Brasília, 01 de agosto de 2025.

CONTRIBUIÇÃO BRASSCOM | TOMADA DE SUBSÍDIOS: DADOS PESSOAIS SENSÍVEIS - DADOS BIOMÉTRICOS

ENTIDADE DESTINATÁRIA: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

SUMÁRIO EXECUTIVO

A Lei Geral de Proteção de Dados Pessoais (LGPD) classifica o dado biométrico como dado pessoal sensível, mas não fornece uma definição expressa sobre o que o caracteriza. Referências internacionais, como o GDPR europeu, são importantes fontes de hermenêutica para tal.

Segundo referências internacionais, a identificação de um dado como biométrico exige, cumulativamente, três critérios objetivos:

1. Referência a características físicas, fisiológicas ou comportamentais de uma pessoa natural (ex: voz, impressões digitais, traços faciais);

2. Tratamento técnico específico, com extração, codificação ou conversão dessas características;

3. Finalidade de identificação ou autenticação individual do titular.

Dessa forma, imagens, vídeos, áudios ou dados similares não deveriam ser automaticamente considerados biométricos — apenas se forem tratados de maneira técnica e específica, com finalidade de identificação única. Tecnologias que apenas detectam atributos ou rastreiam usuários de forma anonimizada, como fingerprinting de dispositivos, não se enquadrariam como tratamento de dados sensíveis, exceto quando associadas à identificação pessoal.

A própria ANPD, no Guia sobre Biometria e Reconhecimento Facial, adota entendimento semelhante, alinhado a órgãos como o European Data Protection Board (EDPB) e a Information Commissioner's Office (ICO) do Reino Unido: a categorização como dado sensível depende da finalidade do tratamento e do uso de técnicas que permitam a identificação única do titular.

A imutabilidade relativa, embora não seja critério obrigatório, é um indicativo importante: características como impressão digital ou estrutura facial são mais estáveis que padrões comportamentais, como marcha ou assinatura, que podem variar por contexto.

A biometria comportamental, portanto, não deve ser equiparada à biometria tradicional de forma automática, pois sua confiabilidade e estabilidade são distintas. A aplicação de

uma abordagem excessivamente ampla comprometeria a segurança jurídica e inviabilizaria o uso legítimo e de baixo risco de tecnologias inovadoras, inclusive em áreas sensíveis como saúde, pesquisa e prevenção a fraudes.

Entende-se que a ANPD deveria adotar abordagem tecnica e cautelosa, alinhada às boas práticas internacionais, para evitar interpretações excessivamente amplas que comprometam a segurança jurídica e o uso responsável de tecnologias. O reconhecimento de um dado como biométrico deve depender da combinação entre as características intrínsecas, a técnica aplicada e a finalidade do tratamento, garantindo o equilíbrio entre proteção de dados e inovação.

A transparência no tratamento de dados biométricos deve considerar o contexto específico da operação de tratamento, conforme orientações do Information Commissioner's Office (ICO), do Reino Unido. Não há uma fórmula única, sendo necessário ponderar variáveis como o caso de uso, o tipo de relação com o titular e a natureza dos dados tratados. Quanto mais previsível e consolidado o tratamento (como no caso de verificação biométrica em serviços de telefonia), menor a exigência por medidas ativas, bastando mecanismos usuais de aviso, como cláusulas contratuais, QR Codes e informações no ponto de atendimento.

Apesar disso, boas práticas de transparência devem sempre ser observadas, mesmo quando os dados não forem sensíveis, incluindo a explicitação de finalidades específicas, legítimas e compatíveis com os propósitos declarados.

Além disso, vale destacar que a LGPD prevê múltiplas bases legais igualmente válidas para o tratamento de dados pessoais, inclusive os sensíveis, como os biométricos. A escolha da base mais adequada depende do contexto e da finalidade do tratamento, não havendo hierarquia entre elas.

O consentimento pode ser utilizado para o tratamento de dados biométricos, desde que atenda aos requisitos legais de ser livre, informado, inequívoco, específico e destacado. A LGPD não proíbe o condicionamento do serviço à coleta de dados, desde que:

- haja transparência sobre a necessidade do tratamento; e
- não haja desvantagens desproporcionais ou discriminatórias ao titular.

Essa interpretação se alinha ao princípio da autodeterminação informativa, conferindo ao titular o direito de escolher com quais serviços e práticas de tratamento deseja se relacionar, especialmente em um mercado digital competitivo e plural. Assim, o consentimento pode ser considerado válido mesmo que sua recusa implique na indisponibilidade do serviço, desde que este não seja essencial ou obrigatório.

No entanto, o consentimento não será sempre a base legal mais adequada — ou sequer válida —, especialmente em situações onde:

- não há alternativa técnica viável ao uso da biometria;

- há risco de fraude em caso de flexibilização;

- ou a biometria é condição necessária à prestação do serviço (como em pesquisas específicas).

Nesses casos, a LGPD prevê, no art. 11, II, "g", a base legal da prevenção à fraude, que dispensa o consentimento quando o tratamento biométrico é necessário para processos de identificação e autenticação.

Esse fundamento legal reflete uma ponderação entre o direito à privacidade e o interesse coletivo na segurança e estabilidade das relações digitais e econômicas. No Brasil, o elevado número de fraudes — como os 1,24 milhão de tentativas registradas só em janeiro de 2025 — demonstra a relevância prática dessa base, que viabiliza o uso de tecnologias biométricas para proteger tanto os titulares quanto o ecossistema digital.

Comparado ao GDPR europeu, a LGPD é mais avançada por reconhecer expressamente a prevenção à fraude como base legal autônoma. A ausência dessa previsão na Europa tem gerado entraves jurídicos e operacionais para empresas que lidam com autenticação biométrica em ambientes privados.

A base legal da prevenção à fraude deve ser reconhecida como legítima, necessária e proporcional ao tratamento de dados biométricos em diversos contextos, inclusive como alternativa válida ao consentimento. A flexibilidade normativa da LGPD, aliada a salvaguardas técnicas e organizacionais, assegura um equilíbrio entre proteção de direitos, segurança pública e inovação econômica.

No contexto do desenvolvimento e aperfeiçoamento de sistemas de IA, o uso de dados biométricos para o treinamento de modelos voltados à detecção e prevenção de vieses discriminatórios configura medida essencial para a efetividade dos deveres constitucionais e legais de promoção da igualdade. Ao possibilitar que os sistemas reconheçam, mensurem e corrijam distorções decorrentes de recortes raciais, de gênero, idade ou deficiência, o uso técnico e controlado desses dados serve diretamente ao objetivo de evitar tratamentos injustos ou excludentes por parte de sistemas baseados em IA e atendem o interesse público de combate à discriminação.

Esse uso encontra fundamento jurídico sólido na Constituição Federal (arts. 3º, IV e 5º, caput) e em legislações como o Estatuto da Igualdade Racial e o Estatuto da Pessoa com Deficiência, que impõem obrigações específicas para mitigação de desigualdades estruturais. Nessa perspectiva, o tratamento de dados biométricos pode ser legitimamente enquadrado na base legal do art. 11, II, "a" da LGPD — cumprimento de obrigação legal ou regulatória.

O tratamento de dados biométricos de crianças e adolescentes está sujeito a uma análise concreta e contextualizada do princípio do melhor interesse do menor, conforme o art. 14 da LGPD, o ECA e o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU. Tal avaliação deve ponderar o interesse do menor em conjunto com outros direitos

fundamentais, assegurando margem de atuação para que o controlador demonstre, caso a caso, a legitimidade do tratamento.

De acordo com o Enunciado nº 1/2023 da ANPD, o tratamento pode se basear em qualquer das hipóteses legais previstas nos arts. 7º e 11 da LGPD, desde que respeitado o melhor interesse da criança ou adolescente. Quando adotado o consentimento, ele deve ser inequívoco, informado e transparente para os representantes legais.

Ainda, o cumprimento do princípio da necessidade exige a utilização estritamente limitada aos dados indispensáveis à finalidade legítima. Exemplo internacional relevante é o caso polonês sobre uso de biometria em escolas, no qual o tribunal reconheceu a validade do consentimento e a proporcionalidade do uso, reformando decisão anterior da autoridade de proteção de dados.

Diante do alto potencial lesivo decorrente de eventuais violações de dados biométricos, como o roubo de identidade, é indispensável a adoção de medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem atuado proativamente nesse sentido, incorporando mecanismos avançados de segurança da informação — como criptografia, segmentação de bases, anonimização, controle de acesso e rastreabilidade — desde as fases iniciais do desenvolvimento de produtos e sistemas. Além disso, muitas empresas já implementam práticas sofisticadas de privacy by design e by default, realizando o tratamento de dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem que haja identificação ou reidentificação de uma pessoa natural, o que reduz significativamente os riscos à privacidade.

Para garantir a conformidade com a LGPD, é essencial que as organizações adotem parâmetros mínimos de avaliação contínua de riscos, por meio de relatórios de impacto à proteção de dados (RIPDs) e monitoramento de possíveis vieses ou falhas de segurança. A definição de políticas internas claras, a capacitação de equipes e a governança ativa sobre o ciclo de vida dos dados também são medidas fundamentais para assegurar o tratamento responsável e proporcional desses dados sensíveis. Esse conjunto de ações, já amplamente adotado por empresas do setor, demonstra que é possível conjugar inovação tecnológica com proteção integral dos titulares de dados.

O uso de dados biométricos anonimizados, por sua vez, quando submetido a testes de robustez e medidas técnicas eficazes, deixa de configurar dado pessoal nos termos do art. 12 da LGPD. Isso viabiliza seu uso para fins como treinamento e calibração de modelos de IA, sem que haja necessidade de aplicação das restrições previstas para dados pessoais sensíveis.

BLOCO I - Princípio do melhor interesse

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados

Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo "dados biométricos", mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) não fornece uma definição expressa do que se entende por "dado biométrico", limitando-se a incluí-lo como uma das espécies de dado pessoal sensível (art. 5º, II). Diante dessa lacuna conceitual, a adequada interpretação do que constitui dado biométrico exige a conjugação dos critérios previstos na própria LGPD com referências internacionais consolidadas, especialmente o Regulamento Geral sobre a Proteção de Dados (GDPR), bem como posicionamentos de autoridades de proteção de dados estrangeiras e entidades especializadas.

De início, é imprescindível considerar que, nos termos da LGPD, apenas se considera dado pessoal aquele que permite identificar ou tornar identificável uma pessoa natural. Esse critério é fundamental: características corporais ou comportamentais somente serão tratadas como dados pessoais sensíveis quando estiverem associadas, direta ou indiretamente, à identidade do titular.

Nesse sentido, o GDPR, em seu artigo 4o, n.o 14, define dado biométrico como o resultado de um "tratamento técnico específico" aplicado a características físicas, fisiológicas ou comportamentais de um indivíduo com o propósito de

permitir ou confirmar sua identificação única. O considerando 51 reforça que imagens brutas, como fotografias ou vídeos, não são, por si só, dados biométricos, salvo se forem processadas tecnicamente para fins de identificação.

Esse entendimento é corroborado pelo European Data Protection Board (EDPB), que esclarece que o simples registro de imagens não configura, por si só, o tratamento de dados pessoais sensíveis. Isso só ocorre quando essas imagens passam por algoritmos ou técnicas que extraem medidas biométricas — como vetores faciais ou mapas dactiloscópicos — e os utilizam com a finalidade de identificar ou autenticar indivíduos.

Autoridades nacionais europeias têm adotado critérios semelhantes. A Autoridade de Proteção de Dados do Reino Unido (ICO), por exemplo, sustenta que dados biométricos devem (i) referir-se a características físicas, fisiológicas ou comportamentais, (ii) ser objeto de tratamento técnico específico, e (iii) ter como finalidade permitir a identificação única de uma pessoa. A autoridade holandesa segue linha semelhante, dado biométrico é o que (i) diz respeito a características pessoais geralmente permanentes; (ii) resulta de tratamento técnico que compara medidas a uma referência; e (iii) tem como propósito estabelecer ou confirmar a identidade de alguém.

Com base no entendimento da Autoridade de Proteção de Dados do México (INAI) , e do art. 16 ter da Lei de Proteção de Dados Chilena, consideram-se dados biométricos aqueles que, cumulativamente, atendem aos seguintes requisitos:

a) estejam relacionados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; e

b) resultem de um tratamento específico (em regra, uma forma de medição), cuja finalidade seja identificar, de maneira única, o titular.

Dessa forma, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, isoladamente, considerados dados biométricos. Apenas o resultado do tratamento específico dessas informações que objetive identificar unicamente indivíduos pode ser considerado um dado biométrico.

Além disso, o Future of Privacy Forum (FPF) propõe uma taxonomia útil para distinguir os diferentes usos de dados corporais. A entidade divide esses usos em cinco categorias: detecção, caracterização, rastreamento único e persistente, verificação (1:1) e identificação (1:N). De acordo com essa tipologia, somente as duas últimas envolvem tratamento com capacidade efetiva de

identificação única e, portanto, se enquadram claramente como dados pessoais sensíveis.

Diante disso, é possível extrair três critérios objetivos que devem ser cumulativamente observados para que determinado dado possa ser considerado biométrico à luz da LGPD:

1. Referência a características físicas, fisiológicas ou comportamentais inerentes a uma pessoa natural (por exemplo: impressões digitais, traços faciais, voz, marcha);

2. Submissão a tratamento técnico específico, mediante uso de tecnologias que extraiam, codifiquem ou convertam essas características em medições ou templates;

3. Finalidade de identificação ou autenticação individual, ou seja, o uso do dado com o propósito de permitir ou confirmar quem é o titular.

Logo, não basta que uma tecnologia capture características do corpo humano para que esteja automaticamente tratando dados pessoais sensíveis. A identificação (ou identificabilidade) do titular é elemento indispensável. Tecnologias que apenas detectam presença, inferem atributos sem identificação ou realizam rastreamento anonimizado não devem ser enquadradas, por si só, como tratamento de dados pessoais sensíveis. A técnica de *fingerprinting*, por exemplo, envolve a coleta de várias características de um dispositivo ou navegador, como sistema operacional, versão do navegador, idioma, resolução da tela, plugins instalados e outros detalhes, criando uma "impressão digital" única que pode ser usada para identificar o dispositivo, e não características inerentes ao corpo ou ao comportamento individual da pessoa natural. Ainda que possa, em determinados contextos, contribuir para a singularização de um usuário, a informação extraída refere-se ao dispositivo e não ao titular, o que afasta a natureza biométrica da informação tratada.

O uso dessa técnica em contextos legítimos de prevenção à fraude e segurança da informação, especialmente quando anonimizada ou pseudonimizada, não objetiva a identificação direta do indivíduo, mas sim a detecção de padrões suspeitos de comportamento digital, sendo, portanto, desproporcional o enquadramento como dado sensível. Tal interpretação ampliada poderia comprometer a eficácia de medidas de segurança amplamente utilizadas pelo setor, além de distorcer o equilíbrio normativo proposto pela LGPD entre proteção de dados e inovação tecnológica.

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

Nesse sentido, pertinente esclarecer que a simples coleta de dados que podem revelar informações biométricas não pode ser considerada automaticamente uma atividade de tratamento de dados pessoais sensíveis. É necessária uma justificativa específica, de forma que somente dados utilizados para identificar ou autenticar titulares podem ser considerados biométricos. Além disso, se a informação não for operada por meio técnico que permita a identificação, não será considerada dado biométrico. Esse entendimento alinha-se ao sustentado pela autoridade de proteção de dados do Reino Unido ("ICO"), a qual afirma que os dados biométricos somente serão considerados dados sensíveis quando forem utilizados com a finalidade de identificar uma pessoa de forma única, de modo que a sua categorização dependerá da finalidade do tratamento. Conclui-se, portanto, que o mero tratamento de fotografias, sem a aplicação de técnicas específicas capazes de permitir a identificação inequívoca ou a autenticação de uma pessoa natural, não deve ser considerado, de forma sistemática, como tratamento de dados pessoais sensíveis nos termos do art. 5º, II, da LGPD.

Portanto, sugere-se que a ANPD adote uma abordagem criteriosa e tecnicamente orientada, alinhando-se às boas práticas internacionais, reconhecendo que o conceito de dado biométrico não deve ser aplicado de forma ampla ou imprecisa, mas apenas quando estiverem presentes os três critérios mencionados. Tal postura é essencial para garantir segurança jurídica, evitar distorções interpretativas e permitir o uso responsável de tecnologias que operam com dados corporais, mas que não necessariamente expõem os titulares a riscos relevantes de identificação.

No contexto de empresas que atuam como operadoras, como é o caso de empresas que disponibilizam sistemas com funcionalidades de autenticação biométrica a outras empresas, é essencial reconhecer que a caracterização do dado como dado pessoal sensível dependerá da forma como o controlador irá definir o tratamento. A empresa operadora, embora seja responsável por garantir padrões técnicos e de segurança da informação, não define a finalidade, base legal ou escopo do tratamento. Assim, é necessário que a regulamentação da ANPD reconheça que a análise da sensibilidade dos dados deve considerar o

papel desempenhado pelo operador que o enquadramento como dado biométrico requer a combinação da técnica aplicada com a finalidade determinada pelo controlador.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Conforme a Autoridade de Dados do Reino Unido (ICO), não existe metodologia única aplicável a todos os casos sobre como a transparência pode ser garantida, incluindo medidas ativas a serem adotadas pelos controladores. A forma mais eficiente de transparecer o uso de dados biométricos ao titular deverá ponderar fatores, como: i) o caso de uso; ii) a natureza de relacionamento com o titular; e iii) os dados envolvidos na atividade de tratamento.

Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência.

Quando o tratamento de dados pessoais ocorre no contexto da validação da identidade do titular, durante a contratação ou utilização de produto ou serviço — por exemplo, a verificação biométrica no processo de contratação ou portabilidade de plano de telefonia. Trata-se de prática consolidada no mercado, em que a coleta de dados biométricos é clara e previsível para o titular, inclusive devido à: (i) existência de regulamentações que requerem que empresas de telefonia adotem mecanismos de prevenção a fraudes, como o art. 65-M, da Resolução ANATEL 738/2020; e (ii) o fato de que fraudes no acesso às linhas de telefone dos usuários podem servir de ponto de partida para a realização de novas práticas criminosas, incluindo a obtenção de contas de e-mail, a estes vinculadas enquanto mecanismos de recuperação de senhas, e, a partir destas, contas de diversos serviços em que o titular está inscrito. Nesses casos, o fornecimento do Aviso de Privacidade ao longo da jornada do usuário, nos termos de seu contrato de prestação de serviço ou, no caso de atendimento presencial, por meio de QR Codes disponibilizados em telas, cartazes ou materiais similares dentro do local físico, ou mesmo breve explicação pelo atendente, é suficiente para assegurar o atendimento do dever de transparência.

De qualquer forma, as boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível, como é o caso do dado biométrico. Dessa forma, medidas que garantam, aos titulares, o acesso de informações claras e precisas acerca da realização do tratamento de dados, informando a finalidade dos

respectivos tratamentos, mediante indicação de propósitos legítimos, específicos e explícitos, bem como a limitação do tratamento de dados de forma incompatível com as finalidades determinadas são referência de boas práticas no que tange à transparência.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Como abordado na resposta nº 1, a LGPD não apresenta definição específica para "dado biométrico", limitando-se a classificá-lo como uma categoria de dado pessoal sensível. Nesse contexto, a caracterização de um dado como biométrico exige uma análise baseada em critérios objetivos que levem em conta a finalidade e a forma de tratamento do dado. De acordo com a própria LGPD, um dado só será considerado pessoal se puder tornar o titular identificado ou identificável. Essa premissa é essencial para o enquadramento dos dados biométricos, pois apenas informações capazes de individualizar o titular podem ser qualificadas como tal.

Dessa forma, dados que possam conter características biométricas, sejam elas imagens captadas em vídeo, fotografias ou gravações de voz, não devem ser, isoladamente, considerados dados biométricos ou mesmo dados pessoais sensíveis, nos termos da LGPD. Se uma fotografia, por exemplo, for empregada para treinar um modelo de IA com o objetivo de aprimorar funcionalidades gerais — como detecção de objetos, identificação de padrões de métrica facial, ou classificação de imagens — sem a intenção de identificar ou autenticar uma pessoa natural de forma individualizada, não há que se falar em tratamento de dado pessoal sensível.

A interpretação conforme a LGPD deve se apoiar na finalidade específica e concreta do tratamento, conforme preceitua o princípio da necessidade (art. 6º, III) e da finalidade (art. 6º, I). A mera possibilidade teórica de que um dado possa vir a ser utilizado para identificação não é suficiente para que se imponha, de forma automática, o regime jurídico mais rigoroso aplicável aos dados sensíveis. Essa interpretação extensiva — e, portanto, desproporcional — comprometeria a segurança jurídica e inviabilizaria aplicações legítimas e de baixo risco da IA, inclusive em setores como pesquisa, saúde, educação e prevenção de fraudes.

Além disso, a Brasscom entende que a biometria comportamental não deve ser automaticamente equiparada à biometria tradicional apenas por estar vinculada

ao corpo humano. Dessa forma, enquanto a biometria tradicional se baseia em características físicas relativamente estáveis e imutáveis (como digitais, íris ou estrutura facial), a biometria comportamental envolve padrões que podem variar significativamente conforme o contexto. Por exemplo, a forma de caminhar de uma pessoa pode se modificar se ela sofrer uma lesão, passar por treinamento militar ou envelhecer. O mesmo se aplica a padrões de digitação, ritmo de voz ou movimento ocular. Tais variabilidades impactam diretamente a exatidão e confiabilidade desses dados, e devem ser levadas em conta na aplicação dos princípios da qualidade e da segurança.

Para suprir a ausência de definição legal no Brasil, o conceito adotado pelo Regulamento Europeu de Proteção de Dados (GDPR) serve como importante referência. Segundo o art. 4.14 do GDPR, dado biométrico é o resultado de tratamento técnico específico aplicado a características físicas, fisiológicas ou comportamentais de uma pessoa natural, com o objetivo de permitir ou confirmar sua identificação única.

O Information Commissioner's Office (ICO), autoridade britânica de proteção de dados, reforça essa definição ao estabelecer que apenas são considerados dados biométricos os que:

> (i) se referem a características físicas, fisiológicas ou comportamentais;
> (ii) foram submetidos a tratamento técnico específico, como extração e codificação; e
> (iii) têm como finalidade identificar ou autenticar uma pessoa de forma única.

Aplicando esses critérios aos dados biométricos comportamentais, como dinâmica de digitação, assinatura manuscrita, padrão de marcha ou entonação vocal, conclui-se que a mera coleta ou análise desses comportamentos não é suficiente para que se caracterizem como dados biométricos. Conforme o ICO, apenas quando essas informações são submetidas a algoritmos que as codificam em formatos técnicos específicos — como vetores ou templates — para fins de identificação ou autenticação individual, é que se poderá falar em dados pessoais sensíveis.

Outro elemento importante para essa análise é o conceito de imutabilidade relativa, abordado pelo European Parliamentary Research Service (EPRS). Segundo o estudo, o termo "biométrico" pressupõe certo grau de permanência: trata-se de características que o indivíduo não pode modificar voluntariamente, como o rosto ou a impressão digital. Por isso, técnicas que analisam gestos, assinatura, voz ou marcha — apesar de envolverem comportamento — podem ser consideradas biométricas, pois se baseiam em padrões corporais relativamente constantes. Em contrapartida, comportamentos voluntários e

amplamente modificáveis, como preferências de navegação, hábitos de consumo ou conteúdo de comunicação, não se enquadram como dados biométricos, por não refletirem uma característica física ou comportamental estável e intrínseca ao corpo da pessoa.

Diante disso, para que um dado comportamental seja considerado dado pessoal sensível nos termos da LGPD, é necessário que preencha três requisitos cumulativos:

1. Referência a uma característica física, fisiológica ou comportamental do indivíduo;
2. Tratamento técnico específico, com extração, conversão ou codificação por meio de algoritmos;
3. Finalidade de identificação ou autenticação única do titular, permitindo sua distinção individual em sistemas de verificação (1:1) ou identificação (1:N).

A presença de imutabilidade relativa serve como indicativo complementar relevante, embora não exclusivo, para a classificação do dado como biométrico.

Em síntese, a simples natureza comportamental do dado não é suficiente para enquadrá-lo automaticamente como dado pessoal sensível. É imprescindível avaliar o modo de tratamento técnico e a finalidade de uso. Essa abordagem evita uma interpretação excessivamente ampla e desproporcional da categoria de dados biométricos, e assegura um equilíbrio entre proteção de direitos e inovação tecnológica, em consonância com os princípios da LGPD.

Nos casos em que a biometria comportamental é utilizada por meio de soluções de autenticação embarcadas em softwares comercializados, é fundamental que a categorização do dado como biométrico considere a finalidade determinada pelo controlador. O operador pode realizar o tratamento técnico (como extração, processamento e codificação), mas não necessariamente define o propósito do uso, tampouco se os dados tratados serão utilizados para identificação única ou apenas como fator comportamental complementar.

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Antes de se responder de maneira direta, cumpre lembrar que existem diversas bases legais previstas na LGPD, e a mais apropriada dependerá do contexto específico, não havendo nenhum tipo de hierarquização entre elas, isto é, todas as hipóteses previstas são igualmente válidas e podem ser utilizadas sem haver a necessidade de se priorizar uma em detrimento de outras.

Para que o consentimento para o tratamento de dados biométricos seja considerado livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD, é fundamental que o titular tenha clareza sobre a finalidade do tratamento, compreenda suas implicações e possa manifestar sua vontade de forma autônoma, sem coerção ou engano.

A exigência de que o consentimento seja livre não implica, necessariamente, a ausência de qualquer condicionamento. O que a LGPD veda é a coação, a ausência de transparência ou a imposição de desvantagens excessivas ao titular. A simples oferta de um serviço vinculada ao tratamento de dados pessoais — inclusive biométricos — não invalida, por si só, o consentimento. A simples oferta de um serviço em troca do consentimento não o invalida, desde que:

- Haja transparência quanto à necessidade dos dados para a prestação do serviço; e

- O titular não seja compelido a consentir sob pena de sofrer desvantagens desproporcionais ou discriminatórias.

Importante reconhecer que o titular de dados pessoais detém a liberdade de determinar quais serviços deseja utilizar, podendo consentir ou não com o tratamento de seus dados, com base nas informações claras e suficientes que lhe forem apresentadas pelos agentes de tratamento. Tal premissa é a essência do princípio da autodeterminação informativa que norteia a estrutura de proteção de dados pessoais no Brasil. O ecossistema digital, caracterizado por elevada dinamicidade, competitividade e pluralidade de soluções, confere ao titular meios concretos para exercer essa autodeterminação informativa, optando por serviços que melhor se alinhem às suas preferências e expectativas. Assim, o consentimento pode ser livre, mesmo quando sua negativa resulte na indisponibilidade de determinado serviço, desde que não se trate de serviço essencial ou de acesso obrigatório.

Diante da relevância do consentimento como base legal no tratamento de dados pessoais sensíveis, é fundamental que a ANPD reconheça, em suas orientações e interpretações normativas, as nuances e particularidades envolvidas na aferição do consentimento livre, especialmente no contexto da economia digital. Tal reconhecimento é essencial para evitar abordagens excessivamente restritivas que possam comprometer a viabilidade jurídica e econômica de modelos de negócio legítimos, amplamente utilizados na oferta de serviços digitais. Ao considerar a liberdade do titular em escolher, com base em informações claras, quais serviços deseja utilizar e com quais práticas de tratamento de dados concorda, a ANPD contribuirá para a consolidação de um ambiente regulatório equilibrado, que simultaneamente protege os direitos dos titulares e garante a sustentabilidade da inovação e da competitividade no ambiente digital brasileiro.

De fato, há casos em que o consentimento não será a base legal mais adequada - e mesmo a efetivamente correta - para o tratamento de dados pessoais sensíveis, razão pela qual o art. 11, em seu inciso II, traz outras hipóteses nas quais o tratamento do dado biométrico dispensa o consentimento. Nesse sentido, destaca-se a alínea "g", a qual prevê expressamente a dispensa do consentimento para garantia da prevenção à fraude em processos de identificação e autenticação de cadastro. Nota-se, portanto, que o referido tratamento tem por finalidade proteger a segurança do próprio titular do dado contra usos indevidos de sua identidade. Nesse mesmo contexto, a exigência do consentimento poderia inviabilizar mecanismos de segurança automatizados, como as autenticações por reconhecimento facial ou impressão digital.

O consentimento não será a base legal adequada nas situações em que os requisitos de validade não podem ser satisfeitos, tipicamente isso transcorrerá em situações como quando não for viável oferecer alternativa à biometria facial ao titular de dados. **Por exemplo, em processos de prevenção a fraudes, nos quais eventual opção poderia facilitar a atuação de fraudadores, ou nos casos em que a biometria é essencial para a prestação do serviço ou funcionamento do produto.** Essa hipótese admite exceção quando não houver outra base legal aplicável e a ausência de consentimento tornar inviável o prosseguimento do tratamento biométrico - nesses casos, o prejuízo decorrente da negativa do titular é consequência necessária da própria impossibilidade de realizar a atividade. Por exemplo, se o titular deseja participar (com ou sem remuneração) de pesquisa conduzida por ente privado com fins lucrativos que envolva o uso de dados biométricos, a continuidade da participação estará legitimamente condicionada à oferta do consentimento, já que o tratamento dos dados é imprescindível para a execução da pesquisa.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A utilização de dados biométricos com a finalidade de prevenção à fraude deve ser analisada à luz da LGPD a partir de uma ponderação entre os direitos fundamentais à privacidade e à proteção de dados, de um lado, e o interesse coletivo na segurança, na estabilidade econômica e na prevenção de ilícitos, de outro. Trata-se de uma típica aplicação do princípio da proporcionalidade, que exige a verificação da adequação, necessidade e proporcionalidade em sentido estrito da medida. No contexto brasileiro, marcado por altos índices de fraudes bancárias, golpes digitais e uso indevido de identidades falsas, o tratamento de dados biométricos para fins de autenticação representa, muitas vezes, a medida mais segura, eficaz e menos invasiva disponível para proteger os usuários e o sistema financeiro como um todo - contexto que faz com que a base legal de prevenção à fraude seja extremamente relevante.

Vale mencionar que, de acordo com a Serasa, somente em janeiro de 2025, foram registradas 1,24 milhão de tentativas de fraude no Brasil, um aumento de 41,6% em relação ao ano anterior – o equivalente a uma tentativa de golpe a

cada 2,2 segundos. Dados da Serasa Experian mostram que em 2024 as tentativas de fraude contra bancos e cartões cresceram 10,4% em relação a 2023, representando 53,4% de todas as fraudes registradas no ano. Se não tivessem sido evitadas, graças ao uso de mecanismos de autenticação de usuário, essas fraudes poderiam ter causado um prejuízo estimado em R$ 51,6 bilhões.

Sendo assim, a base legal da prevenção à fraude, prevista expressamente no art. 11, II, "g", da LGPD, reflete esse equilíbrio e representa um avanço normativo em comparação ao GDPR europeu, que não contempla essa hipótese de forma específica. A ausência dessa base legal na legislação europeia tem gerado dificuldades práticas, levando empresas a depender de hipóteses frágeis como o consentimento — que, em muitos casos, não se revela uma base jurídica adequada, especialmente quando há desequilíbrio entre controlador e titular ou impossibilidade de negativa real. A própria EDPB (European Data Protection Board) já reconheceu os obstáculos criados por essa lacuna normativa para o uso de biometria em contextos privados de prevenção à fraude.

No Brasil, o reconhecimento legal da prevenção à fraude como hipótese legítima para o tratamento de dados sensíveis deve ser interpretado como uma expressão dos princípios constitucionais da segurança jurídica e da ordem econômica (CF, art. 170), além de compatível com o princípio da necessidade previsto na LGPD. A utilização da biometria, desde que acompanhada de salvaguardas técnicas e organizacionais adequadas — como minimização de dados, medidas de segurança robustas, governança e avaliação de impacto —, é não apenas proporcional, mas socialmente desejável. Além de proteger o titular, a biometria pode atuar como mecanismo de inclusão digital e potencializar o exercício de direitos fundamentais por parte dos titulares, permitindo o acesso seguro a serviços essenciais, por exemplo.

Portanto, diante da realidade nacional e da necessidade de proteção contra ameaças sistêmicas, o tratamento de dados biométricos para fins de prevenção à fraude deve ser reconhecido como legítimo, necessário e proporcional, dentro de uma leitura equilibrada da LGPD que assegure tanto os direitos individuais quanto a segurança das relações sociais e econômicas.

Conforme Guia sobre o Legítimo Interesse da ANPD, os requisitos para o enquadramento do tratamento de dados biométricos na base legal de "prevenção à fraude" são semelhantes aos aplicáveis ao legítimo interesse. Nesse sentido, são aplicáveis os mesmos critérios do Teste de Balanceamento para enquadramento no "legítimo interesse", ressalvada a proibição de tratamento de dados pessoais sensíveis.

Isso não implica dizer que a realização prévia de Teste de Balanceamento ("LIA") seja medida obrigatória para garantir a licitude da atividade, pois inexiste obrigação legal nesse sentido. Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de ausência de atendimento dos requisitos mínimos.

Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de ausência de atendimento dos requisitos mínimos.

No setor de telecomunicações, por exemplo, o uso de dados biométricos é, em regra, legítimo com base no art. 11, II, "g", da LGPD. Essa prática encontra respaldo nas condutas usualmente adotadas pelo mercado e se justifica não apenas pela prevenção a fraudes no acesso aos serviços de telecomunicações, mas também pela necessidade de proteger a segurança de diversos serviços da sociedade da informação acessados por esses canais.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o "cumprimento de obrigação legal ou regulatória" (art. 11, II, "a", LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

No contexto do desenvolvimento e aperfeiçoamento de sistemas de IA, o uso de dados biométricos para o treinamento de modelos voltados à detecção e prevenção de vieses discriminatórios configura medida essencial para a efetividade dos deveres constitucionais e legais de promoção da igualdade. Ao possibilitar que os sistemas reconheçam, mensurem e corrijam distorções decorrentes de recortes raciais, de gênero, idade ou deficiência, o uso técnico e controlado desses dados serve diretamente ao objetivo de evitar tratamentos injustos ou excludentes por parte de sistemas baseados em IA e atendem o interesse público de combate à discrimação.

Tal prática encontra respaldo normativo na Constituição Federal, que consagra o princípio da igualdade (art. 5º, caput) e impõe como objetivo fundamental da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV). Do mesmo modo, diversas normas infraconstitucionais — como o Estatuto da Igualdade Racial (Lei nº 12.288/2010) e o Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015) — impõem obrigações concretas ao poder

público e aos entes privados para adotar medidas que previnam e combatam a discriminação estrutural em diferentes esferas da vida social.

Nesse cenário, o tratamento de dados biométricos com a finalidade de garantir que modelos de IA se comportem de forma ética e não discriminatória deve ser interpretado como um instrumento de cumprimento de obrigação legal ou regulatória, em consonância com os princípios da finalidade, da boa-fé, da responsabilidade e da prestação de contas previstos na LGPD.

No mesmo sentido do item anterior, entende-se que a adequada aplicação da hipótese legal do cumprimento de obrigação legal ou regulatória pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamento de dados sensíveis. Na ótica de segurança, vislumbra-se a implementação de técnicas de proteção, tais quais medidas de rastreamento e monitoramento, controle de acesso, registro das operações de tratamento.

No que tange o princípio da necessidade, observam-se medidas que visem à utilização dos dados biométricos apenas de forma estritamente necessária para o atingimento da finalidade, atentando-se para a disponibilização de informação aos titulares acerca da finalidade do tratamento, de forma clara, precisa e facilmente acessível. Dessa forma, a adequada aplicação da hipótese legal de "cumprimento de obrigação legal ou regulatória" prevista no artigo 11, II, "a" da LGPD, pressupõe a observância dos princípios da necessidade e finalidade e implementando boas práticas de governança e segurança da informação, com o objetivo de prover medidas de controle e rastreabilidade, bem como de proteção dos dados biométricos.

Em relação às salvaguardas a serem adotadas para mitigação de riscos, entendemos que devem ser as mesmas aplicáveis aos agentes de tratamento que utilizam a base legal de "prevenção à fraude". Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento. Assim, os controles e as salvaguardas adequados para mitigar os riscos decorrentes do uso de dados biométricos permanecem os mesmos, seja a base legal "prevenção à fraude", "cumprimento de obrigação legal" ou outra prevista na LGPD.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais

salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Nesse sentido, é importante esclarecer que o dado anonimizado se caracteriza pelo dado que não é capaz de permitir da reidentificação posterior. Corrobora esse entendimento o conceito de dado anonimizado previsto no art. 5º, III da LGPD. Diante desse cenário, em caso de uso de dados anonimizados, medidas técnicas de anonimização, bem como a aplicação de testes de robustez para validar se o dado está efetivamente anonimizado, conforme recomenda a ANPD em Guia de Boas Práticas de Anonimização e Pseudoanonimização, podem ser consideradas como salvaguardas para garantir a eficácia do processo de anonimização do dado. Uma vez garantido o processo de anonimização, referido dado não é considerado como dado pessoal, em conformidade com o art. 12º da LGPD, tendo em vista que não é possível identificar o titular. Consequentemente, portanto, o dado deixa de figurar como dado pessoal.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

É importante reconhecer que, em determinados contextos, como a prevenção à fraude no sistema financeiro ou em serviços digitais, o uso de tecnologias de reconhecimento facial pode ser não apenas legítimo, mas essencial para proteger direitos de usuários e garantir a integridade das operações. Nesses casos, o reconhecimento facial pode ser a única ferramenta viável para evitar fraudes de identidade e acessos indevidos, desde que seu uso seja proporcional à gravidade do risco e cercado de salvaguardas adequadas.

Ainda assim, a proteção contra riscos à privacidade e à dignidade dos titulares permanece central. O princípio da necessidade exige que o uso dessa tecnologia se restrinja ao mínimo indispensável para atingir a finalidade de prevenção à fraude, sem derivações para outras finalidades não autorizadas. Já a proporcionalidade demanda uma avaliação clara de que os benefícios, especialmente em termos de interesse coletivo na segurança, na estabilidade econômica e na prevenção de ilícitos, superam os impactos aos direitos dos titulares. A transparência, por sua vez, impõe o dever de informar de forma clara sobre a coleta, uso e retenção desses dados, garantindo o exercício dos direitos previstos na LGPD.

Em síntese, o reconhecimento facial pode desempenhar um papel legítimo e relevante na prevenção à fraude, desde que seu uso seja cuidadosamente balizado por critérios técnicos, jurídicos e éticos que garantam a proteção dos direitos fundamentais e evitem abusos.

Nos casos em que o reconhecimento facial é oferecido como funcionalidade técnica por software, é imprescindível reconhecer que a conformidade com os princípios da LGPD depende não apenas das capacidades da tecnologia, mas também da forma como o controlador a configurar e utilizar. O operador é

responsável por salvaguardas técnicas, porém não detém ingerência sobre a definição da base legal, da finalidade específica ou da proporcionalidade do uso em contextos concretos.

No que tange ao atingimento do princípio da necessidade e da proporcionalidade, tem-se como alternativa a análise da indispensabilidade do reconhecimento facial. Ou seja, avaliação se o reconhecimento facial é a forma mais adequada e, caso seja, medidas minimizem o uso irrestrito do reconhecimento. Nessa ótica, ressalta-se que, para a finalidade de prevenção à fraude, o reconhecimento facial destaca-se como uma tecnologia de suma importância no contexto de proteção do titular. Ao usar dados biométricos únicos, a tecnologia mitiga consideravelmente a ocorrência de acessos indevidos, falsificações e usos fraudulentos de informações pessoais. O reconhecimento facial, portanto, é um recurso que fortalece mecanismos de autenticação, contribuindo significativamente para a proteção dos dados e integridade das operações.

Na ótica do princípio da transparência, é necessário garantir que o titular tenha ciência do tratamento de reconhecimento facial, disponibilizando informações acerca da finalidade deste reconhecimento. No aspecto técnico, medidas de mitigação de vieses e testes de acurácia utilizando uma base ampla e diversificada contribuem para evitar situações de discriminação ilícita ou abusiva. Na visão jurídica, entende-se como mitigador a correta identificação da base legal amparada pelo atingimento dos princípios acima observados. No que tange à visão institucional, as medidas de monitoramento, controle de acesso e rastreamento do tratamento dos dados, conforme já explicitado, visam contribuir com os riscos mapeados neste item.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas de reconhecimento facial devem ser concebidos e implementados desde sua origem com base no princípio do *privacy by design*, adotando salvaguardas técnicas e organizacionais que garantam alta acurácia e minimizem riscos aos direitos dos titulares. Para garantir eficácia e confiabilidade, é essencial que esses sistemas sejam treinados com bases de dados amplas, diversificadas e representativas da população, a fim de reduzir

vieses e minimizar erros de identificação, como falsos positivos (identificação incorreta) e falsos negativos (falha na identificação de quem deveria ser reconhecido).

O tratamento de dados biométricos que não permitem a identificação de uma pessoa natural — ou seja, que não configuram dados pessoais nos termos da LGPD — é essencial para o treinamento e aprimoramento de sistemas de reconhecimento facial. Esses dados, quando anonimizados ou utilizados de forma a não tornar possível a reidentificação do titular, são indispensáveis para garantir a eficácia, a equidade e a acurácia desses sistemas, especialmente na redução de vieses e na melhoria da performance técnica dos algoritmos. Diante disso, é fundamental que a ANPD reconheça expressamente essa premissa, conferindo segurança jurídica para o desenvolvimento tecnológico responsável e compatível com os princípios da proteção de dados, sem impor restrições desproporcionais ao uso de informações que não configuram dados pessoais.

Os sistemas de reconhecimento facial devem ser projetados com base nos princípios de privacy by design e privacy by default, incorporando, desde a fase de concepção, medidas técnicas e organizacionais voltadas à precisão, segurança e mitigação de riscos. A utilização de algoritmos robustos e continuamente testados em bases de dados diversificadas é essencial para reduzir a incidência de erros de identificação, como falsos positivos e falsos negativos, especialmente considerando a variabilidade de características demográficas. Adicionalmente, destaca-se a implementação de mecanismos de monitoramento contínuo do desempenho do sistema e rotinas de atualização e revalidação dos modelos utilizados.

No contexto de empresas que atuam como operadoras, é importante destacar que diversos aspectos relacionados à forma de coleta, parametrização e uso dos dados podem ser definidos ou ajustados pelos controladores, de acordo com o ambiente e a finalidade do tratamento. Dessa forma, cabe ao controlador assegurar que tais ajustes estejam alinhados aos princípios da LGPD, considerando os riscos da operação.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O reconhecimento facial não será mecanismo apropriado quando existirem meios adequados e proporcionais para se alcançar o mesmo resultado sem uso dessa tecnologia, especialmente se houver forma de tratamento menos intrusiva e capaz de atender à finalidade pretendida, inclusive outras formas de autenticação biométrica. Em outras palavras, o reconhecimento facial deve ser evitado sempre que métodos alternativos possam garantir nível de identificação equivalente, ou minimamente suficiente diante dos riscos envolvidos.

Por exemplo, podemos citar algumas soluções alternativas para auxiliar na verificação da identidade do titular:

- Soluções de prevenção a fraudes baseadas em dados para verificar se o número de telefone e outras informações de contato coincidem com as informações apresentadas pelo titular no momento de registro junto à empresa, confirmar se a localização de uma transação corresponde à localização do dispositivo do titular e identificar indícios de práticas fraudulentas, como o SIM Swap.
- Utilização de tecnologias de captação e transmissão de voz para desenvolver formas de verificação da identidade baseadas em validação biométrica da voz – as quais podem ser consideradas menos intrusivas do que a biometria facial, vez que tende a permitir a inferência de menos dados pessoais sensíveis (como dados de saúde ou etnia) do que a biometria facial.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras

sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos. Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes. Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados. Com base nisso, questiona-se:
11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante do alto potencial lesivo decorrente de eventuais violações de dados biométricos, como o roubo de identidade, é indispensável a adoção de medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem atuado proativamente nesse sentido, incorporando mecanismos avançados de segurança da informação — como criptografia, segmentação de bases, anonimização, controle de acesso e rastreabilidade — desde as fases iniciais do desenvolvimento de produtos e sistemas. Além disso, muitas empresas já implementam práticas sofisticadas de privacy by design e by default, realizando o tratamento de dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem que haja identificação ou reidentificação de uma pessoa natural, o que reduz significativamente os riscos à privacidade.

Para garantir a conformidade com a LGPD, é essencial que as organizações adotem parâmetros mínimos de avaliação contínua de riscos, por meio de relatórios de impacto à proteção de dados (RIPDs) e monitoramento de possíveis vieses ou falhas de segurança. A definição de políticas internas claras, a capacitação de equipes e a governança ativa sobre o ciclo de vida dos dados também são medidas fundamentais para assegurar o tratamento responsável e proporcional desses dados sensíveis. Esse conjunto de ações, já amplamente adotado por empresas do setor, demonstra que é possível conjugar inovação tecnológica com proteção integral dos titulares de dados. Alguns parâmetros básicos são:

a) Definir critério de riscos: estabelecer, com base no apetite de risco organizacional, as regras e os parâmetros para aceitação de riscos;

b) Identificar os Riscos: contemplando identificar os(as): i) ativos envolvidos; ii) ameaças potenciais a esses ativos; iii) controles existentes; e iv) vulnerabilidades.

c) Analisar os riscos: identificar os potenciais consequências decorrentes da concretização dos riscos e a probabilidade de sua ocorrência, definindo, por meio de ambos os elementos, o nível do risco.

d) Tomar decisão: avaliar, de acordo com o critério de riscos, se ele é aceitável e tomar uma decisão – isto é, modificar (mitigar), reter (aceitar), compartilhar ou evitar (elimina) o risco.

e) Monitoramento: é necessário que os elementos que compuseram a identificação do risco sejam monitorados, para que, em caso de sua

modificação (por exemplo, o surgimento de nova ameaça) os efeitos desta alteração sejam computados na análise do risco.

É de suma importâncias que os controladores do tratamento dos dados biométricos adotem medidas técnicas e administrativas robustas, entre as quais destacam-se:

- Programa de Segurança da Informação: implementação de medidas de segurança contra qualquer ameaça ao Tratamento dos dados Pessoais;
- Gestão de Acesso: estabelecimento de padrões de controle sobre o Tratamento dos Dados Pessoais com responsabilidades definidas e gestão de acesso tanto de colaboradores quanto de prestadores de serviços, bem como o estabelecimento de mecanismos de autenticação de acesso aos Dados Pessoais;
- Relatório de Tratamento dos Dados Pessoais: manter o registro detalhado de todo o tratamento realizado, como informações quanto ao momento, a duração, a identidade do representante responsável pelo tratamento designado pelas partes e os dados pessoais tratados, inclusive quando tal tratamento é feito para cumprimento de obrigações legais ou determinações por parte de autoridades; e,
- Inviolabilidade dos Dados Pessoais: uso de soluções de gestão dos registros do Tratamento por meio de técnicas que garantam a inviolabilidade dos dados pessoais, como encriptação ou medidas de proteção equivalentes.
- Elaboração de Relatório de impacto DPIA/LIA, quando aplicável.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Para evitar que a exigência de autenticação biométrica em serviços não essenciais configure discriminação ilícita ou prática abusiva, é fundamental que o tratamento desses dados observe os princípios da LGPD bem como esteja devidamente enquadramento em uma das bases legais autorizativas para o tratamento, em especial, da necessidade, não discriminação e transparência, como todo e qualquer tratamento de dados deve observar.

Na situação em que o tratamento do dado biométrico é amparado no consentimento, o titular deve ter garantido o direito ao opt-out, de forma simples, acessível e sem que isso implique em restrições desproporcionais do serviço. A limitação de funcionalidades pode ser considerada legítima, entretanto, quando houver justificativa técnica concreta para sua implementação. Nessa ocasião, tal limitação deve ser previamente comunicada de forma clara e transparente.

Entendemos que a recusa em fornecer a biometria implicaria em exercício de fato do direito de oposição. Consequentemente, o não oferecimento da funcionalidade, serviço ou produto resguardado pelo acesso biométrico será lícito se uma das seguintes condições for satisfeita: (a) não seja faticamente possível ofertar a funcionalidade sem o tratamento de dados biométricos, aplicando-se aqui o mesmo descrito quanto ao consentimento; ou (b) os direitos e interesses protegidos ao se exigir a biometria não sejam sobrepujados pelo direito do titular de não a ofertar – isto é, existe razão pela qual a validação biométrica é necessária, como a existência de bem protegido relevante – é o caso típico dos serviços de telecomunicação, cuja fraude, nos termos já vistos, são comumente meio para condutas criminosas significativamente mais lesivas, para o titular afetado ou para a sociedade globalmente considerada – seja obtendo indevidamente a linha do titular para obter acesso a outros bens e serviços vinculados a ela, inclusive serviços bancários, seja se utilizando da linha fraudulentamente obtida para a práticas de crimes, incluindo fraudes movidas a engenharia social.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

A proteção eficaz no tratamento de dados biométricos exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destacam-se:

- Treinamento e Capacitação: oferecer treinamento específico quanto ao tema;
- Políticas e Procedimentos: reforçar as informações de forma detalhada sobre como deve ser realizado o tratamento de dados para essa categoria de dados;
- Relatório de Impacto à Proteção de Dados Pessoais (DPIA), quando aplicável.

Em relação às medidas de transparência, a obrigatoriedade legal se refere ao fornecimento das informações previstas no art. 9º, da LGPD. A forma adequada de disponibilização dessas informações, conforme indicado nos questionamentos nºs 2 e 8, com base no posicionamento do ICO, dependerá de uma série de fatores – como o caso de uso, a natureza do relacionamento com o titular e os elementos envolvidos na atividade de tratamento. Em síntese, quanto mais evidente for a atividade de tratamento analisada – considerando, inclusive, as práticas habituais de mercado e obrigações regulatórias –, menor será a exigência de adoção de práticas ativas de transparência para o fornecimento das informações legalmente requeridas ao titular. A título exemplificativo, dadas as obrigações regulatórias que atingem o setor de telecomunicações, as práticas habituais de mercado e os riscos já abordados relacionados a ocorrência de fraudes no setor e a própria divulgação do uso de biometria facial no setor pela própria ANATEL, entendemos que a disponibilização do Aviso de Privacidade é suficiente para atender às obrigações regulatórias em proteção de dados.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

-

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não

possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento, especialmente no setor de tecnologia, têm avançado significativamente na implementação de práticas que asseguram o respeito aos direitos dos titulares, inclusive em contextos complexos como o tratamento automatizado de dados biométricos. Empresas de tecnologia vêm adotando medidas técnicas e organizacionais que facilitam o exercício dos direitos previstos na LGPD — como o direito à informação clara, ao acesso, à correção de dados e à revogação do consentimento — por meio de interfaces amigáveis, políticas de privacidade mais acessíveis e canais digitais eficientes de atendimento ao titular.

Além disso, o setor tem investido em soluções inovadoras para promover maior transparência, como painéis de controle de dados, logs de acesso e funcionalidades que permitem ao titular visualizar, corrigir ou apagar dados de forma autônoma. No caso específico da biometria, diversas empresas já incorporam salvaguardas como o design voltado à privacidade (privacy by design), o uso de dados pseudonimizados para treinamento de sistemas e a oferta de mecanismos para revisão humana de decisões automatizadas, quando necessário. Esses esforços demonstram um compromisso com o uso ético e seguro de tecnologias avançadas, promovendo a proteção dos dados pessoais sem comprometer a funcionalidade e a inovação.

Cumpre destacar que o direito à informação clara, o direito de acesso e à correção dos dados são direitos dos titulares que pressupõem todo e qualquer tratamento, independentemente de o referido tratamento estar ou não inserido no contexto de uma decisão tomada exclusivamente em tratamento automatizado de dados pessoais. Nesse sentido, medidas de transparência, tais quais previsões claras e precisas em políticas de privacidade e divulgação de canais de atendimento são imprescindíveis para que o titular possa exercer seus direitos.

Em relação ao direito de acesso, conforme o ICO, há dificuldade técnica em fornecer os dados biométricos propriamente ditos, uma vez que, em geral, são outputs matemáticos complexos, não compreensíveis ("ilegíveis") por seres humanos. Diante disso, o fornecimento pode ser substituído por uma declaração explicativa, que: (a) justifique a impossibilidade de entrega direta do dado; (b) descreva a natureza do dado em questão; e (c) esclareça como esse dado é mantido pela organização

No que diz respeito à possibilidade de revogação, nos casos em que a base legal para o tratamento dos dados for o consentimento, o titular deve dispor de um canal de fácil acesso, viabilizando a revogação de forma simples, acessível e facilitada. Por sua vez, conforme disposto na LGPD, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

Dessa forma, enquanto requisito para a garantia e a aplicação do referido direito, é certo que a leitura do dispositivo deve considerar que a revisão ocorra apenas nos casos em que a decisão foi tomada unicamente de forma automatizada, bem como que os interesses dos titulares tenham sido afetados de forma ilícita ou abusiva e contrária à legislação. Nesse sentido, importante destacar que a leitura e interpretação de referente direito do titular deve observar os requisitos dispostos no artigo 20 da LGPD, quais sejam: (i) decisão tomada unicamente com base em tratamento automatizado de dados pessoais; e (ii) decisão que afete os interesses do titular. Com efeito, esses requisitos devem ser observados em qualquer decisão automatizada, seja ela referente ao tratamento de dados biométricos ou qualquer outro tipo de dado. Com efeito, cumpre destacar que, no que tange ao conceito de decisão tomada unicamente com base em tratamento automatizado de dados pessoais, considera-se um processo de tomada de decisão que é totalmente automatizado e exclui qualquer influência humana no resultado. Um processo ainda pode ser considerado totalmente automatizado se um humano insere os dados a serem tratados e, então, a tomada de decisão é realizada por um sistema automatizado.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?
O princípio do melhor interesse, previsto no art. 14 da LGPD, deve ser interpretado de forma concreta, contextualizada e não apriorística. Essa abordagem está em consonância com o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que destaca o caráter flexível, relacional e multidimensional do conceito, exigindo sua ponderação em conjunto com outros direitos fundamentais. Reconhece-se, ainda, a condição peculiar da criança e do adolescente como pessoas em desenvolvimento, conforme o Estatuto da Criança e do Adolescente (ECA). Nesse sentido, recomenda-se que a ANPD assegure margem de autonomia aos controladores para que possam demonstrar, caso a caso, como o tratamento atende ao melhor interesse, inclusive com a possibilidade de adotar ajustes e salvaguardas adicionais. A base legal para o tratamento de dados biométricos, ainda que envolva crianças e adolescentes como titulares dos dados, decorre do art. 11 da LGPD. Neste contexto, a própria ANPD, por meio do Enunciado nº 1/2023, acertadamente esclareceu que "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7o ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei". Assim, o consentimento, quando adotado como base legal, deve ser inequívoco e refletir claramente as finalidades do tratamento, sendo essencial a transparência com os representantes legais. Por outro lado, o tratamento também pode ser realizado com base em outras hipóteses legais, desde que haja legítima finalidade, proporcionalidade e salvaguardas adequadas. É importante destacar que o cumprimento do princípio da necessidade não se limita à mera minimização da coleta de dados, mas sim à utilização de dados estritamente necessários para finalidades legítimas, em conformidade com os princípios da LGPD e com o melhor interesse de crianças e adolescentes. Neste contexto, a relação entre proteção dos dados e segurança deve ser avaliada no caso concreto. Casos internacionais ajudam a ilustrar a complexidade dessa ponderação. O uso de dados biométricos por escolas europeias, por exemplo, foi inicialmente considerado incompatível com o GDPR por algumas

autoridades de proteção de dados. A autoridade polonesa (UODO) entendeu que o uso de leitores biométricos para acesso ao refeitório escolar era desproporcional, mesmo com consentimento dos pais, pois existiam meios menos intrusivos para alcançar o mesmo fim. Contudo, o Tribunal Administrativo Provincial de Varsóvia reformou a decisão e considerou que, desde que o tratamento estivesse vinculado a uma finalidade legítima e houvesse consentimento válido, ele seria admissível. O caso evidencia que a compatibilidade entre o tratamento de dados biométricos e os princípios legais depende de uma análise contextual, proporcional e ancorada no melhor interesse do menor.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

A hipótese de Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, "g", LGPD"). Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento, especialmente considerando as disposições do Enunciado nº 1/2023 da ANPD. Nesse cenário, é imprescindível que haja a devida transparência do tratamento e suas finalidades para os representantes do menor.

Sobre as medidas técnicas e organizacionais, destacam-se as medidas de segurança relevantes para todo e qualquer tratamento de dados, independentemente de o titular figurar como criança ou adolescentes, quais sejam: implementação de programas de Segurança da Informação, medidas de controle e gestão de acesso e, quando aplicável, elaboração de Relatório de Tratamento dos Dados Pessoais (DPIA).

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Para compatibilizar a prática de verificação de idade com o princípio da necessidade, é essencial que a coleta de dados biométricos seja limitada ao

mínimo necessário para atingir a finalidade pretendida, evitando excessos, tratamentos desproporcionais ou tratamentos a posteriori para outras finalidades. A biometria, por ser um dado sensível, deve ser utilizada apenas quando não houver outra forma menos invasiva de verificar a idade do usuário. Além disso, é fundamental garantir a transparência do processo, com informações claras e acessíveis aos pais ou responsáveis, incluindo a finalidade da coleta, os direitos dos titulares e os mecanismos disponíveis para exercer esses direitos.

O tratamento de dados biométricos para casos de verificação ou estimação de idade de crianças e adolescentes deve priorizar a proteção do menor, evitar riscos à sua dignidade, liberdade e segurança, de forma a se garantir o melhor interesse do menor.