idec
Instituto Brasileiro de Defesa do Consumidor

INTERNETLAB
pesquisa em direito e tecnologia

RECONHECIMENTO FACIAL E O SETOR PRIVADO

GUIA PARA A ADOÇÃO DE BOAS PRÁTICAS

RECONHECIMENTO FACIAL E O SETOR PRIVADO

GUIA PARA A ADOÇÃO DE BOAS PRÁTICAS

idec
Instituto Brasileiro de Defesa do Consumidor

INTERNETLAB
pesquisa em direito e tecnologia

RECONHECIMENTO FACIAL E O SETOR PRIVADO

Guia para a adoção de boas práticas

QUEM SÃO O INTERNETLAB E O IDEC?

O InternetLab é um centro independente de pesquisa interdisciplinar, que produz conhecimento e promove o debate em diferentes áreas que envolvem tecnologia, direitos e políticas públicas. Somos uma entidade sem fins lucrativos baseada em São Paulo, que atua

como ponto de articulação entre pesquisadores e representantes dos setores público, privado e da sociedade civil. Partimos da ideia de que a formulação de boas políticas públicas depende de diagnósticos mais precisos sobre a relação entre as novas tecnologias de informação e comunicação – como a internet – e os direitos das pessoas. Veja mais no nosso site: www.internetlab.org.br

O Idec (Instituto Brasileiro de Defesa do Consumidor) é uma associação de consumidores sem fins lucrativos. Nossa missão é promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com independência política e econômica. Trabalhamos por políticas de universalização dos serviços de telecomunicações e acesso à internet no Brasil, com garantia de níveis adequados de qualidade e respeito aos direitos de informação, transparência, não discriminação e proteção de dados pessoais. Maiores informações no site: https://idec.org.br/

QUAL O OBJETIVO DESTE DOCUMENTO?

Este relatório, produzido de forma colaborativa pelo InternetLab e pelo Idec, busca introduzir boas práticas que possam nortear o setor privado no desenvolvimento de suas atividades, no que diz respeito ao oferecimento de produtos e serviços com base em tecnologias de reconhecimento facial. O relatório oferece um panorama das principais questões ligadas à utilização de tecnologias de reconhecimento facial por pessoas jurídicas de direito privado no Brasil, apresentando as características básicas de funcionamento dessas ferramentas e alguns conceitos necessários para a compreensão da discussão. Acreditamos que adoção de boas práticas na utilização de tecnologias de reconhecimento facial é uma necessidade ética e legal para as empresas que pretendem promover a inovação de forma responsável.

AGRADECIMENTOS

O processo de elaboração desse relatório envolveu workshops com representantes da sociedade civil e do setor privado, cujos insumos foram essenciais para a elaboração de um guia mais completo e detalhado. O InternetLab e o Idec agradecem a todos que participaram desses workshops e da concepção desse docu-

mento. Para não gerar injustiças com todos os que nos ajudaram, não mencionamos seus nomes individualmente, mas reiteramos o reconhecimento de suas essenciais contribuições.

EQUIPE DO PROJETO

Elaboração:

Bárbara Simão (Pesquisadora da área de telecomunicações e direitos digitais do Idec)

Nathalie Fragoso (Coordenadora da área de privacidade e vigilância do InternetLab)

Enrico Roberto (Pesquisador no InternetLab)

Colaboração:

Diogo Moyses (Coordenador da área de telecomunicações e direitos digitais do Idec)

Juliana Oms (Pesquisadora da área de telecomunicações e direitos digitais do Idec)

Francisco Brito Cruz (Diretor do InternetLab)

Heloísa Massaro (Coordenadora da área de informação e política do InternetLab)

Dennys Antonialli (ex-diretor do InternetLab, até outubro/2019)

Como citar

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas.* InternetLab/IDEC, São Paulo, 2020

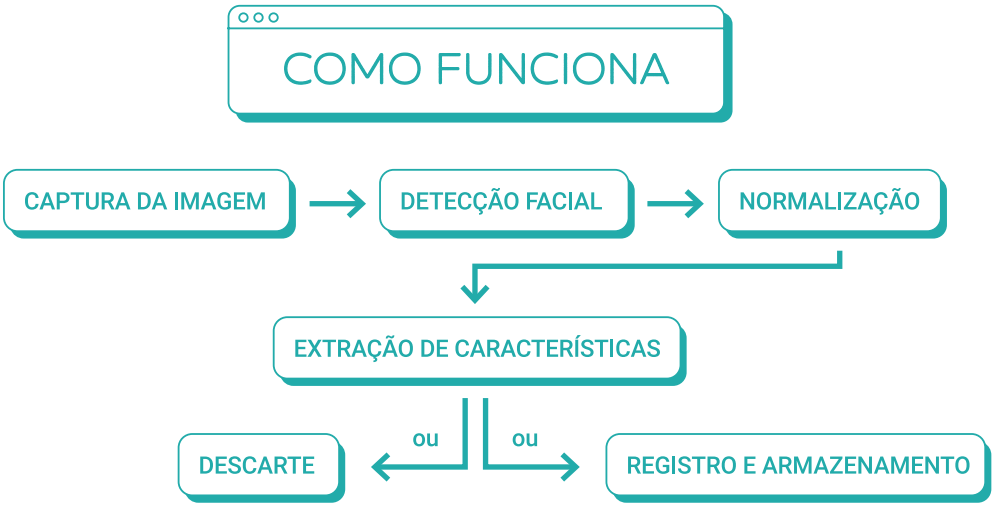
SUMÁRIO EXECUTIVO

1. RECONHECIMENTO FACIAL – O QUE É, COMO FUNCIONA E PARA QUE FINS?

DEFINIÇÃO

RECONHECIMENTO FACIAL →

Processamento automatizado de imagens que contenham faces de indivíduos, com o objetivo de identificar, verificar ou categorizar esses indivíduos



2. PREMISSAS

_ Toda tecnologia capaz de detectar um rosto humano pode ser considerada reconhecimento facial

Ainda que o objetivo final da tecnologia não seja a identificação de uma pessoa determinada, para que a detecção aconteça, é necessário coletar e tratar dados de rostos humanos, ocorrendo um processo de leitura dos atributos e pontos de referência de uma face.

_ Dados referentes a rostos humanos são dados pessoais

De acordo com o art. 5º, inciso I, da Lei Geral de Proteção de Dados, toda informação relacionada a pessoa natural *identificada ou identificável* é dado pessoal. Em geral, considera-se que a imagem de uma pessoa e as informações dela decorrentes constituem dado pessoal, assim se inserindo sob o alcance dessa legislação.

_ Todo reconhecimento facial envolve o tratamento de dados pessoais

Todo processo de reconhecimento facial demanda o tratamento de imagens de rostos humanos. Isso porque, para que as funcionalidades básicas de um algoritmo de reconhecimento facial possam ser executadas, será sempre necessário que um rosto seja detectado e sua imagem tratada, mesmo que tais dados sejam posteriormente excluídos ou anonimizados.

Por envolver o tratamento da imagem de um rosto – um dado pessoal, é impossível pensar em reconhecimento facial sem pressupor o tratamento de dados pessoais.

_ Dados de rostos humanos tratados no contexto do reconhecimento facial são dados (biométricos) sensíveis

A partir do momento em que um sistema de reconhecimento facial é capaz de analisar os pontos de referência de uma face, extraindo destes pontos inferências sobre suas características pessoais, ela realiza tratamento de dado sensível. Especificamente, de um dado biométrico: Mesmo que a lei brasileira não traga uma definição exata de dado biométrico[1], aquela traçada pelo Regulamento Geral de Proteção de Dados na Europa pode ser ilustrativa: tratam-se de "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."

Além disso, a partir da extração de características de um rosto, diversas informações íntimas podem ser inferidas: sua origem racial ou étnica, idade, gênero etc.

1. Apesar de ainda discutido no legislativo, o Decreto nº 10.046/2019, que institui o Cadastro Base do Cidadão, traz a seguinte definição de atributos biométricos: "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (Art. 2º, II)

_ Eventual anonimização dos dados não descaracteriza o tratamento de dados pessoais

Embora após a anonimização os dados não possam mais ser individualizados, o processamento ocorrido até então envolve o tratamento da imagem de uma pessoa. A posterior anonimização ou exclusão das imagens, portanto, não deve isentar o operador de cumprir com as exigências e princípios constantes na legislação aplicável.

3. RISCOS DO RECONHECIMENTO FACIAL

_ Abuso de direitos e controle

O reconhecimento facial é uma tecnologia cujo uso permite a identificação e a obtenção de informações sensíveis sobre indivíduos àqueles que controlam e acessam o sistema. Se mal utilizadas, deliberadamente ou pela negligência em mitigar riscos, podem servir como ferramentas de controle e resultar em práticas abusivas, discriminação[2] e invasão de privacidade. Se os dados biométricos armazenados no contexto dessa tecnologia não forem cuidados com o devido zelo, ou se forem compartilhados com autoridades policiais e governamentais, por exemplo, podem servir de base também a ferramentas de vigilância. Estão em questão, portanto, riscos potenciais a direitos fundamentais, entre eles o direito à proteção de dados pessoais.

_ Discriminação e viés

Outra fonte de risco diz respeito ao "viés algorítmico", i.e., a reprodução de padrões discriminatórios nos resultados apresentados ou no uso feito pelos algoritmos. Por exemplo, no caso de uma ferramenta de reconhecimento facial treinada com referência a um banco de dados constituído majoritariamente por pessoas de pele branca, sua acurácia será reduzida quando usada para identificar pessoas de pele negra, gerando resultados discriminatórios. Estudos vêm mostrando que a taxa de erro dessas ferramentas é sistematicamente maior para mulheres negras em comparação a outros grupos, por exemplo[3]. A discriminação por algoritmos pode

2. Ressaltamos que discriminação, neste relatório, é termo usado principalmente em seu sentido jurídico, ou seja, de lesão ao direito fundamental de igualdade e de dignidade, em especial contra grupos historicamente oprimidos ou minoritários. Não se refere à discriminação como mera categorização.

levar a práticas discriminatórias (negação de serviços, distinção de preços), tecnologias essenciais que não funcionam bem com toda a população (autenticação facial de pessoas negras, por exemplo), e outros problemas potenciais.

_ Riscos à privacidade

Em maior ou menor grau, o reconhecimento facial permitirá acesso a diversos dados de natureza privada dos titulares: gênero, idade, raça etc. A utilização desses dados em excesso ou descumprimento às finalidades de sua coleta podem representar violações à privacidade dos indivíduos analisados pelo reconhecimento facial.

_ Reconhecimento falho de emoções

O reconhecimento de emoções vem sendo questionado quanto a sua acurácia. A dificuldade de se obter resultados confiáveis pode representar um risco, por exemplo, caso tais sistemas sejam utilizados como critério de acesso ao exercício de um direito – tal como uma entrevista de emprego automatizada que leve em consideração as emoções do candidato, por exemplo.

---

3. https://ieeexplore.ieee.org/document/6327355; Buolamwini e Gebru conduziram um estudo que analisou três ferramentas de reconhecimento facial disponíveis no mercado que detectam o gênero do indivíduo. A pesquisa testou a acurácia desse sistema e concluiu que as taxas de erro das três ferramentas são significativamente maiores em mulheres negras quando comparadas a homens brancos. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

_ Incidentes de segurança

A segurança no armazenamento desses dados é outro ponto crucial, sobretudo por envolver dados biométricos. Diferentemente de senhas ou endereços de e-mail, que podem ser alterados, dados biométricos são imutáveis, agravando as consequências de potenciais vazamentos.

4. BOAS PRÁTICAS

_ Análise prévia de proporcionalidade e respeito a princípios

A utilização de sistemas de reconhecimento facial apresenta, mesmo com o cumprimento das recomendações que trazemos nesse relatório, riscos a direitos fundamentais. As boas práticas que apontamos buscam mitigar tais riscos, mas não têm, nem pretendem ter, o condão de afastá-los totalmente.

Assim, antes do uso de qualquer sistema de reconhecimento facial, a empresa deverá avaliar se se trata da única forma de atingir seus objetivos. Caso maneiras menos invasivas e com menores riscos sejam possíveis, essas deverão ser adotadas.

Além disso, deve-se analisar se a tecnologia que se quer implementar está em consonância com os princípios da legislação aplicável. Por exemplo, deve-se analisar se as finalidades da coleta estão sendo respeitadas, se medidas de responsabilização e prestação de contas estão sendo adotadas, entre outros.

_ Transparência aos Titulares

Pré-requisito para o exercício do consentimento e do conjunto de direitos fundamentais envolvidos, a transparência exige a prestação de informações completas e precisas aos titulares, especialmente sobre: *a utilização de dispositivos de coleta de imagens; os dados coletados, sua forma de tratamento e as finalidades para as quais este é realizado; o prazo, as condições de armazenamento e as medidas de segurança adotadas para a sua proteção; as hipóteses de compartilhamento com terceiros; os direitos dos titulares sobre seus dados e os riscos envolvidos neste tratamento de dados.*

Na prática, dispositivos como *tablets*, televisores ou placas podem ser posicionados nas entradas dos estabelecimentos, além de alertas indicando o uso da tecnologia, apresentando as políti-

cas da empresa em relação à coleta desses dados, apontando as câmeras que capturam as imagens e as informações de contato para o exercício de direitos relacionados.

Trata-se de maneira de empoderar, por meio da informação, as pessoas submetidas ou potencialmente submetidas ao reconhecimento facial. Por meio da transparência, os titulares devem ter a capacidade de tomar decisões conscientes sobre o uso de seus dados biométricos.

_ Transparência Pública

No caso do reconhecimento facial, não somente os titulares devem ter meios para agir de forma consciente, mas também medidas de controle público, responsabilização (*accountability*) e auditoria devem ser adotadas.

Por exemplo, todas as práticas adotadas na implementação e execução dessa tecnologia devem ser documentadas em relatórios de impacto à proteção de dados pessoais. Como boa prática, tais relatórios devem ser ainda disponibilizados ao público, e devem conter, também, previsões sobre quais direitos fundamentais poderão ser afetados pelo sistema e o que está sendo feito para mitigar tais impactos, em formato similar ao *Fundamental Rights Impact Assessment* defendido pela União Europeia.

Além disso, informações regulares sobre a utilização do sistema devem ser publicamente disponibilizadas, tal como o próprio fato de sistema estar sendo utilizado, sua finalidade, locais de uso e pessoas afetadas etc.

E, por fim, órgãos internos independentes que analisem e acompanhem o uso da tecnologia pela empresa devem ser instituídos. Tais órgãos deverão fazer recomendações, prestar contas às autoridades públicas e à população, garantir o respeito às medidas adotadas, elaborar políticas internas de acesso e uso dos dados etc.

_ Consentimento

A obtenção de consentimento é uma das principais exigências legais para esta forma de tratamento de dados pessoais. No Brasil, o consentimento deve ser livre, expresso e informado, além de, em se tratando de dados sensíveis, fornecido de forma específica e em destaque. Mesmo se tratando de exigência legal, boas práticas podem ser adotadas para maximização de sua proteção aos direitos fundamentais.

Para tanto, é imprescindível que titulares permaneçam podendo ter acesso ao produto, serviço ou funcionalidade ainda que não consintam com a captura dos dados de seu rosto. Além disso, a obtenção do consentimento deve ocorrer antes do início da captura de imagens, que, portanto, dependerá de uma ação positiva do titular (como a sua concordância expressa por meio de um dispositivo disponível na entrada da loja ou por meio de um código QR de ativação).

Como a tecnologia envolve dados sensíveis, o tratamento não pode ocorrer com base no legítimo interesse. Os dados somente poderão ser tratados para os usos específicos com que os titulares consentirem.

_ Locais de uso das câmeras

As câmeras devem ser instaladas em locais que permitam a obtenção do consentimento prévio dos titulares. Isso significa dizer que o consumidor deve ter a opção de não estar sujeito à coleta de sua imagem, sem que isso implique o cerceamento de outros direitos, como o de acesso a bens e serviços ou ao seu fácil deslocamento.

_ Medidas Antidiscriminatórias

Em todos os momentos do desenvolvimento e uso desse tipo de sistema, especial atenção deve ser dada para que categorias como raça, gênero, etnia, orientação sexual e outras não sejam acionadas de forma discriminatória. Por exemplo, não devem ser utilizadas, direta ou indiretamente, e sob qualquer hipótese, para a negação de bens ou serviços, variação de preços ou oferecimento de condições desvantajosas.

Na prática, isso exige providências não somente daqueles que usam o sistema, mas também daqueles que o desenvolvem. Assim, devem ser adotadas medidas de controle, teste e correção dos algoritmos para averiguar se tais informações têm influência nos resultados do sistema, além de esforço e treinamento ativo de todos os envolvidos na cadeia de desenvolvimento e utilização do sistema.

_ Exclusão, anonimização e proteção dos dados biométricos

Uma vez coletadas as imagens e delas extraídas as características desejadas, as imagens devem ser permanentemente excluídas, de forma que não seja possível, nem pelos desenvolvedores do sistema, seu posterior resgate.

Além disso, todos os dados armazenados permanentemente e/ou apresentados para os operadores do sistema devem ser anonimi-

zados – por exemplo, somente devem ser expostos dados volumétricos, gráficos e similares.

Por fim, sem prejuízo do emprego de outras medidas de segurança, recomenda-se que todo armazenamento (temporário) de imagens de rostos se dê em ambientes seguros e criptografados, separados logicamente dos ambientes onde os dados anonimizados são armazenados. Idealmente, o armazenamento desses dados deve ser sempre offline, e qualquer conexão utilizada para acessá-los deve ser criptografada.

_ Crianças e adolescentes

Em conformidade com a legislação brasileira, e buscando interpretá-la nos melhores interesses das crianças e adolescentes, o reconhecimento facial desse grupo não poderá ocorrer exceto se consentido especificamente por seu responsável legal. No caso de adolescentes entre 16 e 18 anos, ainda, seu consentimento também deverá ser coletado.

Além disso, deve ocorrer em seu melhor interesse, o que exclui a possibilidade de uso de seus dados em pesquisa de mercado, como direcionamento de publicidade ou inteligência de negócio.

Na prática, isso significa apontar na porta do estabelecimento que a entrada de crianças ou adolescentes desacompanhados é proibida e que, caso acompanhados, os responsáveis deverão fornecer seu consentimento. Fora isso, caso haja a captura (consentida) da imagem de uma criança ou adolescente, sua imagem deverá ser excluída, e, como apontado acima, dados referentes a ela eventualmente capturados ou inferidos não poderão ser utilizados para fins comerciais, especialmente para direcionamento de publicidade.

_ Incidentes de segurança

Por se tratar de atividade eminentemente sensível e de elevado risco social, todo e qualquer incidente de segurança deve ser investigado, informado imediatamente às autoridades públicas, à sociedade civil e aos titulares dos dados, especialmente se acarretar risco ou dano relevante.

SUMÁRIO

1. APRESENTAÇÃO

Este relatório, produzido de forma colaborativa pelo InternetLab e pelo Instituto Brasileiro de Defesa do Consumidor (Idec), oferece um panorama das principais questões ligadas à utilização de tecnologias de reconhecimento facial por pessoas jurídicas de direito privado no Brasil.

Além de apresentar as características básicas de funcionamento dessas ferramentas e introduzir alguns conceitos legais necessários para a compreensão da discussão, buscamos introduzir boas práticas que possam nortear o setor privado no desenvolvimento de suas atividades, no que diz respeito ao oferecimento de produtos e serviços com base em tecnologias de reconhecimento facial.

Cada vez mais, intensificam-se as demandas dos titulares de dados por proteção da privacidade, segurança e pelo efetivo controle sobre seus dados, pelo respeito às finalidades para as quais tais

informações foram coletadas e por garantias de uso não discriminatório. Nesse sentido, mais do que um sinal de boa-fé, a adoção de boas práticas na utilização de tecnologias de reconhecimento facial é uma necessidade ética e legal para as empresas que pretendem promover a inovação de forma responsável.

Trata-se, naturalmente, de tecnologia em franco desenvolvimento, de alta complexidade e usos possíveis, e é possível que, rapidamente, a situação fática que exploramos nesse relatório se modifique. Não temos a pretensão, portanto, de esgotar as boas práticas cabíveis ao setor. Da mesma forma, esperamos poder voltar a este documento e revisá-lo caso novos desenvolvimentos assim o exijam.

QUEM SÃO O INTERNETLAB E O IDEC?

O InternetLab é um centro independente de pesquisa interdisciplinar, que produz conhecimento e promove o debate em diferentes áreas que envolvem tecnologia, direitos e políticas públicas. Somos uma entidade sem fins lucrativos baseada em São Paulo, que atua como ponto de articulação entre pesquisadores e representantes dos setores público, privado e da sociedade civil. Partimos da ideia de que a formulação de boas políticas públicas depende de diagnósticos mais precisos sobre a relação entre as novas tecnologias de informação e comunicação – como a internet – e os direitos das pessoas. Veja mais no nosso site: www.internetlab.org.br

O Idec (Instituto Brasileiro de Defesa do Consumidor) é uma associação de consumidores sem fins lucrativos. Nossa missão é promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com independência política e econômica. Trabalhamos por políticas de universalização dos serviços de telecomunicações e acesso à internet no Brasil, com garantia de níveis adequados de qualidade e respeito aos direitos de informação, transparência, não discriminação e proteção de dados pessoais. Maiores informações no site: https://idec.org.br/

AGRADECIMENTOS

O processo de elaboração desse relatório envolveu workshops com representantes da sociedade civil e do setor privado, cujos insumos

foram essenciais para a elaboração de um guia mais completo e detalhado. O InternetLab e o IDEC agradecem a todos que participaram desses workshops e da concepção desse documento. Para não gerar injustiças com todos os que nos ajudaram, não mencionamos seus nomes individualmente, mas reiteramos o reconhecimento de suas essenciais contribuições.

EQUIPE DO PROJETO

Elaboração:

Bárbara Simão (Pesquisadora da área de telecomunicações e direitos digitais do Idec)

Nathalie Fragoso (Coordenadora da área de privacidade e vigilância do InternetLab)

Enrico Roberto (Pesquisador no InternetLab)

Colaboração:

Diogo Moyses (Coordenador da área de telecomunicações e direitos digitais do Idec)

Juliana Oms (Pesquisadora da área de telecomunicações e direitos digitais do Idec)

Francisco Brito Cruz (Diretor do InternetLab)

Heloísa Massaro (Coordenadora da área de informação e política do InternetLab)

Dennys Antonialli (ex-diretor do InternetLab, até outubro/2019)

Como citar

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020

2. INTRODUÇÃO

A capacidade de reconhecer rostos é uma atividade trivial para seres humanos. O exercício dessas funções por um computador, todavia, até recentemente não era tão simples: a taxa de erro do melhor sistema de reconhecimento facial em 1997 era de 54%, valor que chegou a 0,3% em 2010[4].

O avanço da tecnologia viabilizou a disseminação de seu uso, tanto pelo setor público quanto pelo setor privado. A resolução de imagens captadas por câmeras melhorou, a acurácia desses sistemas foi aperfeiçoada e a capacidade de armazenamento cresceu. A coleta e o processamento desses dados, que antes exigiam recursos computacionais e financeiros significativos,

4. RING, T. Privacy in peril: is facial recognition going too far too fast? Biometric Technology Today, Vol. 2016, issues 7-8, julho-agosto 2016, p. 7. Disponível em: https://www.sciencedirect.com/science/article/pii/S0969476516301230. Acesso em: 10/01/2020.

vêm se tornando atividades gradativamente mais baratas e rápidas[5]. Por outro lado, tais avanços não lograram extinguir seus riscos potenciais, conforme veremos.

O ESCOPO DO RELATÓRIO: *USO COMERCIAL*

Como mencionado, é o escopo desse relatório de boas práticas **o uso comercial de tecnologias de reconhecimento facial pelo setor privado**. Do ponto de vista da terminologia legal, portanto, são também abarcadas finalidades como a prevenção a fraudes, medidas de segurança e similares, mesmo que tais finalidades disponham de estatutos jurídicos específicos que não tenhamos abarcado diretamente aqui.

A amplitude de nosso escopo resulta naturalmente em limitações. Não é possível tecer recomendações únicas que caibam para todo e qualquer sistema de reconhecimento facial. Não só as empresas montam seus sistemas de formas diferentes, como também usam palavras e conceitos diferentes para explicá-los, e podem estar envolvidas em somente algumas das diferentes fases de desenvolvimento de um sistema de reconhecimento facial.

Em especial, ressaltamos que não se trata nosso guia de boas práticas de uma tentativa de criar um "guia jurídico" sobre como implementar o reconhecimento facial, ou que apresente uma interpretação exaustiva da lei para essas situações. Se discutimos conceitos legais aqui, é para solidificar determinados posicionamentos chave, fornecer interpretações protetivas – mas não exaustivas – e inserir as práticas que recomendamos no debate sobre privacidade e proteção de dados. Trata esse relatório primordialmente, ressaltamos, de apresentar boas práticas para guiar um uso responsável e socialmente consciente da tecnologia. Além disso, e como mencio-

→

5. COSERARU, R. Facial Recognition Systems and Their Data Protection Risks Under The GDPR

nado, com a velocidade da mudança tecnológica, seria impossível que nossas recomendações fossem exaustivas ou mesmo universalmente aplicáveis.

Com isso, um ponto específico deve ser apontado: por se tratarem de boas práticas, nossas recomendações pretendem exatamente ir além do texto da lei. Assim, por exemplo, se determinada finalidade do uso do reconhecimento facial encontra subsídio legal para ser realizada de determinada maneira (e.g. abrir mão da necessidade de consentimento no caso de prevenção à fraude), isso não significa que a boa prática aqui apontada (e.g. exigência de consentimento em todos os casos) necessariamente não possa ser aplicada – mesmo que, a depender do caso, determinada boa prática seja na prática impossível de ser seguida. As boas práticas aqui trazidas poderão não ser suficientes ou terem difícil aplicação em determinados casos concretos. Devem, portanto, ser interpretadas e aplicadas conforme as especificidades do caso concreto, **buscando-se mesmo assim, sempre que possível, aplicá-las em sua totalidade.**

Esse relatório busca, antes de tudo, sugerir práticas que possam mitigar tais riscos aos titulares e à sociedade, contribuindo desta maneira com o desenvolvimento saudável dos potenciais dessa tecnologia para o setor privado.

São inúmeras as possibilidades de uso comercial da tecnologia. Por exemplo, sistemas de reconhecimento facial são instalados para coletar dados que informem um lojista a respeito do perfil de seus clientes, como o número de pessoas que frequenta determinada loja e suas diferentes sessões, além do gênero, etnia e faixa etária desses indivíduos. Também são usados para detectar as emoções esboçadas pelo público diante de um produto ou publicidade, ou, ainda, para o direcionamento de um anúncio a partir das características de quem está vendo ou interagindo com ele. No mundo inteiro são vistos casos de adoção de tecnologias de reconhecimento facial, de modo que a discussão hoje sobre seus usos, riscos e limites é mundial[6].

No Brasil, o uso comercial do reconhecimento facial também vem sendo adotado em diversos contextos. A empresa ViaQuatro, concessionária da Linha 4 Amarela do metrô de São Paulo – primeiro contrato de parceria público-privada do País –, instalou nas plataformas de embarque e desembarque por ela administradas um sistema de "Portas Interativas Digitais". A tecnologia consiste basicamente em câmeras, instaladas junto a painéis de publicidade, que identificam a presença de rostos humanos e reconhecem as emoções das pessoas diante de determinado anúncio publicitário, além de permitir a coleta de dados sobre o número de pessoas que transitam na plataforma e suas características de gênero, etnia e faixa etária.

Neste caso, a prática pouco transparente e operacionalizada sem que fosse dada opção de consentimento ao usuário foi questionada pelo Idec – Instituto Brasileiro de Defesa do Consumidor – por meio de uma ação civil pública, por violar a legislação consumerista, de privacidade, dos usuários do serviço público e de proteção de dados[7].

Além da ViaQuatro, outras empresas vêm adotando ferramentas de reconhecimento facial no país. A Hering inaugurou uma "loja conceito" em São Paulo que contava com um sistema de câmeras que permitia a coleta de dados sobre o gênero, faixa etária e humor dos clientes que frequentam o espaço. A loja possuía, ainda, um painel de publicidade com câmera para o direcionamento de anún-

6. Wiewiórowski, Wojciech. Facial recognition: A solution in search of a problem? Disponível em: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en. Acesso em 10/01/2020.

7. https://idec.org.br/idec-na-imprensa/justica-determina-que-empresa-pare-de-coletar-dados-faciais-do-metro-em-sp

cios com base nas características identificadas do cliente. Outras empresas, como a Quod e o Itaú, implementaram o reconhecimento facial como ferramenta de autenticação da identidade de clientes para acesso a aplicativos e liberação de crédito. O mesmo foi adotado pela 99, aplicativo de táxis e carros particulares, em parceria com o Denatran, para confirmar a identidade de seus motoristas. Já a Zaitt, outra empresa que usa o reconhecimento facial para autenticação de identidade de clientes no país, implementou a tecnologia em seu mercado 100% autônomo. Em todos esses casos, o Idec notificou as empresas com o objetivo de obter informações sobre como a tecnologia vem sendo usada e como se dá a coleta, o tratamento, o uso, o armazenamento e potenciais compartilhamentos dos dados capturados ou inferidos pelos sistemas[8].

Nesse cenário, é importante 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.

8. https://idec.org.br/noticia/idec-notifica-itau-e-quod-sobre-uso-de-reconhecimento-facial-de-clientes
https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade

3. O QUE É O RECONHECIMENTO FACIAL?

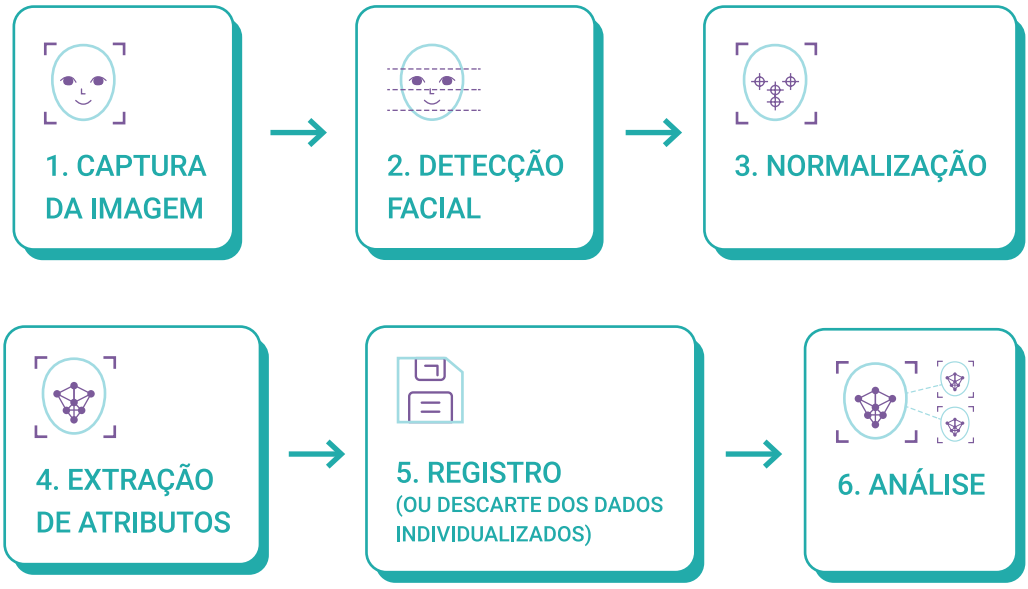
O reconhecimento facial é uma das funcionalidades dos *algoritmos classificatórios*. Trata-se de uma das aplicações de uma vertente específica da inteligência artificial: o aprendizado de máquina – ou *machine learning*, como é conhecido em inglês.

Grosso modo, para poderem desempenhar essa funcionalidade, tais algoritmos utilizam uma base de treinamento, ou seja, uma base de fotos pré-classificadas por seres humanos como (em seu

nível mais simples) “rosto humano” ou “não rosto humano”, gerando um modelo estatístico que irá representar os atributos mais presentes nos rostos apresentados (e.g. a presença de sobrancelhas, nariz, distância entre os olhos etc.) Com base nisso, poderão *detectar* a presença de um rosto humano na imagem analisada.

Ao buscar e identificar determinados padrões, o algoritmo poderá, ao se deparar com uma base de dados não classificada (e.g. novas imagens, coletadas de câmeras de segurança), detectar se se trata de um rosto ou não. Os atributos pré-classificados que mencionamos, como é claro, geralmente não buscarão somente identificar a presença de rostos humanos; características como idade, gênero e raça, ou mesmo uma identificação individual, podem também ser pré-classificados por quem desenvolve a ferramenta e utilizadas para treinamento do sistema de reconhecimento facial. Tais características alimentadas ao sistema, e, grosso modo, selecionadas por seus desenvolvedores, serão então utilizadas como parâmetro para identificação ou classificação de novas pessoas.

Em linhas gerais, o funcionamento da ferramenta pode ser normalmente dividido nos seguintes passos[9]:



9. Imagem e explicações extraídas do Jain, Anil K., and Stan Z. Li. Handbook of face recognition. New York: springer, 2011.

Assim, após a primeira e necessária etapa de (1) captura da imagem, a segunda etapa do reconhecimento facial é a identificação daquilo que é ou não determinante para sua análise, ou seja, os rostos humanos presentes na imagem. Trata-se do momento da (2) detecção facial, que consiste em categorizar a imagem ou porções dela, como mencionamos acima, em "face humana ou não face humana". Aqui, as imagens das faces são segmentadas do restante do quadro, que pode conter elementos diversos e que não interessam à análise, como a paisagem natural, objetos, animais etc.

Há inúmeros fatores do ambiente que podem alterar a percepção de uma imagem. A incidência de iluminação e o grau de rotação da cabeça são alguns elementos que podem modificar substancialmente a leitura sobre características de uma pessoa. Para que as imagens possam ser analisadas e seus atributos identificados, portanto, é necessário minimizar essas diferenças externas ao máximo. Isso ocorre no processo de (3) normalização, pelo qual um recorte padrão é aplicado a todas as imagens, alterando padrões de cor, rotação e iluminação para possibilitar sua análise de maneira mais uniforme.

A partir da normalização, há então a (4) extração de atributos. É nesse momento que os pontos de referência da face são analisados para a extração de quaisquer informações úteis à sua análise. As características geométricas apresentam a forma, localização e distância dos componentes faciais (boca, nariz, sobrancelha etc.), que são então extraídos e registrados para posterior análise.

Existem duas possibilidades para a continuidade do processo de reconhecimento facial a partir da extração de atributos. Na primeira, os dados sobre a face seriam descartados imediatamente, sendo o produto da operação um relatório estatístico sobre os transeuntes e/ou o direcionamento de propagandas em tempo real para o consumidor. Na segunda, há o efetivo (5) registro de tais dados, o que permite a posterior comparação entre imagens (e.g. uma armazenada e aquela obtida em tempo real) para verificação ou identificação de uma pessoa.

É importante destacar que, independentemente do uso que se faça em seguida à coleta de informações, e independentemente de as imagens terem sido descartadas após a detecção facial,

esse processo de leitura da imagem envolveu *necessariamente* o tratamento de dados referentes a um ou mais rostos. Isso pode ter importantes repercussões legais e conceituais, conforme discutiremos adiante.

Por fim, a última etapa do reconhecimento facial é a (6) análise dos dados obtidos, que se dá, grosso modo, por meio da verificação de similaridades entre a amostra que se quer analisar e algum outro banco de dados previamente registrado no sistema. São três os objetivos mais comuns desta etapa:

- ☑ Categorização, processo em que se extrai características da imagem do indivíduo para categorizá-lo de acordo com seu humor, idade, gênero etc.;
- ☑ Verificação/Autenticação, na qual uma pessoa busca ser reconhecida pelo sistema como sendo ela mesma, numa espécie de substituição do login e senha pessoal; e/ou
- ☑ Identificação, processo no qual o sistema busca identificar e reconhecer os indivíduos com base em um ban-

co de dados previamente obtido, podendo ainda formar um novo banco de dados com o armazenamento das identificações realizadas.

Vale dizer que uma tecnologia de reconhecimento facial não precisa necessariamente se dividir entre esses três objetivos. A diferença analítica é útil para esclarecer e delimitar os processos, mas é possível que uma tecnologia almeje, ao mesmo tempo, a categorização, identificação e verificação dos titulares, por exemplo, ou que use técnicas características de cada um deles de forma concomitante. Ainda assim, para maior sistematização e didática sobre o assunto, trataremos abaixo mais detidamente de cada um desses objetivos, com especial atenção para seus potenciais e para os usos reais que já vêm sendo feito no contexto de cada um.

A definição que trazemos para o reconhecimento facial é admitidamente ampla, e tem como intenção abrangir diferentes aspectos e fases de um mesmo tipo de tecnologia em um único conceito. Definições similares podem ser encontradas, por exemplo, na "Opinion 02/2012 on facial recognition in online and mobile services", do Working Party 29 na União Europeia.[10] Trata-se de escolha não somente didática, mas com importantes repercussões práticas e conceituais. Outros locais preferem distinguir entre "detecção facial" e "reconhecimento facial", como discutimos no item 5 abaixo, ou trazem à luz a distinção entre reconhecimento facial e "análise ou caracterização facial", por exemplo.[11] Nesses casos, as distinções são muitas vezes traçadas em relação à intenção final do sistema: caso não exista a intenção de utilizá-lo para identificar uma pessoa, não se estaria falando em reconhecimento facial. E, como é claro, sistemas cujo objetivo final sejam a identificação individual são, de fato, mais arriscados, e exigirão maiores cuidados pelas empresas que o utilizam e mais incisiva regulação futura.

Essa distinção, no entanto, por deixar de fora sistemas que não têm como objetivo final a identificação, acaba

→

por relevar os riscos e boas práticas potencialmente aplicáveis a tais situações. Mesmo sistemas de "detecção facial" ou de "análise facial" passam pela coleta e tratamento, mesmo que em alguns casos só por um momento, de dados pessoais, e se encontram também sujeitos à possibilidade de mau uso e abusos: podem, mesmo que eventualmente em menor grau, ser enviesados, ser utilizados para discriminar, caracterizar-se como excessivos, violar direitos consumeristas e outros direitos fundamentais. Um sistema comercial que analisa o perfil de consumidores de uma loja, por exemplo, pode ser treinado com base em dados enviesados e discriminar seus clientes injustamente. Se não for desenhado com os devidos cuidados de segurança e posterior anonimização, também, pode expor a vazamentos e violações de privacidade os dados originalmente coletados pelas câmeras dos transeuntes analisados, mesmo que o operador final do sistema não tenha acesso a tais dados. Por isso, acreditamos que as boas práticas que trazemos aqui devem ser utilizadas, dentro do máximo limite possível no caso concreto, em todos os casos de reconhecimento facial no âmbito de relações comerciais, independentemente de seus objetivos finais.

10. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 02/2012 on facial recognition in online and mobile services, disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>

11. Veja por exemplo trecho do relatório "Understanding Facial Recognition Systems", da Partnership on AI: "O "reconhecimento facial" é às vezes descrito como abrangendo sistemas de caracterização facial - também chamados de análise facial - que detectam atributos faciais em uma imagem e, em seguida, classificam os rostos por categorias como cor de cabelo, gênero ou raça. Não consideramos tais sistemas como parte dos sistemas de reconhecimento facial porque não são utilizados para prever a identidade de uma pessoa." (Partnership on AI, Understanding Facial Recognition Systems. Disponível em: <https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf>, tradução livre)

4. OBJETIVOS DO RECONHECIMENTO FACIAL

4.1. CATEGORIZAÇÃO

Como mencionado anteriormente, o reconhecimento facial é uma das funcionalidades dos *algoritmos classificatórios*: com base em uma base de dados de treinamento pré-classificada, é capaz de localizar atributos presentes em tal base de treinamento em novos dados apresentados ao sistema. Com efeito, tal funcionalidade é uma das mais importantes dessa tecnologia, e a categorização

dos titulares importante utilidade comercial do reconhecimento facial. Mencionamos acima a possibilidade de classificação por gênero, idade, raça e etnia, mas merece atenção aqui, também, a detecção e categorização de *emoções*.

A ideia de que determinadas emoções são acompanhadas de reações características da face não é nova. Diversos estudos já mostraram como um levantar de sobrancelha e um movimento de contração dos lábios podem ser o reflexo dos sentimentos em determinado momento, ainda que inconscientes. O que tecnologias capazes de determinar a expressão facial fazem é inferir, a partir dessas reações, um conjunto de emoções, que podem variar entre nojo, medo, alegria, surpresa, tristeza e raiva[12]. Há tecnologias que são capazes até mesmo de estimar a frequência cardíaca dos usuários[13].

As possibilidades de uso vão desde a mera contagem de pessoas dentro de um ambiente até processos de maior complexidade. Sistemas desse tipo são capazes, por exemplo, de permitir que um lojista entenda e busque prever a atitude de seu público em relação a um produto, bem como estime a predisposição de compra dos clientes de determinada etnia, gênero e faixa etária. Um exemplo desse mercado é o do *Digital Signage*, um sistema de exibição automatizada de anúncios utilizado por empresas para fins de marketing e análise do público-alvo de publicidade[14]. Neste caso, o software de reconhecimento facial é acoplado ao sistema, que dispõe de câmeras instaladas junto às telas de exibição dos anúncios publicitários. Quando indivíduos passam em frente ou interagem com as telas, o sistema faz a análise de sua reação, identificando também o tempo de exposição à tela e suas características demográficas. Assim, há a geração de estatísticas precisas sobre os consumidores de determinado local. A depender das características da pessoa que passe em frente à tela e de suas preferências pessoais, um anúncio personalizado pode também ser exibido em poucos segundos[15].

12. Jain, Anil K., and Stan Z. Li. Op. Cit. pp. 489

13. LEWINSKI, P.; TRZASKOWSKI, J.; LUZAK, J. Face and Emotion Recognition on Commercial Property under EU Data Protection Law. Psychology & Marketing, v. 33, n. 9, p. 729-746, 2016. p. 743

14. BATAGELJ, B.; RAVNIK, R.; SOLINA, F. Computer vision and digital signage. 2018. p. 3-4

15. COSERARU, R. Op. Cit. p. 18

Caso haja o registro das informações pessoais da face dos consumidores, uma empresa pode utilizar a tecnologia do *Digital Signage* (ou outras similares) para o perfilamento de seus clientes, identificando quais são seus "membros de fidelidade", quais são aqueles que olharam por mais tempo para um anúncio específico e quais voltaram para a loja depois de determinado tempo, por exemplo[16]. Seria possível, nesses casos, identificar as rotas e hábitos de um cliente em particular. Isto ocorreria, por exemplo, por meio da combinação das imagens da câmera com outras tecnologias, como o rastreamento, por meio de "*beacons*", de celulares com os sensores de *wi-fi* ou *bluetooth* ligados, permitindo identificar a localização de seus portadores, ou até mesmo com os dados das compras realizadas pelos consumidores, a depender de onde está localizada a câmera. *Existindo o cruzamento de suas características faciais com outras fontes de dados, seria possível inclusive chegar ao conhecimento sobre a identidade real do indivíduo, o que permitiria, por exemplo, o envio de propagandas e ofertas personalizadas em seu e-mail ou redes sociais*[17].

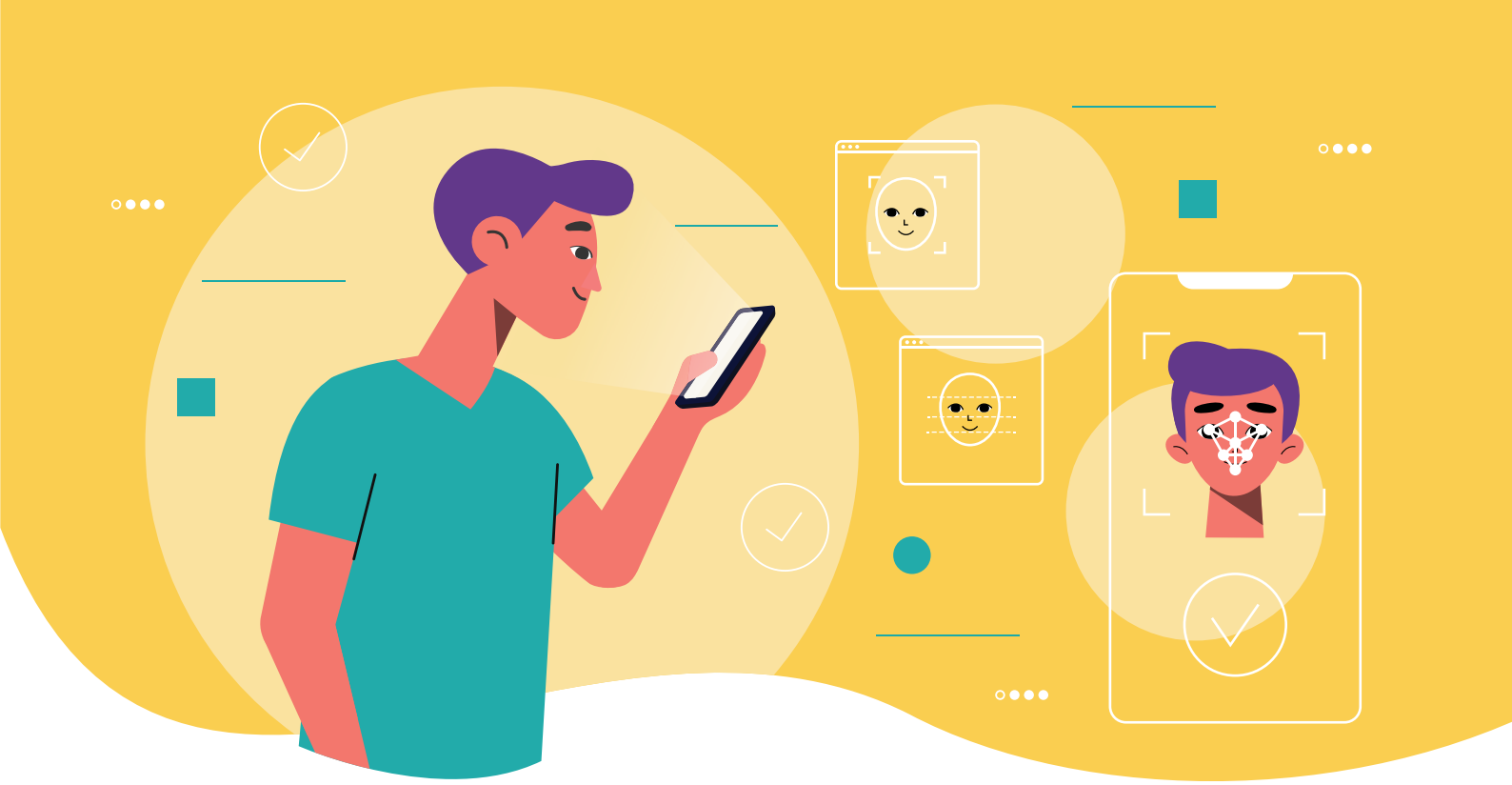
Em suma, a categorização por meio do reconhecimento facial vem sendo usada por estabelecimentos comerciais para o reconhecimento de, principalmente, (i) estados psicológicos (emoções básicas, orientação da cabeça e dos olhos), (ii) características sociodemográficas (gênero, idade, etnia) e (iii) reações dos clientes à loja (quantidade de tempo despendido na loja ou com determinado produto, locais que determinado cliente visitou etc.)

4.2. VERIFICAÇÃO/AUTENTICAÇÃO

O processo de verificação envolve um *pareamento de um para um*, que compara a imagem de *uma* face já armazenada com outra, detectada pelo sistema de reconhecimento facial. Busca, portanto, em outras palavras, analisar se *um* rosto capturado corresponde aos dados de *um* rosto armazenado na base de dados em questão. Tal armazenamento prévio pode ocorrer, por exemplo, depois de determinado usuário ser detectado pela primeira vez pelo sis-

16. LEWINSKI, P.; TRZASKOWSKI, J.; LUZAK, J. Op. Cit. p. 730-731

17. COSERARU, R. Op. Cit. p. 19



tema, gerando-se para ele um "modelo de referência", ou caso ele próprio forneça os dados de seu rosto por meio de um aplicativo ou tecnologia equivalente, por exemplo. No final, o modelo de referência é comparado com uma nova imagem (da pessoa que tenta ser verificada, por exemplo) e se houver compatibilidade entre os dois, o acesso será permitido e a verificação/autenticação se consuma. Esse caso é usado normalmente como substituição a um *login* tradicional com uma senha e nome de usuário, com a finalidade de verificar e controlar a admissão em qualquer serviço[18].

Casos como esse já são bastante comuns para autenticação em dispositivos móveis como celulares e computadores. Outro uso menos usual, porém em expansão, é a utilização do sistema de reconhecimento facial em "lojas conceito" de redes de supermercado, varejo ou similares que operam sem atendentes de caixa. Nesses casos, o acesso à loja ocorre mediante cadastro prévio em um aplicativo da empresa, no qual o consumidor insere seus dados pessoais e de pagamento – incluindo, frequentemente, fotos de seu rosto para futura autenticação. Com isso, para que ele consiga entrar na loja, ocorre a verificação de seu perfil por meio de reconhecimento facial ou leitura de um *QR Code* fornecido pelo aplicativo.

Um exemplo desse tipo de aplicação é o da rede de lojas sem caixas da Amazon, chamada Amazon Go. Patenteada como "just

18. Idem, p. 21

walk out" ("apenas saia", em inglês), a tecnologia já está sendo utilizada pela empresa nas cidades de Seattle, Chicago e São Francisco, com planos de expansão[19]. No Brasil, as primeiras lojas desse tipo foram implementadas pela empresa Zaitt, que hoje possui estabelecimentos nas cidades de Vitória e São Paulo[20].

4.3. IDENTIFICAÇÃO

Além disso, existe também o reconhecimento facial com o objetivo de identificação de uma pessoa desconhecida. Esse pode ser o caso, por exemplo, de câmeras de vigilância acopladas com sistemas de reconhecimento facial, pelas quais determinados ambientes são monitorados. A ferramenta de reconhecimento facial analisa os transeuntes procurando identificar pessoas a partir de uma base previamente registrada ou com base em um certo perfil previamente definido.

A principal diferença em relação à autenticação é que a base de dados a partir da qual a pessoa será identificada é mais ampla: a tentativa de identificar uma pessoa desconhecida, que não

19. https://www.nytimes.com/2018/01/21/technology/inside-amazon-go-a-store-of-the-future.html

20. https://portalnovarejo.com.br/2019/03/zaitt-abre-primeiro-supermercado-100-autonomo-em-sao-paulo/

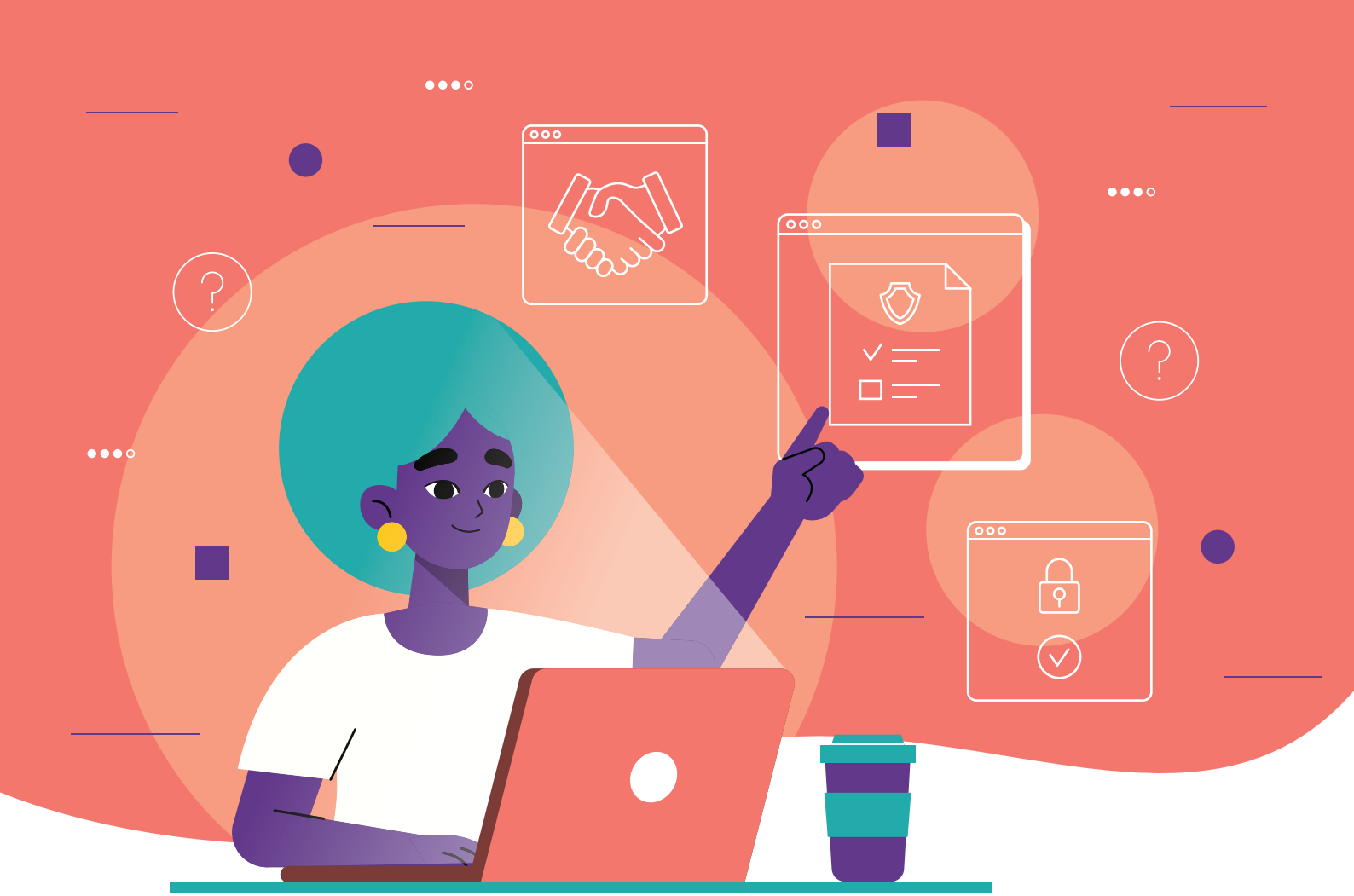
necessariamente tem seu rosto armazenado previamente pelo sistema, pode envolver a detecção de suas características pessoais (local onde se encontra, raça, gênero etc.) e o cruzamento de sua imagem, uma vez analisada, com uma grande quantidade de dados (por exemplo, novamente, geolocalização, raça, gênero etc.), com o intuito de desvendar sua identidade. Por não se tratar da mera busca por um modelo de referência numa base de dados, e sim no cruzamento de diversos dados para identificar pessoalmente determinada pessoa, fala-se de um pareamento de *um para muitos* – em detrimento do paramento de *um para um* ocorrido na verificação/autenticação.

Embora o caso das câmeras de vigilância seja o mais evidente, o uso do reconhecimento facial com objetivo de identificar pessoas também tem muitas aplicações comerciais. No tópico 2.2 comentou-se sobre a possibilidade de categorização, mencionando a possibilidade de identificação de consumidores específicos, com base em cruzamentos com outros bancos de dados, para monitoramento de seus hábitos de consumo, criação de programas de fidelidade e ofertas personalizadas, por exemplo.

Outro exemplo é o das redes sociais. Tais serviços geralmente permitem a seus usuários a vinculação de uma imagem a seus perfis, além de permitirem o *upload* de novas imagens e disponibilizarem ferramentas de marcação de outros usuários da plataforma. Com isso, o serviço pode criar um modelo de referência para cada usuário registrado e, através do uso de um sistema de reconhecimento facial, sugerir automaticamente *tags* para novas imagens à medida que são carregadas[21].

Devemos ressaltar aqui, mais uma vez, que a diferença analítica entre os objetivos da tecnologia que apontamos acima pode ser útil para esclarecer e delimitar os processos de desenvolvimento e uso desse tipo de sistema. No entanto, é possível e comum que um sistema de reconhecimento facial se utilize, ao mesmo tempo, de técnicas abordadas em mais de um dos itens apontados acima. Isso não afasta as conclusões trazidas por nós aqui.

21. DATA PROTECTION WORKING PARTY. Opinion 02/2012 on facial recognition in online and mobile services (00727/12/EN WP 192). p. 4



5. PREMISSAS

Nesse ponto, importante mencionar novamente que esse documento não busca apresentar um guia jurídico para a implantação do reconhecimento facial, nem tem a pretensão de exaurir as leis potencialmente cabíveis à atividade. Como mencionado, buscamos propor boas práticas que possam ser largamente utilizadas em relações comerciais, de forma que sua aplicação e desenvolvimento ocorram de forma socialmente consciente e responsável.

Isso posto, as boas práticas que propomos emaranham-se, em muitos momentos, com os ditames legais, ou deles dependem para que possam ser propriamente esclarecidas. Nossas recomendações, por exemplo, muito têm a ver com o enquadramento das imagens biométricas no contexto do reconhecimento facial como dados pessoais sensíveis.

As boas práticas e os ditames legais, no entanto, não se confundem. Mesmo que em diversos momentos façamos referência, nesse relatório, à lei, buscamos com isso meramente suportar nossas recomendações de boas práticas, ou fazê-las a partir e além do que seria minimamente exigido por lei. Assim, abaixo, passamos a explorar determinados conceitos básicos cuja importância para a utilização responsável do reconhecimento facial não poderia ser ignorada.

Destacamos contudo, nesse contexto, que a adoção de boas práticas, como pretendemos incentivar com este relatório, não demanda somente o cumprimento das leis brasileiras de proteção de dados, mas também o compromisso com práticas responsáveis e inovadoras de proteção à privacidade, a outros direitos fundamentais, e aos direitos dos consumidores e dos usuários do serviço público.

Por se tratar de um relatório de escopo amplo e embasado em interpretações legais protetivas, as boas práticas devem ser adotadas e interpretadas de acordo com as especificidades do caso concreto, sempre com vistas, no entanto, à sua aplicação integral.

O direito à privacidade, o direito ao livre desenvolvimento da personalidade e o direito à não discriminação – que compõem importante fração da proteção de dados pessoais – têm assumido papel central nas regulações que surgem no bojo da chamada sociedade da informação. No Brasil, o direito à privacidade, por exemplo, além de estar protegido constitucionalmente, tem sido consubstanciado em uma série de diplomas normativos, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e a Lei do Cadastro Positivo. Mais recentemente, foi aprovada também a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que representa um marco na imposição de regras a serem atendidas nas operações de coleta e tratamento de dados pessoais no Brasil.

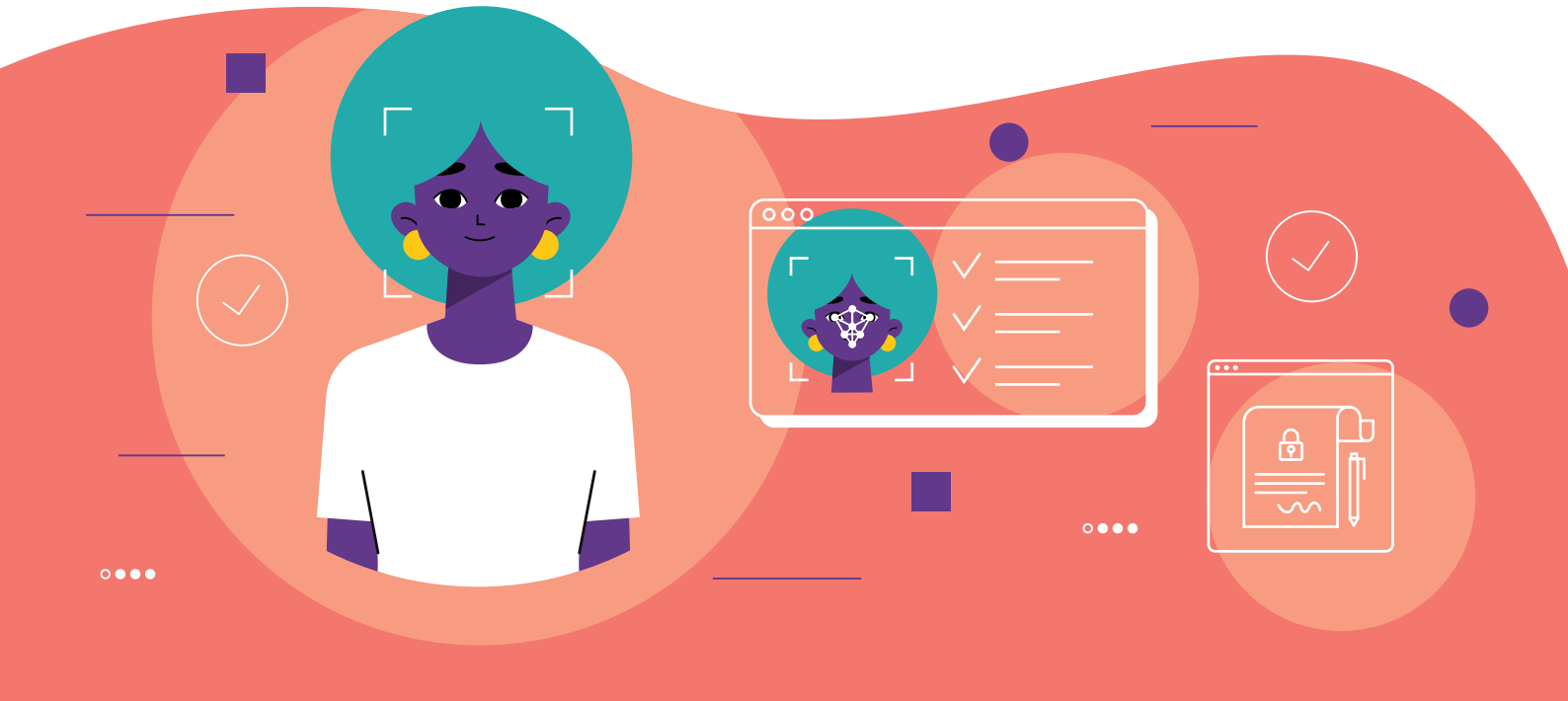
5.1. DADOS REFERENTES A ROSTOS HUMANOS SÃO DADOS PESSOAIS

De acordo com o art. 5º, inciso I, da Lei Geral de Proteção de Dados, toda informação relacionada a uma pessoa natural identificada ou *identificável* é dado pessoal. Em geral, considera-se que a imagem de uma pessoa e as informações dela decorrentes podem constituir, em si, dado pessoal, e assim se inserir sob o alcance da legislação de proteção de dados.

5.2. TODA TECNOLOGIA DE RECONHECIMENTO FACIAL IMPLICA COLETA E TRATAMENTO DE DADOS PESSOAIS

***Todo processo de reconhecimento facial funciona mediante o tratamento de imagens de rostos humanos*. Isso porque, para que as funcionalidades básicas de um algoritmo de reconhecimento facial possam ser exercidas – identificação de um indivíduo ou extração de estatísticas sobre o público de determinado local, por exemplo – será sempre necessário que um rosto seja originalmente detectado e sua imagem tratada, mesmo que tais dados sejam, posteriormente, excluídos ou anonimizados.**

Por sempre envolver o tratamento da imagem de um rosto – um dado pessoal –, o reconhecimento facial pressupõe o tratamento



de dados pessoais. Ou seja: ainda que uma tecnologia esteja sendo empregada somente para extrair informações demográficas do público de uma loja, por exemplo, sem a subsequente identificação de quem são as pessoas, do fato de a extração de informações ter exigido a coleta e o tratamento dos dados dos rostos das pessoas que ali estiveram decorre que houve, mesmo que somente por um instante, o tratamento de dados pessoais.

Deve-se notar aqui que é defendido, em alguns locais, que a anonimização dos dados coletados no âmbito desses sistemas afastaria a incidência das leis de proteção de dados, já que, argumenta-se, o sistema deixaria de implicar o tratamento de dados pessoais. No entanto, como apontado aqui, todo e qualquer sistema de reconhecimento facial precisará passar, para que possa funcionar, pela etapa inicial da detecção facial – etapa em que a imagem de um rosto é detectada e, pelo menos naquele momento, um dado pessoal é tratado. Mesmo que a utilização posterior do sistema se dê somente com dados anonimizados (por exemplo, com dados volumétricos), seu funcionamento não pode, logicamente, deles prescindir.

Naturalmente, ainda, técnicas de *pseudonimização* dos dados, ou seja, a supressão de uma ou outra informação pessoal de determinada base, mas que ainda permita, mediante esforços razoáveis (por exemplo de engenharia reversa), que a pessoa *volte* a ser identificada, igualmente não afastam a incidência da legislação cabível. Será geralmente o caso, por exemplo, da criação de perfis de clientes.

Defende-se também, em outros locais, que a *detecção* facial seria tecnologia distinta do *reconhecimento* facial: no caso da primeira, não haveria a determinação dos rostos de quem se encontra na imagem, apenas a detecção de sua presença; no caso da segunda, a identificação ou reconhecimento efetivo do indivíduo.[22] Trata-se de divisão didática, mas que não faz jus à realidade da tecnologia, geralmente mais complexa e nuançada do que essa dicotomia pode fazer crer. Nesse relatório utilizamos "reconhecimento facial" como um termo mais amplo do que a simples identificação de um indivíduo mediante sua imagem, como proposto por tal taxonomia, abarcando todas as fases de tal tecnologia[23]. Qualquer reconhe-

22. BRAGA, Luiz Filipe Zenicola. "Sistemas de Reconhecimento Facial". Diss. Universidade de São Paulo, 2013. P. 23. Disponível em < https://periodicos.set.edu.br/index.php/exatas/article/download/1897/1076>

cimento facial *deve* passar pela *fase* da detecção facial para que possa chegar a quaisquer conclusões sobre os rostos presentes na imagem analisada. Mesmo que o sistema, em último caso, não armazene ou analise detidamente os rostos detectados, seu funcionamento depende, no momento da captura da imagem, do tratamento de um dado pessoal. Trata-se a detecção facial, para nossos fins e com finco na realidade da tecnologia, de fase do reconhecimento facial, e não de tecnologia dela distinta. Caso as faces detectadas sejam posteriormente classificadas e/ou identificadas e tratadas, tão maiores serão os riscos envolvidos e a abrangência do tratamento de dados pessoais no caso concreto. Eventualmente, pode haver tecnologia que realize detecção facial e não avance para as demais fases do reconhecimento facial aqui descritas (item 3) - isto é, realize apenas contagem de rostos. No entanto, sugerimos igualmente as recomendações deste guia, considerando que ainda há tratamento de dado pessoal e tendo em vista a linha tênue existente na interrupção entre uma fase e outra da tecnologia e a assimetria de informação perante o consumidor analisado.

5.3. EVENTUAL ANONIMIZAÇÃO DOS DADOS ANALISADOS NÃO DESCONFIGURA O TRATAMENTO DE DADOS PESSOAIS

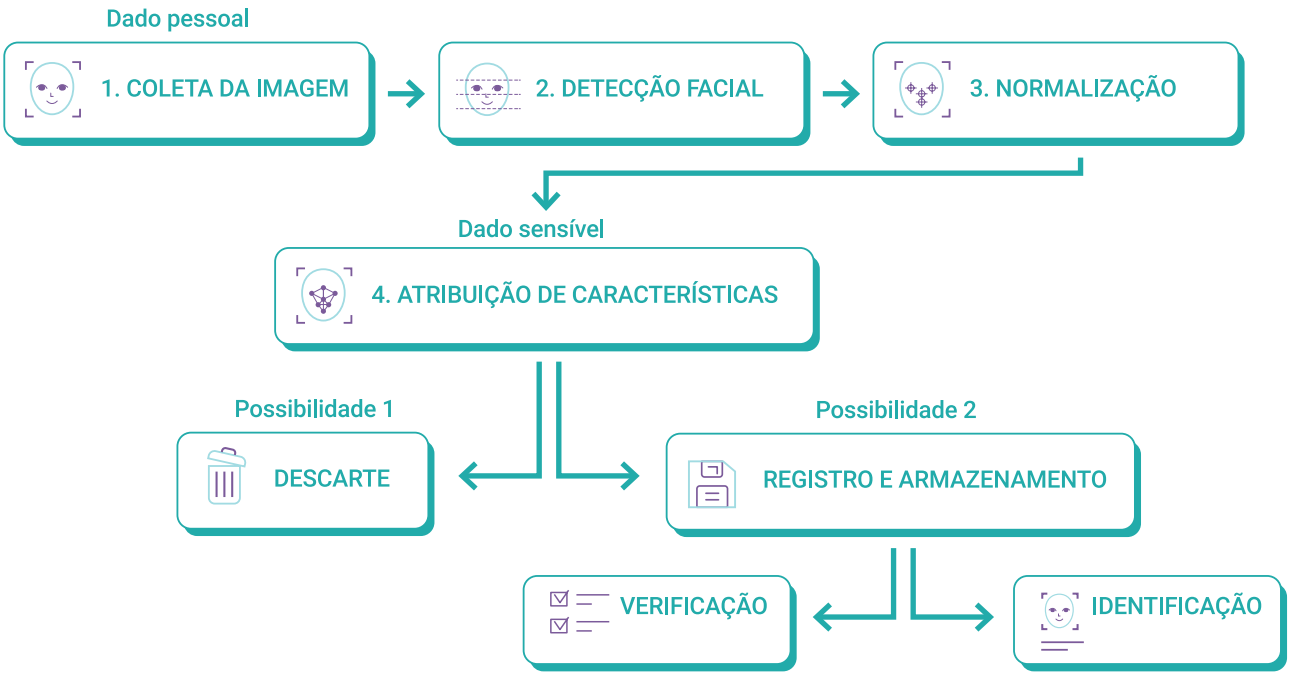
Embora após a aplicação de técnicas efetivas de anonimização os dados não possam mais ser individualizados, o caminho percorrido para se chegar até aquele ponto envolveu a coleta, classificação, utilização e processamento – todas operações definidas pela Lei Geral de Proteção de Dados como "tratamento de dados" – da imagem de uma pessoa. Ou seja, mesmo que haja a posterior anonimização, isso não deve isentar o operador do sistema de reconhecimento facial de cumprir com as exigências e princípios constantes na Lei Geral de Proteção de Dados (e nas outras leis brasileiras cabíveis, como o Código de Defesa do Consumidor)[24].

A categorização dos dados tratados no âmbito do reconhecimento facial como dados pessoais, a observação de que qualquer siste-

23. Essa definição está também em consonância com documentos e relatórios sobre o tema, que utilizam "reconhecimento facial" como um termo guarda-chuva para diferentes processos. Ver: DATA PROTECTION WORKING PARTY. Opinion 02/2012 on facial recognition in online and mobile services. [S.l.]. 2012. (00727/12/EN WP 192);

ma de reconhecimento facial envolve o tratamento de tais dados e a interpretação de que, nesse contexto, tratam-se de dados sensíveis biométricos trazem para os fins desse relatório dois resultados: (i) oferecem interpretação protetiva e consistente sobre os impactos legais da tecnologia, mesmo que potencialmente alterável de acordo com o caso concreto; e (ii) inserem-no e explicitam a dimensão de proteção de dados e à privacidade inerentes à discussão. As boas práticas que apresentaremos no item seguinte utilizam-se de tais conceitos e interpretações. De qualquer maneira, mesmo que o caso concreto afaste uma ou outra característica do que aqui se defende, ou que por alguma razão se discorde o que está aqui disposto, as boas práticas se mantêm: devem ser aplicadas sempre que possível, na máxima extensão que a realidade do caso concreto permitir.

O fluxograma a seguir resume de que forma as fases do processo de leitura de imagens implicam a incidência da Lei Geral de Proteção de Dados, ainda que haja posterior anonimização.



24. A Lei Geral de Proteção de Dados adotou uma definição de dado anonimizado que leva em conta também o efeito que determinado tratamento de dados pode ter sobre a esfera da personalidade de uma pessoa. Isto é, mesmo o dado anonimizado, quando utilizado para a definição de um perfil comportamental, pode gerar consequências negativas para uma pessoa específica. Trata-se, conforme Bruno Bioni (2018, pp. 80) de uma definição consequencialista: "Muitas vezes processos de decisões automatizadas valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo - grouping. É pelo fato dela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem individualizá-la diretamente"

5.4 DADOS REFERENTES À BIOMETRIA DE ROSTOS HUMANOS SÃO DADOS PESSOAIS SENSÍVEIS

Mais do que simples dados pessoais, no entanto, imagens de rostos humanos tratadas no contexto de tecnologias de reconhecimento facial devem ser consideradas dados sensíveis. A partir do momento em que uma câmera é capaz de analisar os pontos de referência de uma face, extraindo destes pontos inferências sobre suas características pessoais, ela realiza tratamento de dado sensível. Especificamente, de um dado biométrico.

Isso porque dizem respeito a características físicas únicas de cada indivíduo, como, por exemplo, distância entre olhos, nariz, boca e orelhas, traços e formatos dos órgãos e da face, cor da pele etc. Mesmo que a lei brasileira não traga uma definição exata de dado biométrico[25], aquela traçada pelo Regulamento Geral de Proteção de Dados na Europa pode ser ilustrativa: tratam-se de "*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.*"

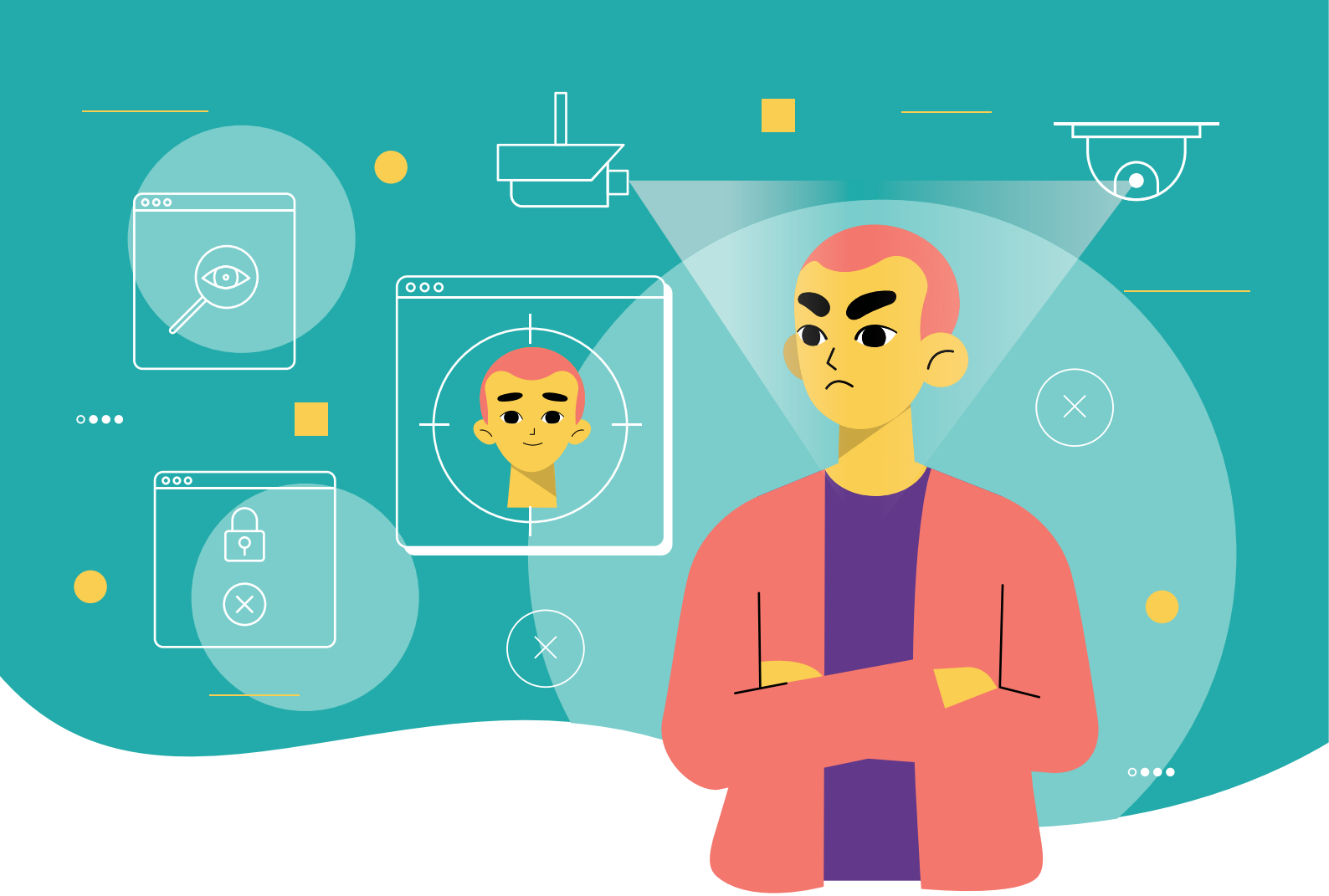
De acordo com o art. 5º, inciso II, da Lei Geral de Proteção de Dados, será considerado sensível o dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou *biométrico*, quando vinculado a uma pessoa natural. Assim, sendo os dados referentes a rostos humanos tratados no âmbito de tecnologias de reconhecimento facial são considerados dados biométricos, conclui-se que devem atender também às regras referentes a dados pessoais sensíveis. É importante notar que nas fases de extração de características, registro e análise, o dado pessoal da imagem

25. Apesar de ainda discutido no legislativo, o Decreto nº 10.046/2019, que institui o Cadastro Base do Cidadão, traz a seguinte definição de atributos biométricos: "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (Art. 2º, II)

passa a permitir também a inferência de diversas informações sensíveis sobre o indivíduo, como sua origem racial ou étnica.

Mesmo que o objetivo desse relatório não seja apresentar interpretações exaustivas e que a configuração dos dados tratados no contexto do reconhecimento facial como dados sensíveis ofereça maior segurança aos titulares, trata-se, admitidamente, de interpretação em disputa. É claro que *nem sempre* a imagem de um rosto precisará configurar dado biométrico: mencionamos aqui a interpretação trazida pelo Considerando 51 do Regulamento Geral de Proteção de Dados Europeu, que explicita que "o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular", juntamente com o Artigo 4.14 dessa lei. Trata-se de posicionamento que deve ser registrado, mas que não altera a interpretação que propomos, segundo a qual o uso de dados pessoais no contexto do reconhecimento facial, em vista de seu potencial de identificação individual e inferência sobre informações sensíveis do indivíduo – especialmente após análise dos pontos de referência da face –, deve ser considerado como tratamento de dados biométricos. Nesse sentido, tanto a tecnologia de reconhecimento facial que realiza identificação e autenticação de indivíduos, quanto aquela que realiza a categorização ou classificação de indivíduos[26], envolvem tratamento de dados sensíveis.

26. Conforme finalidades do reconhecimento facial descritas no item 4



6. RISCOS

O reconhecimento facial é uma tecnologia com implicações potenciais sobre o exercício de direitos, dada sua capacidade de identificar e fornecer informações sensíveis sobre indivíduos. Se mal utilizadas – seja pela má intenção de quem detém os dados, seja pela negligência em mitigar riscos –, podem alimentar práticas de vigilância, além de viabilizar práticas abusivas, discriminação e invasão de privacidade.

Trata-se de situação que apresenta claros riscos a direitos fundamentais, bem como, evidentemente, de violação aos direitos do consumidor. Mesmo com o

→

cumprimento das recomendações que trazemos nesse relatório, a utilização de sistemas de reconhecimento facial sempre apresentará riscos. Com o respeito a um framework estrito e voltado aos interesses da coletividade, no entanto, tais riscos podem ser mitigados, mesmo que nunca completamente afastados.

Por ser tecnologia em franca expansão e com grandes potenciais ainda não realizados, muitos dos riscos apontados aqui vêm se mostrando ainda como potencialidades, por mais que inúmeros casos de discriminação algorítmica e violações a direitos fundamentais já tenham sido demonstrados (em muitos casos, no entanto, ainda associados à utilização dos sistemas pelo poder público e autoridades policiais). Não é possível, portanto, dada a natureza incipiente da tecnologia, que apontemos todos os riscos de maneira concreta ou já realizada: deve-se muito mais ter consciência da sensibilidade da informação coletada e dos potenciais lesivos a direitos fundamentais de uma tecnologia tão potente.

Importante dimensão do risco do reconhecimento facial tem a ver com seu uso discriminatório: seja a discriminação intencional (e.g. no caso de negação de serviços a determinado grupo) ou não (e.g. no caso de mal funcionamento de determinada tecnologia com determinado grupo). A questão do viés algorítmico, nesse contexto, merece atenção e é tradicionalmente associada a bancos de dados enviesados ou pouco representativos[27]. Sendo tais sistemas baseados em algoritmos de *machine learning* – capazes de identificar padrões em bases de dados, como expusemos acima – quaisquer problemas ou tendências nos dados usados para treinar o sistema serão reproduzidos em seus resultados. No caso de uma ferramenta de reconhecimento facial treinada com referência a um banco de dados constituído majoritariamente por pessoas de pele branca, por exemplo, sua acurácia será reduzida

27. BIGONHA, Carolina. Inteligência Artificial em Perspectiva. Panorama Setorial da Internet, ano 10, n. 2, out. 2018.

quando usada para identificar pessoas de pele negra, gerando resultados discriminatórios. Estudos vêm mostrando que a taxa de erro dessas ferramentas é sistematicamente maior para mulheres negras em comparação a outros grupos, por exemplo[28].

Deve-se ter em mente, de qualquer forma, que a possibilidade de viés e discriminação não se limita à simples falta de representatividade em bases de dados. A falta ou enviesamento dos dados sobre grupos minoritários, por exemplo, frequentemente será estrutural: dados do PNAD de 2014 mostram que somente 38,5% das pessoas brancas não usam a internet no Brasil, contra 60,5% da população negra[29]. Isso, dentre diversos outros fatores, resulta em menos dados sobre essa população (por exemplo, em menor quantidade de fotos em redes sociais que possam ser usadas para treinamento de algoritmos de reconhecimento facial). Por exemplo, para melhorar a representatividade da base de dados dos sistemas de reconhecimento facial de um futuro celular seu, o Google, conforme reportagens, buscou ativamente pagar para que negros, incluindo pessoas em situação de rua, disponibilizassem seus rostos para o treinamento dos algoritmos da empresa, levantando uma série de acusações sobre práticas enganosas e antiéticas na coleta destes dados.[30]

O problema da acurácia e os resultados discriminatórios que podem ser gerados vêm sendo bastante discutidos no caso do uso dessas ferramentas por forças policiais. Nesses casos, falsos positivos podem levar a buscas e prisões ilegais, violando direitos fundamentais dos cidadãos[31]. O uso da inteligência artificial no setor privado, no entanto, também apresenta sérios riscos nesse sentido: mencionamos aqui o caso de um hospital nos Estados

28. https://ieeexplore.ieee.org/document/6327355; Buolamwini e Gebru conduziram um estudo que analisou três ferramentas de reconhecimento facial disponíveis no mercado que detectam o gênero do indivíduo. A pesquisa testou a acurácia desse sistema e concluiu que as taxas de erro das três ferramentas são significativamente maiores em mulheres negras quando comparadas a homens brancos. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

29. https://www.nexojornal.com.br/grafico/2016/05/30/Quem-%C3%A9-a-popula%C3%A7%C3%A3o-sem-acesso-%C3%A0-internet-no-pa%C3%ADs

30. https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color

31. A empresa Amazon, por exemplo, foi pressionada por acionistas, pesquisadores e organizações da sociedade civil para que deixasse de comercializar seu software de reconhecimento facial para órgãos governamentais (https://techcrunch.com/2019/05/20/amazon-shareholder-pressure-face-recognition/). Neste caso também as taxas de erro da ferramenta eram maiores para mulheres negras (http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf).

Unidos que, em vista da automação de determinados sistemas seus, direcionava mais recursos a pacientes brancos do que a pacientes negros com o mesmo estado de saúde.[32] No caso do reconhecimento facial também: sistemas de autenticação para desbloqueio da tela de *smartphones* pelo rosto sistematicamente não funcionam com negros.[33] O uso de ferramentas de reconhecimento facial (e, nota-se, da inteligência artificial no geral) pelo setor privado pode perpetuar – e esconder, sob o manto da pretensa objetividade da tecnologia, – tais realidades estruturais.

Além disso, a tecnologia de reconhecimento facial utilizada para reconhecer emoções ainda possui outros problemas de acurácia. Seu funcionamento é baseado em fundamentos científicos contestados, muitas vezes falhando em fornecer resultados precisos ou até mesmo válidos[34]. Além da possibilidade de a categorização incorporar vieses[35], o reconhecimento mais preciso de emoções

32. O viés, no caso, ocorreu porque o algoritmo foi treinado não com base em dados diretamente associados à saúde do paciente, e sim com base em dados referentes a recursos de saúde efetivamente despendidos com pacientes passados. Se, por acessarem hospitais de menor qualidade, terem menos condições de ir com frequência ao médico, ou situações similares, menos dinheiro for gasto com pacientes negros, o algoritmo falsamente concluirá que negros são mais saudáveis do que pacientes brancos igualmente doentes.

33. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

34. AI NOW 2019 Report, p. 50.

35. Rhue, Lauren, Racial Influence on Automated Perceptions of Emotions (November 9, 2018). Available at SSRN: https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765

dependeria de informações contextuais[36], para além de movimentos faciais[37]. Tal dificuldade em se obter resultados confiáveis pode apresentar um risco caso tais sistemas sejam utilizados como critérios de acesso de usuários ao exercício de direitos – tal como uma entrevista de emprego automatizada que leve em consideração as emoções do candidato, por exemplo[38].

As inferências sobre gênero feitas pela categorização facial também funcionam com base em fundamentos científicos contestados[39]. Baseiam-se em concepções fisionômicas equivocadas de gênero, que assumem uma concepção binária (dividida apenas entre homem e mulher) e na visão de que o sexo e características fisiológicas refletem necessariamente o gênero. Acreditar que uma análise feita com base na captura de características faciais é capaz de inferir gênero é assumir padrões estereotipados, em que determinados traços são atribuídos necessariamente a determinado gênero (como maxilares largos, barba, cabelo comprido, lábios grossos etc., características cuja associação a um único gênero binário leva a discriminações e erros). A categorização facial que infere gênero inerentemente perpetua padrões contestáveis de gênero, resultando tanto em falhas para as análises comerciais, quanto em discriminação da população trans e não binária.

A acurácia e discriminação desses sistemas, todavia, não são as únicas questões relacionadas aos riscos e impactos à privacidade e à segurança dos indivíduos. A segurança no armazenamento desses dados é outro ponto crucial, sobretudo por envolverem o processamento de dados biométricos, conforme detalharemos em seguida.

---

36. A ProPublica, por exemplo, reportou que diversas escolas americanas têm usado Inteligência Artificial de vigilância desenvolvido pela empresa Sound Intelligence para monitorar possíveis tiroteios em massa. Contudo, pesquisa pelos pesquisadores da ProPublica evidenciou que o sistema tende a igualar agressão a sons como passos altos ou tosse. (https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/)

37. AI NOW 2019 Report, p. 51.

38. Um exemplo do uso de reconhecimento facial para entrevistas de emprego é a HireVue, usada por mais de cem empregadores nos Estados Unidos, como Hilton, Unilever e Goldman Sachs. Os supostos melhores candidatos são selecionados a partir de características como linguagem corporal, tom de voz e palavras-chaves reunidas, ou seja, a ferramenta "pode acabar penalizando oradoras não nativos, entrevistados visivelmente nervosos ou qualquer pessoa que não se enquadre no modelo de aparência e fala" (https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/).

39. Keyes, Os. (2018). The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. Proceedings of the ACM on Human-Computer Interaction. 2. 1-22. 10.1145/3274357. Disponível em: https://ironholds.org/resources/papers/agr_paper.pdf.

Em agosto de 2019, pesquisadores israelenses, por meio de uma vulnerabilidade em um sistema de segurança biométrico usado ao redor do mundo (o Biostar 2, gerido pela Suprema, empresa Sul-Coreana), foram capazes de acessar informações de reconhecimento facial e outros dados de aproximadamente 1 milhão de pessoas[40]. Diferentemente de senhas, PINs ou endereços de e-mail que podem ser alterados após um vazamento, os dados biométricos são imutáveis e característicos de uma pessoa, agravando as consequências de um potencial vazamento causado por problemas de segurança da informação. O caso do vazamento de dados da empresa Suprema – cujo sistema de segurança biométrico é usado tanto por órgãos governamentais quanto por agentes privados, como bancos – é apenas um exemplo de como o uso comercial dessa tecnologia pode trazer riscos à privacidade e à segurança de seus usuários. Em fevereiro do mesmo ano, pesquisadores holandeses de segurança cibernética conseguiram acessar a base de dados de reconhecimento facial da empresa chinesa SenseNets[41], que cria sistemas de software de segurança baseados em inteligência artificial para reconhecimento facial, análise de multidões e verificações. Além dos dados faciais, a falha de segurança expôs informações como número do cartão de identificação, localização nas últimas 24 horas, sexo, nacionalidade, endereço, fotos do passaporte e aniversário de mais de 2,5 milhões de pessoas.

Os casos de falhas de segurança explicitam os importantes riscos à privacidade trazidos pela tecnologia. Por envolver o tratamento de dados de natureza privada dos indivíduos, usos não permitidos da tecnologia, seja por falhas de segurança, seja pelo desvio da finalidade de sua coleta ou pela extrapolação de seu uso de forma segura e consciente, o reconhecimento facial pode facilmente levar a violações da privacidade dos titulares.

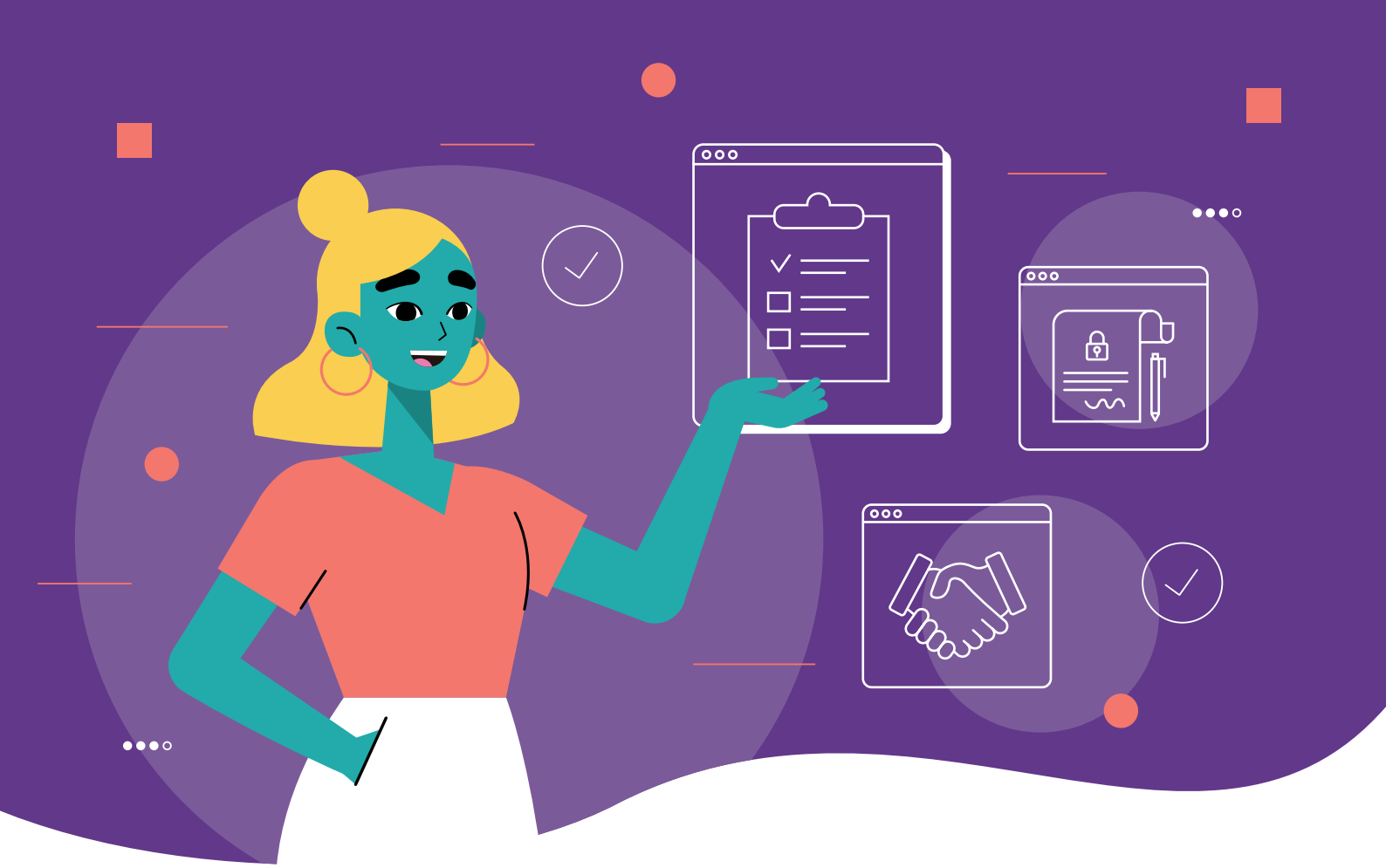
A possibilidade de erros, vazamentos e discriminação no uso de ferramentas com tamanho potencial de abusos deve ser bem avaliada por todo os atores envolvidos. Sem controle social e regras claras e rígidas sobre seu uso, a tecnologia pode servir para práticas abu-

40. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

41. https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/#788f83aafb40

sivas contra os titulares dos dados, além de violar seus direitos consumeristas, sua privacidade, e outros direitos fundamentais. Além disso, se não houver controle estrito sobre o acesso aos dados coletados pelo setor privado, com compartilhamentos, por exemplo, com o setor público e com autoridades policiais, a prática pode habilitar o monitoramento de indivíduos de forma pervasiva sem que os mesmos saibam que e por que motivo isso está ocorrendo, expondo-os à vigilância e ao desrespeito às garantias fundamentais ao devido processo legal e à ampla defesa, por exemplo.

Os limites entre os bons e maus usos nem sempre estão claros. Tampouco é sempre fácil identificar *qual* o uso está sendo feito, quem efetivamente tem acesso às imagens armazenadas e por quê. Para as empresas que controlam a tecnologia, ainda, seu mau uso, como o compartilhamento indevido de dados com outras entidades ou negligência em proteger as bases de dados com padrões de segurança adequados, pode resultar em punições severas sob as leis consumeristas, de proteção aos usuários do serviço público e de proteção de dados brasileiras.



7. BOAS PRÁTICAS

A elaboração de boas práticas no uso de tecnologias de reconhecimento facial tem sido um esforço conjunto de diversos atores ao redor do mundo. Como mencionado anteriormente, ressaltamos que as recomendações abaixo não se limitam às exigências legais para a utilização dessas tecnologias no Brasil. Buscam, na verdade, ir além, e propor parâmetros de implementação destas tecnologias afinados com as melhores práticas internacionais.

Tais práticas são inspiradas, mas não se limitam, em propostas consubstanciadas em relatórios e documentos elaborados por órgãos como a Federal Trade Comission (FTC), a National Telecommunications and Information Administration (NTIA), o Future of Privacy Forum, European Union Agency for Fundamental Rights (FRA), e a Autoridade Holandesa de Proteção de Dados (*Autoriteit Persoonsgegevens*). Mesmo que formulados em modelos regula-

tórios significativamente distintos, há grande convergência no que se entende por práticas mais adequadas para promover a proteção dos direitos fundamentais e dos consumidores quando da adoção de tecnologias de reconhecimento facial pelo setor privado.

Mais do que um conjunto de regras úteis às equipes jurídica e de *compliance* das empresas, é salutar que as recomendações a seguir sejam parte do processo de criação e desenvolvimento das equipes de todas as áreas, do marketing à tecnologia e segurança da informação.

7.1. ANÁLISE PRÉVIA DE PROPORCIONALIDADE E RESPEITO A PRINCÍPIOS

Nesse ponto, importante ressaltar que a utilização de sistemas de reconhecimento facial apresenta, mesmo com o cumprimento das recomendações que trazemos aqui, riscos à privacidade. As boas práticas que apontamos buscam mitigar tais riscos, mas não têm, nem pretendem ter, o condão de afastá-los totalmente.

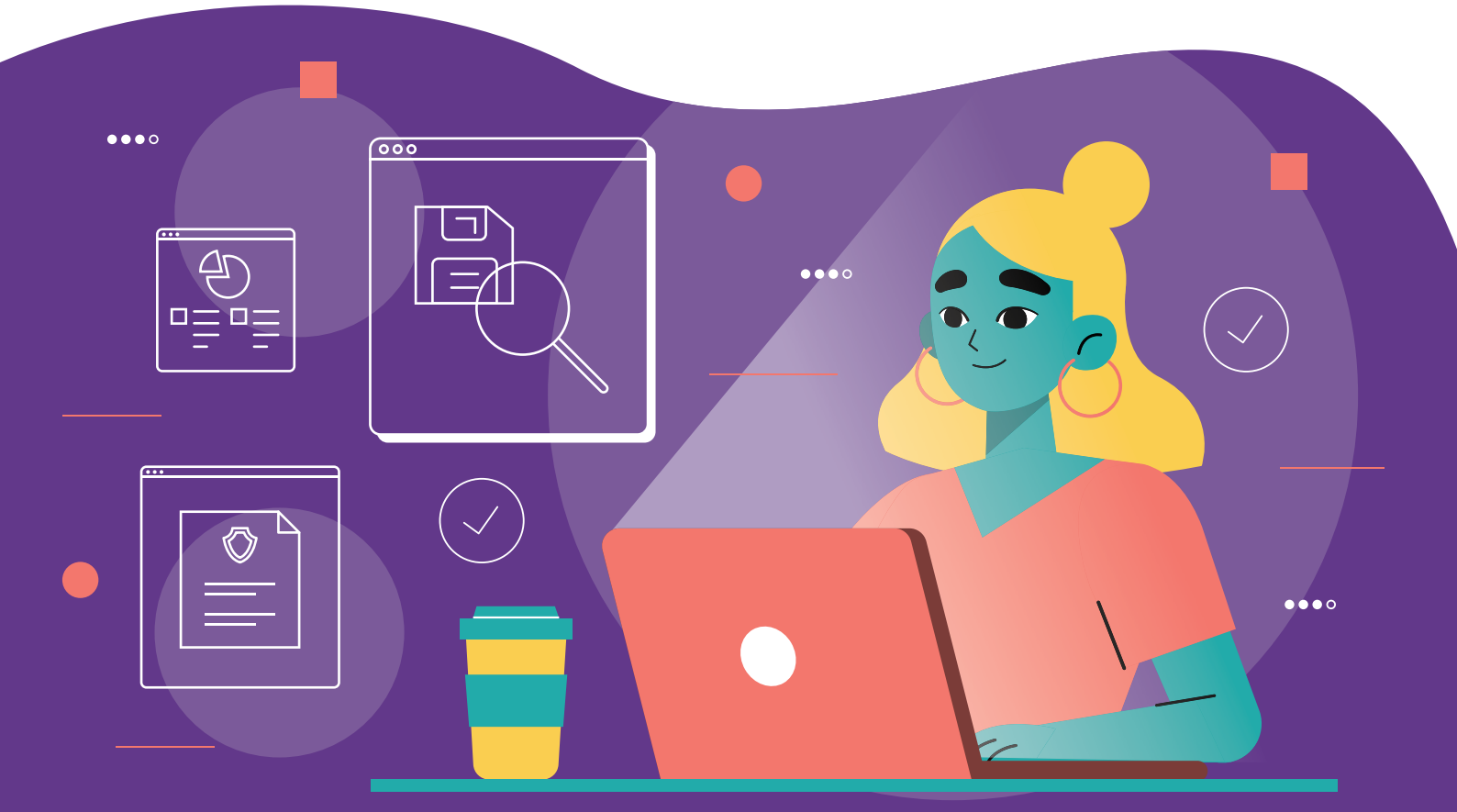
Assim, toda vez que se considerar o uso do reconhecimento facial, a empresa deverá avaliar se sua adoção é efetivamente necessária. Caso maneiras menos invasivas à privacidade dos titulares e com menores riscos, por exemplo associados ao armazenamento de dados biométricos – imutáveis, sejam possíveis, essas deverão ser adotadas em detrimento do reconhecimento facial.

Além disso, deve-se analisar previamente se a tecnologia que se quer implementar está em consonância com os princípios da legislação aplicável à matéria, em especial a LGPD. Trata-se, naturalmente, de boa prática em consonância com as determinações legais, mas que busca maximizar os benefícios de seu cumprimento. Por exemplo, deve-se analisar se as finalidades da coleta dos dados e para as quais houve consentimento estão sendo respeitadas, se a menor quantidade de dados possível está sendo coletada para se atingir a finalidade desejada, se medidas de responsabilização e prestação de contas estão sendo adotadas etc.

7.2. TRANSPARÊNCIA AOS TITULARES

Em todos os documentos de boas práticas na utilização de tecnologias de reconhecimento facial, a transparência é tida como central. Devemos notar aqui que a transparência é, como se sabe, um dos princípios da Lei Geral de Proteção de Dados, do Marco Civil da Internet e de outras leis aplicáveis à atividade. Mais do que cumprir com os requisitos mínimos da lei nesse contexto, no entanto, a transparência que propomos aqui deve ser exercida como maneira de empoderar, por meio da informação, as pessoas submetidas ou potencialmente submetidas ao reconhecimento facial. Por meio da transparência, os titulares devem ter a capacidade de tomar decisões conscientes sobre o uso de seus dados biométricos – e tal capacitação e empoderamento devem ser, a todo momento, o objetivo das práticas de transparência ao titular adotadas no uso do reconhecimento facial.

Ressaltamos que a transparência pode ter também o objetivo de prestar informações para que ações *coletivas*, pelo público ou pelo governo, e não necessariamente pelos titulares, sejam tomadas. Exploramos algumas práticas de transparência dessa natureza no item a seguir.



Assim, pré-requisito para o exercício do consentimento e do conjunto de direitos fundamentais envolvidos, a transparência exige a prestação de informações completas e precisas aos titulares, especialmente sobre:

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

Na prática, dispositivos como *tablets*, televisores ou placas podem ser posicionados nas entradas do estabelecimento, além de avisos dentro da própria loja, apontando para o uso das tecnologias de reconhecimento facial e apresentando as políticas da empresa em relação à coleta desses dados. Além disso, as câmeras que capturam as imagens também devem ser visíveis e facilmente identificadas.

É imprescindível, nesse contexto, que os profissionais responsáveis pelo atendimento ao público estejam cientes dessas políticas e possam prestar informações e sanar dúvidas a respeito da utilização dessas tecnologias por parte da empresa. Devem ser disponibilizados, ainda, números de telefone e/ou e-mails de contato para que os titulares possam contatar a empresa para exercerem os direitos previstos em lei (tal como os direitos de exclusão dos dados, reparação, portabilidade etc.) e obter mais informações quanto ao uso de seus dados.

7.3. TRANSPARÊNCIA PÚBLICA

Como apontado nesse relatório, o uso do reconhecimento facial, inclusive para finalidades comerciais, é atividade com importan-

tes riscos a direitos. Trata-se de situação na qual não somente os titulares de dados devem ter meios para poder agir de forma consciente, mas cujo desenvolvimento socialmente responsável depende da existência de medidas de controle público, responsabilização (*accountability*) e auditoria. Tais medidas, que aglutinamos nesse item sob a noção de "transparência pública", incluem (mas não se limitam a) ferramentas como Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), práticas de transparência contínua e a instituição de órgãos internos independentes.

A elaboração de RIPDs encontra-se em consonância com a legislação. Como o reconhecimento facial coloca riscos a direitos fundamentais, nos termos da Lei Geral de Proteção de Dados, todas as práticas adotadas no contexto dessa tecnologia, inclusive aquelas referentes ao seu funcionamento técnico, devem ser documentadas por meio de um RIPD. Trata-se de recomendação cabível não somente às empresas que fazem uso da tecnologia (como é o caso da maior parte das recomendações desse relatório), mas também às empresas que desenvolvem os próprios sistemas de reconhecimento facial.

Concretamente, além da descrição dos processos de tratamento de dados, com a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, o RIPD deve conter as salvaguardas e mecanismos para mitigação de riscos adotados. Como boa prática, na linha da maximização dos deveres de transparência, tais relatórios devem ser disponibilizados ao público, e devem conter, também, previsões sobre quais direitos fundamentais poderão ser afetados pelo sistema, e o que está sendo feito para mitigar tais impactos, tais como o *Fundamental Rights Impact Assessment* defendido pela União Europeia.[42]

Além da publicação de um relatório como o apontado acima, outras medidas de transparência devem ser exercidas durante a utilização do sistema de reconhecimento facial. Em todas as situações, informações regulares sobre sua utilização devem ser publicamente disponibilizadas, tal como: o fato de tal sistema estar

42. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/application-charter/incorporating-fundamental-rights-eu-legislative-process_en

sendo utilizado, incluindo informações sobre sua finalidade, locais de uso e pessoas afetadas; quantas pessoas foram analisadas pelo sistema; com que frequência o sistema está sendo utilizado, dentre outras cabíveis à situação concreta e que sejam necessárias para efetiva transparência pública e *accountability* perante os usuários do sistema.

Para a execução das recomendações trazidas nesse item, e para responsabilização e contato com o público quanto às medidas adotadas, recomenda-se ainda, por fim, a instituição de órgãos internos independentes que analisem e acompanhem o uso da tecnologia pela empresa. Tais órgãos deverão fazer recomendações, prestar contas às autoridades públicas e à população, garantir o respeito às medidas adotadas, elaborar políticas internas de acesso e uso dos dados etc.

7.4. CONSENTIMENTO

A obtenção de consentimento, além de boa prática, é uma das principais exigências das legislações de proteção de dados ao redor do mundo, como a Lei Geral de Proteção de Dados. No caso do Brasil, o consentimento deve obedecer às adjetivações da lei – deve ser livre, expresso e informado, além de, por se tratar do tratamento de dados sensíveis[43], ser fornecido de forma específica e em destaque.

No entanto, como se sabe, tais adjetivações ainda não foram objeto de delimitação legal ou jurisprudencial clara. Nossas recomendações buscam, assim, apresentar melhores práticas sobre como obter o consentimento dos titulares dos dados de forma efetiva e voltada a seus melhores interesses.

Para tanto, a medida mais importante é garantir que **titulares tenham sempre a opção de ter acesso ao produto, serviço ou funcionalidade mesmo que não consintam com a captura dos dados de seu rosto**. Isso significa dizer que, para que o consentimento seja, de fato, livre, dele não deve depender o acesso ao serviço. Essa

43. Este documento considera, como afirmado anteriormente (pp. 13-14), que o dado da imagem de uma pessoa é sensível a partir da fase de extração de características em uma tecnologia de reconhecimento facial.

medida é, ainda, uma garantia à liberdade de escolha do consumidor, direito básico previsto no Código de Defesa do Consumidor (art. 6º, II), complementar ao dever de consentimento. Assim, por exemplo, caso uma empresa de transporte aéreo decida oferecer a possibilidade de se realizar *check in* por meio de reconhecimento facial, deve ser oferecida também modalidade de *check in* que não dependa da utilização da tecnologia.

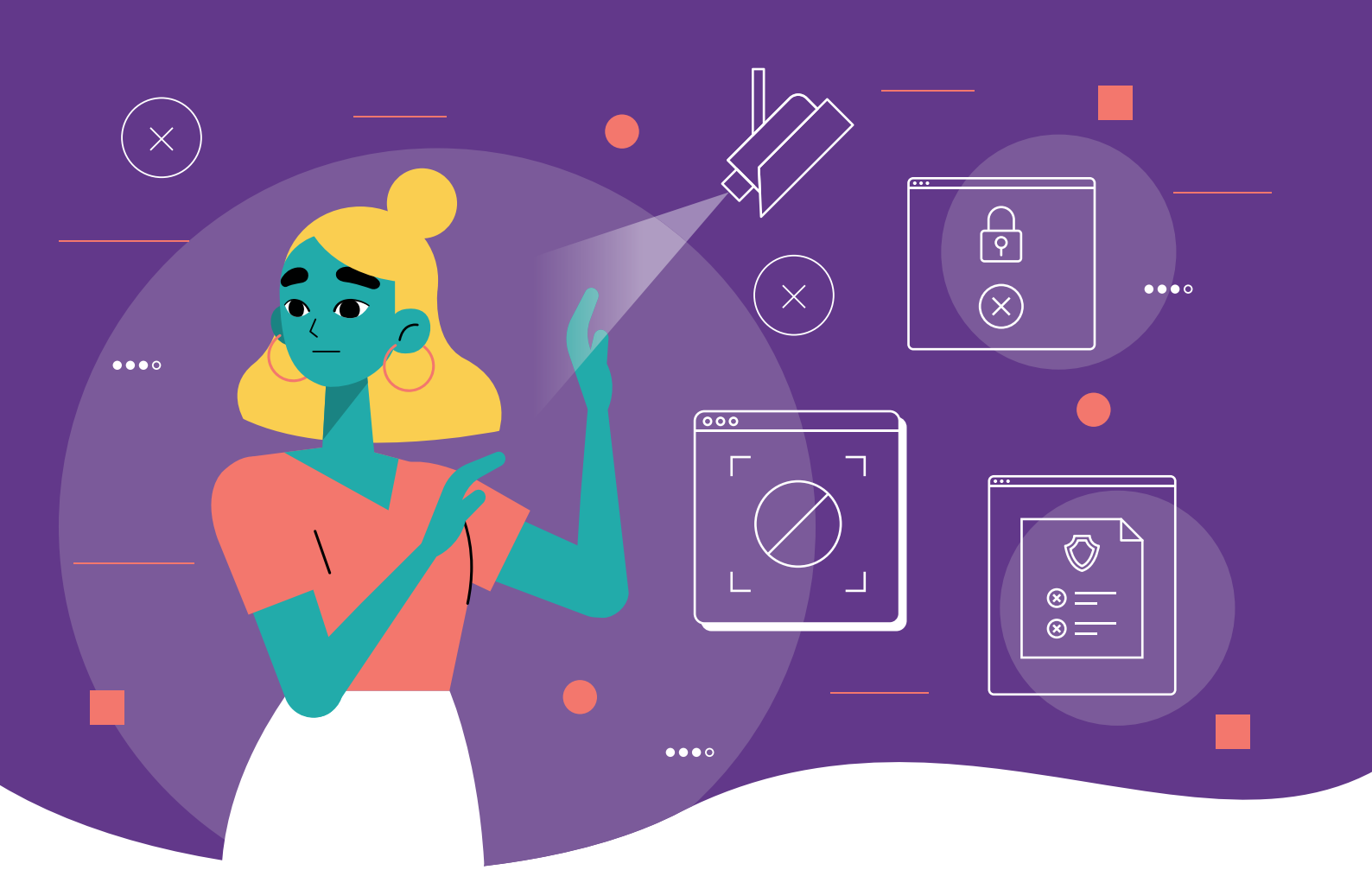
Além disso, a obtenção do consentimento deve ocorrer antes do início da captura de imagens, que, portanto, dependerá de uma ação positiva do titular (como a sua concordância expressa por meio de um dispositivo disponível na entrada da loja ou por meio de um código QR de ativação). Isso pode interferir no local de disposição das câmeras, bem como na forma de sua ativação e alcance.

Ainda, para que se obtenha o consentimento de forma válida, a empresa deve oferecer informações completas a respeito dos dados que serão coletados, das finalidades de seu tratamento, prazo e condições de armazenamento e hipóteses de compartilhamento com terceiros. Essas informações precisam ser apresentadas de maneira clara, acessível e destacada, não devendo ser apresentadas de forma intrincada em contratos de adesão, por exemplo. Trata-se de boa prática que se emaranha com as exigências legais: caso tais documentos coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade, poderão ser consideradas nulas de pleno direito (Código de Defesa do Consumidor, Art. 51, IV).

Devemos ressaltar aqui, também, que como a tecnologia de reconhecimento facial envolve dados sensíveis, o tratamento não pode ocorrer com base no legítimo interesse. Os dados somente poderão ser tratados para os usos específicos com que os titulares consentirem. Novos usos, compartilhamentos, finalidades etc. só são permitidos mediante nova obtenção de consentimento específico.

Para se alinharem às melhores práticas no que diz respeito à obtenção do consentimento, as empresas devem investir em

- ☑ formas inovadoras e acessíveis de apresentação das informações referentes à coleta e utilização das imagens



de rostos dos consumidores, como vídeos, animações, panfletos e avisos;

- ☑ alternativas eficientes para aqueles que não desejem se submeter às tecnologias de reconhecimento facial; e
- ☑ projetos de instalação de câmeras que considerem a livre circulação também daqueles que não tiverem consentido com a prática.

7.5. LOCAIS DE USO DAS CÂMERAS

As câmeras devem ser instaladas em locais que permitam a obtenção do consentimento prévio dos titulares. Na prática, isso significa dizer que o consumidor deve, a todo momento, ter a opção de não estar sujeito à coleta de sua imagem, sem que isso resulte no cerceamento desproporcional de outros direitos seus, como o de acesso a bens e serviços ou ao seu fácil deslocamento.

Disso decorrem limitações importantes para o projeto de disposição das câmeras de reconhecimento facial, especialmente aquelas voltadas para ou instaladas em locais de acesso público,

tais como ruas, calçadas, corredores de shoppings, aeroportos ou meios de transporte públicos, já que o deslocamento em tais locais deve continuar sendo possível também para aqueles que não consentirem o uso de seus dados biométricos.

7.6. MEDIDAS ANTIDISCRIMINATÓRIAS

Como mencionado anteriormente, o uso e criação de sistemas de reconhecimento facial (assim como de qualquer inteligência artificial) geralmente reproduzirá discriminações sistêmicas em seus resultados: seja por vieses decorrentes da base de dados, seja pela seleção e construção do modelo, seja pelas próprias finalidades do sistema. Para que se possa fazer frente a esse desafio, medidas antidiscriminatórias positivas devem ser adotadas por todos os envolvidos na criação e uso de um sistema de reconhecimento facial. Assim, nas recomendações que trazemos neste item, acabamos por abarcar também, excepcionalmente, boas práticas a serem tomadas na *criação* das tecnologias – em contraste com as recomendações do resto do documento que têm um foco muito mais premente na sua *utilização*.

Isto posto, no momento da coleta e tratamento das imagens de rostos para extração das características desejadas, assim como no momento de utilização e interpretação dos dados gerados pelo tratamento, mesmo que anonimizados, especial atenção deve ser dada para que categorias como raça, gênero, etnia, orientação sexual e outras não sejam utilizadas de forma discriminatória. Por exemplo: não devem ser utilizadas, direta ou indiretamente, e sob qualquer hipótese, para a negação de bens ou serviços, variação de preços ou oferecimento de condições desvantajosas.

Na prática, isso implica que:

- ☑ O uso de informações, que, por exemplo, infiram condições socioeconômicas ou outras características a partir de dados sensíveis ou potencialmente discriminatórios, deve ser evitado ou controlado. Caso não seja possível a criação do sistema com base em dados representativos ou o controle e compensação estatística (transparente) das possíveis hipóteses de discriminação, o sistema não deverá ser utilizado ou substituído por outro;

- ☑ Para evitar discriminação, o treinamento dos algoritmos de reconhecimento facial deve utilizar uma base de dados com diversidade racial, de gênero e etária, isto é, deve envolver homens, mulheres, pessoas negras, indígenas e asiáticas, idosos, pessoas transexuais e gênero não binário;

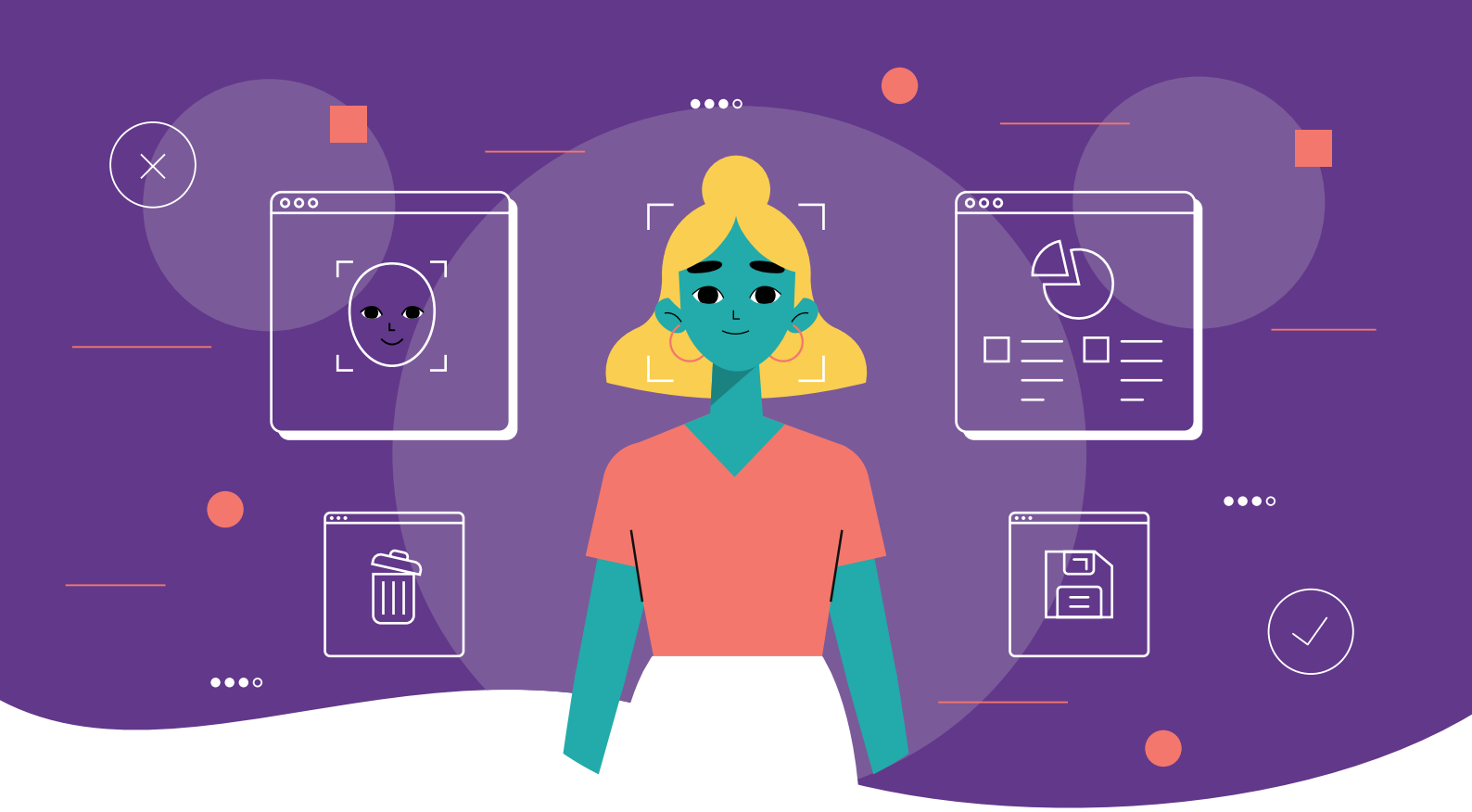
- ☑ Uma vez criado determinado sistema, seus resultados e sua acurácia devem ser testados antes de sua implementação real, com o intuito de aferir se características potencialmente discriminatórias (gênero, raça, condições socioeconômicas etc.) têm influência sobre tais resultados ou acurácia. As tecnologias devem apresentar níveis de precisão equivalentes para os diferentes grupos da sociedade, não reproduzindo ou exacerbando as chances de discriminação às quais já estão expostos;

- ☑ Deve existir um esforço e treinamento ativo dos operadores finais da tecnologia – os que têm acesso aos dados anonimizados, por exemplo – para que práticas discriminatórias, como as apontadas acima, sejam prevenidas;

- ☑ A equipe de operadores finais da tecnologia e seus desenvolvedores deve ser multidisciplinar e diversa. A presença de profissionais do campo das humanas, como psicólogos ou cientistas sociais, e de indivíduos diretamente afetados pela discriminação, como mulheres negras, auxilia a identificação e compreensão de aspectos discriminatórios no funcionamento da tecnologia;

- ☑ As tecnologias empregadas devem ser testadas regularmente após sua implementação, para verificar se análises discriminatórias estão sendo realizadas pelos algoritmos. Tal verificação deve idealmente ser feita através de auditorias técnicas independentes e realizadas periodicamente;

- ☑ Considerando as fragilidades de embasamento científico, recomenda-se que o uso do reconhecimento facial para identificação de emoções não tenha um papel importante na tomada decisões que impactem a vida das pessoas, como, por exemplo, contratação de recursos humanos, avaliação de desempenho ou contratação de empréstimos.



7.7. ARMAZENAMENTO E COMPARTILHAMENTO DOS DADOS BIOMÉTRICOS

Para que informações comercialmente relevantes sejam obtidas a partir das tecnologias de reconhecimento facial, é necessária a coleta e o tratamento de imagens de rostos humanos. De forma a preservar a privacidade dos titulares, assim, recomenda-se que tal coleta e armazenamento ocorra pelo menor prazo possível.

Na prática, isso quer dizer que:

- ☑ Uma vez coletadas as imagens e delas extraídas as características desejadas, as imagens devem ser permanentemente excluídas, de forma que não seja possível, nem pelos desenvolvedores do sistema, seu posterior resgate;

- ☑ Todos os dados armazenados permanentemente e/ou apresentados para os operadores do sistema devem ser anonimizados. Os painéis de controle e sistemas de armazenamento somente compreenderão, por exemplo, dados agregados (e.g. volumétricos), gráficos e similares, sempre de forma a impossibilitar a identificação de pessoas naturais individualizadas;

- ☑ Sem prejuízo do emprego de outras medidas de segurança, recomenda-se que todo armazenamento (temporário) de imagens de rosto se dê em ambientes seguros e criptografados, separados logicamente dos ambientes onde os dados agregados e anonimizados são armazenados. Idealmente, o armazenamento desses dados deve ser sempre offline, e qualquer conexão utilizada para acessá-los deve ser criptografada; e

- ☑ Recomenda-se que seja viabilizada a responsabilização ou *accountability* dos processos descritos nos itens anteriores, de modo a garantir seu efetivo cumprimento. Para tal, sem limitação, a realização de auditorias independentes regulares nos sistemas da empresa, assim como publicização dos resultados gerais das auditorias, é recomendada.

Além disso, importante notar que os dados biométricos coletados e armazenados no contexto de um tal sistema não podem ser compartilhados para finalidades distintas daquelas cobertas pelo consentimento obtido, conforme previsto em lei. Mais especificamente, recomenda-se que os dados não sejam compartilhados, em hipótese alguma, para finalidades de vigilância e segurança pública no geral, em especial com quaisquer autoridades governamentais e policiais.

7.8. CRIANÇAS E ADOLESCENTES

Em conformidade com a legislação brasileira, em especial com o Art. 14 da Lei Geral de Proteção de Dados, o reconhecimento facial de *crianças* não poderá ocorrer exceto se consentido especificamente por seu responsável legal (Art. 14, § 1º da LGPD). No entanto, mesmo que esse dispositivo não mencione adolescentes, não faria sentido deixá-los desprovidos de tal proteção. Como boa prática, assim, o consentimento dos responsáveis deve sempre ser exigido para o tratamento dos dados tanto de crianças quanto de adolescentes.

Trata-se de prática em compasso com a melhor interpretação da lei: Mesmo não sendo mencionados os adolescentes no Art. 14, § 1º da LGPD, trata-se, a proteção de seus dados, de um ato da vida civil. Deve-se atentar, portanto, ao fato de menores de 16 anos

serem absolutamente incapazes de exercer pessoalmente tais atos, e de aqueles entre 16 e 18 anos serem relativamente incapazes para tal, nos termos do Art. 3º do Código Civil. Assim, nessa esteira, no caso de adolescentes entre 16 e 18 anos, tanto o consentimento de seus responsáveis quanto o seu próprio deverão ser coletados antes do tratamento de seus dados pessoais.

Portanto, o consentimento do responsável legal, ou, conjuntamente, do responsável legal e do adolescente, será necessário para a simples captura da imagem da criança ou adolescente no caso do reconhecimento facial. Como a captura é inevitável nesses casos, como vimos acima, o consentimento deve ser obtido antes que crianças e adolescentes adentrem as áreas de alcance das câmeras.

Além da obtenção do consentimento, no entanto, deve-se ter em mente a estrita finalidade para que os dados obtidos poderão ser utilizados (e, portanto, a estrita finalidade que poderá ser abarcada pelo consentimento): dados pessoais sobre crianças e adolescentes não poderão ser utilizados para quaisquer finalidades comerciais, incluindo qualquer forma de pesquisa de mercado, direcionamento de publicidade ou inteligência de negócios.

Assim, mesmo com o consentimento para a captura da imagem, uma vez que o sistema reconheça a presença de uma criança ou adolescente, a imagem deverá ser imediata e permanentemente excluída, e nenhum outro dado referente a ela poderá ser armazenado para finalidades comerciais.

Trata-se de boa prática igualmente em compasso com a melhor interpretação da lei: qualquer publicidade direcionada à criança pode ser considerada abusiva pelo Código de Defesa do Consumidor (art. 37, §2º), em especial caso faça uso de técnicas de reconhecimento facial para direcionamento ou outra forma de personalização, pois se aproveita da deficiência de julgamento e experiência da criança. A resolução nº 163/2014 do Conanda, ainda, prevê importantes limitações à publicidade direcionada à criança e ao adolescente, e o próprio *caput* do Art. 14 da LGPD prevê que o tratamento de dados de crianças e adolescentes deve ocorrer em seu melhor interesse.

Na prática, isso significa apontar, antes da área de alcance das câmeras de reconhecimento facial, que a entrada de crianças ou adolescentes desacompanhados é proibida e que, caso acompa-

nhados por seus pais ou responsáveis, estes devem fornecer seu consentimento de forma compatível com a legislação. Tal consentimento, no entanto, abarcará somente a captura da imagem e sua posterior exclusão, não podendo envolver o uso de dados pessoais de crianças e adolescentes para finalidades comerciais, especialmente para direcionamento de publicidade.

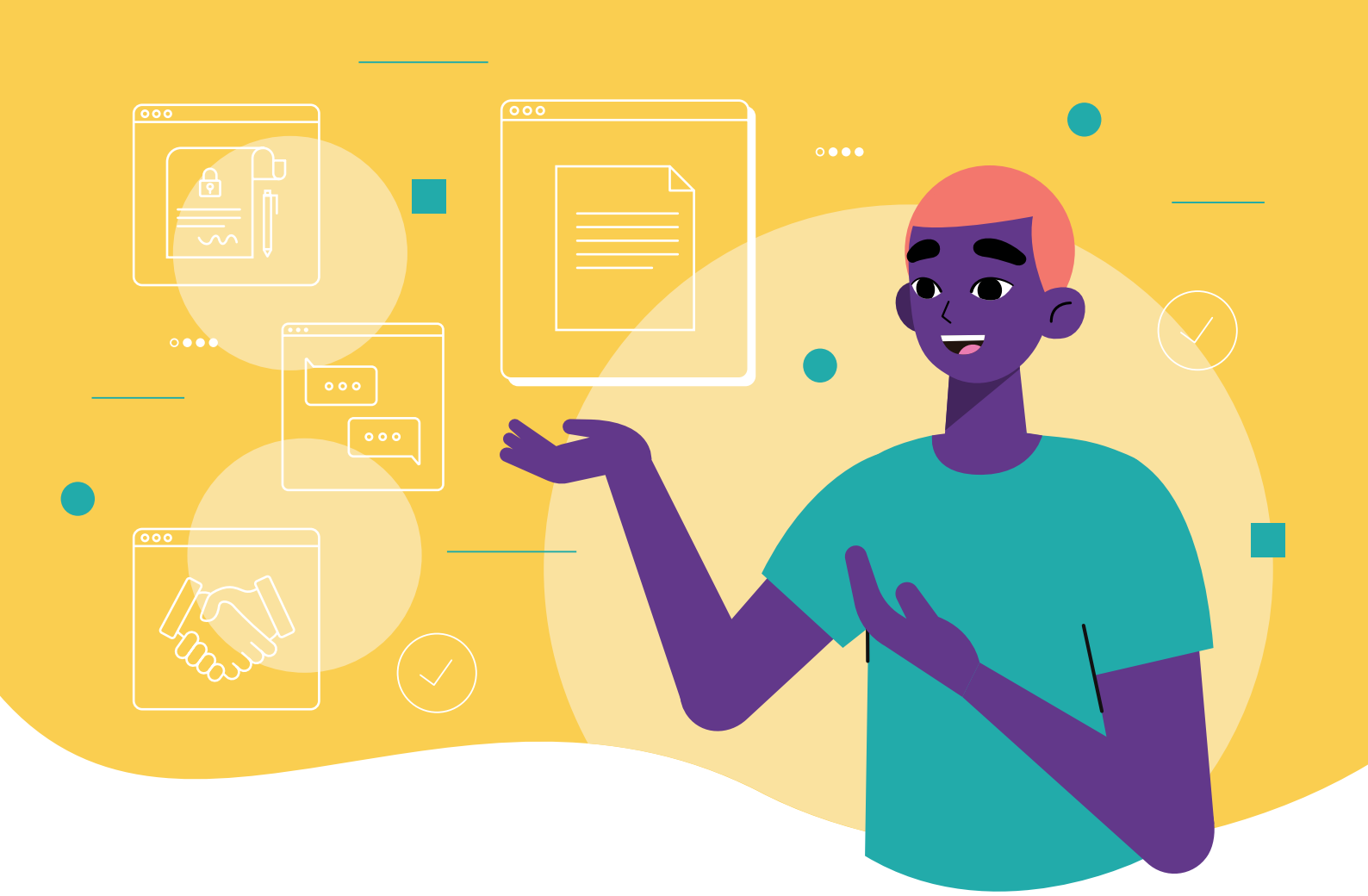
7.9. INCIDENTES DE SEGURANÇA

Por se tratar de atividade eminentemente sensível e de elevado risco social, com potencial de violações graves à privacidade dos afetados, todo e qualquer incidente de segurança, seja ele voltado aos dados biométricos ou aos dados anonimizados, deve ser:

- ☑ Investigado imediatamente, de forma a cessar ou minimizar seus efeitos, inclusive por meio do desligamento completo da tecnologia até que se tenha certeza de que pode funcionar de maneira a proteger a privacidade dos titulares de dados;

- ☑ Informado imediatamente às autoridades públicas e à sociedade civil, por exemplo por meio de postagens no site da empresa ou em suas redes sociais; e

- ☑ Informado imediatamente aos titulares dos dados, especialmente se acarretar risco ou dano relevante, nos termos do art. 48 da Lei Geral de Proteção de Dados.



8. RECOMENDAÇÕES PARA A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Dada a franca expansão da utilização de tecnologias de reconhecimento facial no Brasil e no mundo, este documento teve o intuito de apresentar boas práticas a serem seguidas em sua implementação, considerando-se os riscos e impactos à privacidade já conhecidos a titulares. Mesmo que a utilização de sistemas de

reconhecimento facial apresente, mesmo com o cumprimento das recomendações que trazemos aqui, altos riscos à privacidade e outros direitos fundamentais, tais riscos podem ser mitigados se houver o respeito a um *framework* estrito e voltado aos interesses da coletividade. Atender a recomendações dessa natureza pode permitir ganhos significativos de segurança dessas ferramentas e fomentar a confiança que os usuários depositam sobre sua utilização em ambientes comerciais.[44]

Não obstante este primeiro esforço de delimitação de padrões éticos e boas práticas para a utilização desta tecnologia, dada a novidade e o seu permanente desenvolvimento, persistem zonas cinzentas em relação às possibilidades de sua aplicação e suas consequências. Assim, é da máxima importância insistir no debate sobre a sua utilização e atentar para a imprescindível manifestação da Autoridade Nacional de Proteção de Dados (ANPD) sobre o tema.

São ainda necessárias delimitações claras a respeito do exercício dos direitos de transparência, consentimento dos usuários, proibição de condutas abusivas e até mesmo a proibição do uso em certos casos, assim como o estabelecimento de limites claros em determinados espaços, como locais de circulação pública ou igrejas[45]. Assim, quando constituída, a Autoridade deve promover consultas públicas e audiências com o intuito de fomentar o diálogo sobre este tema, bem como de formular normativas que o regulamentem.

44. Pesquisas recentes mostram como usuários não confiam em tecnologias de reconhecimento facial utilizadas para fins comerciais. Uma pesquisa do Ada Lovelace Institute (Beyond Face Value: public attitudes to facial recognition technology, 2019) mostra que apenas 7% de consumidores aprova o uso de tecnologias de reconhecimento facial em supermercados para monitorar o comportamento dos consumidores ou direcionar publicidade com base em suas características. Outra pesquisa do Pew Research Center (disponível em: https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/) mostra que apenas 15% dos consumidores entrevistados confiam em tecnologias que mensuram a reação do público a propagandas por meio de tecnologias de reconhecimento facial.

45. https://apublica.org/2019/11/empresas-lancam-servico-de-reconhecimento-facial-para-igrejas-no-brasil/

REFERÊNCIAS

ACKERMAN, M.; DARRELL, T.; WEITZNER, D. Privacy in Context. *Human-Computer Interaction*, v. 16, n. 2-4, p. 167-176, 2001.

ACQUISTI, A.; GROSS, R.; STUZMAN, F. Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, 2, 2014. 1-20.

BATAGELJ, B.; RAVNIK, R.; SOLINA, F. *Computer vision and digital signage*. [S.l.]: [s.n.], 2018.

BIONI, B. R. *Proteção de Dados Pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BUCLKEY, B.; HUNTER, M. Say cheese! Privacy and facial recognition. *Computer Law and Security Review*, v. 27, p. 637-640, 2011.

BUOLAMWINI, J.; GEBRU, T. *Gender Shades:* Intersectional Accuracy Disparities in Commercial Gender Classification. [S.l.]: [s.n.].

COSERARU, R. *Facial Recognition Systems and their Data Protection Risks under the GDPR.* Tilburg University. Tilburg. 2017.

CRAWFORD, Kate, et al. *AI Now 2019 Report*. NewYork: AI Now Institute, 2019. Disponível em: https://ainowinstitute.org/AI_Now_2019_Report.html.

DATA PROTECTION WORKING PARTY. *Opinion 02/2012 on facial recognition in online and mobile services.* [S.l.]. 2012. (00727/12/EN WP 192).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Under watchful eyes: biometrics, EU IT systems and fundamental rights.* União Europeia. Luxemburgo. 2018.

EUROPEIA, C. *Orientações éticas para uma IA de confiança.* Grupo de peritos de alto nível sobre a inteligência artificial. Bruxelas. 2019.

FARINELLA, G. M. et al. Face Re-Identification for Digital Signage Applications. *International Workshop on Video Analytics for Audience Measurement in Retail and Digital Signage*, p. 40-52, 2014.

FEDERAL TRADE COMMISSION. *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies.* Federal Trade Comission. [S.l.]. 2012.

GARVIE, C.; BEDOYA, A.; FRANKIE, J. *The Perpetual Line-up: Unregulated Police Face Recognition in America.* Georgetown. 2016.

JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, v. 14, n. 1, p. 1-29, 2004.

KLARE, B. F. et al. Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on Information Forensics and Security* , v. 7, n. 6, 2012.

LEWINSKI, P.; TRZASKOWSKI, J.; LUZAK, J. Face and Emotion Recognition on Commercial Property under EU Data Protection Law. *Psychology & Marketing*, v. 33, n. 9, p. 729-746, Setembro 2016.

MILLIGAN, C. S. Facial Recognition Technology, Video Surveillance, and Privacy. *Southern California Interdisciplinary Law Journal*, v. 9, n. 1, p. 295-334.

PEDRAZA, J. et al. Privacy-by-design rules in face recognition system. *Neurocomputing*, v. 109, p. 49 - 55, 2013.

RING, T. Privacy in Peril: is facial recognition going too far too fast? *Biometric Technology Today*, v. 7, n. 2016, p. 7-11, 2016.

WORLD PRIVACY FORUM ET AL. *Digital Signage Privacy Principles: Critical policies and practices for digital signage networks.* [S.l.]. 2010.

Z. LI, S.; JAIN, A. K. *Handbook of Facial Recognition*. Londres: Springer, 2011.

idec
Instituto Brasileiro de Defesa do Consumidor

INTERNETLAB
pesquisa em direito e tecnologia