consentimento dos usuários do metrô, a presença humana, a quantidade de pessoas que passavam e olhavam para a tela, as suas emoções, gênero e faixa etária. Verifica-se pela imagem a compulsoriedade da pesquisa de opinião, na medida em que a câmera que capta de detecção facial está posicionada acima da tela, "sem informação alguma para o consumidor e usuário do transporte público sobre a captura de seus dados pessoais, [...] sendo tais dados comercializados independentemente de seu consentimento"[480].

FIGURA 22 – PORTAS INTERATIVAS DIGITAIS

[479] Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial. IDEC. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial. Acesso em: 10 jun. 2022. Ver também: IDEC notifica Hering por coleta de dados faciais para publicidade. IDEC. Disponível em: https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade. Acesso em: 10 jun. 2022. Secretaria Nacional do Consumidor aplica multa a empresa por reconhecimento facial. GOVERNO FEDERAL. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-aplica-multa-a-empresa-por-reconhecimento-facial . Acesso em: 10 jun. 2022.

[480] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 37. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

Fonte: AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 36

Diante desta situação, no mesmo ano, o Instituto Brasileiro de Defesa do Consumidor (IDEC) ajuizou uma Ação Civil Pública (ACP) em face da ViaQuatro com o objetivo de cessar o sistema de Portas Interativas Digitais e condenar a ViaQuatro por danos coletivos, ao violar direitos dos usuários consumidores.. Vale ressaltar que a Defensoria Pública do Estado de São Paulo ingressou como litisconsorte e o Instituto Alana[481] como *amicus curiae*. Conforme a ACP, a prática permite uma "espécie de pesquisa de mercado automatizada sem autorização do participante, permite a obtenção de receita a partir da venda desses dados para terceiros que podem então direcionar suas estratégias de publicidade a partir das reações identificadas"[482].

O resultado da ACP foi publicado em maio de 2021, sendo decidido que: (i) ausente finalidade do tratamento dos dados pessoais sensíveis obtidos: sem propósitos legítimos, específicos, explícitos e informados ao titular; (ii) confirmada a liminar de abstenção de captura de imagens, sons e outros dados pessoais dos consumidores usuários sem consentimento;(iii) confirmada a violação ao direito à imagem dos consumidores usuários do serviço público (incluindo dados de crianças e adolescentes); aos dados pessoais sensíveis coletados; aos direitos básicos do consumidor; (iv)pagamento de indenização por danos morais coletivos no valor de R$100.000,00[483].

É imprescindível destacar que, em ambos os casos mencionados, presentes os seguintes elementos em comum: (i)captação de dados biométricos *sem consentimento*; (ii) *sujeito vulnerável*, qual seja, consumidor *e* também crianças e adolescentes envolvidos (possivelmente na Hering também) – titulares duplamente vulneráveis; (iii)*detecção facial* – diferentemente de reconhecimento facial.

[481] Instituição que atua em programas que buscam a garantia de condições para a vivência plena da infância. Ver mais sobre em: https://alana.org.br/.

[482] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 3. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

[483] IDEC. IDEC obtém vitória contra reconhecimento de emoções no Metrô de SP. Disponível em: https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp#:~:text=A%20empresa%20foi%20condenada%20a,publicit%C3%A1rios%20com%20a%20inten%C3%A7%C3%A3o%20de. Acesso em: 20 mai. 2022.

Ainda, vale resssaltar a divergência de que a Hering é uma empresa privada, já a ViaQuatro, quando da prestação de serviço de transporte urbano, concessionária de serviço público. Nesse sentido, em relação à ViaQuatro, não ocorreu a situação de ofertar o seu espaço para anúncios publicitários mas, "o bem lucrativo ofertado pela concessionária são dados obtidos a partir de atividade dos usuários, seus clientes, que transitam pelos trens e estações"[484]. Nesse sentido, a ViaQuatro possui um uso comercial de caráter exclusivo naquele ambiente, posto que era a única concessionária integrante do contrato. Isso faz com que haja um "poder desequilibrado em relação àquele mercado, em que não há nenhuma outra empresa apta para fazer o levantamento feito por ela, que torna as informações demográficas por ela coletadas valiosas para venda a terceiros". Assim sendo:

> Devido a este valor econômico, esta atividade de **detecção facial integra prática comercial.** E, nesse âmbito, seu **caráter é abusivo**, pois uma pessoa, ao utilizar o **serviço de transporte público**, contribui obrigatoriamente com uma **atividade de pesquisa mercadológica**, sem a possibilidade de não fazê-lo**. Isso fere a liberdade de escolha dos cidadãos**. Ou seja, além de obrigar seus usuários a integrar pesquisa demográfica compulsória, a ViaQuatro o faz com exclusividade, sendo a única empresa que tem esse poder naqueles espaços, o que torna essa coleta de informações algo vantajoso economicamente à ViaQuatro.(grifo nosso).[485]

Em relação ao ponto (i)captação de dados biométricos sem consentimento, o Instituto de Referência em Internet e Sociedade (IRIS)[486] refere que houve violação do

[484] TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro), p. 30.. Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 10 jun. 2022.

[485] TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro). Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 10 jun. 2022., p. 25.

[486] TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A.

direito dos usuários em relação ao dever de informação sobre o tratamento, assim como à liberdade de escolha de participar ou não da atividade (consentimento sobre o uso da imagem). Assim refere o Parecer do IRIS sobre o tema: "não há dúvida, portanto, que houve dano, vez que todo o exposto indica que é evidente a violação aos direitos coletivos relacionados ao consentimento, à informação e autodeterminação dos usuários do metrô."[487]. A captação da detecção facial sem consentimento de consumidores, *per si*, já viola vários fundamentos da LGPD, como o respeito à privacidade, a autodeterminação informativa, inviolabilidade da intimidade, da honra e da imagem, defesa do consumidor[488]. Inexistente, por consequência, a boa-fé[489]: princípio norteador da LGPD e essencial em uma relação consumerista, sempre necessário que seja observado a partir de que "circunstâncias concretas em que se deu o consentimento, a finalidade de uso e tratamento dos dados que foi indicada na ocasião e o modo como foram compreendidas as informações prévias oferecidas". Não se espera comportamento contraditório, sendo esperado o respeito à vinculação com a finalidade originalmente informada[490].

Quanto ao ponto (ii) sujeito vulnerável, é previsto em âmbito legal a vulnerabilidade do consumidor ou, ainda, de situação concreta que possa acentuar esta característica – vulnerabilidade agravada[491]. Outrossim, vale referir que crianças e adolescentes também possuem vulnerabilidade agravada[492].

Para tanto, não se pode olvidar que o no tratamento de dados pessoais em relações de consumo deve-se levar em conta a vulnerabilidade do consumidor – tanto técnica – por possuir menos informações que o fornecedor sobre o fluxo dos dados;

(ViaQuatro). Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 10 jun. 2022.

[487] TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro). Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 10 jun. 2022., p. 31.

[488] BRASIL. LEI GERAL DE PROTEÇÃO DE DADOS. Vide Art. 2º, I, II, IV, VI. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jun. 2022.

[489] Ver: MARTINS-COSTA, Judith. **A boa-fé no direito privado:** critérios para a sua aplicação. 2 ed. São Paulo: Saraiva Educação, 2018.

[490] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais. Thomson Reuters. 2019. Online. p. 5

[491] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais. Thomson Reuters. 2019. Online. p. 5

[492] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais. Thomson Reuters. 2019. Online. p.25

como fática; por ter menos recursos "intelectuais e econômicos para a reparação de prejuízos advindos do tratamento de dados; e, a partir disso, assegurar mecanismos de proteção especial[493]" - proteção já assegurada, em certa medida, pela LGPD, ao dispor como fundamento a defesa do consumidor, em seu art. 2º, VI[494]. No caso de dados sensíveis, mereceria a adoção de mecanismos adicionais de segurança.[495]

Quando o consumidor tem os seus dados tratados, há um risco envolvido – tratamento equivocado ou com viés discriminatório, o que pode acarretar em determinada categorização/classificação ou discriminação no mercado de consumo. Esta situação pode "afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais"[496]. Posto isto, Laura Shertel Mendes entende ser necessário o atendimento de duas condições para que um tratamento de dados pessoais seja considerado legítimo nas relações de consumo: (a) em regra, deve ser autorizado pelo consumidor (salvo exceções: quando indispensável para o cumprimento da finalidade contratual ou execução de obrigação legal do fornecedor); (b) deve levar com consideração: a boa-fé objetiva, as expectativas legítimas do consumidor, *os impactos e os riscos do tratamento* de dados pessoais para o consumidor[497].

Assim, cumpre ressaltar que, de acordo com a ACP da ViaQuatro, a coleta de dados biométricos sem o consentimento violou gravemente o Código de Defesa do Consumidor (CDC), quanto aos direitos básicos do consumidor em relação à compreensão informacional dos riscos da coleta das emoções e de como funciona a análise de dados[498]. Observa-se o que dispõe o CDC nesse tema:

---

[493] MENDES, Laura schertel. Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental. São Paulo : Saraiva, 2014, p. 199. Em que pese escrito em 2014, a autora já defendia o reconhecimento de um direito básico do consumidor à proteção de dados pessoais. Sendo este fruto do direito fundamental à inviolabilidade da intimidade e da vida privada (art 5º, X), em dimensão de proteção de dados pessoais, p 202.

[494] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; . BRASIL. LGPD.6

[495] MENDES, Laura Shertel.Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental. São Paulo : Saraiva, 2014, p. 217.

[496] MENDES, Laura Shertel. Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental. São Paulo : Saraiva, 2014, p 198.

[497] MENDES, Laura Shertel Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental. São Paulo : Saraiva, 2014, p 204.

[498] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 28. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

> Art. 6º São direitos básicos do consumidor:
> I - a proteção da vida, saúde e segurança **contra os riscos provocados** por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;
> II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, **asseguradas a liberdade de escolha** e a igualdade nas contratações;
> III - **a informação adequada e clara sobre os diferentes produtos e serviços**, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, **bem como sobre os riscos que apresentem**;[499]
> [...]

Para tanto, conforme a ACP, levando em consideração a ausência de consentimento livre, específico, informado e em destaque dos titulares – "nenhum dos 600 mil usuários [...] -, há uma violação do ordenamento jurídico brasileiro, colocando os consumidores [...] em ausência de controle e autodeterminação informativa sobre seus dados biométricos"[500].

Além de consumidores envolvidos, cumpre referir que a ViaQuatro mencionou ser possível a diferenciação das emoções em adultos, jovens e crianças[501]. Vale destacar o princípio da proteção integral à criança e adolescente na própria Carta Constitucional, em seu Artigo 227:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Não se pode olvidar do que preconiza o Estatuto da Criança e Adolescente (ECA – Lei nº8069/1990):

> Art. 15. A **criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas** em processo de

[499] BRASIL. CÓDIGO DE DEFESA DO CONSUMIDOR. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jun. 2022.
[500] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 29. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.
[501] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 33. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

> desenvolvimento e como sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis.
>
> [...]
>
> Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, **abrangendo a preservação da imagem, da identidade, da autonomia,** dos valores, idéias e crenças, dos espaços e objetos pessoais. (grifo nosso)[502]

Ainda, o Código de Defesa do Consumidor (Lei nº8.078, de 11 de setembro de 1990) refere como prática abusiva: prevalecer-se da fraqueza ou ignorância do consumidor, *tendo em vista sua idade*, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços[503].

Relembre-se o que preconiza a LGPD sobre o tratamento de dados de crianças e adolescentes. Em seu artigo 14: "deverá ser realizado em seu melhor interesse", e "realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal". A ausência de consentimento para o tratamento de dados de menores *somente* será possível quando necessário para "contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, *e, em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o §1º"*. Foi justamente a hipótese ocorrida: repasse a terceiros das emoções de crianças e adolescentes coletadas sem o consentimento, a fins de publicidade direcionada.

Como refere a ACP[504]:

> Em hipótese alguma, a coleta e tratamento de dados pessoais de crianças pode ser feita para obter vantagens econômicas de suas reações a propagandas. Além da ausência de consentimento dos responsáveis, há uma violação de direito muito maior, de Direito Constitucional, relacionada à proteção dos interesses das crianças e adolescentes e reconhecimento de sua hipervulnerabilidade (grifo nosso) .

---

[502] BRASIL. ESTATUTO DA CRIANÇA E DO ADOLESCENTE. http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 jun. 2022.

[503] BRASIL. CÓDIGO DE DEFESA DO CONSUMIDOR. Vide art. 39, IV. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14 jun. 2022.

[504] AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 35. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

Ainda, de acordo com o Relatório produzido pelo Instituto Alana e o InternetLAB, "O direito das crianças à privacidade", "além de os modelos de negócios baseados em dados poderem inicialmente representar graves ameaças à privacidade das crianças, ao mesmo tempo eles desdobram em outras camadas de violações e possíveis impactos em seu desenvolvimento completo". A coleta biométrica sem consentimento, como nos casos exemplificados, é oposta ao melhor interesse da criança, na medida em que pode reforçar vulnerabilidades, gerar ameaças aos direitos de crianças e adolescentes à autodeterminação e a um tratamento igualitário[505].

Por fim, quanto à (iii)*detecção facial* – diferentemente de reconhecimento facial, a detecção facial é uma fase anterior ao reconhecimento facial, como já abordada no capítulo anterior. O que se verifica é que, em ambos os casos mencionados (Hering *Experience* e ViaQuatro), a questão debatida era acerca do uso da detecção facial – e não do reconhecimento facial. Mesmo assim, ambas as situações – devido às suas particularidades; foram levadas ao judiciário, sendo identificado o risco e aplicada uma multa. Ainda, entendeu-se como afronta aos direitos de imagem e personalidade, direito dos consumidores e a abusividade, ainda mais ausente o consentimento dos titulares. Portanto, se as situações expostas já foram tidas como graves quando da análise da detecção facial, quiçá será quando se estiver em face de casos de reconhecimento facial. É indubitável que o cenário será mais nocivo.

2.4 Análise da alínea g) do art. 11 da LGPD e caracterização do consentimento

Tendo sido apresentados casos concretos da utilização de dados pessoais sensíveis no contexto nacional, bem como o significado de tratamento de dados, dados pessoais, dados pessoais sensíveis, hipóteses de tratamento de ambos e também – brevemente; a temática do consentimento e a sua dispensa., é essencial a análise pormenorizada do que dispõe a alínea g), do Art 11, II.

O legislador trouxe uma base legal mais específica, cujo objetivo é a prevenção de fraudes e garantir a segurança do titular, estando vinculada aos interesses dos

[505] INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p. 22

titulares e determinadas entidades, ao invés do legítimo interesse[506], ou da base legal de proteção do crédito[507]. Veja-se o que preconiza a LGPD:

> Art. 11. O tratamento de **dados pessoais sensíve**is somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> [...]
> **II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:**
> **[...]**
> **g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais** (grifo nosso)**[508].**

Caitlin Mulholland refere que a normativa mencionada "representa um desafio na interpretação de seus elementos". Um dos cernes está justamente na identificação do *lócus* do tratamento de dados na hipótese referida. Mulhollhand refere que o objetivo do legislador seria a prevenção a fraudes e promoção da segurança do titular de dados e, justamente por isso, a dispensa dada na obtenção do consentimento se justificaria em prol do próprio titular – interpretação idêntica nas alienas "e" e "f"; "constituindo o núcleo duro do que se pode considerar como legítimo interesse do titular dos dados sensíveis em seu tratamento"[509].

Ao analisar o tratamento de dados pessoais sensíveis deste artigo, Mulholland refere este tema como "o *legítimo interesse do titular* de dados pessoais sensíveis e a

---

[506] TEFFÉ, Chiara Spadacccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com.** a.9.n.1. 2020. P. 1-39, p. 32. Disponível em: https://www.academia.edu/42993125/Tratamento_de_dados_pessoais_na_LGPD_estudo_sobre_as_bases_legais. Acesso em: 20 jun. 2022.

[507] Vide Art. 7º, X: "X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.", como previsto em quadro comparativo das bases legais de dados pessoais e dados pessoais sensíveis. Vale ressaltar: "Se a maioria das pessoas não demonstra grande cautela – e nem mesmo preocupação – com o fornecimento de seus dados pessoais, uma diferenciação daquilo que traga maior perigo se faz necessária. Para tanto, dividiu-se a tutela jurídica dos dados pessoais "comuns" em relação aos dados pessoais sensíveis; porém a LGPD brasileira foi até mesmo redundante e pontualmente confusa na delimitação das hipóteses (taxativas!) dos artigos 7º e 11" FALEIROS JUNIOR, José Luiz de Moura. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coord.).**Estudos essenciais de Direito Digital**. Uberlândia: LAECC, 2019, p. 207- 231, p. 218-219; 227.

[508] BRASIL. LGPD. Art. 11.

[509] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 146-147

tutela de sua segurança no processo de identificação e autenticação de cadastro em sistemas eletrônicos"[510]. Explica-se.

Evidente a alteração analítica do legítimo interesse, em que o *foco, nesse momento é o titular*, não o controlador, como anteriormente.[511] A opção do legislador ao fazer isso seria benéfica não só para o próprio titular, mas também para os agentes de tratamento de dados, na medida em delimitaria a sua atuação, "fundamentando as finalidades legítimas do tratamento de dados também em relação ao titular e ao exercício regular de seus direitos e liberdades fundamentais"[512], conforme previsão no art. 10, II, da LGPD:

> Art. 10. O legítimo interesse do controlador **somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas**, consideradas a partir de **situações concretas**, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - **proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais,** nos termos desta Lei. (grifo nosso)[513]

.

Dessa forma, seria uma forma de auxiliar os processos internos de uma organização. Por exemplo, em uma relação de consumo:

> se consideram os dados pessoais do consumidor utilizados para efeito de organização interna do próprio fornecedor ou **na sua relação com parceiros negociais, assim como, com relação ao uso de dados sensíveis com a finalidade de garantir a "prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos** (art.11, ii, "g", LGPD)[514]. (grifo nosso)

[510] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 146
[511] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. BRASIL. LGPD
[512] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p. 147. Vide art.
[513] BRASIL. LGPD.
[514] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais. Thomson Reuters. 2019. Online. p. 8

A partir disso, denota-se que o escopo normativo é a segurança do titular e a prevenção à fraude exclusivamente em processos de *identificação e autenticação em sistemas eletrônicos*[515]. É preciso compreender o que estes significam.. Pormenoriza-se:

a) Garantia da prevenção à fraude

Primeiramente, entende-se por fraude:

> 1 Ato de **má-fé** que tem por objetivo **fraudar ou ludibriar alguém**; cantiga, engano, sofisticação.
> 2 Mentira ardilosa; sicofantia.
> 3 Entrada ilegal de produtos estrangeiros, sem o pagamento dos tributos alfandegários.
> 4 **Ato de falsificar** documentos, marcas e produtos (grifo nosso)[516].

Em resumo, a fraude visa obter de outrem uma vantagem ilícita[517]. Exemplifica-se: boletos falsos, roubo de dados em sites falsos, e pedido de empréstimo com documento falsificado[518]. Ainda, estelionatários podem comprar linhas telefônicas para ter comprovante de residência com do titular para cometer outros crimes, como abertura de empresas (abertura de empresa em nome da vítima – "laranjas")[519]. Para ciência: a cada 17 segundos, uma tentativa de fraude acontece; e-commerce tem mais de R$3,6mil em tentativas de fraude por minuto; 2 empresas são abertas diariamente em São Paulo dom documentos roubados ou extraviados[520]. Entretanto, tanto o setor público quanto privado vem desenvolvendo iniciativas para a prevenção de fraudes.

---

[515] Como os temas da identificação e da autenticação já foram tratados em capítulo anterior, não serão abordados neste momento.

[516] MICHAELIS. DICIONÁRIO ONLINE. Editora Melhoramentos. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude/. Acesso em: 15 jun. 2022.

[517] Ver art. 171 do Código Penal (Decreto-Lei n.2.848, de 7 de dezembro de 1940). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de jun. 2022.

[518] Ver tentativa de compra de carro com documento (CPF) alheio em: POLÍCIA PRENDE HOMENS QUE TENTAVAM COMPRAR CARRO COM DOCUMENTO DE OUTRA PESSOA. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2018/10/02/policia-prende-homens-que-tentavam-comprar-carro-com-documento-de-outra-pessoa.ghtml. Acesso em: 15 jun. 2022. De acordo com o SERASA, golpe do carro financiado com CPF roubado faz vítima a cada 2 dias. TENHA ATITUDE ANTIFRAUDE: MONITORE SEU CPF E ASSINE SERASA PREMIUM. SERASA PREMIUM. Disponível em: https://www.serasa.com.br/premium/blog/antifraude/. Acesso em: 15 jun. 2022;

[519] SAIBA O QUE É FRAUDE E QUAIS OS TIPOS MAIS COMUNS - FRAUDES E GOLPES. SERASA ENSINA. Disponível em: https://www.serasa.com.br/ensina/seu-cpf-protegido/o-que-e-fraude/. Acesso em: 15 jun. 2022.

[520] TENHA ATITUDE ANTIFRAUDE: MONITORE SEU CPF E ASSINE SERASA PREMIUM. SERASA PREMIUM. Disponível em: https://www.serasa.com.br/premium/blog/antifraude/. Acesso em: 15 jun. 2022;

No que tange aos serviços públicos, exemplifica-se com a identificação biométrica no sistema de votação mediado pelo Tribunal Superior Eleitoral (TSE). A tecnologia utilizada pelo Tribunal tem o objetivo de tornar o processo de votação mais seguro, evitando com que uma pessoa votasse no lugar de outra (além de reduzir significativamente a intervenção humana no processo da votação). Funciona da seguinte forma: a urna somente é liberada para o cidadão votar quando o leitor biométrico identifica as impressões digitais do eleitor, havendo a compatibilidade a partir do banco de dados unificado da Justiça Eleitoral[521]. Outro exemplo é o reconhecimento facial do aposentado para fins de concessão do benefício do INSS ao segurado correto, conforme já mencionado. Ainda, empresas de ônibus também passaram a utilizar a biometria facial. Por exemplo, em Porto Alegre (Rio Grande do Sul), a câmera com a tecnologia fica posicionada ao lado da roleta e compara a foto do cadastro do cartão TRI do usuário com a foto tirada no momento em que este passa a roleta. A ferramenta vem sendo utilizada exclusivamente para passageiros isentos ou estudantes (com 50% de desconto), a fim de garantir maior segurança na utilização dos benefícios, evitando fraudes[522].

Em se tratado do setor privado, algumas instituições financeiras vem adotando o uso de tecnologias de autenticação de identidade, como o reconhecimento facial, justamente pelos seus clientes serem alvos de golpes.

É o caso do Itaú, que "busca sempre adequar seus níveis de segurança aos riscos de fraude, levando com conta também a usabilidade e a melhor experiência para nossos clientes". A instituição refere como benefícios da utilização da biometria facial: "prevenção a fraudes e golpes (garantir que é você mesmo na criação de contas e em transações[523]); segurança (dificultar acessos indevidos e aumentar a segurança); precisão [...]; e agilidade (reduzir a necessidade de comparecer às nossas agências)".[524]

Ainda, a Nubank divulgou que transferências instantâneas de alto valor deverão ser confirmadas por reconhecimento facial, objetivando o combate a fraudes (além de as

---

[521] BIOMETRIA. TRIBUNAL SUPERIOR ELEITORAL. Disponível em: https://www.tse.jus.br/eleitor/biometria. Acesso em: 15 jun. 2022.

[522] EMPRESAS DE ÔNIBUS ADAPTAM TECNOLOGIA DA BIOMETRIA FACIAL PARA RECONHECER PASSAGEIROS COM MÁSCARA. ASSOCIAÇÃO DOS TRANSPORTADORES DE PASSAGEIROS – ATP. Disponível em: https://www.atppoa.com.br/2020/08/25/empresas-de-onibus-adaptam-tecnologia-da-biometria-facial-para-uso-da-mascara/. Acesso em 16 jun. 2022.

[523] Veja o Ebook criado pelo Itaú sobre golpes e proteção de dados: SUA VIDA DIGITAL E OS SEUS DADOS ESTÃO SEGUROS? ITAU. Disponível em: https://www.itau.com.br/assets/dam/publisher/01_itau/11_fraudes/02_seg_ebook_pdf/finais/EBK_00_SEGURANCA.pdf. Acesso em: 15 jun. 2022.

[524] BIOMETRIA FACIAL. ITAU. Disponível em: https://www.itau.com.br/privacidade/biometria-facial. Acesso em: 15 jun. 2022.

transações serem liberadas apenas após a inserção da senha do cartão)[525]. O C6 Bank também habilitou o reconhecimento facial para transações no aplicativo. Assim, a biometria facial pode ser requerida pelo próprio banco quando em transações como TED, TEF, pix e pagamentos de valores. A medida foi tomada como camada adicional de proteção se segurança do cliente: "se um rosto diferente ao do dono da conta for exibido na biometria, o app será desativado permanentemente naquele aparelho". A face do cliente já é obtida desde o processo de abertura da conta, em que a biometria facial é usada para a autenticidade do dono da conta. A biometria facial também é analisada em conjunto com recurso *liveness* (prova de vida)[526], em que a instituição verifica se a pessoa que está solicitando a conta está mesmo segurando o celular, não sendo a foto do rosto de um sujeito[527].

Em que pese o reconhecimento facial tenha sido adicionado como uma camada extra de segurança em instituições financeiras, como referido, a própria tecnologia também já foi utilizada na aplicação de novo golpe. Foi o caso do publicitário paulista Piero Rossi, que descobriu ter um financiamento de um carro em seu nome após ter mostrado o seu rosto para o celular de um suposto motoboy para confirmar a sua identidade e receber um "brinde" na sua residência. A liberação do financiamento teria ocorrido pelo banco Itaú[528]. Inclusive, o Procon Paraná[529] alertou a população sobre golpes relacionados identificados em Curitiba e região Metropolitana: "golpe do presente". Conforme o órgão de defesa refere, a vítima recebe um "presente" inesperado. O entregador solicita uma fotografia para acusar o recebimento e também alguns dados pessoais. Com estes dados, e o reconhecimento facial, os golpistas conseguem comprar um veículo ou solicitar empréstimos em nome da vítima[530].

---

[525] NUBANK USA RECONHECIMENTO FACIAL PARA LIBERAR PIX DE ALTO VALOR. TECNOBLOG. Disponível em: https://tecnoblog.net/noticias/2021/04/16/nubank-usa-reconhecimento-facial-para-liberar-pix-de-alto-valor/. Acesso em: 15 jun. 2022.

[526] Também chamado de liveness detection, é um recurso cada vez mais utilizado na prevenção de identidade. Por meio de algoritmos, há a análise se o sujeito está vivo ou se a imagem é reproduzida de uma foto, por exemplo. Por exemplo, quando o sistema pede que a pessoa pisque, movimente a face, olhos, sorria, está buscando elementos de que a pessoa esteja viva.

[527] C6 BANK HABILITA RECONHECIMENTO FACIAL PARA TRANSAÇÕES NO APP. BANCO C6. Disponível em: https://blog.c6bank.com.br/c6-bank-habilita-reconhecimento-facial-para-transacoes-no-app. Acesso em: 15 jun. 2022.

[528] GOLPE DO RECONHECIMENTO FACIAL FAZ VÍTIMA FINANCIAR CARRO PARA TERCEIROS. UOL. Disponível em: https://www.uol.com.br/carros/noticias/redacao/2021/06/04/golpe-do-reconhecimento-facial-faz-vitima-financiar-carro-de-luxo-sem-saber.htm. Acesso em 15 jun. 2022.

[529] Órgão que realiza a defesa e proteção do consumidor

[530] GOLPE "DO PRESENTE" EM COMPRAS NA INTERNET OU NO CARTÃO POR APROXIMAÇÃO: PROCON-PR ALERTA SOBRE COMO SE PROTEGER. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/pr/parana/noticia/2021/11/02/golpe-do-presente-em-compras-na-

O caso de Rossi não foi isolado. Outra fraude cometida com a utilização do reconhecimento facial, dessa vez, em face de idosos. O caso ocorreu em São Vicente do Sul, Rio Grande do Sul e, pelo menos 13 (treze) idosos contrataram, sem saber, empréstimos consignados, acreditando que os valores recebidos eram fruto de ressarcimento de juros abusivos pagos em dívidas antigas. O dinheiro foi liberado sem qualquer necessidade de assinatura contratual, apenas utilizando a biometria facial. Os golpistas fingiam ser funcionários governamentais do INSS e realizaram reuniões em que convenceram os idosos ao suposto ressarcimento. A Defensoria Pública acompanha o caso[531].

É preciso ressaltar que a prevenção à fraude, a depender do caso, também coincide com o objetivo de garantir a segurança do titular. Veja-se:

b) Segurança do titular

Inicialmente, o que o legislador quis dizer com "segurança do titular"? Poder-se-ia pensar em segurança física[532] - exemplo: acesso não autorizado de pessoas; agressão física, proteção da vida; ou segurança de dados – exemplo: incidentes de segurança[533], podendo ser intencionais ou não.

Levando em consideração o contexto em que o termo foi inserido – dispensa de consentimento para o *tratamento de dados* pessoais sensíveis e nos processos de identificação e autenticação de cadastro em *sistemas eletrônicos*; não se pode abordar o

internet-ou-no-cartao-por-aproximacao-procon-pr-alerta-sobre-como-se-proteger.ghtml. Acesso em: 15 jun. 2022.

[531] GOLPISTAS USAM RECONHECIMENTO FACIAL PARA FAZER IDOSOS CONTRATAREM EMPRÉSTIMOS CONSIGNADOS NO RS. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2022/03/28/golpistas-usam-reconhecimento-facial-para-fazer-idosos-contratarem-emprestimos-consignados-no-rs.ghtml. Acesso em: 15 jun. 2022.

[532] Vale lembrar que o artigo não trata do tema da segurança pública, havendo espaço próprio destinado à matéria.

[533] Entende-se por incidente e incidente de segurança: "**INCIDENTE** - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;"; **INCIDENTE DE SEGURANÇA** - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;" BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 06 jun. 2022.

tema de segurança sem falar de *segurança da informação*[534]. De acordo com o Glossário de Segurança da Informação[535], é possível definir o termo como:

> **SEGURANÇA DA INFORMAÇÃO** - ações que objetivam viabilizar e assegurar a **disponibilidade,** a **integridade**, a **confidencialidade** e a **autenticidade** das informações;(grifo nosso)

Consoante a Portaria N.218, de 19 de maio de 2020, que Institui a Política da Segurança da Informação do Ministério da Economia[536], entende-se disponibilidade, integridade, confidencialidade e autenticidade como:

> ANEXO I
> CONCEITOS E DEFINIÇÕES
> 1. Para os fins da Política de Segurança da Informação do Ministério da Economia, fica estabelecido o significado dos seguintes termos e expressões:
> [...]
> 1.2. **autenticidade:** propriedade pela qual se assegura que a **informação foi produzida, expedida, modificada ou destruída** por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
> [...]
> 1.4. **confidencialidade**: propriedade pela qual se assegura que a **informação não esteja disponível ou não seja revelada** a pessoa, a sistema, a órgão ou a entidade **não autorizados nem credenciados**;
> [...]
> 1.6. **disponibilidade**: propriedade pela qual se assegura que a informação **esteja acessível e utilizável sob demanda** por uma pessoa física ou determinado sistema, órgão ou **entidade devidamente autorizados;**
> [...]
> 1.11. **integridade:** propriedade pela qual se assegura que a **informação não foi modificada ou destruída de maneira não autorizada ou acidental** (grifo nosso)

A segurança da informação está intrinsecamente relacionada à proteção de dados, haja vista que a LGPD propõe a adoção de medidas de segurança e boas práticas

[534] Ver também sobre o tema: ISO/IEC 27001, norma internacional que define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).
[535] BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 06 jun. 2022.
[536] BRASIL. PORTARIA N. 2018, DE 19 DE MAIO DE 2020. Institui a Política de Segurança da Informação do Ministério da Economia. Disponível em: https://extranet.economia.gov.br/wp-content/uploads/2020/10/Portaria-no-218-Institui-a-Poli%CC%81tica-de-Seguranc%CC%A7a-da-Informac%CC%A7a%CC%83o.pdf. Acesso em 16 jun. 2022.

para a segurança do tratamento de dados[537]. Não é sem motivo a previsão do princípio da segurança:

> VII - **segurança:** utilização de **medidas técnicas e administrativas** aptas a **proteger os dados pessoais** de **acessos não autorizados** e de **situações acidentais** ou i**lícitas de destruição, perda, alteração, comunicação ou difusão**[538]; (grifo nosso)

De acordo com a normativa, os agentes de tratamento devem:

> Art. 46. Os agentes de tratamento devem **adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.**
> § 1º **A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo,** considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, **especialmente no caso de dados pessoais** sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a **fase de concepção do produto ou do serviço até a sua execução**.
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, **mesmo após o seu término.**
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular **a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.**
> **[...]**
> Art. 49. Os **sistemas utilizados** para o tratamento de dados pessoais devem ser estruturados de forma a atender aos **requisitos de segurança, aos padrões de boas práticas e de governança e aos**

[537] Sobre o tema, ver também o o Art. 13, do Decreto N. 8.771, DE 11 DE MAIO DE 2016, que regulamenta o Marco Civil da Internet: Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de **controle estrito sobre o acesso** aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão **de mecanismos de autenticação de acesso** aos registros, usando, por exemplo, sistemas de **autenticação dupla** para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de **inventário detalhado** dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de **soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados**, como encriptação ou medidas de proteção equivalentes.(grifo nosso).

[538] BRASIL. LGPD. Vide art. 6º, VII.

> **princípios** gerais previstos nesta Lei e às demais normas regulamentares[539]. (grifo nosso)

Nesse sentido, exemplificam-se duas medidas de segurança que os agentes de tratamento podem tomar para garantir maior segurança dos dados pessoais dos clientes: Autenticação de Dois Fatores (*2 Factor Authentication*) e a Autenticação de Multifatores (MFA), que objetivam aumentar a segurança dos dados (pessoais ou não) do titular:

> **AUTENTICAÇÃO DE DOIS FATORES** (*2 FACTOR AUTHENTICATION*) - processo de segurança que exige que os usuários forneçam **dois meios de identificação** antes de acessarem suas contas;
>
> **AUTENTICAÇÃO DE MULTIFATORES (MFA)** - utilização de **dois ou mais fatores de autenticação para concessão de acesso** a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, *tokens*, códigos enviados por SMS, dentre outros); **algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial**, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito)[540]; (grifo nosso)

Em termos práticos, a segurança da informação atua na proteção dos dados pessoais do titular. Nesse sentido, refere a Apple em relação à tecnologia do Face ID[541]:

> Grande parte de nossa vida digital está armazenada no Iphone e no Ipad, e é imprescindível **proteger tais informações**. Assim como o Touch ID revolucionou a autenticação usando a impressão digital, o Face ID a revolucionou usando o reconhecimento facial. O Face ID garante **autenticação intuitiva e segura** e é ativado pelo sistema de câmera TrueDepth de última geração, que usa tecnologias avançadas para mapear a geometria do rosto **com precisão**. [...] O Face ID

[539] BRASIL. LGPD.. Nesse sentido, ver também os principios da prevenção e da responsabilização e prestação de contas: Art. 6º, VIII - VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[540] BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 06 jun. 2022.

[541] SOBRE A TECNOLOGIA AVANÇADA DO FACE ID. APPLE. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2022.

> adapta-se automaticamente às mudanças no visual, como o uso de maquiagem ou barba crescida. [...] Além disso, **funciona em ambientes externos e internos e até mesmo no escuro**. Com o IOS 15.4 e o Iphone 12 ou posterior, o Face ID **funciona até com máscaras**[542]. (grifo nosso)

O Face ID foi desenvolvido para proteger contra falsificação com máscaras ou outras técnicas. O sistema reconhece também a atenção do usuário: " isso dificulta ainda mais que alguém desbloqueie o dispositivo sem que você saiba (caso você esteja dormindo, por exemplo)[543]. De acordo com a empresa, a probabilidade de que outra pessoa aleatória possa desbloquear o dispositivo é menor que 1 em 1.000.000 (usando ou não máscara). A probabilidade estatística é maior[544] para gêmeos e irmãos similares, e entre crianças menores de 13 anos,na medida em que as características faciais distintas ainda não estarem totalmente desenvolvidas. Em caso de preocupação, a Apple sugere adicionar um código para autenticação[545].

Ao contrário da marca que aposta na sua tecnologia, a Samsung não recomenda a utilização do reconhecimento facial dos seus dispositivos[546]:

> Ao usar o reconhecimento facial para desbloquear seu dispositivo, seu **telefone pode ser desbloqueado por alguém ou algo parecido com sua imagem**. [...] No entanto, **existem limitações técnicas para lidar com todas as tentativas de falsificação**, como imagens de alta resolução. Portanto, não recomendados o uso de reconhecimento facial para aplicativos de autenticação de alta segurança**, o reconhecimento facial é menos seguro do que o Padrão, Pin ou Senha**, recomendamos o uso de impressão digital, Padrão, Pin ou Senha para bloquear o dispositivo. (grifo nosso).

Caso o cliente opte pelo uso do reconhecimento facial, a empresa refere que a utilização de acessórios e máscara pode afetar o processo de reconhecimento, a área

[542] De acordo com a Apple, "os dados do Face ID, incluindo representações matemáticas do rosto, são criptografados e protegidos por uma chave disponível apenas para o Secure Enclave". SOBRE A TECNOLOGIA AVANÇADA DO FACE ID. APPLE. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2022.

[543] SOBRE A TECNOLOGIA AVANÇADA DO FACE ID. APPLE. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2022.

[544] Não foi divulgado o percentual aproximado.

[545] SOBRE A TECNOLOGIA AVANÇADA DO FACE ID. APPLE. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2022.

[546] TUDO O QUE VOCÊ PRECISA SABER SOBRE O DESBLOQUEIO COM RECONHECIMENTO FACIAL EM SEU SMARTHPONE. SAMSUNG. Disponível em: https://www.samsung.com/br/support/mobile-devices/tudo-que-voce-precisa-saber-sobre-o-desbloqueio-com-reconhecimento-facial-em-seu-smartphone/. Acesso em 16 jun. 2022.

deve estar iluminada, a lente do dispositivo limpa e o dispositivo só reconhece o rosto se os olhos estiverem abertos[547].

Ademais, a normativa em análise refere que a garantia da prevenção à fraude e a segurança do titular se dê nos processos de identificação e autenticação de cadastro em sistema eletrônico. Merece destaque o apontamento de Mullholand:

> Por processos de **identificação e autenticação** em sistemas eletrônicos compreendem-se todos os meios disponibilizados de forma **eletrônica ou digital** que permitam tecnicamente a **identificação do titular de dados** – por exemplo, do uso de identificadores por radiofrequência (RFID) ou biometria -, e que concedam **veracidade aos dados pessoais**, por meio de processos **de reconhecimento e verificação de procedência daqueles dados** – por exemplo, de uso de criptografia e tecnologia *blockchain*. (grifo nosso).[548]

Assim, cumpre referir a essencialidade de o processo de identificação e autenticação se dar por meio eletrônico ou virtual (sistema eletrônico). .Mulholland exemplifica – como já mencionado; onde seria possível encontrar esses processos de identificação e autenticação em sistemas eletrônicos: "sistemas de vigilância por meio de câmeras de filmagem instalados em ônibus, condomínios e elevadores; nos sistemas de identificação de por meio de biometria utilizados em bancos [...], no uso de tecnologia de reconhecimento facial em aparelho de telefonia celular;"[549]. Outros exemplos prático apontados por Chiara Teffé e MarioViola:

> Instituições bancárias e empregadores podem tratar dados biométricos para prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de **confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancára por meio de um caixa eletrônico**, por exemplo. Adicionalmente, pode-se mencionar a exigência para **atendimento médico-hospitalar**, com a **utilização de seguro ou plano de assistência à saúde, que o segurado/beneficiário coloque seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que**

[547] TUDO O QUE VOCÊ PRECISA SABER SOBRE O DESBLOQUEIO COM RECONHECIMENTO FACIAL EM SEU SMARTHPONE. SAMSUNG. Disponível em: https://www.samsung.com/br/support/mobile-devices/tudo-que-voce-precisa-saber-sobre-o-desbloqueio-com-reconhecimento-facial-em-seu-smartphone/. Acesso em 16 jun. 2022.

[548] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p.148

[549] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p.148-149

> **outra pessoa utilize a cobertura securitária em seu lugar.(**grifo nosso)[550]

Merece destaque o fato de que "estaria legitimado o tratamento de dados sensíveis com *dispensa do consentimento* do titular se, *e somente se*, esse tratamento beneficiasse diretamente o titular dos dados, demonstrando, no caso, a necessidade de proteção qualificada de sua *vulnerabilidade*"[551]. Justificando assim, a complementaridade normativa da alínea g) quando dispõe: **"**resguardados os direitos mencionados no **art. 9º desta Lei** e exceto no caso de prevalecerem **direitos e liberdades fundamentais do titular** que exijam a proteção dos dados pessoais"[552]. O art. 9 da LGPD assim consta:

> Art. 9º O titular tem **direito ao acesso facilitado** às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma **clara, adequada e ostensiva** acerca de, entre outras características previstas em regulamentação para o atendimento do **princípio do livre acesso:**
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (grifo nosso). [553]

---

[550] TEFFÉ, Chiara Spadacccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com.** a.9.n.1. 2020. P. 1-39, p. 32. Disponível em: https://www.academia.edu/42993125/Tratamento_de_dados_pessoais_na_LGPD_estudo_sobre_as_bases_legais. Acesso em: 20 jun. 2022.

[551] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p.149

[552] Vide art. 11, II, g. LGPD. BRASIL.

[553] BRASIL. LGPD. Art. 9º; Ver também artigo 18: Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

Portanto, em caso de eventual "colisão entre os interesses de segurança e de prevenção de fraude no tratamento de dados e a proteção de direitos e de liberdades fundamentais do titular de dados que requeiram a sua tutela, esta deve prevalecer". Para Mulholland, esta exceção específica "parece servir como um reforço argumentativo para a proteção do titular de dados e de sua condição de vulnerabilidade". Assim sendo, quando da colisão de direitos, sendo que de um lado "encontram-se tutelados direitos fundamentais de pessoa vulnerável, estes devem ser privilegiados, em conformidade com os ditames constitucionais", justamente para fins de "[...] fortalecer o respeito aos direitos fundamentais e impedir o tratamento de dados sensíveis qualificado por sua abusividade e ilegitimidade"[554].

Mas, questiona-se como seria feita a ponderação. Seria possível utilizar – de fato, o reconhecimento facial apenas com interesse focado no próprio titular? A previsão autorizativa de dispensa de consentimento da normativa em análise não retiraria o caráter de autodeterminação informativa do titular? A seguir, busca-se responder algumas das perguntas.

2.5 Desafios, alternativas e metodologias orientativas

Diante dos fatores apresentados e da análise breve do artigo, o presente tópico busca responder os seguintes questionamentos: (a) Se for considerada eficaz e/ou segura se justificaria a utilização do reconhecimento facial consoante aliena g? (b) Há alternativas possíveis que não o uso de biometria facial? (c)Que metodologias ou

---

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador. § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

[554] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156, p.150

propostas podem ser elencadas para mitigar riscos no uso do reconhecimento facial quando da alínea g, Art. 11, II?

Como visto anteriormente, o reconhecimento facial tem sido aplicado em diferentes áreas sob diferentes justificativas e finalidades. Já abordado que há vários fatores que desafiam o reconhecimento automatizado de rostos, como variações de pose, e iluminação [555], o que impede com que seja uma tecnologia 100% eficaz[556] – há erros. Este fato precisa ser encarado de forma séria. Os índices de acurácia se, benéficos - "acurácia positiva"; geram consequências positivas, como liberação de passagem em determinadas zonas, liberação de benefício ao confirmar a identidade de um sujeito. Entretanto, é preciso também atentar-se para os percentuais de erro.

Ao se observar a parte do percentual que gera erros – "acurácia negativa"; são geradas consequências negativas, seja permitindo com que um sujeito cometa uma fraude em nome de outro, negando benefício a cidadão que tem direito, privando alguém de liberdade – o mais grave.

A tecnologia deve ter um papel em prol do benefício da sociedade, devendo ser usada com cautela e sob risco de ameaça aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[557]. Haja vista o potencial discriminatório de um sistema de reconhecimento facial, é preciso aceitar que antes que seja implementada em múltiplas áreas (como já vem sendo feita), é necessário voltar um passo e repensar sobre a sua utilização, ainda mais nos caos em que ausente o consentimento do titular – Art. 11, ii, g).

---

[555] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik. Introduction to Biometrics. New York:Springer, 2011, p. 98;ver capítulo 1

[556] Estudos trazidos no capítulo 1: NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. United States Department of Commerce. 2020. Disponível em: https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report_6b.pdf. Acesso em: 01 fev. 2022; NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6A: Face Recognition accuracy with masks using pré-COVID-19 algorithms. . United States Department of Commerce. 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf. Acesso em: 01 fev. 2022. NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015, p. 8; BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018. Disponível em: https://damprod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf. Acesso em 05 fev. 2022,; MUTHUKUMAR, Vidya; PEDAPATI, Tejaswini; RATHA, Nalini; SATTIGERI, Prasanna; WU; Chai-Wah; KINGSBURY, Brian; KUMAR, Abhishek; THOMAS, Samuel; MOJSILIVIC, Aleksandra; VARSHNEY, Kush. Understanding Unequal Gender Classification Accuracy from face Images. 2018. Disponível em: https://arxiv.org/pdf/1812.00099.pdf. Acesso em 08 fev. 2022., p. 2

[557] Como bem assevera o Art. 2º, VII, da LGPD. BRASIL. LGPD.

Ana Frazão alerta para o fato de que "empresas de tecnologia e seus programadores estão desenhado [...] sistemas e podem estar fazendo isso em prol dos seus próprio interesses". Nesse sentido, "não raro os programadores constroem sistemas algorítmicos sem conhecer as peculiaridades e as intenções dos usuários e sem considerar vários dos possíveis resultados práticos". A autora entende que o "próprio ecossistema de criação de modelos algorítmicos tem se mostrado bastante falho, pois tais sistemas estão sendo planejados sem o devido cuidado, sem as necessárias preocupações éticas e jurídicas por parte de programadores e empresas de tecnologia"[558]. O apontamento da autora é fundamental para a questão: se se entender eficaz e/ou segura se justificaria a utilização do reconhecimento facial consoante aliena g? – mesmo levando em conta potencial risco discriminatório e de privação de liberdade? A própria normativa analisada preconiza, em segundo momento esta hipótese: "resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"[559].

Uma questão é certa: é preciso um exercício de ponderação, em que não bastaria determinar a viabilidade ou eficácia – ainda se estaria a debater critérios de utilização. Entende-se que o papel orientador e educativo deve ser iniciado por sujeitos neutros, sem vieses comerciais ou interesses, como a ANPD e a SENACON.

Consoante o Guia de Boas Práticas da Lei Geral de Proteção de Dados do Governo Federal, para enquadramento na hipótese do art. 11, II, g) "deve-se avaliar se não há outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis.". Por exemplo, "deve-se avaliar se não há outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis"[560]. Portanto, questiona-se se não há alternativas possíveis que não o uso de biometria facial? Se sim, qual(is)? Cumprem o mesmo papel? São mais ou menos seguras que o reconhecimento facial?;

Primeiramente, é preciso relembrar quais são as características biométricas mais comuns que foram mencionadas no capítulo 1º - sem levar em consideração o

[558] FRAZÃO, Ana. Discriminação algorítmica: a responsabilidade dos programadores e das empresas. JOTA. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-a-responsabilidade-dos-programadores-e-das-empresas-14072021. Acesso em: 10 jun. 2022.
[559] Vide Art. 11, II, g. BRASIL. LGPD.
[560] GOVERNO FEDERAL. Guia de boas práticas – Lei Geral de Proteção de Dados (LGPD), p.1-69, p. 28.. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 20 jun. 2022.

reconhecimento facial; (a) impressão digital (*fingerprint*); (b) impressão da palma (*palmprint*), (c) íris (*iris*); (d) voz (*voice*). A seguir, brevemente os seus desafios em caso de uso alternativo ao reconhecimento facial.

Assim sendo, em relação à impressão digital, como já abordado anteriormente, o padrão único biométrico pode ser danificado temporariamente, em caso de lesões superficiais na área ou, excepcionalmente, de forma definitiva, em danos mais profundos[561]. Ainda, a tecnologia pode ser contornada com métodos que copiam ou replicam impressões digitais, como o dedo de outra pessoa ou o dedo de um sujeito que está dormindo ou inconsciente[562].

No que tange à impressão da palma, a área a ser captada é maior – o que faz com que a imagem obtida tenha mais distinção, como linhas e rugas. .Por consequência, há a necessidade de um dispêndio maior de investimento tecnológico em *scanners*, não sendo tão conveniente o seu uso quando comparado com a impressão digital, por exemplo.[563]

O Iris é um órgão interno que se encontra bem protegido e, por isso, a probabilidade machucados possam influenciar na digitalização é baixa. Ainda, possui um nível grande de aleatoriedade entre os indivíduos. Mas, em que pese seja teoricamente mais específica, a captura da Iris ainda é recente e requer melhorias. O método normalmente requer uma posição próxima do titular e uma boa iluminação, o que pode dificultar a sua extensão em larga escala[564].

Quanto ao reconhecimento de voz, é uma característica também única de cada indivíduo, sendo possível, inclusive, que haja a distinção entre gêmeos idênticos, por exemplo. Vale ressaltar que, em que pese a biometria de voz seja mais segura que senha – "pois não há como fraudadores conseguirem informações da vítima, através de engenharia social, para aplicar golpes com esse tipo de segurança"; sugere-se a sua utilização em conjunto com outros fatores de autenticação, como outras tecnologias

---

[561] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik. Introduction to Biometrics. New York:Springer, 2011,p. 62

[562] 5 POPULAR TYPES OF BIOMETRIC AUTHENTICATION: PROS AND CONS. PHONEXIA. Disponível em: https://www.phonexia.com/blog/5-popular-types-of-biometric-authentication-pros-and-cons/. Acesso em: 10 jun. 2022.

[563] JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik. Introduction to Biometrics. New York:Springer, 2011, p. 85; JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik. Introduction to Biometrics. New York:Springer, 2011, p. 31; 85

[564] 5 POPULAR TYPES OF BIOMETRIC AUTHENTICATION: PROS AND CONS. PHONEXIA. Disponível em: https://www.phonexia.com/blog/5-popular-types-of-biometric-authentication-pros-and-cons/. Acesso em: 10 jun. 2022.

biométricas ou outros dados[565]. Ainda, pontua-se que lugares barulhentos (situação externa) e também variações na voz do titular, como doenças respiratórias, rouquidão (situação do titular) podem prejudicar a identificação [566].

Tendo sido pontuadas resumidas desvantagens das outras tecnologias biométricas, é relevante balancear se as consequências negativas de cada qual são, em certa medida, melhores, do que as relativas ao reconhecimento facial, permitindo uma proposição de substituição equivalente ou, se se entender pela impossibilidade substitutiva: há uma melhor alternativa? Destaca-se que, dentre as tecnologias em análise, o reconhecimento facial é a única que pode ser obtida à longa distância do titular e também de forma encoberta. Este fato pode ser visto como algo benéfico ou temerário.

De igual sorte, um ponto que merece relevo é: se o *reconhecimento facial pode ser substituído*[567], de fato, não é realmente necessária a sua utilização – princípio da necessidade. Entretanto, tal premissa parte da perspectiva de que existiria uma forma substitutiva em geral, sendo que, no caso concreto, seria necessário *ponderar a substituição*: no âmbito penal em se tratando de privação de liberdade não valeria a pena uma alternativa mais segura, por exemplo? Depreende-se, portanto, que a possibilidade ou não de substituição não dependeria *apenas* de outra tecnologia biométrica, mas também da finalidade proposta, da acurácia do sistema, do nível de investimento tecnológico[568] e, também, do próprio titular em cooperar – não adianta concluir pelo reconhecimento facial como melhor opção se os titulares não possuem uma aceitação da

[565] ALBUQUERQUE, Karol. Descubra mitos e verdades sobre a biometria de voz. OLHAR DIGITAL. Disponível em: https://olhardigital.com.br/2022/03/09/tira-duvidas/descubra-mitos-e-verdades-sobre-a-biometria-de-voz/. Acesso em: 12 jun. 2022

[566] 5 POPULAR TYPES OF BIOMETRIC AUTHENTICATION: PROS AND CONS. PHONEXIA. Disponível em: https://www.phonexia.com/blog/5-popular-types-of-biometric-authentication-pros-and-cons/. Acesso em: 10 jun. 2022.

[567] O que leva justamente à pergunta: Por que as outras tecnologias biométricas foram substituídas pelo reconhecimento facial?

[568] Nesse sentido: " o quadro jurídico aplicável ao tratamento de dados biométricos através do reconhecimento facial deve, em complemento aos elementos mencionados no ponto 1, contemplar e abordar: - as diferentes fases da utilização das tecnologias de reconhecimento facial, incluindo a criação de bases de dados e as fases de implantação; - os setores em que essas tecnologias são utilizadas; - a intrusão de tipos de tecnologias de reconhecimento facial, como tecnologias de reconhecimento facial ao vivo ou não, fornecendo orientações claras sobre a legalidade". Tradução livre do autor. COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021, p. 5. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022.

tecnologia, não cooperam no fornecimento da face em frente ao sistema, dentre outras situações passíveis de ocorrer[569].

Nesse sentido, entende-se pela impossibilidade de substituição do reconhecimento facial por outra tecnologia, *em regra*. Mas, elenca-se a seguir metodologias e propostas para mitigar riscos no uso do reconhecimento facial quando da alínea g, Art. 11, II.

Indaga-se: há alguma regra, normativa, proposta sobre o reconhecimento facial (e, em específico que abrangeria a especificidade do art. 11, ii, g)? Tem alguma legislação que permite ou bane? Brevemente observam-se os campos público e privado. Quando para os fins exclusivos de segurança, defesa e relacionados ao âmbito penal, a LGPD não se aplica se o tratamento de dados por para a finalidade exclusiva de investigação e repressão de infrações penais[570]. A própria normativa, em seu art. 4º, §1º, estabelece que a matéria seja redigida por *legislação específica*, a qual "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular".

Assim, quando dos casos dispostos na exceção, requer-se análise do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, primeira iniciativa sobre a matéria. Sobre Assim, previsto no art. 5º, XIX, da LGPD penal[571], visa "instruir o processo legislativo acerca da *autorização para a utilização de tecnologias de vigilância* e o tratamento de dados pessoais por autoridades competentes que implique elevado risco aos direitos, liberdades e garantias dos titulares dos dados".

Por fim, quanto à segurança pública, o art. 43 preconiza sobre a *proibição* da utilização de tecnologias de vigilância com técnica que permita a "identificação de pessoas indeterminadas *em tempo real e de forma contínu*a quando não houver a

[569] Relembre a pesquisa mencionada no capítulo 1º: ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facialrecognition-technology/ . Acesso em 03 mar. 2022,

[570] "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou **d) atividades de investigação e repressão de infrações penais**; [...] (grifo nosso). BRASIL. LGPD.

[571] BRASIL. ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 20 mai. 2022.

conexão com a atividade de persecução penal individualizada e *autorizada* por lei e decisão judicial"[572].

No âmbito federal, aponta-se o *Projeto de Lei* nº572, de 2021[573], que visa alterar a Lei nº13.812, de 16 de março de 2019 e cria o Banco Nacional de Dados de Reconhecimento Facial e Digital, "com a finalidade de auxiliar na prevenção e localização de crianças e adolescentes desaparecidos"[574]. Para atingir esta finalidade, "os órgãos de identificação podem captar as imagens para reconhecimento facial e digital de todos os menores de dezoito anos por ocasião da identificação ou expedição da segunda via da carteira de identidade"[575].

Pontua-se também o *Projeto de Lei* nº 6197, de 2019[576], cujo objetivo é a criação de um banco nacional de face, íris e voz, assim como a previsão de instalação de câmeras para reconhecimento facial em locais públicos. O documento, em seu art. 3º, também identifica que a tecnologia de *reconhecimento facial e emocional trata-se de dado pessoal sensível*. Ademais, interessante a previsão constante no art. 7º: "Os agentes que apliquem ou utilizem as tecnologias de que trata esta Lei [...], devem sinalizar o uso ou aplicação, de forma clara e visível". Ainda, quando em local aberto ou público, o §3º deste artigo dispõe que deverá existir uma sinalização "visível e clara aos transeuntes do local"[577]. Ainda, o *Projeto de Lei* n. 9736, de 2018, que visa alterar a Lei de Execução Penal (LEP – Lei 7.210/84) para tornar obrigatória a identificação por

[572] BRASIL. ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 20 mai. 2022.

[573] BRASIL. Projeto de Lei nº 572, de 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1966599&filename=PL+572/2021. Acesso em: 20 jun. 2022.

[574] Vide art. 5º-A. BRASIL. Projeto de Lei nº 572, de 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1966599&filename=PL+572/2021. Acesso em: 20 jun. 2022.

[575] Vide Art. 5º- A, §1º. Ver também: § 2º Os instrumentos de que trata o § 1º devem permitir comparações analíticas de projeção de envelhecimento do indivíduo, além de incluir as bases de dados existentes, de forma a possibilitar resultados múltiplos. § 3º Aplica-se o disposto nos arts. 4º e 5º ao banco de dados referido no caput, devendo ser imediatamente integrados ao Cadastro Nacional de Pessoas Desaparecidas os dados de pessoa dele constantes na hipótese de desaparecimento. (NR)". BRASIL. Projeto de Lei nº 572, de 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1966599&filename=PL+572/2021. Acesso em: 20 jun. 2022.

[576] BRASI.. Projeto de Lei nº 6197, de 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8049424&ts=1630439166989&disposition=inline. Acesso em 20 set, 2021.

[577] BRASI.. Projeto de Lei nº 6197, de 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8049424&ts=1630439166989&disposition=inline. Acesso em 20 set, 2021.

reconhecimento facial de todo preso que ingressar em estabelecimento penal[578]. No mesmo ano, o *Projeto de Lei* n. 4612, de 2019[579], que dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos.

Já na seara estadual, pontua-se a *Lei* nº 6.712, de 10 de novembro de 2020, do Distrito Federal[580]. Esta lei dispõe acerca do uso de tecnologia de reconhecimento facial[581] – TRF na segurança pública e dá outras providências.[582] Posteriormente, no art. 3º, há a vedação de utilização desta tecnologia para vigilância contínua, independentemente se for de um indivíduo ou grupo[583]. Ainda, no Estado da Paraíba foi editada a *Lei* n. 11858, de 25 de março de 2021, que obriga o aviso sobre reconhecimento facial em estabelecimentos comerciais. Em relação a projetos de lei sobre a matéria em âmbito estadual, no Rio de Janeiro, foi elaborado o *Projeto de Lei* n.1033/2019[584], que dispõe sobre o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos. Em São Paulo, destaca-se o *Projeto de Lei*

---

[578] BRASIL Projeto de Lei nº 9736, de 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1643053. Acesso em: 20 jun. 2020.

[579] BRASIL. Projeto de Lei nº. 4612, de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1794019&filename=PL+4612/2019. Acesso em 11 jun. 2022.

[580] BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022. Ver também: REIS, Carolina. Nota Técnica Lei 6.712/20. 10 recomendações para o uso de reconhecimento facial para segurança pública no DF. Laboratório de Políticas Públicas e Internet – LAPIN. 2021. Disponível em: https://lapin.org.br/2021/02/22/nota-tecnica-lei-distrital-6712-2020-df/. Acesso em: 20 abr. 2022.

[581] "Art. 2º Para os efeitos desta Lei, considera-se: I – tecnologia de reconhecimento facial: a tecnologia que analisa as características faciais usada para a identificação pessoal exclusiva de indivíduos em imagens estáticas ou em vídeos; II – vigilância contínua: a utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem, durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos." BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022

[582] BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022

[583] BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022

[584] BRASIL. Projeto de Lei n. 1033, de 2019. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/f7745acb22d37589032586390074cefb?OpenDocument&Highlight=0,1033. Acesso em: 10 jun 2022.

nº865, de 2019[585], que torna obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, bem como no interior dos vagões das composições[586].

Por fim, observa-se que, ausente em *âmbito nacional* – ainda; legislação sobre a matéria. Os projetos de lei em andamento podem auxiliar para uma melhor compreensão na regulamentação da matéria, mas vislumbra-se uma fragilidade: não se sabe se serão aprovados e, se o forem, quando passarão a vigorar como lei. Ainda, o tema do reconhecimento facial possui uma particularidade inerente: pode adentrar em várias esferas: consumidor, administrativo, cível, penal., etc., sendo que a criação de projetos de leis esparsos em diferentes assuntos pode prejudicar a regulamentação da matéria, tanto se tratando de quem pretende utilizar a tecnologia no âmbito empresarial ou público, quanto para a proteção dos titulares (e também de sua autodeterminação informativa). Mas, seria necessária, de fato, uma normativa específica para a regulação desta tecnologia, quiçá seria interessante uma normativa tratando especificamente de dados pessoais sensíveis, ou, ainda, se se entender pela desnecessidade de numerosas regulações esparsas - como os projetos de lei específicos; se não seria o caso de apoiar-se no diálogo das fontes[587] e construir casuisticamente uma solução no caso concreto com base nos princípios constitucionais e de proteção de dados (enraizados antes mesmo da LGPD).

O cenário brasileiro aponta: o reconhecimento facial é utilizado[588] e não deixará de o ser. O fato é que, no que tange à norma analisada (art. 11, II, g), será utilizada sem o consentimento - como bem respaldado em legislação; sendo necessárias melhores orientações, sob pena de regressão à proteção dos direitos dos titulares adquiridos desde a publicação da LGPD (e normas anteriores setoriais de proteção de dados nacionais). Nesse sentido, o cenário ideal seria a criação de guias orientativos ou norteadores, seja

[585] BRASIL. Projeto de Lei nº. 865, de 2019. Disponível em: https://www.al.sp.gov.br/propositura/?id=1000278098. Acesso em: 16 jun. 2022.

[586] Veja a Nota Técnica escrita pelo opinando pelo veto ao PL 885/2019 SP, alegando ser inconstitucional e contrário ao interesse público: NOTA TECNICA PL N. 885/19. LAPIN, Laboratório de Políticas Públicas e Internet; ACESS NOW; ITS RIO, Instituto de Tecnologia e Sociedade do Rio. Disponível em: https://itsrio.org/wp-content/uploads/2021/03/Nota-tecnica-PL-865-2019.pdf. Acesso em: 10 jun. 2022.

[587] Para compreender o tema, ver: MARQUES, Claudia Lima. Diálogo das fontes: do conflito à coordenação de normas no direito brasileiro. São Paulo: RT, 2021

[588] Em relação ao videomonitoramento, até maio de 2019, foram, pelo menos, 48 casos publicamente reportados de implementação da tecnologia por autoridades públicas. IGARAPÉ. Infográfico: Reconhecimento facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 05 jul. 2022.

pela própria Autoridade Nacional de Proteção de Dados – ANPD[589], seja por órgãos de proteção ao consumidor, como a Secretaria Nacional do Consumidor – SENACON[590].

Imprescindível a menção de que o objetivo não seria substitutivo à legislação – por óbvio; mas complementativo. Inclusive, o próprio documento Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas[591] refere que a publicação "não busca apresentar um guia jurídico para a implantação do reconhecimento facial, nem tem a pretensão de exaurir as leis potencialmente cabíveis à atividade"[592]. É preciso que

> [...] se avance no debate sobre os **riscos e os impactos decorrentes da adoção do reconhecimento facial, não só no âmbito governamental, mas também em suas aplicações pelo setor privado.** Isso porque se, por um lado, para esses atores privados, o reconhecimento facial pode **viabilizar inovações nas formas de identificação e relacionamento com os consumidores, por outro, apresenta uma série de desafios** em relação, entre outros, ao seu **potencial discriminatório**, às questões relativas à **transparência** e ao **consentimento,** ao impacto sobre a **privacidade** e a **segurança** das informações e imagens coletadas. (grifo nosso)[593].

Até porque, além dos objetivos de verificar/autenticar e identificar um sujeito, o reconhecimento facial também vem sendo utilizado para *categorização*, por exemplo, para reconhecer " (i) estados psicológicos (emoções básicas, orientação da cabeça e dos olhos), (ii) características sociodemográficas (gênero, idade, etnia) e (iii) reações dos clientes à loja (quantidade de tempo despendido na loja ou com determinado produto, locais que determinado cliente visitou etc.)"[594]. É o caso da Hering *Experience* e também da ViaQuatro.

---

[589] Ver mais sobre: GOVERNO FEDERAL. ANPD. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 10 jun. 2022. A ANPD já publicou guias orientativos, como: Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público; Guia Orientativo da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral

[590] Ver: GOVERNO FEDERAL. SENACON. Como proteger seus dados pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 12 jun. 2022.

[591] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020

[592] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020, p. 36

[593] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020, p. 23

[594] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020, p. 32

É necessário entender o quis o legislador com a inclusão do art. 11, II, g: para que seja possível a aplicação de sanções e multas, quando se entender pela violação da lei em direitos fundamentais e às liberdades, que se possa compreender o motivo de ter errado, e onde pode ser melhorado.

Ciente de que inexistem diretrizes a serem seguidas em relação ao reconhecimento facial na esfera nacional de proteção de dados, é preciso que, ao menos, minimamente sejam cumpridos os seguintes princípios previstos na LGPD, quando o tratamento envolver esta tecnologia: (a)finalidade; (b) transparência; (c) necessidade; e (d) não discriminação. De acordo com Chiara Teffé e Mario Viola:

> O tratamento de dados sensíveis é possível e, inclusive, pode ser necessário em determinadas circunstancias. Contudo, **deverá ser pautado estritamente nos ditames legais, pela relevância dos valores em questão, e legitimado apenas quando tal tratamento não servir para a realização de discriminações ilícitas ou abusivas**[595]. (grifo nosso)

Não só. Seguir alguns princípios da legislação não torna a organização preparada para atuar com complexa tecnologia. É preciso mais. Além de medidas mitigatórias, é necessário ainda um planejamento pró-ativo. Outro norteador, é a sugestão de elaboração do Relatório de Impacto à proteção de dados pessoais (DPIA)[596], considerado "um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição"[597]. Assim é disposto o tema no art. 5º da LGPD:

> XVII - relatório de impacto à proteção de dados pessoais: **documentação do controlador** que contém a **descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentai**s, bem como

[595] TEFFÉ, Chiara Spadacccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com.** a.9.n.1. 2020. P. 1-39, p. 37. Disponível em: https://www.academia.edu/42993125/Tratamento_de_dados_pessoais_na_LGPD_estudo_sobre_as_bases_legais. Acesso em: 20 jun. 2022.

[596] No Regulamento Geral de Proteção de Dados europeu (GDPR – 2016/679) a nomenclatura do documento é é *Data Protection Impact Assesment* (DPIA). Ao longo do Regulamento, encontra-se menções ao DPIA: ((84); (89); (90); (91); (92); (93); (94)) e, ainda, possui artigo específico para tal, qual seja, o Artigo 35. A LGPD refere como Relatório – e não Avaliação, como a legislação europeia. Em que pese a diferença de nomenclatura, não há diferença prática.

[597] GOVERNO FEDERAL. Guia de boas práticas – Lei Geral de Proteção de Dados (LGPD), p.1-69, p. 30. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 20 jun. 2022.

> **medidas, salvaguardas e mecanismos de mitigação de risco**;[598] (grifo nosso)

Em que pese a LGPD não aborde o relatório de impacto mais detalhadamente[599] – ao contrário do RGPD[600]; vale mencionar que a palavra *risco* é mencionada 11 (onze) vezes na normativa brasileira. Igualmente não há a descrição de risco, o tratamento de dados pessoais será *irregular* "quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradasas circunstâncias relevantes, entre as quais [...] o resultado e os *riscos que razoavelmente dele se esperam"*[601].

Em síntese, a LGPD dispõe que a ANPD *poderá* requerer o relatório de impacto: (i) a agentes do *Poder Público* (art. 32); (ii) quando o tratamento de dados possuir como

---

[598] BRASIL. LGPD. Ver também o Art. 10, §3º; Art. 38 caput e parágrafo único, da LGPD.

[599] Vale referir que o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal tece algumas considerações sobre o tema: "Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados"; "Art Art. 42. A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância. § 1º Para fins de avaliação do risco, deve-se considerar, pelo menos: I - a natureza dos dados pessoais envolvidos; II - as finalidades específicas do tratamento; III - a quantidade de agentes de tratamento de dados envolvidos; IV - a quantidade de titulares de dados potencialmente atingidos; V - se é utilizado algum tipo de nova tecnologia; VI - a possibilidade de tratamento discriminatório; e VII - as expectativas legítimas do titular de dados.". BRASIL. ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 20 mai. 2022. Ver também: COMENTÁRIOS AO ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA A SEGURANÇA PÚBLICA: TECNOLOGIA DE RECONHECIMENTO FACIAL. ITS. LEMOS, Alessandra, et al.2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf. Acesso em: 15 jun. 2022.

[600] A normativa europeia possui um artigo específico sobre o tema (data protection impact assessment - DPIA) – Art. 35 do RGPD; no qual constam determinados elementos, como a obrigatoriedade da avaliação e quem deverá elaborar. Segundo o RGPD, a elaboração do DPIA não é obrigatória sempre, somente nos casos em que: houver um alto risco aos direitos e liberdades das pessoas naturais. Diante da ausência de maiores explicações sobre o significado de alto risco na legislação de proteção de dados europeia, o European Data Protection Board – EDPB (antigo Article 29 Data Protection Working Party) elaborou um documento indicando diretrizes. De acordo com a publicação, é considerado alto risco as seguintes atividades: i) avaliação ou pontuação, envolvendo a criação de perfis; (ii) **decisões automatizadas** com efeito legal ou semelhante; (iii**) monitoramento sistemático**, cujo intuito é observar, monitorar ou também controlar os titulares; **(iv) dados sensíveis ou altamente pessoais; (v) dados processados em larga escala,** considerando-se o número de titulares envolvidos, volume de dados, duração e a extensão geográfica da atividade de processamento; (**vi) correspondências ou combinação de bases de dados;** (vii) **titulares de dados vulneráveis**, como crianças, funcionários, idosos**; (viii) inovação ou aplicação de soluções tecnológicas** ou organizacionais e; (ix) o processamento impede o exercício de um direito, serviço ou contrato. (grifo nosso). ARTICLE 29 DATA PROTECTION WORKING PARTY. . **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a "high risk" for the purposes of Regulation 2016/679.** Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.Acesso em:02 jun. 2022, p. 9-10.

[601] BRASIL. LGPD. Vide art. 44, II.

fundamento o *interesse legítimo do controlador* (art. 10, §3º); e (iii) a pedido da ANPD, referente às operações de tratamento de dados**,** *inclusive de dados pessoais sensíveis* (art. 38)[602] . Sugere-se a elaboração do RIPD quando, no tratamento de dados pessoais sensíveis, houver reconhecimento facial[603] - sem consentimento (Art. 11, G, II)[604].

Em que pese o direcionamento seja optar pelo *privacy by design*[605] – RIPD desde o tratamento de dados da organização; sabe-se que nem sempre isso será possível. Neste caso, adota-se a opção da *privacy by default*.

Válido também a exigência de exigir um comportamento reativo. Questiona-se se, em caso de algum incidente de segurança[606] envolvendo os dados pessoais sensíveis coletados pelo reconhecimento facial, o mesmo deve ser o protocolo quando de dados pessoais[607]. A ANPD refere:

> **Em que situação e o que comunicar ao titular dos dados?**
> Sempre que o incidente de segurança possa acarretar um risco ou dano relevante aos titulares afetados.

---

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

[603] As entidades que utilizarem reconhecimento facial precisam realizar avaliação de impacto antes do processamento de dados, na medida em que há o processamento de dados biométricos e apresenta riscos elevados para os direitos fundamentais dos titulares dos dados. COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022., p. 14

[604] Sobre a elaboração de RIPD e reconhecimento facial, ver: MENKE, Fabiano; LEVENFUS, Sílvia. O reconhecimento facial no setor público e a proteção de dados pessoais. CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves; RAMOS, Rafael (orgs.). Lei Geral de Proteção de Dados e o poder público. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena, 2021.

[605] Ver mais sobre o tema em: CAVOUKIAN, Ann. **The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices** [s.l]; [s.d.], p 1- 12. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf Acesso em 14 abr. 2021.

[606] Entende-se incidente de segurança por: "qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais." GOVERNO FEDERAL. **Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 13 jun. 2022.

[607] AANPD refere o que deve ser feito em um incidente envolvendo dados pessoais, quem deve fazer a comunicação do incidente, em que situação e o que comunicar ao titular, qual o prazo para comunicar um incidente , como comunicar para a ANPD. GOVERNO FEDERAL. **Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 13 jun. 2022

> **Critérios mais objetivos serão objeto de futura regulamentação e não poderão ser aqui exigidos sob pena de se inovar na LGPD.** De toda forma, pode-se extrair da lei que a **probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis** ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, **ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes** financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados. (grifo nosso)[608]

Por fim, o que se observa é a despreparação do campo jurídico normativo e regulatório brasileiro para tratar tema tão sério que é o reconhecimento facial. É o que aponta Bruno Bioni e Maria Luciano: " [...] diante da experiência estrangeira e do que foi mapeado em termos regulatórios de tecnologias de reconhecimento facial, a lei geral brasileira de proteção de dados/LGPD apresenta um modelo fraco e janelas muito incipientes para a construção de um modelo de governança".[609] Veja-se:

> Diante desse novo cenário de adoção progressiva e iminente de uma ferramenta que ainda apresenta tantos riscos, surge a necessidade de se pensar uma regulação eficiente que permita, ao mesmo tempo, o uso responsável e a garantia da preservação de direitos[610].

Assim sendo, o que se verifica na atualidade é que inexiste uma regulação[611] ou orientação geral autorizando tacitamente - ou banindo; o uso do reconhecimento facial. Justamente por isso, alguns Estados brasileiros tiveram iniciativas para regular a

---

[608] GOVERNO FEDERAL. **Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 13 jun. 2022

[609] BIONI, Bruno Ricardo. LUCIANO, Maria. Princípio da precaução como vetor de regulação de Inteligências Artificial: seriam as leis de proteção de dados pessoais o seu portal de entrada? In Inteligências Artificial (Organizadores Caitlin Sampaio et al). Rio de Janeiro, 2019, p. 207-231, p. 222.

[610] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé. Data Privacy BR. 2020, p. 2-3. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

[611] Ver também: TEFFÉ, Chiara Spadaccini; FERNANDES, Elora Raad. Reconhecimento facial: laissez-faire, regular ou banir? Migalhas. 2020. Disponível em: Reconhecimento Facial: laissez-faire, regular ou banir? - Migalhas. Acesso em: 22 jun. 2022.

tecnologia, no mesmo sentido do cenário americano (ainda que em uma direção oposta, no qual há uma autorização para uso e as regulações cumprem o âmbito federal)[612]

Não se pode olvidar que a "disciplina de proteção de dados pessoais diz respeito a uma matéria em constante evolução e que o ordenamento jurídico brasileiro deve ficar atento para os desenvolvimentos tecnológicos que cotidianamente alteram a vida dos cidadãos [...]"[613], quiçá o tema do reconhecimento facial.

[612] RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituito Igarapé. Data Privacy BR. 2020, p. 18. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

[613] DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da Nova Lei Geral de Proteção de Dados brasileira. In: CAVALLI, Olga; BELLI, Luca. Governança e regulações da internet na América Latina:. p. 309 – 325, 2019. Disponível em: . Acesso em: 18 mai. 2022.P. 481

CONSIDERAÇÕES FINAIS

Compreender o tema do reconhecimento facial não é tarefa simples. Envolve muito além dos aspectos técnicos e acadêmicos. Inclui sensibilidade, ponderação e ética. A sociedade visa benefícios com a inovação, utilizar tecnologias que facilitem o seu dia a dia, agilizem processos, tornem a vida mais "fácil".

Mas, ninguém deseja sofrer discriminação por isso: ter um benefício negado, ser impedido de acessar um local ou usar um serviço, ser preso injustamente por um equívoco de sistema de reconhecimento facial.

Delineadas considerações gerais sobre a tecnologia, traçou-se um cenário internacional normativo sobre o tema e, após, adentrou-se na matéria em âmbito brasileiro. Buscou-se entender o significado trazido pelo legislador com o Art. 11, II, "g" – tema específico e com pouco aprofundamento acadêmico nacional.

Vislumbrou-se a ausência de legislação ou normativas no Brasil para abordar o tema do reconhecimento facial em contexto amplo, o que se confirmou a hipótese de pesquisa: a insuficiência, *a priori*, do ordenamento jurídico nacional para lidar com a matéria do reconhecimento facial.

Diante disto, buscou-se alternativas, como a proposição de guias orientativos e metodologias e construção de planejamento pró ativo e reativo de organizações. Não se olvida a necessidade de observância à Carta Magna e legislações esparsas, bem como aos princípios e fundamentos preconizados na LGPD.

Não se pretende esgotar a temática nem a pesquisa neste momento. O estudo visa apenas lançar luz a assunto tão complexo e que requer um olhar atento. Entende-se haver mais desafios e questionamentos do que respostas – resultado esperado para pesquisa.

Ademais, em que pese expostas consequências negativas, não se defende a proibição do reconhecimento facial, pois este também pode trazer consequências benéficas para determinados grupos, como aposentados que não precisariam deslocar-se para receber o benefício do INSS.

O que se defende é a necessidade de um exercício ponderativo e casuístico – (desafio normativo), para que a tecnologia seja não só estudada no campo teórico, mas seja capaz de ser aplicada no campo prático, de forma a exercer o seu verdadeiro papel na sociedade: não substituir tarefas, mas complementar, agregar, facilitar.

Este caminho deve ser pautado pela autodeterminação informativa, privacidade e consentimento, quando for a base legal adequada.

Resta aos juristas, legisladores e também à sociedade civil, a difícil arte de pensar sobre a inovação tecnológica sem que esta afronte a privacidade e os direitos dos titulares de dados. Refletir as consequências a curto, médio e longo prazo, desenvolver métodos e orientar organizações é necessário.

É por isso, que incumbe à academia e aos juristas, a difícil tarefa de ponderação e dogmática. Sem antes, contudo, preocupar-se com o necessário pragmatismo de tema tão relevante.

É um pouso extremamente incerto, mas que merece a sua devida reflexão.

REFERÊNCIAS BIBLIOGRÁFICAS

5 POPULAR TYPES OF BIOMETRIC AUTHENTICATION: PROS AND CONS. PHONEXIA. Disponível em: https://www.phonexia.com/blog/5-popular-types-of-biometric-authentication-pros-and-cons/. Acesso em: 10 jun. 2022.

AÇÃO CIVIL PÚBLICA. IDEC – Instituto Brasileiro de Defesa do Consumidor em face da CONCESSIONÁRIA DA LINHA 4 DO METRO DE SÃO PAULO. p1-55, p. 37. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 jun. 2022.

ADA LOVELACE INSTITUTE. Beyond face value: public attitudes to facial recognition technology. 2019. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ . Acesso em 03 mar. 2022

AEPD. Guía sobre El uso de videocâmaras para seguridad y otras finalidades. Agencia Espanõla de Protección de Datos. 2021. Disponível em: https://www.aepd.es/sites/default/files/2019-12/guia-videovigilancia.pdf. Acesso em: 20 jun. 2022.

AEROPORTO DA CAPITAL DO PAÍS TESTA EMBARQUE COM RECONHECIMENTO FACIAL. GOVERNO FEDERAL. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/noticias/2021/8/aeroporto-da-capital-do-pais-testa-embarque-com-reconhecimento-facial. Acesso em: 15 jun. 2022.

AEROPORTO DE BRASILIA TESTA EMBARQUE DE PASSAGEIROS FEITO POR RECONHECIMENTO FACIAL. GOVERNO FEDERAL. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/aeroporto-de-brasilia-testa-embarque-de-passageiros-feito-por-reconhecimento-facial. Acesso em: 15 jun. 2022.

AEROPORTO DE CONGONHAS TESTA EMBARQUE POR RECONHECIMENTO FACIAL COM TRIPULANTES. GOVERNO FEDERAL. Disponível em: https://www.gov.br/anac/pt-br/noticias/2021/aeroporto-de-congonhas-testa-embarque-por-reconhecimento-facial-com-tripulantes. Acesso em: 15 jun. 2022.

ALBUQUERQUE, Karol. Descubra mitos e verdades sobre a biometria de voz. OLHAR DIGITAL. Disponível em: https://olhardigital.com.br/2022/03/09/tira-duvidas/descubra-mitos-e-verdades-sobre-a-biometria-de-voz/. Acesso em: 12 jun. 2022
Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial. IDEC. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial. Acesso em: 10 jun. 2022.

APPLE. About Face ID advanced technology. Disponível em: https://support.apple.com/en-us/HT208108. Acesso em: 20 fev. 2022.

ARENDT, Hannah. A condição humana. RAPOSO, Roberto (trad). 13 ed. Rio de Janeiro: Forense Universitária, 2020

ARTICLE 29 DATA PROTECTION WORKING PARTY. . **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a "high risk" for the purposes of Regulation 2016/679.** Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.Acesso em:02 jun. 2022

BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013.
BBBC. Schools pause facial recognition lunch plans. Disponível em: https://www.bbc.com/news/technology-59037346. Acesso em: 05 fev. 2022.

BBC. Facebook to end use of facial recognition software. Disponível em: https://www.bbc.com/news/business-59143323. Acesso em: 05 fev. 2022

BBC. Google apologises for Photos app's racist blunder. Disponível em: https://www.bbc.com/news/technology-33347866. Acesso em: 08 fev. 2022

BBC. Legal action over alleged Uber facial verification bias. Disponível em: https://www.bbc.com/news/technology-58831373 Acesso em 05 fev. 2022.

BBC. O que é o Pokémon Go e por que está causando tanto furor no mundo dos games? 2016. Disponível em: https://www.bbc.com/portuguese/geral-36802725. Acesso em 02 fev. 2022; https://pokemongolive.com/pt_br/

BIOMETRIA FACIAL. ITAU. Disponível em: https://www.itau.com.br/privacidade/biometria-facial. Acesso em: 15 jun. 2022.

BIOMETRIA. TRIBUNAL SUPERIOR ELEITORAL. Disponível em: https://www.tse.jus.br/eleitor/biometria. Acesso em: 15 jun. 2022.

BIONI, Bruno Ricardo. LUCIANO, Maria. Princípio da precaução como vetor de regulação de Inteligências Artificial: seriam as leis de proteção de dados pessoais o seu portal de entrada? In Inteligências Artificial (Organizadores Caitlin Sampaio et al). Rio de Janeiro, 2019, p. 207-231

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

BJORN, Vance. Logical Acess Control. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.01-05. New York: Springer, 2015

BOSTON GLOBE MEDIA PARTNERS. Boston City Council unanimously passes ban on facial recognition technology. Disponível em: https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban/. Acesso em: 05 fev. 2022

BOULAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Acucuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018. Disponível em: https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf. Acesso em 05 fev. 2022

BOULAMWINI, Joy; ORDÓNEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial Recognition Technologies: a primer. Algorithmic Justice League, 2020

BRASIL Projeto de Lei nº 9736, de 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1643053. Acesso em: 20 jun. 2020.

BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. 2019.Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf . Acesso em: 15 jun, 2022.

BRASIL. CÓDIGO DE DEFESA DO CONSUMIDOR. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jun. 2022.

BRASIL. DECRETO. N. 10,046, DE 09 DE OUTUBRO DE 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração federal e institui o cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Vide art. 2º, II. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 jun. 2022.

BRASIL. ESTATUTO DA CRIANÇA E DO ADOLESCENTE. http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 jun. 2022.

BRASIL. Glossário de Segurança da Informação. Governo Federal. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em 07 jun. 2022.

BRASIL. LEI N. 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 jun. 2022.

BRASIL. Lei N. 13.444, DE 11 DE MAIO DE 2017. Disponível em: L13444 (planalto.gov.br). Acesso em: 15 jun. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 fev 2022.

BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022.

BRASIL. LEI N.6.712, DE 10 DE NOVEMBRO DE 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 20 abr. 2022

BRASIL. PL N. 4060/2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0ju06izhj6peecftv2zrqmw5o11591812.node0?codteor=1001750&filename=PL+4060/2012. Acesso em: 06 jun. 2022.

BRASIL. PORTARIA N. 2018, DE 19 DE MAIO DE 2020. Institui a Política de Segurança da Informação do Ministério da Economia. Disponível em: https://extranet.economia.gov.br/wp-content/uploads/2020/10/Portaria-no-218-Institui-a-Poli%CC%81tica-de-Seguranc%CC%A7a-da-Informac%CC%A7a%CC%83o.pdf. Acesso em 16 jun. 2022.

BRASIL. PORTARIA N. 248, DE 2 DE FEVEREIRO DE 2018. MINISTÉRIO DA SAÚDE. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2018/prt0248_05_02_2018.html. Acesso em 15 jun. 2022.

BRASIL. Projeto de Lei n. 1033, de 2019. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/f7745acb22d37589032586390074cefb?OpenDocument&Highlight=0,1033. Acesso em: 10 jun 2022.

BRASIL. Projeto de Lei nº 572, de 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1966599&filename=PL+572/2021. Acesso em: 20 jun. 2022.

BRASIL. Projeto de Lei nº 6197, de 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8049424&ts=1630439166989&disposition=inline. Acesso em 20 set, 2021.

BRASIL. Projeto de Lei nº. 4612, de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1794019&filename=PL+4612/2019. Acesso em 11 jun. 2022.

BRASIL. Projeto de Lei nº. 865, de 2019. Disponível em: https://www.al.sp.gov.br/propositura/?id=1000278098. Acesso em: 16 jun. 2022.

C6 BANK HABILITA RECONHECIMENTO FACIAL PARA TRANSAÇÕES NO APP. BANCO C6. Disponível em: https://blog.c6bank.com.br/c6-bank-habilita-reconhecimento-facial-para-transacoes-no-app. Acesso em: 15 jun. 2022.

CAVOUKIAN, Ann. **The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices** [s.l]; [s.d.], p 1- 12. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf Acesso em 14 abr. 2021.

CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.4. Disponível em: https://openresearch-

repository.anu.edu.au/bitstream/1885/46248/27/03Paper02.pdf . Acesso em 24 dez, 2021.
CLARKE, Roger. Information Technology and Dataveillance. DUNLOP, C; KLING, R (Eds). Controversies in Computing. Academic Press. 1991. Disponível em: http://www.rogerclarke.com/DV/CACM88.html. Acesso em: 02 fev. 2022. Online

CNET. Facial recognition banned in another city. Oakland, California, hás followed San Francisco as the second Bay Area city to vote down the use os the technology. Disponível em: https://www.cnet.com/tech/mobile/facial-recognition-banned-in-another-city/. Acesso em: 05 fev. 2022

CNN. EUA: Polícia prende inocente a partir de sistema de reconhecimento facial. Disponível em: https://www.cnnbrasil.com.br/internacional/sistema-de-reconhecimento-facial-enviou-este-homem-inocente-para-a-prisao/. Acesso em: 05 fev. 2022

CONSELHO NACIONAL DE JUSTIÇA. RESOLUÇÃO N. 306 DE 17 DE DEZEMBRO DE 2019. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3146. Acesso em: 15 jun, 2022.

COSTA, Guilherme Spillari; LEVENFUS, Silvia. O uso de câmeras no ambiente empresarial e a LGPD. Revista digital ESA/OAB. V. 10. N. 2. Porto Alegre. 2021. Disponível em: https://www.oabrs.org.br/arquivos/file_611ac48b0587d.pdf. Acesso em: 03 mar. 2022.

COUNCIL OF EUROPE. Guidelines on Facial Recognition CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 03 jun. 2022.

CRUMPLER, William. How accurate are facial recognition systems – and why does it matter? Center for Strategic & International Studies. 2020. Disponível em: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter . Acesso em: 25 fev. 2022.

DANTCHEVA, Antitza; ELIA, Petros; ROSS, Arun. What Else Does Your Biometric Data Reveal? A survey on Soft Biometrics. IEEE Transactions on Information Forensics and Security, 2015

DAY, David. Biometric Applications Overview. In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015, p. 169-170.

DE ACORDO COM O SERASA, golpe do carro financiado com CPF roubado faz vítima a cada 2 dias. TENHA ATITUDE ANTIFRAUDE: MONITORE SEU CPF E ASSINE SERASA PREMIUM. SERASA PREMIUM. Disponível em: https://www.serasa.com.br/premium/blog/antifraude/. Acesso em: 15 jun. 2022

DETROIT FREE PRESS. Controversial Detroit facial recognition got him arrested for a crime He didn't commit. Disponível em: https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-

recognition-detroit-michael-oliver-robert-williams/5392166002/. Acesso em: 05 fev. 2022.
DICIO. Dicionário Online de Portugês. Acurácia. Disponível em: https://www.dicio.com.br/acuracia/. Acexso em: 10 fev. 2022

DONEDA, Danilo. Da privacidade à proteção de dados pessoais Fundamentos da Lei Geral de Proteção de Dados. 3. Ed. São Paulo: Thomson Reuters Brasil, 2021

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da Nova Lei Geral de Proteção de Dados brasileira. In: CAVALLI, Olga; BELLI, Luca. Governança e regulações da internet na América Latina:. p. 309 – 325, 2019

EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses os AI that can lead to unfair discrimination. European Data Protection Supervisor – EDPS. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en. Acesso em: 20 jun. 2022.

EKENEL, Hazm Kemal; STIEFELHAGEN, Rainer. Why is facial occlusion a challenging problem? In: TISTARELLI, Massimo; NIXON, Mark (Eds.). Advances in Biometrics. Third Internacional Conference ICB. Springer: Itália, 2009, p. 299- 308
.
EMPRESAS DE ÔNIBUS ADAPTAM TECNOLOGIA DA BIOMETRIA FACIAL PARA RECONHECER PASSAGEIROS COM MÁSCARA. ASSOCIAÇÃO DOS TRANSPORTADORES DE PASSAGEIROS – ATP. Disponível em: https://www.atppoa.com.br/2020/08/25/empresas-de-onibus-adaptam-tecnologia-da-biometria-facial-para-uso-da-mascara/. Acesso em 16 jun. 2022.

EPOCA NEGÓCIOS. Quem é a funcionária do Google demitida após acusar empresa de racismo e censura. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2020/12/quem-e-funcionaria-do-google-demitida-apos-acusar-empresa-de-racismo-e-censura.html. Acesso em: 05 fev. 2022.

ESCOLA MUNICIPAL DE MATÃO ADOTA RECONHECIMENTO FACIAL PARA CONTROLAR FREQUENCIA DOS ALUNOS. G1. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/sp/sao-carlos-regiao/noticia/2019/12/11/escola-municipal-de-matao-adota-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml. Acesso em: 15 jun. 2022.

ESCOLAS PÚBLICAS DE MUNICÍPIO BAIANO USAM RECONHECIMENTO FACIAL PARA CONTROLAR FREQUENCIA DOS ALUNOS. Globo notícias. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2022/02/09/escolas-publicas-de-municipio-baiano-usam-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml. Acesso em: 10 jun. 2022.

EUROPA. Opinion 02/2012 on facial recognition in online and móbile services. DATA PROTECTION WORKING PARTY. Bruxelas, 2012

EUROPEAN COMMISSION. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. Brussels, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206. Acesso em: 10 jun. 2022.

FACEPLUSPLUS. Disponível em: https://www.faceplusplus.com/. Acesso em 08 fev. 2022

FACHINETTI. Aline Fuke. LGPD: fotos, inferências e a sensibilidade de dados pessoais. JOTA. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-fotos-inferencias-e-a-sensibilidade-de-dados-pessoais-03092019#sdfootnote1sym. Acesso em: 20 jun. 2022.

FALEIROS JUNIOR, José Luiz de Moura. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coord.).**Estudos essenciais de Direito Digital**. Uberlândia: LAECC, 2019, p. 207- 231

FEDERAL TRADE COMMISSION. Best Practices for Common Uses of Facial Recognition Technologies. 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf. Acesso em: 10 jun. 2022.

FIGHT FOR THE FUTURE. Ban Facial Recognition. Disponível em: https://www.banfacialrecognition.com/map/ Acesso em: 05 fev. 2022

FRAZÃO, Ana. Discriminação algorítmica: a responsabilidade dos programadores e das empresas. JOTA. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-a-responsabilidade-dos-programadores-e-das-empresas-14072021. Acesso em: 10 jun. 2022.

GARAVAGLIA, Aaron. Data extracted from photographs: covered under BIPA? National Law Review, v. XI, n. 84. 2022. Disponível em: https://www.natlawreview.com/article/data-extracted-photographs-covered-under-bipa. Acesso em: 22 jun. 2022.

GOLPE “DO PRESENTE” EM COMPRAS NA INTERNET OU NO CARTÃO POR APROXIMAÇÃO: PROCON-PR ALERTA SOBRE COMO SE PROTEGER. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/pr/parana/noticia/2021/11/02/golpe-do-presente-em-compras-na-internet-ou-no-cartao-por-aproximacao-procon-pr-alerta-sobre-como-se-proteger.ghtml. Acesso em: 15 jun. 2022.

GOLPE DO RECONHECIMENTO FACIAL FAZ VÍTIMA FINANCIAR CARRO PARA TERCEIROS. UOL. Disponível em:

https://www.uol.com.br/carros/noticias/redacao/2021/06/04/golpe-do-reconhecimento-facial-faz-vitima-financiar-carro-de-luxo-sem-saber.htm. Acesso em 15 jun. 2022.

GOLPISTAS USAM RECONHECIMENTO FACIAL PARA FAZER IDOSOS CONTRATAREM EMPRÉSTIMOS CONSIGNADOS NO RS. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2022/03/28/golpistas-usam-reconhecimento-facial-para-fazer-idosos-contratarem-emprestimos-consignados-no-rs.ghtml. Acesso em: 15 jun. 2022.

GOOGLE DEVELOPERS. Face Detection. Disponível em: https://developers.google.com/ml-kit/vision/face-detection. Acesso em: 03 fev. 2022.

GOVERNMENT TECHNOLOGY. Portland, Maine, councilors ban facial recognition tech. Disponível em: https://www.govtech.com/public-safety/portland-maine-councilors-ban-facial-recognition-tech.html. Acesso em: 05 fev. 2022

GOVERNMENT TECHNOLOGY. Virginia Bill to put de facto ban on facial recognition tech. Disponível em: https://www.govtech.com/policy/virginia-bill-to-put-de-facto-ban-on-facial-recognition-tech.html. Acesso em: 05 fev. 2022.

GOVERNO DO ESTADO DA BAHIA. Reconhecimento Facial impede entrada de homicida em circuito. Secretaria da Segurança Pública. SSP/BA. 2019. Disponível em: http://www.bahia.ba.gov.br/2019/03/noticias/carnaval/reconhecimento-facial-impede-entrada-de-homicida-em-circuito/. Acesso em: 06 jun. 2022.

GOVERNO DO ESTADO DO CEARÁ. Chefe de organização criminosa é preso após ser identificado por reconhecimento facial. 2021. Disponível em:https://www.policiacivil.ce.gov.br/2021/05/01/chefe-de-organizacao-criminosa-e-preso-apos-ser-identificado-por-reconhecimento-facial/. Acesso em: 20 jun. 2022;

GOVERNO FEDERAL. ANPD. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 10 jun. 2022.

GOVERNO FEDERAL. Guia de boas práticas – Lei Geral de Proteção de Dados (LGPD), p.1-69, p. 28.. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 20 jun. 2022.

GOVERNO FEDERAL. **Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 13 jun. 2022.

GOVERNO FEDERAL. SENACON. Como proteger seus dados pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 12 jun. 2022.

GUEDES, Paula. 7 Recomendações para a regulação do Reconhecimento Facial. Instituto de Tecnologia e Sociedade do RIO – ITS RIO. Disponível em:

https://itsrio.org/pt/artigos/7-recomendacoes-para-a-regulacao-do-reconhecimento-facial/. Acesso em: 03 jun. 2022.
GUO, Guodong. Gender Classification. In: In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.169-174. New York: Springer, 2015

HOLLISTER, Sean. How Tencent's sweeping new facial scans Will atch Chinese kids playing past curfew. The Verge. Disponível em: https://www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace. Acesso em 02 fev. 2022.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law And Security Review*, Kassel, n. 25, p. 84-88, 2009

HOWARD, John; SIROTIN, Yevgeniy; TIPTON, Jerry. Revisiting the Fitzpatrick Scale and Face Photo-based Estimates of Skin Phenotypes. Homeland Security. Science and Technology. Maryland Test Facility. NIST.2020

IBM. Watson Visual Recognition. Disponível em: https://www.ibm.com/fi-en/cloud/watson-visual-recognition. Acesso em: 08 fev. 2022

ICO. The use of live facial tecognition technology in public places. Information Commissioners Opinion. 2021. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 20 jun. 2022.

ICO. What is special type of data? Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/. Acesso em: 15 jun. 2022.
IDEC notifica Hering por coleta de dados faciais para publicidade. IDEC. Disponível em: https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade. Acesso em: 10 jun. 2022.

IDEC. IDEC obtém vitória contra reconhecimento de emoções no Metrô de SP. Disponível em: https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp#:~:text=A%20empresa%20foi%20condenada%20a,publicit%C3%A1rios%20com%20a%20inten%C3%A7%C3%A3o%20de. Acesso em: 20 mai. 2022.

IGARAPÉ. Infográfico: Reconhecimento facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 05 jul. 2022.

INSTITUTO ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020, p.34-35. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em: 15 jun. 2022.

Internacional Organization for Standardization. ISO/IEC 2382-37: 2017 – Information Technology – Vocabulary – Part. 37: Biometrics. Switzerland, 2017. Disponível em: https://www.iso.org/standard/66693.html. Acesso em: 20 dez, 2021. Online

JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Introduction to Biomet**rics. New York:Springer, 2011

JAIN, Anil K; ROSS, Arun A; NANDAKUMAR, Karthik**. Soft Biometrics.** . In: STAN Z, Li; JAIN, Anil K (Eds**). Encyclopedia of Biometrics**. 2. ed, p.1425- 1429. New York: Springer, 2015

JAIN, Anil Kumar; NANDAKUMAR, Karthik; ROSS, Arun. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letter*. Elsevier, 2016

JAIN, Anil Kumar; PANKANTI, S; PRABHAKAR, Salil. Biometric Recognition: Security and Privacy Concerns. **IEEE Security and Privacy Magazine,** v. 1, p.33-42, mar-abr, 2003

JAIN, Anil. Introduction to Biometrics. In: JAIN, Anil K; BOLLE, Ruud; PANKANTI, Sharath (Eds.). **Biometrics.** Personal Identificaation in Network Society. New York: Springer, 1996, p. 01-40

JILLSON, Elisa. Aiming for truth, fairness, and equity in your company'suse of AI. Federal rade Commission. FTC. 2021. Disponível em: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Acesso em: 10 jun. 2022.

KAUFMAN, Dora. Proposta Europeia de Regulamentação da IA: impressões preliminares. EPOCA NEGÓCIOS. 2021. Disponível em: https://epocanegocios.globo.com/colunas/IAgora/noticia/2021/04/proposta-europeia-de-regulamentacao-da-ia-impressoes-preliminares.html. Acesso em: 15 jun. 2022.

KRISH, Ashok. Biometrics: **The Benefits and Challenges of Remote Authentication Systems**. Forbes Business Council. 2020. Disponível em: https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/07/biometrics-the-benefits-and-challenges-of-remote-authentication-systems/?sh=794390397bbc. Acesso em: 21. dez. 2021.

LEO, Marco et AL. Automatic Emotion Recognition in Robot-Children Interaction for ASD treatment. IEEE Internacional Conference on Computer Vision Workshop (ICCVW). 2015, p-537-545

LI, Stan Z.; JAIN, Anil K. Introduction. In: LI, Stan Z; JAIN, Anil K (Eds). Handbook of Face Recognition. 2ed. New York: Springer, 2011, p. 1- 15

LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Rio de Janeiro: Zahar, 2013

LYON, David. The Eletronic Eye. The rise of surveillance society. Estados Unidos: Universidade de Minnesota, 1994

MADIEGA, Tambiama; MILDEBRATH, Hendrik. EUROPEAN PARLIAMENT. Regulating facial recognition in the EU. 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Acesso em: 10 jun. 2022.

MARQUES, Claudia Lima. Diálogo das fontes: do conflito à coordenação de normas no direito brasileiro. São Paulo: RT, 2021

MARTINS. Leonardo. Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais. Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016

MARTINS-COSTA, Judith. **A boa-fé no direito privado:** critérios para a sua aplicação. 2 ed. São Paulo: Saraiva Educação, 2018.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. POLZONOFF JUNIOR, Paulo (trad). Rio de Janeiro: Elsevier, 2013

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a histórica de um conceito. Fortaleza: Pensar. V. 25, n. 4, p. 1-18, 2020

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

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, v. 120. São Paulo: Ed. RT, nov.-dez. 2018, p. 469-483

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coords). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015, p. 205- 230

MENKE, Fabiano; LEVENFUS, Sílvia. O reconhecimento facial no setor público e a proteção de dados pessoais. CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves; RAMOS, Rafael (orgs.). Lei Geral de Proteção de Dados e o poder público. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena, 2021.

META. Na update on our use of face recognition. 2021. Disponível em: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ . Acesso em: 05 fev. 2022

MICHAELIS. DICIONÁRIO ONLINE. Editora Melhoramentos. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude/. Acesso em: 15 jun. 2022.

MICROSOFT. Azure. API de Detecção Facial. Um serviço de IA que analisa rostos e imagens. Disponível em: https://azure.microsoft.com/pt-br/services/cognitive-services/face/#overview. Acesso em: 08 fev. 2022

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais. Thomson Reuters. 2019. Online.

MOREIRA ALVES, Jose Carlos. Direito Romano 16 ed. Rio de Janeiro: Forense, 2014.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitling (Org); A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago: 2020, p.121-156

MUTHUKUMAR, Vidya; PEDAPATI, Tejaswini; RATHA, Nalini; SATTIGERI, Prasanna; WU; Chai-Wah; KINGSBURY, Brian; KUMAR, Abhishek; THOMAS, Samuel; MOJSILIVIC, Aleksandra; VARSHNEY, Kush. Understanding Unequal Gender Classification Accuracy from face Images. 2018. Disponível em: https://arxiv.org/pdf/1812.00099.pdf. Acesso em 08 fev. 2022.

NGAN, Mei L; GROTHER, Patrick. Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg: 2015

NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6A: Face Recognition accuracy with masks using pré-COVID-19 algorithms. . United States Department of Commerce. 2020, s.n

NGAN, Mei; GROTHER, Patrick; HANAOKA, Kayee. NIST. Ongoin Face Recognition Vendor test (FRVT). Part. 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. United States Department of Commerce. 2020. Disponível em: https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report_6b.pdf. Acesso em: 01 fev. 2022

NISHA, Srinivas; KARL, Ricanek; MICHALSKI, Danai; BOLME, David; MICHAEL, King. Face Recognition Algoritm Bias: Performance Differences on Images of Children and Adults. United States . 2019. Disponível em: https://www.osti.gov/biblio/1559665. Acesso em 05 fev.2022

NISSENBAUM, Helen. Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press: California, 2010

NORRIS, Clive; ARMSTRONG, Gary. CCTV and the social structuring of surveillance. In: PAINTER, K; TILLEY, N (Eds.) *Crime Prevention Studies*. Criminal Justice Press. v.10. New York: 1999, p. 157 – 178

NOTA TECNICA PL N. 885/19. LAPIN, Laboratório de Políticas Públicas e Internet; ACESS NOW; ITS RIO, Instituto de Tecnologia e Sociedade do Rio. Disponível em: https://itsrio.org/wp-content/uploads/2021/03/Nota-tecnica-PL-865-2019.pdf. Acesso em: 10 jun. 2022.

NUBANK USA RECONHECIMENTO FACIAL PARA LIBERAR PIX DE ALTO VALOR. TECNOBLOG. Disponível em: https://tecnoblog.net/noticias/2021/04/16/nubank-usa-reconhecimento-facial-para-liberar-pix-de-alto-valor/. Acesso em: 15 jun. 2022.

PAIVA, Letícia. Reconhecimento facial para segurança avança na América Latina mesmo sem normas claras. JOTA. Disponível em: https://www.jota.info/justica/reconhecimento-facial-seguranca-publica-03052021. Acesso em: 05 jun. 2022.

PARANAVAÍ É PREMIADA POR SISTEMA DE RECONHECIMENTO FACIAL NAS ESCOLAS. PORTAL DA CIDADE. Disponível em: https://paranavai.portaldacidade.com/noticias/cidade/paranavai-e-premiada-por-sistema-de-reconhecimento-facial-nas-escolas-0654. Acesso em: 15 jun. 2022

PARLAMENTO EUROPEU. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 10 jun. 2022.

PIRONTI, Rodrigo; KEPPEN, Mariana Tomasi. As fotografias, as câmeras de segurança e os dados sensíveis na LGPD. CONJUR. 2021. Disponível em: https://www.conjur.com.br/2021-ago-23/opiniao-fotografias-cameras-seguranca-dados-sensiveis#author. Acesso em: 21 jun. 2022.

POLÍCIA PRENDE HOMENS QUE TENTAVAM COMPRAR CARRO COM DOCUMENTO DE OUTRA PESSOA. GLOBO NOTÍCIAS. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2018/10/02/policia-prende-homens-que-tentavam-comprar-carro-com-documento-de-outra-pessoa.ghtml. Acesso em: 15 jun. 2022.

PREFEITURA DE BETIM INSTALA RECONHECIMENTO FACIAL NAS ESCOLAS DA REDE MUNICIPAL. PREFEITURA DE BETIM. Disponível em: https://www.betim.mg.gov.br/portal/noticias/0/3/11327/prefeitura-de-betim-instala-reconhecimento-facial-nas-escolas-da-rede-municipal/. Acesso em: 17 jun. 2022.

PREFEITURA LANÇA SISTEMA DE RECONHECIMENTO FACIAL NAS ESCOLAS E CMEIS DE GOIÂNIA. PREFEITURA DE GOIÂNIA. Disponível em: https://www.goiania.go.gov.br/prefeitura-lanca-sistema-de-reconhecimento-facial-nas-escolas-e-cmeis-de-goiania/. Acesso em: 15 jun. 2022.

PROFESSORES DO IFES REALIZAM CHAMADAS POR RECONHECIMENTO FACIAL. A GAZETA. Disponível em: https://www.agazeta.com.br/es/gv/professores-

do-ifes-realizam-chamadas-por-reconhecimento-facial-1019?utm_medium=redacao&utm_source=twitter&origin_r=leiaag. Acesso em 10 jun 2022.

RECONHECIMENTO FACIAL NO BRASIL. INSTITUTO IGARAPÉ. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em 15 jun. 2022

RECONHECIMENTO FACIAL PELO APLICATIVO MEU GOV.BR É A PRIMEIRA ETAPA DA PROVA DE VIDA DOS APOSENTADOS. GOVERNO FEDERAL. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/agosto/reconhecimento-facial-pelo-aplicativo-meu-gov-br-e-a-primeira-etapa-da-prova-de-vida-dos-aposentados. Acesso em: 15 jun. 2022.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. Acesso em: 10 mai. 2022.

REIS, Carolina. Nota Técnica Lei 6.712/20. 10 recomendações para o uso de reconhecimento facial para segurança pública no DF. Laboratório de Políticas Públicas e Internet – LAPIN. 2021. Disponível em: https://lapin.org.br/2021/02/22/nota-tecnica-lei-distrital-6712-2020-df/. Acesso em: 20 abr. 2022.

RIELLI, Mariana Marques; FRANCISCO, Pedro Augusto; HUREL; Louise, Marie. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituito Igarapé. Data Privacy BR. 2020, p. 1. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 18 jun. 2022.

RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje.. DONEDA, Danilo; DONEDA, Luciana Cabral (trad). Renovar: Rio de Janeiro, 2008.
SAIBA O QUE É FRAUDE E QUAIS OS TIPOS MAIS COMUNS - FRAUDES E GOLPES. SERASA ENSINA. Disponível em: https://www.serasa.com.br/ensina/seu-cpf-protegido/o-que-e-fraude/. Acesso em: 15 jun. 2022.

SATI; Vishwani et AL. Face Detection and Recognition, Face Emotion Recognition Trough NVIDIA Jetson Nano. In: Ambient Intelligence – Software and Applications. Internacional Symposium on Ambient Intelligence. 11. 2020, p. 177-185

SCHWABE, J. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. MARTINS, Leonardo; HENNIG, Beatriz et al (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005

Secretaria Nacional do Consumidor aplica multa a empresa por reconhecimento facial. GOVERNO FEDERAL. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-aplica-multa-a-empresa-por-reconhecimento-facial . Acesso em: 10 jun. 2022.

SIGNIFICADOS. Significado de Antropometria. Disponível em: https://www.significados.com.br/antropometria/. Acesso em 18 jan. 2022

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020

SISTEMA DE RECONHECIMENTO FACIAL JÁ FUNCIONA NAS ESCOLAS DE IPATINGA. DIÁRIO DO AÇO. Disponível em: https://www.diariodoaco.com.br/noticia/0075842-sistema-de-reconhecimento-facial-ja-funciona-nas-escolas-de-ipatinga. Acesso em: 15 jun. 2022

SOBRE A TECNOLOGIA AVANÇADA DO FACE ID. APPLE. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2022.

SOLOVE, Daniel J. Nothing to Hide. The False Tradeoff between Privacy and Security. London: Yale University Press, 2011

STOIMCHEV, Marjan; IVANOVSKA, Marija; STRUC, Vitomir. Learning to Combine Local and Global Image Information for Contactless Palmprint Recognition. *Sensors*, 2022

TEFFÉ, Chiara Spadaccini; FERNANDES, Elora Raad. Reconhecimento facial: laissez-faire, regular ou banir? Migalhas. 2020. Disponível em: Reconhecimento Facial: laissez-faire, regular ou banir? - Migalhas. Acesso em: 22 jun. 2022.

TEFFÉ,Chiara Spadacccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com.** a.9.n.1. 2020. P. 1-39, p. 32. Disponível em: https://www.academia.edu/42993125/Tratamento_de_dados_pessoais_na_LGPD_estudo_sobre_as_bases_legais. Acesso em: 20 jun. 2022.

TENHA ATITUDE ANTIFRAUDE: MONITORE SEU CPF E ASSINE SERASA PREMIUM. SERASA PREMIUM. Disponível em: https://www.serasa.com.br/premium/blog/antifraude/. Acesso em: 15 jun. 2022

TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro), p. 30.. Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 10 jun. 2022.

THE EDPS VIDEO-SURVEILLANCE GUIDELINES. European Data Protection Supervisor. EDPS.Brussels: 2010. Disponível em: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf. Acesso em: 20 jun. 2022.

THE GUARDIAN. ICO to step in after schools use facial recogntion speed up lunch queue. 2021. Disponível em:

https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk. Acesso em 05 fev. 2022

THE LENS. New Orleans Ciry Council bans facial recognition, predictive policing and other surveillance tech. Disponível em: https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech/. Acesso em: 05 fev. 2022

THE NEW YORK TIMES. San Fransciso Bans Facial Recognition Technology. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 05 fev. 2022

THE VERGE. Detroit man sues Police for wrongfully arresting him based on facial recognition. Disponível em: https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest. Acesso em: 05 fev. 2022

TUDO O QUE VOCÊ PRECISA SABER SOBRE O DESBLOQUEIO COM RECONHECIMENTO FACIAL EM SEU SMARTHPONE. SAMSUNG. Disponível em: https://www.samsung.com/br/support/mobile-devices/tudo-que-voce-precisa-saber-sobre-o-desbloqueio-com-reconhecimento-facial-em-seu-smartphone/. Acesso em 16 jun. 2022.

TUNHOLI, Murilo. China proíbe menores de 18 anos de jogar videogame por mais de 3h semanais. Tecnoblog. Disponível em: https://tecnoblog.net/noticias/2021/08/30/china-proibe-menores-de-18-anos-de-jogar-videogame-por-mais-de-3h-semanais/. Acesso em: 02 fev. 2022

UBER. Engineering Safety with Uber's real-Time ID Check. Disponível em: https://eng.uber.com/real-time-id-check/. Acesso em: 05 fev. 2022; UBER. Por que preciso tirar uma foto minha?. Disponível em: https://help.uber.com/driving-and-delivering/article/por-que-preciso-tirar-uma-foto-minha--?nodeId=7fa8a60d-cf6f-49ac-9a50-b4bf6a3978ef. Acesso em: 05 fev. 2022

UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em 02 fev. 2022.

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MICHIGAN SOUTHERN DIVISION. Dsiponível em: https://www.aclumich.org/profiles/aclu_affiliates/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclumich.org%2Fsites%2Fdefault%2Ffiles%2Ffield_documents%2F001_complaint_1.pdf#page=1&zoom=auto,-12,798. Acesso em 05 fev. 2022.

UNITED STATES. BIOMETRIC INFORMATION PRIVACY ACT (BIPA). ACLU. Disponível em: https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa. Acesso em: 10 jun. 2022

UNITED STATES. ILLINOIS GENERAL ASSEMBLY. (740 ILCS 14/) Biometric Information Privacy Act. Disponível em: 740 ILCS 14/ Biometric Information Privacy Act. (ilga.gov). Acesso em: 10 jun. 2022.

UNITED STATES. NATIONAL BIOMETRIC INFORMATION PRIVACY ACT OF 2020. 2.4400. Disponível em: Text - S.4400 - 116th Congress (2019-2020): National Biometric Information Privacy Act of 2020 | Congress.gov | Library of Congress. Acesso em: 14 jun. 2022.

UNITED STATES. TEXAS. Texas Business and Commerce Code §503.001, Capture or use of biometric identifier. Disponível em: https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001. Acesso em: 15 jun. 2022.

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. AGENCIA BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 01 jul. 2022.

VARKARAKIS, Viktor; YAO, Wang; CORCORAN, Peter. Towrads End-to –End Neural Face Authentication in the Wild – Quantifying and Compensating for Directional Lighting Effects. *Pattern Recognition Letters*. 2021.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review. V. 4. N. 5. 1890 – p.193-220.

WASHINGTON BECOMES THIRD STATE TO ENACT BIOMETRIC PRIVACY LAW. Privacy & Information Securtity Law blog. Disponível em: https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/. Acesso em: 10 jun. 2022.

WENG, John J; SWETS, Daniel L. Face Recognition. In: JAIN, Anil; BOLLE, Ruud; PANKANTI, Sharath (Eds). Biometrics. Personal Identification in Networked Society. Nova Iorque: Springer, 2006, p.65-86

ZENG, Dan; VELDHUIS, Raymond; SPREEUWERS, Luuk. A survey of face recognition techniques under oclusion. University of Twente,Netherlands,2020. Disponível em: https://arxiv.org/pdf/2006.11366.pdf. Acesso em: 20 fev. 2022

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro mais humano na nova fronteira do poder. SCHLESINGER, George (trad). 1. Ed. Rio de Janeiro: Intrínseca, 2020