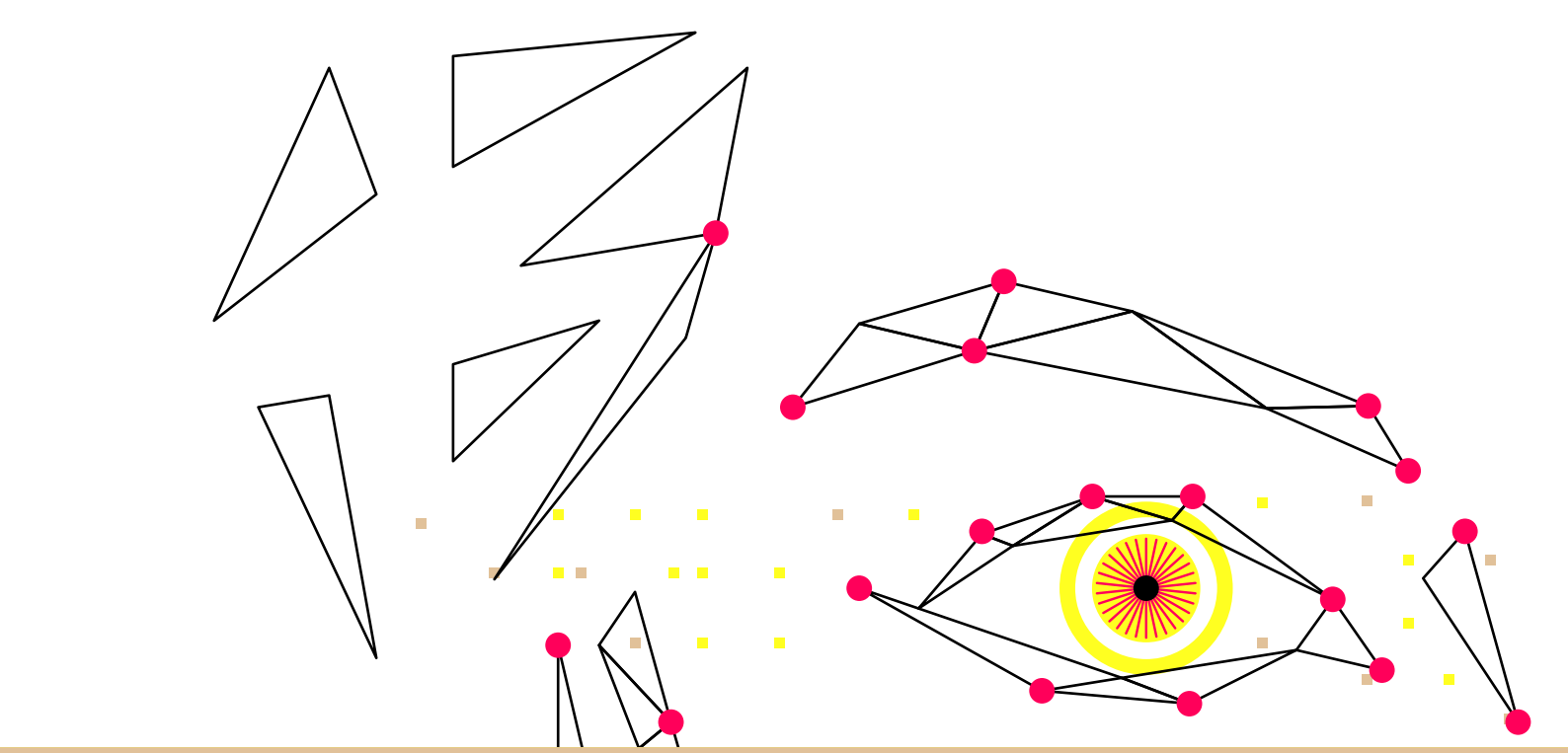
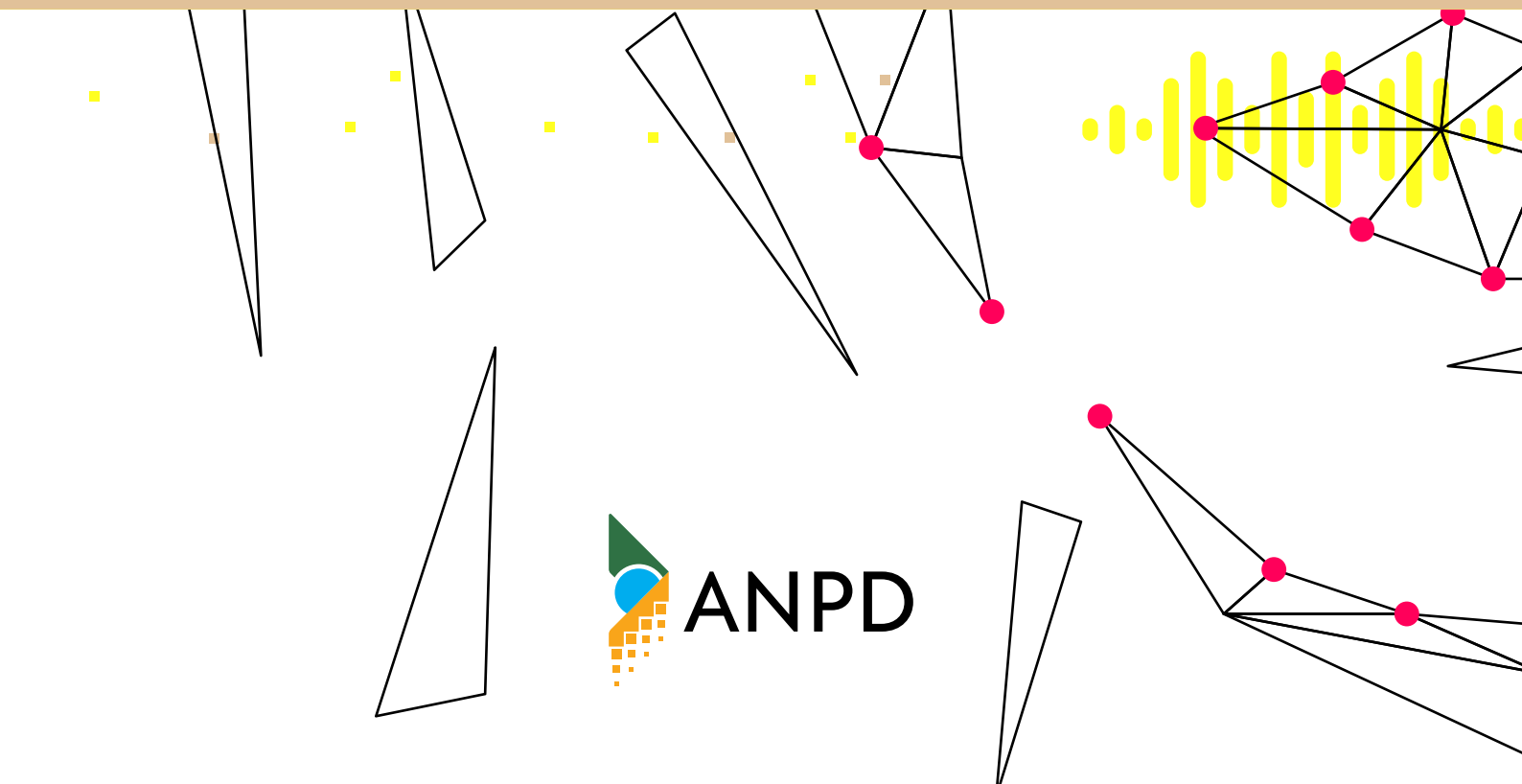


‹ radar tecnológico ›

biometria e reconhecimento facial



ANPD

Autoridade Nacional de Proteção de Dados

‹ radar tecnológico ›

n° 2

biometria e reconhecimento facial

estudos preliminares

Fabiana S. P. Faraco Cebrian
Gustavo do Amaral Prudente
Marcelo Santiago Guedes
Maria Carolina Ferreira da Silva
Maria Luiza Duarte Sa
Thiago Guimarães Moraes

ANPD
Brasília, DF
2024

ANPD
Autoridade Nacional de Proteção de Dados

Diretor-Presidente
Waldemar Gonçalves Ortunho Junior

Diretores
Arthur Pereira Sabbat
Joacil Basilio Rael
Miriam Wimmer

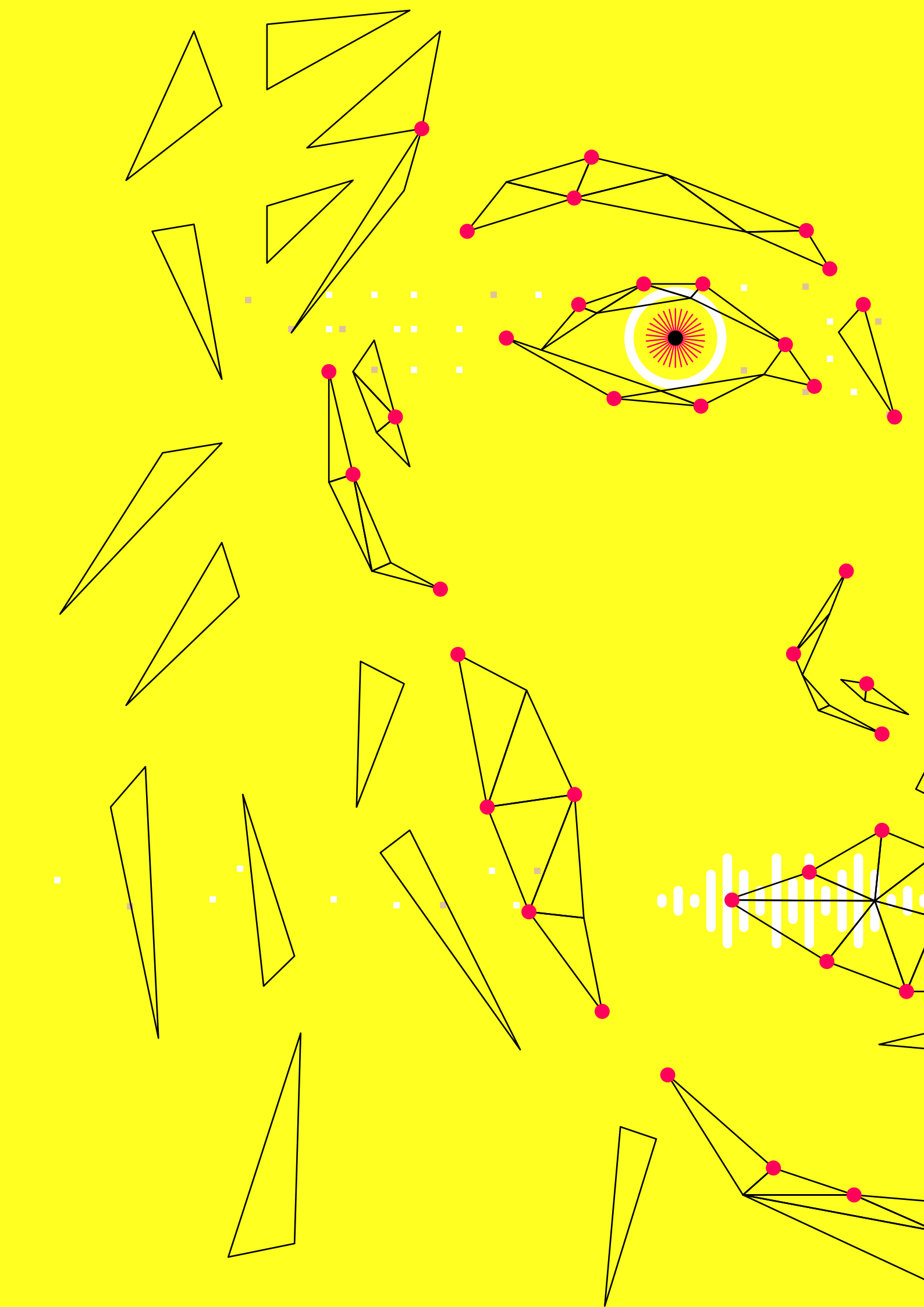
Equipe de elaboração
Coordenação-Geral de Tecnologia e Pesquisa (CGTP)
Fabiana S. P. Faraco Cebrian
Gustavo do Amaral Prudente
Marcelo Santiago Guedes
Maria Carolina Ferreira da Silva
Maria Luiza Duarte Sa
Thiago Guimarães Moraes

Projeto gráfico / editoração eletrônica / capa
André Scofano Maia Porto

1ª edição
Publicação digital – PDF
Radar Tecnológico, Número 2, JUN 2024

ANPD
SCN, Qd. 6, Conj. A,
Ed. Venâncio 3000, Bl. A, 9º andar
Brasília, DF · Brasil · 70716-900
t. (61) 2025-8101
www.anpd.gov.br

‹ sumário ›



‹ sumário executivo ›

A biometria é a análise técnica, realizada por meios matemáticos e estatísticos, das características fisiológicas (tais como impressão digital, face, íris, geometria da mão, vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar *etc*.) de um indivíduo. Quanto maior a quantidade de dados presentes na amostra biométrica provenientes de uma ou mais características, maior será a probabilidade de que ela tenha uma correspondência única, ou seja, a amostra apresentará maior qualidade para que a análise seja mais precisa e confiável.

A popularização da biometria está embasada na possibilidade de seu uso como incremento para a segurança, como em transações eleitorais e financeiras, ou no provimento de acesso a equipamentos e sistemas. Em conjunto com as técnicas de biometria, o uso de câmeras, sistemas de monitoramento e inteligência artificial – IA têm proporcionado o avanço do reconhecimento facial, que, por sua vez, pode ser empregado na verificação de identidade em diversas circunstâncias, como em controles de fronteira, de ambientes, de frequência escolar, de estádios de futebol, entre outros.

Teoricamente, os resultados sugeridos pelo uso do reconhecimento facial são otimistas, mas seus contrapesos na aplicação real são relevantes, tendo em vista que os dados biométricos são dados pessoais sensíveis e afetam massas populacionais, inclusive grupos vulneráveis. Igualmente, os algoritmos utilizados são passíveis de erro e podem refletir e perpetrar aspectos discriminatórios.

O tratamento de dados biométricos, além de ser pauta da Agenda Regulatória da ANPD para o biênio 2023–2024, suscita preocupações significativas sobre a privacidade e a proteção dos dados pessoais dos titulares, principalmente em relação ao reconhecimento facial e sua crescente popularidade.

A Coordenação-Geral de Tecnologia e Pesquisa – CGTP da Autoridade Nacional de Proteção de Dados – ANPD estudou diversos casos de uso

de biometria, em particular de reconhecimento facial no País. Foram levantados casos de segurança pública nos estados da Bahia, Goiás e Rio de Janeiro, bem como outras situações de relevância, relacionadas, por exemplo, à Linha Amarela do Metrô de São Paulo, à rede estadual de ensino do Paraná, aos aeroportos de São Paulo e Rio de Janeiro e a estádios de futebol. Também foram analisados casos do uso da biometria em sistemas de pagamentos e serviços de autenticação.

A seguir são elencados os principais pontos deste estudo preliminar:

1

As tecnologias de biometria empregadas no reconhecimento facial são utilizadas para diversos propósitos, como controle de fronteiras e aeroportos, segurança pública, sistema de saúde, transações financeiras e pagamentos, marketing e experiência do cliente e controle de acesso, podendo empregar técnicas de detecção (descobrir e localizar faces nas imagens e vídeos), identificação (quem é a pessoa da imagem?), verificação (a pessoal existe ou está cadastrada?) e classificação (categorizar o indivíduo por meio de atributos como gênero, etnia, raça, idade ou detecção de emoções, como alegria, felicidade, nervosismo *etc.*).

2

As inovações decorrentes do reconhecimento facial, apoiadas, em especial, pelas tecnologias de Inteligência Artificial, como *machine learning* e *deep learning*, otimizaram os sistemas tradicionais de reconhecimento facial ao permitir, por exemplo, uma identificação mais rápida e precisa, uma vez que os algoritmos são rotineiramente treinados para aprender e extrair características e propriedades faciais de grandes conjuntos de dados. Porém, esse avanço suscita riscos de intrusão à privacidade e aos direitos e liberdades civis dos titulares de dados.

3

Há de se considerar que os vieses e normas culturais e sociais dos indivíduos responsáveis pelo tratamento dos dados biométricos podem se refletir nos algoritmos e nos modelos de aprendizagem, levando a efeitos discriminatórios de ordem racial, social, étnica, de gênero, econômica, entre outros.

4

Os aspectos relacionados à capacidade de um sistema de reconhecimento facial em identificar corretamente uma pessoa podem variar de acordo com o método e a tecnologia utilizada pelo desenvolvedor, ou com a diversidade da população a qual tenham sido aplicados. Isso propicia riscos consideráveis para as pessoas em casos de identificação errônea, como o ocorrido no estado do Rio de Janeiro[1].

5

Os casos estudados estão permeados de questões que por vezes carecem de transparência acerca do tratamento dos dados pessoais e seu compartilhamento, bem como das medidas de segurança necessárias adotadas pelos controladores, as hipóteses legais e as finalidades informadas aos titulares, sem excessos ou desvios, tendo em vista a natureza sensível dos dados.

6

A motivação para a introdução do reconhecimento facial no ambiente escolar pode se fundar, por exemplo, no registro automático de frequência dos estudantes, que, por sua vez, serviria para subsidiar políticas de otimização da gestão do ambiente escolar, de combate à evasão e de segurança. Contudo, o uso das tecnologias de biometria nas escolas suscita preocupação, pois, além de envolver o tratamento de dados sensíveis, há maior vulnerabilidade dos titulares que, por serem crianças e adolescentes em sua maioria, demandam atenção especial, em particular mediante a observância do princípio do melhor interesse, como consta no art. 14 da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018).

7

Recentemente, empresas de tecnologia, como a Apple, Google e Microsoft, anunciaram planos para a adoção e expansão do padrão de autenticação sem senha, que utiliza a biometria como substituto do atual modelo de acesso baseado em senhas aos sistemas e aplicativos.

Ainda que o Brasil não tenha legislação federal específica que trate da implementação de sistemas de videomonitoramento e reconhecimento facial, há propostas legislativas em trâmite no Congresso Nacional sobre

1 *Veja mais no capítulo "Biometria e Reconhecimento Facial no Contexto Brasileiro", subcapítulo "Segurança pública e controle migratório", seção "Estado do Rio de Janeiro", disponível na página 24.*

o tema, que são apresentadas no Anexo I deste estudo.
É importante ressaltar que, ainda que o artigo 4º da LGPD exclua certos tipos de tratamentos de dados de sua abrangência e escopo, os §§ 1º a 5º do artigo supracitado estabelecem regras que devem ser observadas em qualquer hipótese. Assim, conforme o § 1º do art. 4º, ainda que para fins exclusivamente de segurança pública, de investigação ou repressão de infrações penais, o tratamento de dados deve necessariamente observar "o devido processo legal, os princípios gerais de proteção e os direitos do titular" previstos na LGPD. Da mesma forma, devem ser observadas as restrições de tratamento de dados nessas hipóteses por pessoas jurídicas de direito privado (§§ 2º e 4º do art. 4º). Por fim, o § 3º do art. 4º declara que a ANPD emitirá opiniões e recomendações referentes às exceções previstas no inciso III, bem como deverá solicitar aos responsáveis relatório de impacto à proteção de dados pessoais.

Este estudo é apenas um passo inicial da ANPD no tema da biometria e do reconhecimento facial, apresentando os potenciais riscos envolvidos, em particular quanto à privacidade e à proteção de dados pessoais. Apenas com o aprofundamento das análises acerca dessa temática será possível ampliar a compreensão do cenário nacional, bem como a identificação dos riscos, suas formas de mitigação e a relação de uso das tecnologias de biometria com a LGPD.

Por fim, considerando os riscos envolvidos – finalidades secundárias, com compartilhamento dos dados entre controladores; o uso inadequado do consentimento como base legal; a coleta não informada; o nível de acurácia da biometria; os efeitos discriminatórios e a naturalização do uso das tecnologias de reconhecimento facial, sugere-se que o presente documento seja aprofundado em estudos exploratórios em três áreas distintas: i) compartilhamento de dados biométricos coletados inicialmente para finalidade de segurança pública; ii) tratamento de dados biométricos de crianças e adolescentes em ambientes educacionais e iii) uso comercial de dados biométricos.

‹ introdução ›

Os recentes avanços tecnológicos, associados aos interesses público e privado, têm tornado cada vez mais comum o uso de tecnologias de biometria, como o reconhecimento facial.

A popularidade da biometria se baseia na possibilidade de incremento quanto à segurança, como em transações eleitorais e financeiras, no provimento de acesso a equipamentos e sistemas, ou como recurso de não repúdio e verificação de autoria. Além disso, as técnicas de biometria, em conjunto com o uso de câmeras, sistemas de monitoramento e inteligência artificial, têm proporcionado o avanço do reconhecimento facial, que, por sua vez, pode ser empregado na verificação de identidade em diversas circunstâncias, como em controles de fronteira, de frequência escolar, entre outros. Teoricamente, os resultados sugeridos pelo uso dessa ferramenta são otimistas, mas seus contrapesos na aplicação real são relevantes, tendo em vista que os dados biométricos são dados sensíveis e alcançam massas populacionais, inclusive, grupos vulneráveis.

Para além disso, o caso da empresa ViaQuatro, concessionária da Linha Amarela do metrô de São Paulo, tomou protagonismo no ano de 2018 devido ao tratamento e à captura não consentidos de imagens, para fins comerciais, por meio de aparelhos de reconhecimento facial (Zanatta, R. A. F. et al., 2020). De acordo com o Instituto de Defesa de Consumidores – IDEC, o intuito da implementação da tecnologia fugia do escopo da segurança do meio de transporte, pois o objetivo era captar reações das pessoas diante de anúncios publicitários. A ação movida pelo IDEC resultou na condenação da concessionária ao pagamento de R$ 500 mil reais a título de dano moral coletivo e despertou discussões sobre benefícios e riscos da tecnologia (IDEC, 2023).

Mesmo diante de cenários como esse, é possível perceber a crescente popularidade da tecnologia em discussão, especificamente no Brasil. De acordo com o estudo "Tecnologias de Vigilância e Educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras", do centro de pesquisa InternetLab (2023), foram

contabilizadas mais de quinze políticas de adoção de reconhecimento facial nas escolas.

Não obstante, em contraposição às novas possibilidades que o uso da biometria pode proporcionar, surgem preocupações significativas sobre a privacidade e a proteção dos dados pessoais dos titulares dos dados, principalmente em relação ao reconhecimento facial e seu crescente uso no Brasil e no mundo.

Este estudo preliminar objetiva identificar os principais conceitos relacionados à biometria e ao reconhecimento facial, apresentando os potenciais riscos envolvidos. Em paralelo, discorre sobre algumas preocupações advindas com a evolução do tema, em particular quanto à privacidade e à proteção de dados pessoais. Faz, ainda, breve análise sobre o contexto brasileiro e analisa perspectivas de futuro da aplicação dessa ferramenta.

‹ conceitos principais ›

A biometria é a análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo. Segundo o *European Parliamentary Research Service* (EPRS[2], 2021a, p. 1) e o *Office of the Victorian Information Commissioner* – OVIC (2019), a biometria abrange o uso de uma variedade de técnicas e tecnologias diferentes para reconhecer uma pessoa por meio de suas características fisiológicas (tais como impressão digital, face, íris, geometria e vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar *etc*.).

2 *A EPRS – European Parliamentary Research Service, é o centro de pesquisa que realiza estudos para o Parlamento Europeu, subsidiando as atividades legislativas e regulatórias do órgão.*

Quanto maior a quantidade de dados presentes na amostra biométrica, ou seja, dados provenientes de uma ou mais característica, maior será a probabilidade de que ela tenha uma correspondência única. Contudo, haverá a possibilidade de que duas pessoas ou mais possam gerar amostras muito similares ou equivalentes, resultando em um falso-positivo ou falso-negativo. De acordo com Buolamwini *et al*. (2020), o falso-positivo ocorre quando o sistema informa, incorretamente, a relação entre as imagens de duas faces diferentes como sendo a mesma pessoa. Já o falso-negativo ocorre quando o sistema informa que as imagens da face de uma pessoa são diferentes.

As tecnologias de biometria empregadas no reconhecimento facial podem ser utilizadas para diversos propósitos, partindo de uma detecção simples de presença, para níveis mais complexos como identificação, verificação e classificação de indivíduos (EPRS, 2021b).

A detecção consiste em realizar a descoberta e a localização de faces em imagens e vídeos. A constatação da presença de uma face e a localização dela na imagem não se traduz em determinar uma identificação ou atribuição de características, pois representa, apenas, o processo de percepção e determinação da posição das faces na imagem em questão. Ou seja, o processo de detecção é focado em encontrar e localizar faces, não apresentando, portanto, informações sobre a quem pertencem as faces detectadas ou que tipo de pessoas elas podem ser (Buolamwini *et al*, 2020, p. 9).

Após a detecção pela câmera, a imagem da face é capturada e analisada. A depender do método ou do *software* adotado, a análise poderá ser realizada por meio da leitura da geometria da face, de forma a examinar, por exemplo, a distância entre os olhos, a profundidade das órbitas oculares, a distância entre a testa e o queixo, o formato da maçã do rosto, o contorno dos lábios, orelhas e do queixo, dentre outros. Essa análise busca identificar os principais pontos de referência presentes na face capturada e os transforma em um *template* biométrico[3], que será armazenado, após conclusão da análise, juntamente com a imagem original (Buolamwini *et al*, 2020, p. 9).

A identificação consiste em comparar o *template* biométrico de uma pessoa com os demais que estejam no banco de dados ou na galeria de imagens, a fim de descobrir se ele já está cadastrado e a quem pertence (The Alan Turing Institute, 2020, p. 8). A correspondência é positiva quando há a correlação entre o *template* biométrico analisado e o armazenado (EPRS, 2021a, p. 1).

A verificação consiste, basicamente, em realizar a comparação de dois *templates* biométricos a fim de determinar se ambos são compatíveis ou correspondentes (EPRS, 2021a, p. 1). Isto significa que, para a verificação, o que importa é o resultado da comparação entre dois *templates* biométricos ou duas imagens, de forma que não é necessário conhecer, precisamente, a identidade dos indivíduos presentes na imagem ou no *template* para que a correspondência ocorra (The Alan Turing Institute, 2020, p. 8).

A classificação consiste em, baseado no *template* biométrico obtido, categorizar o indivíduo por meio de atributos de classificação (gênero, raça, etnia *etc.*), estimativa (idade), expressão (sorriso, choro *etc.*) ou estado emocional (alegre, feliz, triste, irritado, nervoso, apático *etc.*) (EPRS, 2021a, p. 1).

As inovações trazidas pela tecnologia de reconhecimento facial, apoiadas, em especial, pelas tecnologias de Inteligência Artificial, como *machine learning* e *deep learning*, melhoraram os sistemas tradicionais de reconhecimento facial ao permitir, por exemplo, uma identificação mais rápida e precisa, uma vez que os algoritmos são rotineiramente treinados para aprender e extrair características e propriedades faciais de grandes conjuntos de dados (EPRS, 2021a, p. 2). Porém, tal avanço suscita riscos de violação à privacidade, aos direitos e às liberdades civis.

3 *Os templates biométricos relativos à face também podem ser chamados de faceprints, ou em tradução livre, impressões faciais (Buolamwini et al, 2020).*

‹ funcionalidades da biometria e do reconhecimento facial ›

No início dos anos de 1990, nos Estados Unidos da América – EUA, as tecnologias de biometria eram utilizadas com o foco na identificação e autenticação dos indivíduos, principalmente no setor privado. Mas em 2001, após os atentados terroristas nesse país, houve a expansão do uso das tecnologias biométricas como medidas adicionais de segurança, especialmente em aeroportos (EPRS, 2021b, p. 13).

Apoiada pela evolução tecnológica dos computadores, *hardware*, sistemas e soluções de desenvolvimento de *software*, a biometria tem avançado e se tornado mais barata e robusta, apresentando níveis cada vez menores de erro de identificação (EPRS, 2021b, p. 13 e 15).

A seguir são descritas algumas potencialidades do uso da biometria, em especial as tecnologias de reconhecimento facial, considerando os estudos promovidos pelo EPRS (2021a e 2021b), Dushi (2020), Buolamwini *et al*. (2020), *The Alan Turing Institute* (2020), *Information Commissioner's Office* – ICO (2021), *Office of the Victorian Information Commissioner* – OVIC (2019) e o Laboratório de Políticas Públicas e Internet – LAPIN (2021).

Controle de fronteiras e aeroportos

> O reconhecimento facial, assim como outras técnicas de biometria, pode apoiar os serviços de imigração no controle e fluxo de pessoas, dar celeridade para os processos de identificação, autorização de entrada, registro de saída, embarque e *check-in* e identificar cidadãos que estejam com algum tipo de restrição ou mandado judicial em aberto.

Segurança pública

> O reconhecimento facial, apoiado pelo uso de Circuito Fechado de TV – CFTV ou Centros de Inteligência, como o Centro de Operações Integradas – COI (São Paulo) e Centro Integrado de Inteligência, Comando e Controle – CIICC (Goiás), pode ser utilizado em políticas de segurança pública. Inclusive, há iniciativas de vincular o uso do

reconhecimento facial em programas de cidades inteligentes (vide seção sobre casos de uso no contexto brasileiro).

Sistema de saúde

As tecnologias de biometria podem ser utilizadas para auxiliar os processos de recepção e triagem dos pacientes nas unidades de saúde, tornando-os mais seguros e ágeis. Também podem ser utilizadas para realizar o atendimento de pessoas em estado de inconsciência, já que seria possível a identificação do paciente e verificação do prontuário médico.

Transações financeiras e pagamentos

O reconhecimento facial, bem como outras técnicas de biometria, como a impressão digital, pode ser utilizado para autorizar e confirmar transações financeiras ou pagamentos, proporcionando uma camada extra de segurança.

Marketing e experiência do cliente

O reconhecimento facial pode ser utilizado para direcionar anúncios e promoções personalizados baseados nos interesses e comportamento do cliente, o que possibilitará, por exemplo, experiências mais particulares ao se adentrar em um determinado estabelecimento comercial.

Controle de acesso

Muito além do desbloqueio de computadores e celulares, as tecnologias de biometria podem ser utilizadas na concessão de acesso a edifícios, condomínios, prédios públicos, áreas restritas, bem como registro e frequência de jornada de trabalho, proporcionando níveis de segurança e acurácia mais elevados.

‹ biometria, reconhecimento facial e os dados pessoais ›

A Emenda Constitucional nº 115, de 10 de fevereiro de 2022, alterou a Constituição Federal e incluiu, em seu artigo 5º, a proteção de dados pessoais como um dos direitos e garantias fundamentais.

Logo em seu artigo 1º, a Lei Geral de Proteção de Dados Pessoais deixa claro que visa a preservar os direitos fundamentais à liberdade e à privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural.

O artigo 2º da LGPD apresenta, ainda, o respeito à privacidade (inciso I), a autodeterminação informativa (inciso II) e a inviolabilidade da intimidade, da honra e da imagem (inciso IV). Esses fundamentos fortalecem o controle dos cidadãos sobre suas próprias informações pessoais e o seu protagonismo em relação ao tratamento e à preservação de seus dados pessoais.

Ademais, a LGPD aponta em seu artigo 5º, inciso II, o dado biométrico como um tipo de 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 vinculados a uma pessoa natural".*

Quando as finalidades do tratamento de dados pessoais estão relacionadas à segurança pública, à defesa nacional, à segurança do Estado ou às atividades investigativas ou com o objetivo de impedir a ocorrência de crimes, elas possuem uma aplicação mais restrita da LGPD, conforme pode ser observado pela leitura do artigo 4º, inciso III e suas alíneas.

Ainda que o artigo 4º da Lei Geral de Proteção de Dados Pessoais exclua certos tipos de tratamentos de dados de sua abrangência e escopo, os §§ 1º ao 5º do artigo supracitado estabelecem regras que devem ser observadas em qualquer hipótese. Assim, conforme o § 1º do art. 4º, ainda que para fins exclusivamente de segurança pública, de investigação ou repressão de infrações penais, o tratamento de dados deve necessariamente observar "o devido processo legal, os princípios gerais de proteção e os direitos do titular" previstos na LGPD. Da mesma forma, devem ser observadas as restrições de tratamento de dados nessas hipóteses por pessoas jurídicas de direito privado (§§ 2º e 4º do art. 4º). Por fim, o § 3º do art. 4º declara que a ANPD emitirá opiniões e recomendações

referentes às exceções previstas no inciso III, bem como deverá solicitar aos responsáveis relatório de impacto à proteção de dados pessoais.

Ou seja, a LGPD se aplica ao tratamento de dados biométricos e, ainda que realizado para as finalidades previstas no art. 4º, III da Lei, a ANPD detém competência para firmar entendimentos, estabelecer recomendações ou, como no caso do presente documento, elaborar estudos e manifestações técnicas.

Importante ressaltar que diversos governos e outras autoridades de proteção de dados pelo mundo têm emitido comunicados ou estudos técnicos sobre a biometria e os desafios com relação à privacidade, como é o caso do *Office of the Privacy Commissioner of Canada* – OPC (2022), do OVIC (2019), do ICO (2021), e do EPRS (2021a e 2021b).

As tecnologias de identificação biométrica devem ser usadas com responsabilidade, pois, segundo Dushi (2020, p. 5) e o EPRS (2021a, p. 7), os vieses e normas culturais e sociais dos envolvidos no tratamento dos dados biométricos podem se refletir nos algoritmos e nos modelos de aprendizagem, levando a efeitos discriminatórios de ordem racial, social, étnica, econômica, entre outros.

Como já mencionado, existe, também, o risco de constrangimento às pessoas em decorrência de falha de identificação, onde o sistema possa apresentar um erro de análise combinatória, resultando em um falso-positivo ou falso-negativo. Dessa maneira, um sistema de reconhecimento facial, após a detecção da face e do processo de análise, pode vir a gerar um resultado errôneo de identificação, fazendo com que uma pessoa em pleno exercício de direitos civis e políticos seja confundido com alguém que esteja submetido a medidas restritivas judiciais, por exemplo (EPRS, 2021a, p. 7).

Em 2019, as Autoridades de Proteção de Dados da França e da Suécia mobilizaram uma ação contra a utilização de reconhecimento facial nas escolas que, mediante consentimento prévio, estavam coletando informações através das pupilas dos estudantes. A autoridade francesa considerou que o sistema proposto era contrário aos princípios fundamentais da proporcionalidade e minimização de dados estabelecidos

pela *General Data Protection Regulation* – GDPR (CNIL, 2019). Já a autoridade sueca, após a análise do claro desequilíbrio entre os titulares dos dados e o controlador, considerou que o consentimento não era uma base legal válida (EDPB, 2019).

No ano de 2020, a autoridade de proteção de dados holandesa realizou um aviso formal direcionado a um supermercado que utilizava reconhecimento facial ao vivo, como forma de prevenir furtos, escaneando rostos e comparando-os com as faces de indivíduos previamente banidos do estabelecimento (AUTORITEIT PERSOONSGEGEVENS, 2020). A autoridade afirmou que o uso desse tipo de tecnologia aplicado à segurança pública só era permitido em situações excepcionais, o que não era o caso.

Em 2022, a Autoridade italiana condenou a empresa americana *Clearview AI* ao pagamento de cerca de 20 milhões de euros, em razão da implementação incoerente com os princípios jurídicos da GDPR. De acordo com o órgão, a empresa estadunidense coletava, sem autorização judicial, uma quantidade massiva de fotografias, e, destas, extraía dados biométricos dos cidadãos italianos, rompendo com princípios de transparência, desvio da finalidade e ausência de base legal para a coleta. As autoridades da França (EDPB, 2022b) e Reino Unido (ICO, 2022) também condenaram, em 2022, a *Clearview* ao pagamento de 20 milhões de euros e 7,5 milhões de libras, respectivamente. Essa denúncia foi produto de uma movimentação de um grupo de organizações não governamentais – ONGs no ano de 2021, lideradas pela *Privacy International*. A ação conjunta teve como alvo a atuação da *Clearview AI* na venda da sua tecnologia para serviços de polícia na França, Grécia, Áustria, Itália e Reino Unido.

A ONG *Access Now* realizou uma investigação, em parceria com o LAPIN e entidades de outros países, sobre tecnologia de vigilância na América Latina, trazendo estudos de caso na Argentina, no Brasil e no Equador. A análise do caso argentino problematizou o uso de câmeras de vigilância por vídeo (CFTV) e o Sistema Federal de Identificação Biométrica para a Segurança (SIBIOS), criado em 2011 e administrado pela Polícia Federal argentina sob supervisão do Ministério da Segurança daquele país. O objetivo da iniciativa argentina foi de unificar e digitalizar as bases de dados

de registro dos cidadãos, sendo iniciado por meio da coleta biométrica para emissão de carteiras de identidade e passaportes (*Access Now*, 2021)

Ainda segundo a investigação, nessa coleta eram incluídos dados como impressões digitais, impressões palmares e fotos de rosto, inclusive de pessoas entrando no país. A tecnologia não era utilizada somente no caso de segurança pública e imigração, mas também em programas de previdência social, bancos, impostos, taxas fiscais, educação, eleições e esportes. O estudo constatou falta de transparência e acesso à informação sobre o desenvolvimento dessas políticas, afirmando que o arcabouço normativo demonstra ser insuficiente e que o país carece de questionamentos em torno da coleta de dados massiva decorrente dessa aplicação. O estudo de caso do Brasil apresentou diversos exemplos de uso espalhados por todo território.

Uma preocupação apontada pelo estudo da *Access Now* é a falta de transparência quanto aos acertos e erros dessas tecnologias aplicadas à segurança pública. Durante a pesquisa, ao serem questionados sobre a precisão do sistema, as Secretarias da Segurança Pública da Bahia e o governo de Campina Grande informaram porcentagens de acurácia, mas não proveram detalhes sobre falsos positivos ou negativos, nem pontuaram se os dados permanecem os mesmos em outros cenários, como sob condições não ideais de captura de imagem ou com indivíduos de cores de pele diferentes (*Access Now*, 2021).

No estado da Bahia, o sistema de reconhecimento facial capturou mais de 4,3 milhões de imagens, sendo utilizado em aeroportos, estádios e eventos públicos significativos, culminando até em 42 detenções pela polícia (Farol da Bahia, 2020). Já no Ceará, a tecnologia é aplicada em smartphones da força policial, que capturam rostos de suspeitos quando as autoridades se aproximam (*Access Now*, 2021).

Diante do exposto até aqui e considerando os estudos promovidos pelo EPRS (2021a e 2021b), Dushi (2020), Buolamwini *et al*. (2020), The Alan Turing Institute (2020), ICO (2021), OVIC (2019) e LAPIN (2021 e 2023), a seguir são listados alguns pontos importantes de análise no contexto da privacidade e da proteção de dados pessoais no que tange ao uso de biometria e suas tecnologias.

Uso secundário dos dados pessoais

O uso secundário dos dados pessoais diz respeito ao tratamento posterior de dados pessoais com o fim de alcançar novos objetivos, distintos daqueles que justificaram o tratamento inicial.

Eventual tratamento posterior somente pode ser realizado para uma finalidade que seja compatível com a finalidade original do tratamento, em conformidade com o que dispõem os princípios da finalidade e da adequação (art. 6º, I e II da LGPD). Além disso, a Lei Geral de Proteção de Dados Pessoais estabelece, no inciso III do art. 6º, o princípio da necessidade, de forma que o tratamento de dados pessoais deva ser limitado ao mínimo necessário para a concretização das finalidades previamente estabelecidas pelo controlador, respeitando a abrangência dos dados pertinentes, proporcionais e não excessivos para tal finalidade.

Portanto, se o controlador optar pelo uso dos dados pessoais para finalidades distintas da que justificou o tratamento original, se faz necessário verificar a sua conformidade à LGPD.

Segurança pública como finalidade secundária

Em 2022, a Polícia Rodoviária Federal – PRF contratou o Serviço Federal de Processamento de Dados – SERPRO para realizar a extração completa, com coletas incrementais diárias, da base de dados do Registro Nacional de Carteira de Habilitação – RENACH, de forma a obter uma base de dados única e que contivesse dados biométricos, bem como o histórico de emissões e de demais dados presentes na Carteira Nacional de Habilitação, de todos os condutores registrados na base do RENACH (LAPIN, 2023). Nesse sentido, o caso do compartilhamento dos dados da base do RENACH, que é de propriedade da Secretaria Nacional de Trânsito – SENATRAN, com a PRF, por meio do SERPRO, é um exemplo de uso secundário de dados pessoais.

Inferências e uso secundário de dados biométricos

Dependendo das características do sistema, da infraestrutura do agente de tratamento e de como as informações são armazenadas (seja como *template* ou dados brutos), algumas características biométricas podem revelar outras informações sobre um indivíduo além da assinatura biométrica. Por exemplo, uma imagem bruta de uma biometria facial pode revelar informações de saúde ou características que o titular dos dados pode não querer fornecer ou não consentir no ato da coleta biométrica.

Coleta não informada

Se a coleta de dados biométricos não for realizada de forma transparente, os titulares não conseguirão conceder seu consentimento de forma específica e destacada, o que invalida o uso desta base legal, nos termos do art. 11, I da Lei Geral de Proteção de Dados Pessoais. A falta de transparência também poderá inibir os titulares de exercerem seus direitos previstos na LGPD.

Por exemplo, informações biométricas faciais podem ser capturadas por meio de fotografias que as pessoas não sabem que estão sendo tiradas. Esse risco aumenta ainda mais à medida que as tecnologias se tornam mais avançadas e eficazes na captura de informações biométricas discretamente ou à distância.

Uso inadequado do consentimento como hipótese legal

O consentimento é uma hipótese legal para o tratamento de dados pessoais de característica transacional, ou seja, os titulares dos dados

podem fazer escolhas sobre se e quais dados pessoais serão tratados, bem como precisam saber como, quando e por quanto tempo se dará o tratamento.

No caso de dados pessoais sensíveis, como os dados biométricos, quando não utilizado o consentimento de forma específica e destacada (art. 11, I da LGPD), o controlador poderá utilizar uma das hipóteses legais do inciso II, do art. 11 da Lei.

Efeitos discriminatórios e naturalização da vigilância

O uso cada vez mais difundido da biometria tem implicações potenciais para as identidades dos indivíduos que vão além da autenticação ou da identificação. Reduzir as características biométricas únicas e inatas de um indivíduo a um modelo pode afetar o desenvolvimento de seu senso de identidade e a forma como ele se relaciona com os outros, o que pode resultar em discriminação injusta.

O tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos. Para o InternetLab (2021, p. 77), é necessário considerar os diversos reflexos da psique discriminatória no âmbito da tecnologia digital, pois, os desenvolvedores podem, intencionalmente, produzir tecnologias discriminatórias. Contudo, eles podem, inconscientemente, perpetrar a discriminação com base em visões que partem de estereótipos ou da invisibilidade de grupos minoritários ou vulneráveis, sendo essa visão produto de contextos históricos e reproduzida de forma simbólica em nossa cultura. A discriminação ainda pode se desenvolver segundo vieses ou preconceitos refletidos no ambiente ou na base de dados utilizados no processo de desenvolvimento da tecnologia, os quais também são determinados ou influenciados pelo contexto social.

Além disso, o uso cada vez mais frequente de tecnologias de vigilância e monitoramento nos mais variados contextos pode estimular o senso comum de que estar sob constante vigilância é algo esperado na sociedade contemporânea, o que altera as legítimas expectativas dos titulares quanto à sua privacidade de modo geral.

Acurácia dos sistemas de reconhecimento facial

A acurácia, que é o índice que informa a capacidade de um sistema de reconhecimento facial em identificar corretamente uma pessoa, pode variar de acordo com o método e tecnologia utilizados pelo desenvolvedor ou com a diversidade da população ao qual tenha sido aplicado. Algumas condições, como qualidade da imagem, posição da face, iluminação, oclusão e similaridade populacional, por exemplo, podem colaborar para que o índice de acurácia do sistema seja reduzido.

Assim, se um sistema de verificação ou autenticação biométrica resultar em altas taxas de falsos positivos ou falsos negativos, sua acurácia será baixa.

Desafios à segurança da informação

O uso da identificação biométrica é paralelo à criação e armazenamento de um número crescente de *templates* biométricos. Como qualquer outro dado, os perfis biométricos estão sujeitos a riscos de privacidade, proteção de dados e segurança da informação. Quanto maior for a quantidade de servidores armazenando *template*s biométricos, bem como o tamanho dos bancos de dados, maior será a quantidade de alvos potenciais para ataques cibernéticos e, também, o interesse dos agentes de ameaça (EPRS, 2021b, p. 45).

Assim, ao realizar o tratamento de dados biométricos, o agente de tratamento deverá considerar os riscos aos quais os titulares de dados possam estar expostos, bem como deverá estruturar os sistemas de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios gerais previstos na LGPD e às demais normas regulamentares, conforme consta no art. 49 da Lei Geral de Proteção de Dados Pessoais.

Como consequência do vazamento de dados biométricos pode-se ter, por exemplo, roubo de identidade, danos à reputação, danos morais e materiais, fraude financeira, estresse emocional, problemas com autoridades públicas, dentre tantos outros tipos de transtornos e desgastes para os titulares dos dados.

Portanto, constitui um fator relevante para a mitigação de riscos no tratamento de dados biométrico a implementação de medidas técnicas e administrativas que promovam a proteção dos dados pessoais, que assegurem os diretos dos titulares e que mitiguem os riscos de incidentes de segurança da informação.

‹ biometria e reconhecimento facial no contexto brasileiro ›

Ainda que o índice de precisão seja inferior ao de outras tecnologias de identificação biométrica, como é o caso da impressão digital, a tecnologia de reconhecimento facial tem evoluído substancialmente e, por não requerer contato direto com os indivíduos, tem sua implementação mais facilitada, o que possibilita o uso em espaços públicos sem que as pessoas estejam necessariamente cientes de que estão sendo monitoradas e de que os seus dados biométricos estão sendo tratados.

No Brasil, diferentemente de outros países, como o Reino Unido, não há legislação federal específica que trate da implementação de sistemas de videomonitoramento e reconhecimento facial (Instituto Igarapé, 2020). Contudo, há propostas legislativas em trâmite no Congresso Nacional que dispõem quanto à definição do reconhecimento facial, seu uso no âmbito da segurança pública (Projeto de Lei – PL nº 3.069/2022), sistema financeiro (PL nº 3.822/2023 – Senado) e área cível (PL nº 12/2015), bem como a normatização da IA (PL nº 2.338/2023 – Senado), que são pormenorizadas no Anexo I, ao final deste estudo.

O Centro de Estudos de Segurança e Cidadania (CESeC), fundado pela Universidade Candido Mendes, que é uma das primeiras instituições acadêmicas integralmente dedicadas aos temas de violência e segurança pública no Brasil, possui um projeto de monitoramento da adoção das tecnologias de reconhecimento facial pelas instituições de segurança pública brasileiras chamado de "O Panóptico". Entre 2022 e 2023, o Panóptico conduziu três estudos sobre a adoção do reconhecimento

facial pelos estados de Bahia, Goiás e Rio de Janeiro, que serão abordados mais adiante.

Além dos contextos de segurança pública, a seguir serão apresentados casos de uso para outras finalidades, como em contextos de educação, de controle migratório e de usos comerciais.

Segurança pública e controle migratório

Estado da Bahia

O Governo do Estado da Bahia começou a utilizar tecnologias de videomonitoramento no ano de 2013 quando a Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça, por meio do projeto de integração e articulação entre os órgãos de segurança pública, instalou 400 câmeras de segurança na cidade de Salvador para a Copa das Confederações, em 2013, e para a Copa do Mundo, em 2014 (Nunes, 2023b).

Ainda segundo Nunes (2023b), entre 2018 e 2022, o Governo da Bahia investiu R$ 683 milhões para implementar sistemas de reconhecimento facial. O lançamento do projeto piloto se deu no ano de 2019, às vésperas das festividades de carnaval. Na época, Salvador foi a cidade escolhida e as câmeras foram instaladas nas estações de metrô, no aeroporto Luís Eduardo Magalhães, no estádio Arena Fonte Nova e em terminais rodoviários. No total, 310 câmeras foram espalhadas pela cidade e incorporadas ao sistema de monitoramento já existente.

Contudo, não há documentos sobre o projeto disponíveis nos sites oficiais da Secretaria de Segurança Pública do Estado da Bahia (SSP-BA), o que dificulta a avaliação sobre a forma de coleta, tratamento e segurança dessas informações, os aspectos de privacidade e como poderiam ser utilizadas no futuro. Principalmente pelo fato de que o banco de dados inicialmente utilizado pela SSP-BA possuía informações de mais de 65 mil pessoas.

Ainda em 2019, foi lançado o projeto de expansão do serviço de videomonitoramento com reconhecimento facial para 78 municípios do estado. Na primeira versão do termo de referência do projeto, o "estilo

de cabelo" e o "estilo inferior" foram listados como parâmetros de análise pela tecnologia de reconhecimento facial. Após críticas, o Governo da Bahia revisou o termo de referência e deixou como características e funcionalidades da análise de vídeo somente a identificação do sexo, o grupo etário, a bolsa e a mochila das pessoas no vídeo.

Ainda que a motivação para o uso de tecnologias de reconhecimento facial seja a segurança pública, não foram constatados os efeitos na redução da violência, pois a taxa de criminalidade e os indicadores criminais permaneceram praticamente inalterados, visto que, entre 2018 e 2021, o número de homicídios passou de 1.122 para 1.255. Além disso, o total de mortes decorrentes de ação policial subiu de 790 para 1.010.

Estado de Goiás

O Governo do Estado de Goiás começou a utilizar a tecnologia de reconhecimento facial ainda no ano de 2014 quando, por meio de investimentos próprios e da União, implantou câmeras de segurança na capital goiana.

No ano de 2020, Goiânia já dispunha de mais de 700 câmeras e de *software* de reconhecimento facial desenvolvido pelo estado chamado Harpia. Paulatinamente os municípios goianos foram implementando videomonitoramento e reconhecimento facial, principalmente com o advento da portaria nº 793/2019 do Ministério da Justiça e Segurança Pública – MJSP, que foi lançada para fomentar o uso de tecnologias de videomonitoramento e de reconhecimento facial na segurança a nível nacional (Nunes, 2023a).

O Harpia foi lançado em 2017 e é o resultado de uma parceria entre o Instituto de Identificação da Polícia Civil estadual e a Universidade Federal de Goiás. No ano de seu lançamento, o sistema já possuía um banco de dados com mais de 50 mil fotos, sem que qualquer autoridade tenha declarado de onde as imagens vieram e como esses dados seriam tratados.

No período de 2019 a 2022, dos 89 projetos apresentados nacionalmente em decorrência da portaria nº 793/2019 do MJSP, 51 foram de municípios de Goiás. Desses 51 municípios, 44 mencionaram diretamente em seu termo de referência ou projeto o uso de alguma tecnologia

de reconhecimento facial, ao passo que os outros sete municípios apresentaram propostas para implementação de videomonitoramento sem demais explicações.

Por fim, 37 projetos foram aprovados e receberam os repasses de recursos do Ministério da Justiça e Segurança Pública, o que significou um empenho de pelo menos R$ 8 milhões para diversas cidades[4].

Estado do Rio de Janeiro

No ano de 2019, o Governo do Estado do Rio de Janeiro firmou uma cooperação técnica com a empresa Oi para a implantação de um sistema de videomonitoramento e reconhecimento facial, cuja execução apresentava diversas questões pouco esclarecidas para a população, como o teor do termo de cooperação e os procedimentos operacionais ligados aos monitoramentos e ao tratamento dos dados (Nunes, 2022).

Inicialmente o projeto se deu apenas no bairro de Copacabana, com o total de 34 câmeras, posteriormente, avançou para o bairro do Maracanã e imediações do aeroporto Santos Dumont, totalizando 95 equipamentos de monitoramento e vigilância.

Segundo Nunes (2022), em 2019, o Governo do Rio de Janeiro respondeu que as informações das pessoas identificadas no reconhecimento facial ficam armazenadas e à disposição dos órgãos de segurança pública e justiça criminal para fins de planejamento, investigação e processo, sendo os falsos positivos descartados imediatamente pelo operador do sistema ainda no local de monitoramento.

Muito embora haja a afirmativa de que os falsos positivos são descartados imediatamente pelo operador do sistema ainda no local de monitoramento, uma mulher foi equivocadamente identificada e detida em Copacabana. A confusão foi desfeita na delegacia, onde a mulher teve sua identidade checada e os agentes confirmaram que não se tratava da pessoa que eles procuravam, que, aliás, já estava presa (Globo, 2019).

Aeroportos de São Paulo e Rio de Janeiro

O Governo Federal, por meio do Ministério da Infraestrutura e do Serpro[5], implantou a tecnologia de embarque com reconhecimento facial de

4 *Cidades de Aragarças, Avelinópolis, Bonópolis, Campestre de Goiás, Caturaí, Crixás, Damolândia, Edealina, Inhumas, Ipiranga de Goiás, Itapuranga, Itumbiara, Jataí, Mara Rosa, Mimoso de Goiás, Montes Claros de Goiás, Montividiu, Morrinhos, Mundo Novo, Nazário, Niquelândia, Nova América, Orizona, Padre Bernardo, Palminópolis, Petrolina de Goiás, Piracanjuba, Pirenópolis, Porteirão, Santa Bárbara de Goiás, São Francisco de Goiás, Turvelândia, Valparaíso de Goiás, Goiânia, Pires do Rio, Ipameri e Planaltina*

5 *O Serpro trata dados pessoais de bases de dados do Poder Público para oferecer serviços para órgãos públicos e para o setor privado. Para ver um exemplo de serviço oferecido para o setor privado, ver a seção sobre usos comerciais.*

passageiros e tripulantes[6], dispensando a apresentação, no check-in e no embarque às aeronaves, de bilhetes aéreos e documentos de identificação de pessoas também em voos domésticos partindo dos terminais de São Paulo (Congonhas) e Rio de Janeiro (Santos Dumont) (SERPRO, 2023a).

O processo de reconhecimento facial dos passageiros é realizado em etapas, sendo a primeira no acesso à sala de embarque e, a segunda, no acesso à aeronave. Todo o processo de análise é feito por meio de consulta à base de dados dos órgãos oficiais, onde se verifica a existência de cadastro do passageiro e cartão de embarque válido.

Para o tripulante que optar pelo reconhecimento facial, seu acesso é por meio da aplicação Embarque + Seguro Tripulantes em sua conta pessoal da plataforma gov.br.

As companhias aéreas que operam nos aeroportos de Congonhas e Santos Dumont podem adotar procedimentos próprios de reconhecimento facial, via Serpro, para o cadastramento biométrico e validação do passageiro na base governamental.

Estádios de futebol

A Confederação Brasileira de Futebol e o Ministério da Justiça e Segurança Pública assinaram um acordo de cooperação técnica, chamado de "Estádio Seguro", para a implementação de políticas de segurança pública nos estádios de futebol do País, cuja premissa é implementar um sistema biométrico e de reconhecimento facial que permita a identificação dos torcedores, visando a coibir atos criminosos de racismo e impedir o acesso por parte de torcedores que possuam algum tipo de restrição judicial ou mandados em aberto (CBF, 2023).

Cidades Inteligentes – Cidade Segura Campinas e Smart Sampa

Em alguns casos, tecnologias de reconhecimento facial fazem parte de programas de construção de cidades inteligentes. É

6 *O + Seguro é um sistema de reconhecimento por biometria, que valida a identidade do viajante por selfies tirados na hora.*

o caso dos projetos "Cidade Segura Campinas" (CAMPINAS, 2019) e o da capital paulista, "Smart Sampa" (Folha de São Paulo, 2023). É possível notar, portanto, que a segurança pública faz parte do pacto de políticas públicas que se visa alcançar com esses programas. Na primeira edição da série Radar Tecnológico, explorou-se o tema das cidades inteligentes e a proteção de dados (ANPD, 2023).

O projeto Smart Sampa contará com 20 mil câmeras que serão instaladas no entorno de escolas, unidades básicas de saúde, parques, áreas de grande circulação e com maior incidência de criminalidade e nas entradas e saídas do município. Ao todo, serão implantadas 3.300 câmeras na região central, 6 mil na Zona Leste, 3.500 na Zona Oeste, 2.700 na Zona Norte e 4.500 na Zona Sul. Contudo, o quantitativo de equipamentos poderá ser ampliado para 40 mil, pois o sistema permitirá a integração com mais 20 mil câmeras pertencentes a munícipes, empresas e concessionárias. Além disso, todos os alertas emitidos pelo sistema passarão pela análise de agentes, de forma que as circunstâncias de cada caso sejam averiguadas antes que qualquer medida seja tomada (São Paulo, 2023).

O Smart Sampa também terá um canal de comunicação com a população, via Internet, por meio do acompanhamento marcadores em postagens públicas, *hashtags*, menções de órgãos públicos e comentários em postagens nos canais oficiais dos serviços municipais, o que permitirá identificar as demandas, dúvidas, sugestões e reclamações (São Paulo, 2023).

Educação

O InternetLab, com o apoio da *Privacy International*, publicou em março de 2023 o relatório "Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas

brasileiras", que identificou e analisou quinze políticas de adoção do reconhecimento facial em escolas do Brasil (InternetLab, 2023).

De acordo com o relatório, as finalidades elencadas pelos governos para a implementação do reconhecimento facial nas escolas públicas estão apoiadas em três grupos:

+ **Otimização da gestão do ambiente escolar**: gestão de registro de presença, merendas e material escolar;
+ **Combate à evasão escolar**: coibir registro de presença indevido, comunicação ao Conselho Tutelar e gerenciamento de programas sociais; e
+ **Segurança**: evitar que estudantes saiam sem a autorização e para salvaguarda do patrimônio escolar.

De acordo com o estudo, o Brasil conta com 15 cidades dotadas de iniciativas contendo tecnologias de reconhecimento facial nas escolas, todas pertencentes à rede pública. Porém, até março de 2023, mês de publicação do documento, apenas as iniciativas das cidades de Betim (MG), Jaboatão dos Guararapes (PE) e Goiânia (GO) já estavam em funcionamento.

O Ministério da Educação mencionou que não regulamenta iniciativas que envolvam tecnologias de reconhecimento facial e que as secretarias municipais detêm autonomia nessa questão. Com isso, cabe mencionar que somente o município de Mata de São João (BA) afirmou contar com normas orientativas por meio de leis municipais que versam sobre o tratamento de dados pessoais e a segurança da informação municipal. Dessa maneira, é possível inferir que a ausência de instrumentos normativos acomete a maioria das iniciativas, gerando diversos riscos. Isso porque a tecnologia, não só nesse tipo de aplicação, apresenta imprecisões, o que torna todo seu objetivo incerto e coloca os titulares de dados em uma posição de vulnerabilidade. Um exemplo disso foi visto na iniciativa do município de Xaxim (SC), sendo comprovado que a tecnologia aplicada registrou faltas dos alunos da rede municipal, enquanto eles estavam comprovadamente presentes.

É importante ressaltar que dentre as 15 iniciativas levantadas pelo InternetLab, as cidades de Potirendaba (SP), Rio de Janeiro (RJ), Porto Alegre (RS), Santos (SP) e Fortaleza (CE) descontinuaram a ação. As razões não foram iguais para todos, mas, em suma, as descontinuidades foram motivadas por conta de contestações de órgãos públicos e da sociedade civil e pela ausência de estrutura técnica e de medidas de segurança e governança.

O uso das tecnologias de biometria em ambientes escolares suscita preocupação, pois, além de envolver o tratamento de dados sensíveis, há maior vulnerabilidade dos titulares que, por serem crianças e adolescentes em sua maioria, demandam atenção especial, em particular mediante a observância do princípio do melhor interesse, como consta no art. 14 da LGPD.

Rede Estadual de Ensino do Paraná

O Governo do Estado do Paraná implantou em 2023 um sistema de registro de presença e frequência dos alunos por meio do reconhecimento facial em 1.667 escolas que compõem a rede estadual de ensino, onde todos os alunos tiveram suas fotos cadastradas pelo aplicativo Escola Paraná (Paraná, 2023).

Tendo os alunos cadastrados, o registro de frequência em sala pôde ser feito por meio do aplicativo Escola Paraná Professores ou por meio do sítio Registro de Classe Online (RCO), ambos desenvolvidos pela Companhia de Tecnologia da Informação e Comunicação do Paraná – Celepar.

O Observatório das Metrópoles – Núcleo Curitiba (Universidade Federal do Paraná – UFPR), o JararacaLab, (Pontifícia Universidade Católica do Paraná – PUC-PR) e a Rede LAVITS produziram um relatório sintetizando os achados com relação ao projeto de Reconhecimento Facial nas escolas públicas paranaenses (Jararaca, 2023).

De acordo com o relatório, os instrumentos utilizados, como pedido de consentimento para o tratamento de dados biométricos de crianças e adolescentes e a Política de Privacidade, estão em desacordo com os artigos 11 (inciso I) e 14 da LGPD. Além disso, o Termo de Cessão de Uso de Imagem condiciona o acesso à educação à cessão compulsória da imagem dos estudantes.

O relatório aponta, também, que há incompreensão por parte da Secretaria de Estado e Educação do Paraná de que o tratamento de dados biométricos diz respeito a dados sensíveis. Bem como, não há registro de estudo de impacto à privacidade e a proteção de dados pessoais quanto à implementação do reconhecimento facial.

Por fim, o documento constata que a adoção do sistema de reconhecimento facial como instrumento de registro de frequência nas escolas públicas foi realizada sem consulta pública e sem o escrutínio do poder legislativo estadual e que a possibilidade de realizar o monitoramento de emoções já está contida na tecnologia atualmente em uso, o que a situa numa abrangência fora de um escopo limitado e do consentimento utilizado.

Usos comerciais

Além dos casos já mencionados, serão abordados outros casos de relevância em contextos do setor privado, para usos comerciais, como do Metrô de São Paulo (TJSP, 2023), da Serasa Experian (Serasa Experian, 2023), da rede varejista C&A (STARTSE, 2023), do Serpro (SERPRO, 2023b), e do setor farmacêutico (ANPD, 2023).

Publicidade no Metrô de São Paulo – o caso ViaQuatro

No ano de 2018, a empresa ViaQuatro, concessionária responsável por operar a linha amarela do metrô de São Paulo, implantou um sistema de

reconhecimento facial que identificava emoção, gênero e faixa etária das pessoas que circulavam pelas estações. As imagens captadas eram usadas para fins publicitários e comerciais e, para tanto, a empresa buscava detectar as principais características dos indivíduos, como emoções e reações apresentadas aos anúncios veiculados, que circulavam pelas estações em determinados locais e horários.

Após diversos embates judiciais, a 8ª Câmara de Direito Público do Tribunal de Justiça de São Paulo condenou a empresa ViaQuatro por conduta reprovável caracterizando dano moral coletivo, devido à ausência de prévia autorização para a captação das imagens e considerando o incalculável número de passageiros que transitam pela plataforma de metrô todos os dias. A empresa foi condenada ao pagamento de indenização no valor de quinhentos mil reais.

Controvérsias sobre o reconhecimento facial de emoções

Embora seja comum assumir que o estado emocional de uma pessoa pode ser inferido a partir de seus movimentos faciais, de acordo com Barrett *et al* (2019), há evidências científicas que apontam dificuldades para garantir que expressões faciais possam representar emoções de modo homogêneo, dada a influência, por exemplo, de fatores culturais e fisiológicos.

Essas suposições podem afetar julgamentos legais, decisões políticas, protocolos de segurança nacional e práticas educacionais, bem como o desenvolvimento de aplicações comerciais, além de permear as interações sociais cotidianas. Além disso, o uso de biometria para reconhecer emoções tem o potencial de gerar severos efeitos discriminatórios, a depender da finalidade de seu uso.

Serviços de autenticação – Serasa Experian

Em 2023, no Brasil, empresas como a Serasa Experian, têm ofertado aos segmentos de bancos, *fintechs*, telecomunicações, seguradoras, *e-commerce*, varejo, aplicativos e outros, sistemas de autenticação por meio de reconhecimento facial. Aliás, a própria Serasa Experian informa, em seu portal, possuir mais de 100 milhões de faces únicas (*selfie* + documento) (Serasa Experian, 2023).

Serviços de autenticação – Serpro

Há alguns anos o SERPRO oferece a solução Datavalid, a qual permite a validação dos dados cadastrais e biométricos, em posse dos agentes de tratamento, utilizando as bases oficiais do governo, tais como Receita Federal e Secretaria Nacional de Trânsito. O uso da solução se dá por meio de uma interface de programação de aplicação – API *(Application Programming Interface)*, de forma que o controlador submete os dados ao Datavalid, que por sua vez fará a validação nas bases do governo e devolverá o resultado da validação.

Sistemas de pagamento – Rede varejista C&A

A rede varejista C&A passou a permitir que os clientes realizem os pagamentos, nas lojas físicas, informando apenas o CPF, sua senha e seu reconhecimento facial. Os clientes utilizariam, portanto, o reconhecimento facial para efetuar os pagamentos, não sendo mais necessário o uso de senha. Contudo, tal funcionalidade estaria disponível apenas para os clientes que se cadastraram no serviço de pagamentos da própria marca, chamado de C&A Pay.

Sistemas de pagamento – Setor farmacêutico

Recentemente, a ANPD, por meio da Nota Técnica nº 4/CGTP/ANPD (ANPD, 2023), manifestou-se sobre o tratamento de dados pessoais no setor farmacêutico. Ao discorrer sobre o caso, a Nota Técnica abordou o uso de biometria por parte do Grupo Raia Drogasil e da farmácia Drogaria Iguatemi. Enquanto o Grupo Raia Drogasil estava realizando a utilização da biometria por impressão digital, a Drogaria Iguatemi implantou um sistema de pagamentos por meio do reconhecimento facial.

No caso da Drogaria Iguatemi, o sistema operou em parceria com a Cielo e com a *startup* Payface e as motivações foram a garantia da prevenção à

fraude e à segurança do titular, concessão de descontos e perfilamento de consumo de clientes para sua fidelização.

‹ perspectivas de futuro ›

Passwordless: a substituição de senhas por *templates* biométricos

Com o objetivo de implementar novos modelos de autenticação na Internet, as gigantes da tecnologia Apple, Google e Microsoft anunciaram, em 2022, planos para a adoção e expansão do padrão *passwordless* criado pela FIDO Alliance (Apple, 2022).

FIDO (First Identity Online) Alliance

A FIDO Alliance (associação aberta da indústria da tecnologia) procedeu ao desenvolvimento de um padrão de autenticação *passwordless*, ou seja, um padrão que utiliza a face ou a digital como substituto do atual modelo de autenticação baseado em senhas (Fido Alliance, 2023).

Recentemente o International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) reconheceu as especificações de autenticação remota FIDO UAF e a FIDO CTAP como padrões internacionais oficiais de autenticação.

De acordo com a Microsoft (2020), a adoção dos padrões UAF[7] e CTAP[8] da FIDO Alliance permitirá que as pessoas possam se autenticar em seus equipamentos, aplicativos e serviços com credenciais de *login* sem senha *(passwordless)* e resistentes às técnicas de *phishing*[9].

7 *O FIDO UAF 1.2 é o padrão de autenticação sem senha para dispositivos móveis e que utiliza a biometria como forma de autenticação.*

8 *O FIDO CTAP 2.1 é o padrão destinado aos computadores que permite a autenticação sem senha nos navegadores de internet por meio de tokens e leitores USB, NFC ou BLE.*

9 *Tipo de fraude na qual o golpista tenta obter informações pessoais e financeiras do usuário, combinando meios técnicos e engenharia social (CERT. BR, 2022).*

Interface cérebro-computador e *Neurotechs*

Um dos desdobramentos discutidos em relação aos dados biométricos é a da neurotecnologia. Acredita-se que a evolução da coleta desses dados irá alcançar a atividade neural, suscitando implicações sobre a potencialidade de interfaces que afirmam conseguir monitorar, ler ou alterar atividade do sistema nervoso humano, como é o caso do *brain-computer interface* – BCI, ou interface cérebro-computador.

O BCI é uma técnica de biometria que, por meio de interpretação das ondas cerebrais, permite controlar dispositivos com a mente, podendo ser empregado na reabilitação de pessoas com deficiências e na obtenção de informações sobre o funcionamento do cérebro, o que pode resultar em novas descobertas e tratamentos médicos.

> De acordo com a NeuroTech Analytics, nos últimos 10 anos, os investimentos em neurotecnologia expandiram 21 vezes, totalizando 33.2 bilhões de dólares (NeuroTech Analytics, 2021). Como exemplos da sua evolução ao redor do mundo, é possível apontar iniciativas em diversos países, como a BRAIN Initiative, do governo americano, o Human Brain Project, proveniente da União Europeia, o China Brain Project, de autoria chinesa, entre outros (Strategic Market Research LLP, 2022).
>
> É relevante mencionar que as pesquisas não estão limitadas ao setor governamental. A Microsoft, Johnson & Johnson, DARPA (Defense Advanced Research Projects Agency) e o Meta também são levantados como investidores nesse sentido (NeuroTech Analytics, 2021).

Recentemente, em 28 de julho de 2023, o *Northwell Health's Feinstein Institutes for Medical Research* publicou um artigo informando que

implantaram, com sucesso, microchips no cérebro de um homem tetraplégico e que desenvolveram algoritmos de inteligência artificial para reconectar seu cérebro ao corpo e à medula espinhal. Este duplo desvio neural forma uma ponte eletrônica que permite que a informação flua mais uma vez entre o cérebro e o corpo paralisado do homem, de forma a restaurar o movimento e as sensações em sua mão, punho e braço, mesmo fora do laboratório (Northwell, 2023).

A crescente expansão por esse ramo da tecnologia suscita a discussão sobre seus contrapontos, tendo em vista que o sistema neurológico traz consigo dados sensíveis, referentes ao controle de movimentos, comportamentos, identidades, decisões, sentimentos, opiniões, entre outros. Caso seja possível coletar todas essas informações, o procedimento de governança deverá tomar uma rigidez diferenciada, e os arcabouços normativos e decisórios deverão se revestir de cautela quanto à defesa da privacidade e à segurança de dados dotados desse nível de sensibilidade.

‹ considerações finais ›

O uso das tecnologias de biometria já é algo corriqueiro, podendo ser encontradas como métodos de acesso aos computadores, celulares e sistemas, como fator de segurança para autenticação das transações financeiras. Além disso, são utilizadascomo ferramenta de apoio ao controle de fronteiras, aeroportos e políticas públicas.

Ainda que o artigo 4º da Lei Geral de Proteção de Dados Pessoais exclua certos tipos de tratamentos de dados de sua abrangência e escopo, os §§ 1º a 5º do artigo supracitado estabelecem regras que devem ser observadas em qualquer hipótese. Assim, conforme o § 1º do art. 4º, ainda que para fins exclusivamente de segurança pública, de investigação ou repressão de infrações penais, o tratamento de dados deve necessariamente observar "o devido processo legal, os princípios gerais de proteção e os direitos do titular" previstos na LGPD. Da mesma forma, devem ser observadas as restrições de tratamento de dados nessas hipóteses por pessoas jurídicas de direito privado (§§ 2º e 4º do art. 4º). Por fim, o § 3º do art. 4º declara que a ANPD emitirá opiniões e recomendações referentes às exceções previstas no inciso III, bem como deverá solicitar aos responsáveis relatório de impacto à proteção de dados pessoais.

Os avanços tecnológicos trazem diversos riscos e desafios, principalmente quanto à privacidade, à proteção de dados e à segurança da informação. As tecnologias biométricas evoluíram significativamente nos últimos anos e sua utilização tem se tornado cada vez mais presente e abrangente, envolvendo, inclusive, o uso de inteligência artificial e tratamento de dados em larga escala.

As atuais tecnologias de reconhecimento facial, apoiadas pelo uso de inteligência artificial, têm aumentado sua acurácia, sobretudo quando a sua condução é norteada pelo aprendizado de máquina alimentado em grandes bases de dados. Contudo, é importante reiterar que a acurácia é apenas um dos desafios inerentes a essas tecnologias, no que diz respeito à privacidade e à proteção de dados. Como constatado neste estudo, há diversas outras questões que precisam ser balizadas, seja pelo

setor público, seja pelo setor privado, quando se decide pelo uso de tecnologias de biometria, como o reconhecimento facial.

Este estudo é apenas um passo inicial da ANPD no tema da biometria e do reconhecimento facial, apresentando os potenciais riscos envolvidos, em particular quanto à privacidade e à proteção de dados pessoais. Apenas com o aprofundamento das análises acerca dessa temática será possível ampliar a compreensão do cenário nacional, bem como a identificação das principais controvérsias e a relação das tecnologias de biometria com a LGPD.

‹ anexo 1 ›

Análise sobre projetos de lei em torno do tema biometria e reconhecimento facial

Projeto de Lei	*Tema central*	*Pontos importantes*	*Comentário*	*Artigos da LGPD relacionados*
PL nº 3.822/2023 – Senado Federal	Dispõe sobre a utilização de reconhecimento facial ou de biometria digital na abertura de conta de depósito bancário.	Os dados colhidos na abertura da conta de depósito bancário deverão ser validados por meio do acesso a **bancos de dados biométricos públicos**; Sanções previstas serão consoante o Código de Defesa do Consumidor;	O projeto de lei é curto, mencionando bancos de dados biométricos públicos, que não são detalhados em relação às medidas de segurança e prevenção. Sua justificativa se baseia na mitigação de fraudes.	Art. 2º, IV, art. 10, art. 11, alínea g.
PL nº 2.338/2023 – Senado Federal	Dispõe sobre o uso da Inteligência Artificial.	A Autoridade Nacional de Proteção de Dados já emitiu duas análises acerca do projeto. Disponíveis em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf	É imprescindível a compatibilização das sobreposições e conflitos existentes entre o PL e a LGPD, em especial no que concerne às atribuições legais da ANPD, inclusive as de caráter fiscalizatório; A fim de incentivar a inovação responsável, é necessário que o PL disponha de forma mais específica sobre a proteção de dados pessoais nos *sandboxes* de IA que envolvam o tratamento desses dados.	Art. 4º, art. 6º, art. 9º, art. 14º, art. 18º, art. 19º, art. 20º, art. 38º, art. 46º, art. 49º, art. 50º, art. 52º, art. 53º e art. 55º.

Projeto de Lei	*Tema central*	*Pontos importantes*	*Comentário*	*Artigos da LGPD relacionados*
PL nº 12/2015 – Câmara dos Deputados (apensados PL nº 4.612/2019 e PL nº 4.901/2019)	Dispõe sobre a utilização de sistemas de verificação biométrica, modifica o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, a fim de tipificar o ato de alteração ilícita de dados em sistemas informatizados, e dá outras providências.	O disposto nesta lei não se aplica às hipóteses dos incisos I, II, III e IV do art. 4º da Lei no 13.709, de 14 de agosto de 2018, com aplicação suplementar da LGPD; O armazenamento dos dados biométricos somente ocorrerá por meio do **consentimento livre, informado, inequívoco, expresso e específico de seu titular**, ressalvadas as exceções de interesse público, e terá como finalidade **a confirmação da identidade do seu titular**; Fica vedada a troca, venda, combinação, coleta ou interconexão de dados biométricos não autorizados pelo seu titular, ressalvadas, apenas, as referentes ao interesse público; O recurso a sistemas de verificação biométrica e as demais formas de tratamento de dados biométricos no meio eletrônico **serão regulamentados pela Autoridade Nacional de Proteção de Dados**; O uso de sistemas biométricos deve ser o mais robusto, escalável e interoperável possível, conforme padrões mínimos estabelecidos na regulamentação desta Lei; O titular terá garantido o **livre acesso** aos seus dados biométricos, além da possibilidade **de sua retificação e livre permissão ao cancelamento**, ressalvadas as hipóteses de interesse público; A proteção dos dados biométricos é considerada como uma atividade de risco, submetendo-se ao regime da **responsabilidade objetiva.**	Os apensos tratam sobre as tecnologias de reconhecimento facial e emocional, e do aprimoramento das disposições de identificação biométrica. Adiciona, também, nova tipificação penal para inserção indevida de dados biométricos. Além disso, o projeto de lei traz fatores basilares para o uso ético da tecnologia, como consentimento, transparência e direito de cancelamento.	Art. 4º, incisos I, II, III e IV, art. 5º, XXII, art. 6º, art. 11, art. 55.

Projeto de Lei	*Tema central*	*Pontos importantes*	*Comentário*	*Artigos da LGPD relacionados*
PL nº 3.069/2022	Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências.	Nenhuma ação ou diligência policial de restrição da liberdade de ir e vir poderá ser efetuada simplesmente a partir do reconhecimento facial, sem a confirmação de um especialista; O resultado assertivo e inequívoco para identificação de um alvo ficará sujeito à confirmação **multi biométrica (associação do RF com o exame papiloscópico feito por um profissional habilitado)**; Permite a busca de pessoas eventualmente desaparecidas, **tais como crianças, idosos, pessoas em situação de vulnerabilidade**; Nos locais onde houver captura de imagens para reconhecimento facial (RF), devem ser **fixadas placas visíveis informativas**;	O projeto de lei em questão traz a possibilidade de confirmação multibiométrica, o que poderia, em teoria, mitigar os falsos resultados. Além disso, o projeto permite a busca de pessoas desaparecidas através da tecnologia, mencionando públicos vulneráveis.	Art. 4, III, art. 11, II.
Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal – LGPD Pena[10]	O anteprojeto dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.	O tratamento de **dados pessoais sensíveis somente poderá** ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará a autoridade supervisora, Conselho Nacional de Justiça CNJ. O capítulo VII, que compreende os art. 42 ao 44, aborda o uso de tecnologias de monitoramento e tratamento de dados de elevado risco para direitos, liberdades e garantias dos titulares dos dados.	O anteprojeto aponta o Conselho Nacional de Justiça (CNJ) como autoridade supervisora. A iniciativa do texto do anteprojeto foi o de proporcionar maior segurança jurídica para que os órgãos de investigação e repressão criminais pudessem exercer as suas funções, sem prejuízos para as garantias processuais penais e os direitos fundamentais dos titulares de dados envolvidos.	Artigo 4º, III, art. 6º, art. 17º, art. 18º, art. 19º, art. 20º, art. 21º e art. 22º.

10 *Em novembro de 2020 uma comissão de juristas apresentou à Presidência da Câmara dos Deputados o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal, ficando conhecida como LGPD Penal. Ainda que não seja um projeto de lei, o anteprojeto buscou suprir a demanda apresentada pelo art. 4º, §1º da LGPD e suas estrutura é muito semelhante ao PL nº1515/2022*

Projeto de Lei	*Tema central*	*Pontos importantes*	*Comentário*	*Artigos da LGPD relacionados*
PL nº 1.515/2022	O projeto de lei está baseado em três pilares: **(i)** proteção dos direitos fundamentais de segurança, liberdade e de privacidade; **(ii)** eficiência da atuação dos órgãos responsáveis; e **(iii)** intercâmbio de dados pessoais entre autoridades competentes.	O projeto de lei adota uma estrutura muito semelhante ao do Anteprojeto – LGPD Penal. O compartilhamento de dados pessoais, **inclusive dados sensíveis**, para os fins de segurança do Estado e defesa nacional poderá ser realizado entre os órgãos incumbidos dessas atividades sem dificuldades. O PL traz, nas disposições finais, uma série de modificações à Lei nº 12.037, relativas ao Banco Nacional Multibiométrico e de Impressões Digitais.	O projeto de lei cria regras que permitem aos controladores recusar, adiar ou limitar a prestação de informações ou concessão de acesso quando solicitado pelos titulares. Embora similar ao Anteprojeto da LGPD Penal, o PL nº 1.515/2022 amplia consideravelmente o poder do Estado, o que pode implicar em excessividades capazes de promover usos indiscriminados de dados pessoais por parte de autoridades públicas. Aponta a Autoridade Nacional de Proteção de Dados (ANPD) como autoridade supervisora. E, no capítulo VII, seção I, declara que a ANPD será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional, de forma cumulativa às suas atribuições estabelecidas na Lei nº 13.709, de 14 de agosto de 2018, bem como outras responsabilidades descritas no art. 48.	Artigo 4º, III.
PL nº 522/2022	Modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção.	O Projeto de Lei 522/22 regulamenta a proteção do uso e do tratamento de dados neurais – ou seja, informações obtidas, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador, ou qualquer outra tecnologia, invasiva ou não-invasiva.	**Consentimento do titular**: de acordo com a proposta, o tratamento de dados neurais somente ocorrerá quando o titular ou o responsável legal consentir, de forma específica e destacada, para finalidades específicas, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente.	Altera os art. 5º e 13º da LGPD.

Projeto de Lei	*Tema central*	*Pontos importantes*	*Comentário*	*Artigos da LGPD relacionados*
			Danos à integridade psicológica: o projeto também veda o uso de qualquer interface cérebro-computador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica. Além disso, proíbe a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica. **Definição**: o texto conceitua interface cérebro-computador como qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo.	

‹ referências ›

ACCESS NOW, **Tecnologia de Vigilância na América Latina**: Feita no Exterior, Implantada em Casa, 2021. Disponível em: <https://www.accessnow.org/wp-content/uploads/2021/08/vigilancia-latam-port.pdf>. Acesso em: 01 ago. 2023.

APPLE, ***Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign ins***, 2022. Disponível em: <https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard>. Acesso em: 01 ago. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD, **Nota Técnica nº 4/2023/CGTP/ANPD, 2023**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-nota-tecnica-sobre-tratamento-de-dados-pessoais-no-setor-farmaceutico/NotaTecnica4Atualizada.pdf>.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. **Radar Tecnológico CGTP/ANPD – Cidades Inteligentes**, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf>.

AUTORITEIT PERSOONSGEGEVENS, ***Dutch DPA issues formal warning to supermarket for use of facial recognition technology***, 2020. Disponível em: <https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognition-technology>. Acesso em: 01 ago. 2023.

BARRETT, L. F. et al., ***Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements***, 2019. Psychological Science in the Public Interest, 20, 1–68.

BUOLAMWINI, Joy et al., ***Facial Recognition Technologies: A Primer***, 2020. Disponível em: <https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf>. Acesso em: 01 ago. 2023.

BRASIL. **Constituição da República Federativa do Brasil, 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 01ago. 2023.

BRASIL, **Emenda Constitucional nº 115**, 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 01 ago. 2023.

BRASIL, Lei nº 13.709, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.Acesso em: 01 ago. 2023.

CAMPINAS, Prefeitura Municipal. **UOL destaca Campinas em projeto inédito de reconhecimento facial**, 2019. Disponível em: <https://portal.campinas.sp.gov.br/noticia/35659>. Acesso em: 01 ago. 2023.

CERT.BR, **Phishing e outros golpes**, 2022. Disponível em: <https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishing-golpes.pdf>. Acesso em: 01 ago. 2023.

COMMISSION NATIONALE INFORMATIQUE & LIBERTéS - CNIL, ***Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position***, 2019. Disponível em: <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>. Acesso em: 01 ago. 2023.

COMMISSION NATIONALE INFORMATIQUE & LIBERTéS - CNIL, ***Reconnaissance faciale : sanction de 20 millions d'euros à l'encontre de CLEARVIEW AI***, 2022. Disponível em: <https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai>. Acesso em 01 ago. 2023.

CONFEDERAÇÃO BRASILEIRA DE FUTEBOL - CBF, **Presidente da CBF cumpre extensa agenda de compromissos no Rio e em Brasília**, 2023. Disponível em: <https://www.cbf.com.br/a-cbf/informes/index/presidente-da-cbf-cumpre-extensa-agenda-de-compromissos-no-rio-e-em-b>. Acesso em: 01 ago. 2023.

DUSHI, Desara, ***The use of facial recognition technology in EU law enforcement: Fundamental rights implications***, 2020. Disponível em: <https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content>.Acesso em: 01 ago. 2023.

EUROPEAN DATA PROTECTION BOARD - EDPB, ***Facial recognition in school renders Sweden's first GDPR fine***, 2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv>. Acesso em: 01 ago. 2023.

EUROPEAN DATA PROTECTION BOARD - EDPB, ***Facial recognition: Italian SA fines Clearview AI EUR 20 million***, 2022a. Disponível em: <https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en>. Acesso em: 01 ago. 2023.

EUROPEAN DATA PROTECTION BOARD - EDPB, ***The French SA fines Clearview AI EUR 20 million***, 2022b. Disponível em: <https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en>. Acesso em: 01 ago. 2023.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE - EPRS, ***Regulating facial recognition in the EU***, 2021a. Disponível em: <https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021>.Acesso em: 01. ago. 2023.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE – EPRS, ***Biometric Recognition and Behavioural Detection***, 2021b. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf>. Acesso em: 01 ago. 2023.

FAROL DA BAHIA, **Sistema de Reconhecimento Facial registra 4,3 milhões de imagens no Carnaval**, 2020. Disponível em: <https://www.faroldabahia.com.br/noticia/sistema-de-reconhecimento-facial-registra-43-milhoes-de-imagens-no-carnaval>. Acesso em: 01 ago. 2023.

FIDO ALLIANCE, ***User Authentication Specifications Overview***. Disponível em: <https://fidoalliance.org/specifications/>. Acesso em: 01 ago. 2023.

FOLHA DE SÃO PAULO, **Nunes assina contrato de programa de reconhecimento facial na cidade de SP**, 2023. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2023/08/nunes-assina-contrato-de-programa-de-reconhecimento-facial-na-cidade-de-sp.shtml>. Acesso em: 01 ago. 2023.

GLOBO, **Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano**, 2019. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 01 ago. 2023.

INSTITUTO DE DEFESA DE CONSUMIDORES – IDEC, **Idec vence ação contra uso de reconhecimento facial e ViaQuatro é condenada a pagar indenização de R$ 500 mil**, 2023. Disponível em: <https://idec.org.br/noticia/idec-vence-acao-contra-uso-de-reconhecimento-facial-e-viaquatro-e-condenada-pagar> Acesso em: 19 jun. 2024.

INFORMATION COMMISSIONER'S OFFICE - ICO, ***The use of live facial recognition technology in public places***, 2021. Disponível em: <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>. Acesso em: 01 ago. 2023.

INFORMATION COMMISSIONER'S OFFICE – ICO, ***ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted***, 2022. Disponível em: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>. Acesso em: 01 ago. 2023.

INSTITUTO IGARAPÉ, **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**, 2020. 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: 01 ago. 2023.

INTERNETLAB, **Tutela antidiscriminatória na Lei Geral de Proteção de Dados: problemáticas e alternativas**, 2021. Disponível em: <https://revista.internetlab.org.br/tutela-antidiscriminatoria-na-lei-geral-de-protecao-de-dados-problematicas-e-alternativas/>. Acesso em: 01 ago. 2023.

INTERNETLAB, **Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras**, 2023. Disponível em:

<https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf>. Acesso em: 01 ago. 2023.

JARARACA, **Reconhecimento Facial nas Escolas Públicas do Paraná**, 2023. Disponível em: <https://www.observatoriodasmetropoles.net.br/wp-content/uploads/2023/11/Relatorio_Reconhecimento-Facial_2023.pdf>. Acesso em: 01 ago. 2023.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET – LAPIN. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. 2021. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 01 ago. 2023.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET – LAPIN, **A contratação entre Polícia Rodoviária Federal e SERPRO para extração e fornecimento da base de dados biométricos do RENACH**, 2023. Disponível em: <https://lapin.org.br/2023/05/03/nota-tecnica-a-contratacao-entre-prf-e-serpro-para-extracao-e-fornecimento-da-base-de-dados-biometricos-do-renach/>. Acesso em: 01 ago. 2023.

MICROSOFT, ***Inside Identity: Moving to a passwordless world with the FIDO Alliance***, 2020. Disponível em: <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/inside-identity-moving-to-a-passwordless-world-with-the-fido/ba-p/1464004>. Acesso em: 01 ago. 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, **Portaria nº 793**, 2019. Disponível em: <https://dspace.mj.gov.br/handle/1/1380>. Acesso em: 01 ago. 2023.

NEUROTECH ANALYTICS, ***NeuroTech Industry: Global NeuroTech Industry Investment Digest***, 2021. Disponível em: <https://www.neurotech.com/investment-digest-q4>. Acesso em: 01 ago. 2023.

NORTHWELL HEALTH'S FEINSTEIN INSTITUTES FOR MEDICAL RESEARCH - NORTHWELL, ***Using brain implants, artificial intelligence and novel stimulation technology, double neural bypass technology restores quadraplegic man's sense of touch and movement***, 2023. Disponível em: <https://www.northwell.edu/feinstein-sub/news/the-latest/bioelectronic-medicine-researchers-restore-feeling-lasting-movement-in-man-living-with-quadriplegia?__cf_chl_tk=CLipxRKMdj7aa5zs0GxtKJLXOMw6OGrxbBLVm8suSt4-1691012347-0-gaNycGzNEGU>. Acesso em: 01 ago. 2023.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. **Um Rio de câmeras com olhos seletivos: uso de reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022.

NUNES, Pablo. **Das planícies ao Planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira**. Rio de Janeiro: CESeC, 2023a.

NUNES, Pablo; LIMA, Thallita; CRUZ, Thais. **O sertão vai virar mar: expansão do reconhecimento facial na Bahia** [livro eletrônico]. Rio de Janeiro: CESeC, 2023b.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, ***Biometrics and the Challenges to Privacy***, 2022. Disponível em: <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/>. Acesso em: 01 ago. 2023.

OFFICE OF THE VICTORIAN INFORMATION COMMISSIONER - OVIC, ***Biometrics and Privacy: issues and challenges***, 2019. Disponível em: <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/>. Acesso em: 01 ago. 2023.

PARANÁ, **Tecnologia de reconhecimento facial na chamada chega a 1,6 mil colégios da rede estadual**, 2023. Disponível em: <https://www.aen.pr.gov.br/Noticia/Tecnologia-de-reconhecimento-facial-na-chamada-chega-16-mil-colegios-da-rede-estadual#:~:text=Arquivo%20de%20Not%C3%ADcias-,Tecnologia%20de%20reconhecimento%20facial%20na%20chamada%20chega%20a%201%2C6,privacidade%20e%20seguran%C3%A7a%20de%20dados>. Acesso em: 01 ago. 2023.

SÃO PAULO, Prefeitura Municipal, **Prefeito assina contrato para o início do Smart Sampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras**, 2023. Disponível em: <https://www.capital.sp.gov.br/w/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras>. Acesso em: 01 ago. 2023.

SERASA EXPERIAN, **Biometria Facial**. Disponível em: <https://www.serasaexperian.com.br/solucoes/biometria-facial/>. Acesso em: 01 ago. 2023.

SERPRO, **Embarque + Seguro: uma nova forma de viajar**, 2023a. Disponível em: <https://campanhas.serpro.gov.br/embarque-mais-seguro/#menu>. Acesso em: 01 ago. 2023.

SERPRO, **DATAVALID**, 2023b. Disponível em: <https://www.loja.serpro.gov.br/datavalid>. Acesso em: 01 ago. 2023.

STRATEGIC MARKET RESEARCH LLP, ***Brain-computer interface market will attain a value of USD 5.34 billion by 2030***, 2022. GlobeNewswire News Room. Disponível em: <https://www.globenewswire.com/fr/news-release/2022/07/06/2475404/0/en/Brain-Computer-Interface-market-will-attain-a-value-of-USD-5-34-billion-by-2030.html>. Acesso em: 01 ago. 2023.

THE ALAN TURING INSTITUTE, ***Understanding bias in facial recognition Technologies: An Explainer***, 2020. Disponível em: <https://zenodo.org/record/4050457>. Acesso em: 01 ago. 2023.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO - TJSP, **Acórdão - Ministério Público do Estado de SãoPaulo, IDEC Instituto Brasileiro de Defesa ao Consumidor,Defensoria**

Pública do Estado de São Paulo e Concessionáriada Linha 4 do Metrô de São Paulo S.A. (Via Quatro), 2023. Disponível em: <https://esaj.tjsp.jus.br/pastadigital/abrirDocumentoParaConferencia.do?instancia=SG5TJ&cdDocumento=534319733&cdProtocolo=&cdProcesso=RI006J6T80000&nuProcesso=1090663-42.2018.8.26.0100&cdForo=990&nmAlias=SG5TJ&flOrigem=S&tpOrigem=2&origemDocumento=P>. Acesso em: 01 ago. 2023.

STARTSE, **Pague com seu rosto: o que está por trás do novo método de pagamento da C&A.** 2023. Disponível em: <https://www.startse.com/artigos/cea-pay-pagamento-por-reconhecimento-facial/> Acesso em 19 jun. 2024.

ZANATTA, Rafael A. F.; SIMÃO, Bárbara; OMS, Juliana. **Tutela coletiva e coletivização da proteção de dados pessoais. Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020.

www.anpd.gov.br

ANPD

Autoridade Nacional de
Proteção de Dados