Curitiba/PR, 31 de julho de 2025

À Autoridade Nacional de Proteção de Dados (ANPD)
Setor de Coordenação-Geral de Normatização

Prezados senhores,

Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos direitos fundamentais de privacidade e de proteção de dados, o INPD vem, respeitosamente, em complemento às respostas à Tomada de Subsídios: Dados Pessoais Sensíveis – Dados Biométricos, realizada nesta data através do Portal Participa + Brasil, por intermédio do Login de sua Diretora Jurídica, Izabela Lehn, apresentar os seguintes estudos complementares:

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

De acordo com Jain et al. (2024) dado biométrico é aquele que se qualifica como qualquer característica fisiológica e/ou comportamental humana, desde que satisfaça os seguintes requisitos: **a) Universalidade:** cada pessoa deve apresenta tal característica (face, voz, impressão digital, DNA, entre outras); **b) Distintividade:** quaisquer duas pessoas devem ser suficientemente diferentes em termos da característica analisada; **c) Permanência**: a característica deve ser suficientemente invariável (em relação ao critério de correspondência) ao longo de um período de tempo; **d) Capturável ou Coletável ou Colecionável**: a característica pode ser medida quantitativamente. Deve-se considerar que os dados biométricos valem tanto para indivíduos vivos como mortos, considerando-se as variações e perdas existentes.

Há que se considerar que a biometria – ramo da identificação humana, de modo que a palavra possui origem grega, associando "bios" (vida) com "metron" (medida) - surgiu como área do conhecimento a partir de aplicações de cunho jurídico-legal: investigação criminal de suspeitos – impressão digital; determinação de paternidade – DNA; controle de aeroportos e

fronteiras – chegada e partida de pessoas – face, impressão digital; autorização de segurança para colaboradores da administração pública em atividades periculosas ou de caráter sigiloso – face, íris, impressão digital; sistemas de votação eletrônica (e-voting) – impressão digital; policiamento preditivo e identificação positiva de condenados e prisioneiros – face, impressão digital; perícia forense – escrita, voz, face, impressão digital, padrões de digitação, localização de pessoas desaparecidas – face; uso de aplicativos a exemplo do GOV.br – face; controle e vigilância de pessoas em áreas públicas –face; entre outros). Porém, vem se desenvolvendo e sendo aplicada em muitas aplicações civis: autorização de acesso em edifícios comerciais – face; sistemas de votação eletrônica em cooperativas (e-voting) – face, impressão digital; operações bancárias e financeiras – face; uso de dispositivos móveis – smartphones – face; hospitais e centros de saúde – face; controle de pessoas em áreas privadas, shopping centers, condomínios – face; entre outros.

Sendo assim, entende-se por biometria o reconhecimento automatizado de seres humanos com base nas suas características biológicas, como impressões digitais, formato do rosto, voz e íris ou comportamento, tais como jeito de andar ou falar (LI; JAIN, 2015. Corroborando com esse entendimento, o Radar Tecnológico da ANPD (número 2 de junho de 2024), a biometria é um campo de estudo que se baseia em métodos matemáticos e estatísticos para analisar e identificar indivíduos por meio de suas características fisiológicas e comportamentais. Entre as características fisiológicas mais comuns estão a impressão digital, a face, a íris, a geometria e vascularização da mão, o DNA e a voz. Já as características comportamentais incluem padrões únicos de voz, expressão facial, assinatura, modo de andar, entre outros. De acordo com a Lei Geral de Proteção de Dados (LGPD), os dados biométricos são classificados como dados pessoais sensíveis, pois estão diretamente vinculados à identidade única de cada indivíduo. A LGPD define dados sensíveis como aqueles que, se tratados de forma inadequada, podem representar riscos significativos à privacidade e aos direitos dos titulares. Por sua singularidade e potencial de identificação e personalização, os dados biométricos requerem um nível elevado de proteção, garantindo que seu uso seja seguro e alinhado às normas de privacidade e segurança da informação.

Utilizando como fonte o direito europeu, segundo o RGPD e o posicionamento das agências reguladoras, incluindo o European Data Protection Board (EDPB), destaca-se os seguintes critérios objetivos, para caracterização de um dado biométrico:

Origem do dado: O dado deve derivar de características físicas, fisiológicas ou comportamentais únicas do indivíduo, como impressões digitais,

reconhecimento de voz, facial, íris, geometria da mão, padrões de retina, assinatura, entre outros.

Tratamento específico: A informação para ser considerada biométrica está condicionada a derivar de um processo técnico específico que necessite de aplicação de tecnologia para extrair, registrar, analisar ou comparar essas características com o objetivo de identificação ou autenticação.

Potencial de identificação única: O dado biométrico deve permitir ou confirmar a identificação única de uma pessoa natural. Significa dizer que não basta que a característica seja física ou comportamental, ele precisar ser apta a identificar, de forma individual e inequívoca, o titular de dados.

Finalidade de identificação ou autenticação: O tratamento deve ter como finalidade a identificação ou autenticação do indivíduo, seja para controle de acesso, assiduidade, segurança, entre outros usos legítimos previstos em lei ou mediante consentimento explícito.

"A mera fotografia ou vídeo não os caracteriza como dados biométricos à luz do GDPR, a menos que sejam submetidos a tratamento específico para identificação única."

JAIN, A.; ROSS, A.; PRABHAKAR, S.. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, n. 1, p. 4 – 20, February, 2024. DOI: 10.1109/TCSVT.2003.818349.

Nota Técnica no. 17/2025/CON1/CGN/ANPD - Processo no. 00261.001953/2025-81

Andt.or.br, Calio. Pereira de Oliveira Neto, Reflexões Iniciais quanto ao Uso da Biometria nas relações de Trabalho: Do Paradigma Português às Projeções no Brasil

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?

A transparência ativa no tratamento de dados biométricos, classificados como dados pessoais sensíveis pela LGPD (Lei nº 13.709/2018, art. 5º, II), é essencial para garantir que os titulares compreendam, de forma clara e acessível, como seus dados serão utilizados antes mesmo de fornecê-los.

Quadro Resumo: Boas Práticas em Conformidade com o GDPR e LGPD

Boas Práticas	Referências Legais
Política de Privacidade clara e específica	GDPR: arts. 12, 14 e 5 LGPD: arts. 6(VI), 9 e 41
Avisos no momento da coleta ou previamente	GDPR: arts. 13 e 14 LGPD: arts. 6(VI), 9, 18 e 41
Canal de atendimento ao titular	GDPR: arts. 15-22 LGPD: arts. 18 e 41
Registro de finalidades e bases legais	GDPR: arts. 5, 6 e 9 LGPD: arts. 6(I, II), 7, 11 e 37
Informação sobre compartilhamento e armazenamento	GDPR: arts. 13(1)(e) e 14(1)(e) LGPD: arts. 6(VI) e 48
Materiais educativos e linguagem acessível	GDPR: art. 12 LGPD: arts. 6(VI), 9 e 41

Nesse sentido:

A. Política de privacidade clara e acessível

A política deve conter linguagem simples, objetiva e estar disponível em canais acessíveis (sites, aplicativos, pontos de coleta). Deve informar: Finalidade do uso da biometria; Base legal utilizada, Período de retenção dos dados; Compartilhamento com terceiros; Direitos dos titulares. Gomes (2025) preconiza que a clareza da política de privacidade é um dos pilares da conformidade com a LGPD no uso de biometria.

B. Avisos de privacidade no ponto de coleta

Antes da coleta, o titular deve ser informado por meio de avisos visuais ou sonoros, com destaque para:

Que tipo de dado biométrico será coletado.

Se o consentimento é necessário ou se há outra base legal.

Como exercer seus direitos.

C. Consentimento informado (quando aplicável)

Nos casos em que o tratamento se baseia no consentimento (art. 11, I), este deve ser:

Livre, informado e inequívoco.

Destacado dos demais termos.

Registrado e documentado.

D. Canal de atendimento ao titular

Deve haver um canal funcional para que o titular possa:

Solicitar informações adicionais.

Revogar consentimento, quando esta for a base legal.

Exercer seus direitos (acesso, correção, exclusão etc.).

E. Relatórios de impacto e transparência institucional

A publicação de relatórios de impacto à proteção de dados (DPIA) e de boletins de transparência pode reforçar a confiança dos titulares e demonstrar accountability.

Fonte: Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo - Versão 2.0 EDPB Adotado em 29 de janeiro de 2020.

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?

Ao que se refere à biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) em comparação à biometria tradicional (digital, íris, face), primeiramente é importante compreender as diferenças fundamentais no tratamento de dados biométricos convencionais, de natureza fisiológica, e os de natureza comportamental. A natureza dos dados pessoais do primeiro grupo são constituídos pelo rosto, impressão digital, íris, voz, etc...Já, os dados comportamentais se relacionam com dados

dinâmicos, tais como a maneira como o indivíduo segura um objeto, incluindo o ângulo, o uso da mão e a inclinação do mesmo, o ritmo, a velocidade e a pressão das teclas durante a digitação, dinâmica, pressão e andamento gráfico em assinatura ou escrita humana, maneira de caminhar, incluindo o ritmo, a velocidade e o padrão dos passos, entre outros. Em termos de coleta de dados, os métodos e técnicas se diferenciam principalmente pelo fato de que os dados do primeiro grupo, são estáticos, e no Segundo grupo, podem ser estáticos ou dinâmicos, configurando dados (variáveis) discretos ou contínuos. O European Data Protection Bord (EDPB) recomenda medidas específicas para a biometria comportamental, tais como: i) minimização de dados; ii) anonimização; e, iii) controle do titular por meio do direito à explicação sobre algoritmos da análise comportamental. A Autoridade Bancária Europeia (EBA) orienta que para setores financeiros, a biometria comportamental deve ser complementar e não substitutiva aos métodos tradicionais.

A biometria comportamental, como padrões de digitação, reconhecimento de voz, movimento ocular ou dinâmica de uso de dispositivos, deve ser tratada com o mesmo grau de cautela que a biometria tradicional (impressão digital, íris, face). Porém, deve-se ter especial atenção às suas características específicas de variabilidade, contexto e inferência indireta. Riscos adicionais como o de profiling e vigilância constante podem trazer impactos graves à liberdade individual e riscos de decisões automatizadas injustas. Existem diferenças fundamentais entre biometria comportamental e a biometria tradicional, são elas:

A biometria comportamental pode gerar inferências que extrapolam a simples identificação, o que exige maior rigor na aplicação dos princípios da LGPD.

A biometria comportamental pressupõe o uso de camadas adicionais de proteção, dado seu potencial de vigilância contínua e inferência indireta de aspectos íntimos da personalidade. Em se tratando desse tipo de biometria boas práticas devem ser adotadas:

Consentimento reforçado: Quando aplicável, deve ser informado, granular e destacando a natureza contínua da coleta.

Limitação temporal e contextual: Evitar coleta permanente ou fora do contexto da finalidade.

Minimização e anonimização: Sempre que possível, utilizar dados agregados ou pseudonimizados.

Auditorias algorítmicas: Avaliar se há inferências indevidas ou discriminação algorítmica.

Transparência ativa: Informar claramente que o comportamento está sendo monitorado e para quê.

Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Sim, o uso de tecnologias biométricas, especialmente as mais recentes (biometria comportamental) impõe obrigações específicas aos controladores, com foco especial nos princípios da qualidade dos dados e da segurança, conforme previstos na Lei Geral de Proteção de Dados Pessoais (LGPD). Nesse sentido, as obrigações relacionadas à qualidade dos dados, exige que as informações sejam:

- Exatas, atualizadas e relevantes para a finalidade do tratamento.
- Coletadas de forma não excessiva e com base legal clara.
- Verificadas periodicamente, especialmente em sistemas automatizados que podem gerar falsos positivos.
- A qualidade dos dados é essencial para evitar decisões automatizadas injustas, especialmente em contextos como segurança pública ou crédito.

Quanto as obrigações relacionadas à segurança:

O controlador deve adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, vazamentos, destruição ou perda acidental. No caso da biometria, isso inclui:

- Criptografia e pseudonimização dos dados biométricos.
- Controle de acesso rigoroso aos sistemas que armazenam ou processam esses dados.
- Auditorias periódicas e testes de vulnerabilidade.
- Plano de resposta a incidentes, com notificação à ANPD e aos titulares (Art. 48).
- A segurança deve ser "proporcional ao risco", o que significa que dados sensíveis como biometria exigem nível máximo de proteção.
- Avaliação de Impacto à Proteção de Dados (DPIA): obrigatória em casos de alto risco.
- Minimização de dados: coleta apenas do necessário para a finalidade específica.
- Treinamento contínuo de equipes: para evitar falhas humanas na manipulação de dados sensíveis.
- Auditoria de algoritmos: especialmente em sistemas de reconhecimento facial ou comportamental, para evitar vieses e discriminação.

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?

Segundo as instruções da Norma ISO/IEC 24745, devem ser observados os seguintes critérios técnicos e organizacionais para a adequada utilização da hipótese legal de prevenção à fraude, se não vejamos:

Justificativa da necessidade: A coleta biométrica só se justifica se a fraude representar um risco relevante à operação ou ao titular de dados e não houver meios menos intrusivos;

Avaliação de Impacto (RIPD): A ISO recomenda a realização de uma avaliação de riscos e impactos à privacidade para fundamentar o uso dos dados biométricos. Essa avaliação deve mapear os riscos de exposição ou uso indevido dos dados e identificar medidas técnicas para mitigação de riscos, como uso de templates não reversíveis e criptografia;

Mínima interferência: A ISO recomenda que seja coletado apenas o necessário, de acordo com a finalidade de prevenção à fraude, de acordo com princípio da necessidade (art. 6, III, da LGPD) e exige selecionar tecnologias biométricas com menor impacto, evitar armazenamento centralizado de dados.

Modelos de aplicação adequados: A norma apresenta modelos de aplicação biométrica (seção 8.2), entre os quais alguns oferecem maior segurança e menor risco à privacidade. São eles: **i)** Modelo local ou descentralizado, onde o armazenamento é realizado no cliente e é comparado com o cliente, minimizando o compartilhamento. Alguns exemplos: A impressão digital ou reconhecimento facial em iPhones (Face ID/Touch ID) e Androids e dispositivos de controle de acesso off-line, como fechaduras eletrônicas com leitor biométrico integrado, onde a digital do usuário é armazenada na memória local da fechadura. Nessa modalidade a comparação ocorre localmente, sem o envio de dados biométricos para a nuvem; e, **ii)** Modelo com uso de tokens com armazenamento distribuído, onde as informações biométricas são armazenadas e/ou processadas de forma dividida entre dois ou mais locais. Alguns exemplos desta modalidade são: a) a autenticação multifator em ambientes corporativos em que, a título

ilustrativo, um Smartcard armazena parte dos dados biométricos, enquanto um sistema local ou nuvem realiza a verificação final com base em dados complementares(token + endpoint + backend corporativo); b) soluções de acesso físico a locais de segurança crítica, como data centers, onde o token do usuário (cartão ou pendrive) contém uma parte criptografada da biometria, e a verificação só ocorre quando combinada com a parte armazenada localmente no servidor da sala restrita; e, **iii)** controle de passaporte eletrônico (ePassport), onde a imagem do titular é armazenada no chip RFID do passaporte e o processo de verificação pode ocorrer no servidor da autoridade migratória, comparando com a leitura local da câmara (token + servidor de imigração).

A escolha do modelo deve considerar a compatibilidade com o grau de risco da fraude a ser evitada e com a técnica da organização de proteger os dados.

Portanto, a aplicação da hipótese legal de "garantia da prevenção à fraude e à segurança do titular" (art. 11, II, "g", da LGPD) para o tratamento de dados biométricos exige critérios rigorosos, dada a natureza sensível desses dados e os riscos associados ao seu uso indevido. São critérios para aplicação legítima da hipótese de prevenção à fraude:

Finalidade legítima, específica e proporcional: O tratamento deve estar diretamente vinculado à prevenção de fraudes, como autenticação de identidade em transações financeiras ou acesso a sistemas sensíveis. A coleta de dados biométricos não pode ser genérica ou preventiva sem justificativa concreta.

A finalidade deve ser "específica, explícita e legítima", evitando usos genéricos que ampliem indevidamente o escopo do tratamento.

Demonstração de necessidade: A biometria deve ser estritamente necessária para atingir a finalidade de prevenção à fraude. Se houver meios menos invasivos (como senhas ou tokens), estes devem ser priorizados.

A "necessidade" deve ser avaliada com base em uma análise de proporcionalidade e minimização de dados.

Avaliação de impacto à proteção de dados (DPIA): É recomendável (e em muitos casos essencial) realizar uma DPIA para documentar os riscos e as medidas de mitigação adotadas.

Transparência e informação ao titular: Mesmo sem consentimento, o titular deve ser informado de forma clara sobre: a finalidade do uso da biometria; a base legal utilizada, bem como o acesso, a correção, a oposição etc.).

Segurança técnica e organizacional: A biometria exige medidas de segurança reforçadas, como criptografia, controle de acesso e anonimização.

Proibição de discriminação: O uso da biometria não pode resultar em tratamento discriminatório ou abusivo, especialmente contra grupos vulneráveis. Isso exige auditoria de algoritmos e revisão de vieses.

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?

A compatibilização entre o princípio da necessidade e o uso de dados biométricos para segurança da informação e acesso a serviços bancários exige uma abordagem baseada em proporcionalidade, minimização e justificativa técnica robusta.

Para tanto é se faz necessário: Justificativa técnica e funcional clara; Implementação com medidas de segurança reforçadas; Avaliação de Impacto à Proteção de Dados (DPIA); Transparência e opção ao titular.

A Justificativa técnica e funcional clara: o uso da biometria deve ser estritamente necessário para atingir a finalidade de segurança — como autenticação em transações de alto risco ou acesso a contas digitais. A adoção deve ser precedida de análise técnica comparativa, demonstrando que meios alternativos (como senhas ou tokens) não oferecem o mesmo nível de proteção. A biometria pode ser proporcional quando usada para mitigar riscos concretos de fraude, desde que sua adoção seja precedida de análise técnica e jurídica adequada.

A Implementação com medidas de segurança reforçadas: a biometria, por ser dado sensível, exige criptografia, controle de acesso, segregação de ambientes e anonimização sempre que possível. Isso reduz o impacto em caso de vazamento e reforça a legitimidade do tratamento.

A segurança técnica: é um dos pilares para justificar o uso de biometria em ambientes financeiros, especialmente diante do alto valor dos dados envolvidos Avaliação de Impacto à Proteção de Dados (DPIA). A realização de uma DPIA é essencial para demonstrar que o uso da biometria é necessário, proporcional e que os riscos foram mitigados. Isso também reforça a accountability do controlador.

Transparência e opção ao titular: mesmo quando o consentimento não é exigido (ex: prevenção à fraude), o titular deve ser informado de forma clara sobre: a base legal utilizada; a finalidade específica; seus direitos e formas de exercê-los.

Sempre que possível, deve-se oferecer alternativas menos invasivas para autenticação, respeitando a autodeterminação informativa.

Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados. Danilo Doneda. ISBN: 9786559917969. 2021.

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?

A construção de sistemas eficazes exige:

Bases de dados com diversidade, significância estatística e representatividade populacional;

Avaliações de impacto algorítmico para prever e mitigar riscos;

Mecanismos de avaliação de conformidade são altamente recomendados.

Inobstante a relevância do Sistema de biometria para fins de autenticação do indivíduo, há que se reconhecer que apresentam riscos técnicos, sociais e jurídicos. Entre os principais:

Violação da privacidade e exposição indevida de dados sensíveis;

Discriminação algorítmica, especialmente em razão de raça, idade e gênero;

Falsos positivos e falsos negativos, comprometendo a confiabilidade.

Falta de transparência e explicabilidade algorítmica (Cebrian; Freitas, 2023);

Vigilância massiva e borramento entre espaços públicos e privados (Freitas; Rossi, 2020).

Esses riscos decorrem da complexidade dos modelos de IA e da qualidade dos dados utilizados. Portanto, recomenda-se:

Auditorias frequentes e independentes dos algoritmos.

Implementação de mecanismos de correção tempestiva de erros.

Governança algorítmica baseada em princípios éticos, sociais e técnicos.

Garantia do direito à revisão por humano em decisões automatizadas.

Consoante destaca Freitas (2025), o Direito tradicional, baseado em "coisas físicas", deve se adaptar à era das "não-coisas", exigindo novas estruturas

para lidar com tecnologias como a IA e seus impactos na privacidade, responsabilidade civil e justiça social.

Importante: fotos ou vídeos não são, por si sós, dados biométricos, a menos que tratados para realizar identificação pessoal automatizada.

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 risco representado por uma eventual violação de dados biométricos — como o roubo de identidade, que pode ter consequências graves torna-se imprescindível que organizações adotem medidas técnicas e administrativas robustas, em consonância com os princípios da LGPD e com normas internacionais de boas práticas, como a ISO/IEC 24745:2011.

1. Medidas Técnicas e Administrativas Indispensáveis

Com base na ISO/IEC 24745 e na LGPD, destacam-se os seguintes pilares de segurança e privacidade:

a) Segurança da Informação (art. 46 da LGPD)

Confidencialidade: proteção contra acessos não autorizados aos dados biométricos.

Integridade: garantia de que os dados não serão alterados ou corrompidos de forma indevida.

Disponibilidade: os dados devem estar acessíveis apenas quando necessário e por pessoal autorizado.

Cancelamento e renovação: os dados biométricos devem ser revogáveis ou substituíveis sempre que necessário.

b) Proteção da Privacidade

Irreversibilidade: os templates biométricos devem ser protegidos contra a reconstrução da imagem original.

Desvinculação (unlinkability): impossibilidade de rastrear ou vincular registros biométricos entre bases distintas.

Confidencialidade das operações biométricas: proteção contra extração indevida de informações nos processos de autenticação ou identificação.

c) Governança e Gestão de Dados

Consentimento informado (art. 8º e art. 11 da LGPD): deve ser livre, específico, destacado e com finalidade claramente definida.

Transparência (art. 6º, VI): o titular deve ser informado sobre a finalidade, a base legal e os direitos associados ao tratamento.

Treinamento e conscientização: equipes internas devem ser capacitadas continuamente para o uso ético e seguro da biometria.

Regras claras sobre retenção e descarte (art. 15 da LGPD): os dados devem ser eliminados após o término do tratamento, salvo obrigação legal ou regulatória.

2. Parâmetros Mínimos de Avaliação de Riscos e Monitoramento

Para garantir a conformidade com a LGPD e a proteção integral dos dados biométricos, recomenda-se que as organizações implementem:

Relatório de Impacto à Proteção de Dados Pessoais (RIPD) – art. 38 da LGPD: obrigatório nos casos de alto risco, como tratamento de dados biométricos em larga escala, com detalhamento dos mecanismos de mitigação e justificativas legais.

Mapeamento de fluxos de dados biométricos: identificar todo o ciclo de vida do dado (coleta, uso, armazenamento, compartilhamento e descarte).

Auditorias regulares de segurança e compliance: verificação de conformidade com a LGPD, políticas internas e certificações.

Monitoramento contínuo de incidentes de segurança: com canais de resposta rápida, registro, investigação e notificação à ANPD e ao titular, nos termos do art. 48.

Política de minimização e limitação de acesso: assegurar que apenas pessoas autorizadas tenham acesso aos dados biométricos, de forma proporcional à finalidade do tratamento.

A proteção de dados biométricos exige uma abordagem integrada entre segurança da informação, governança de dados, avaliação de riscos e respeito aos direitos fundamentais dos titulares. A adoção de medidas técnicas alinhadas à ISO/IEC 24745, combinada com diretrizes legais da LGPD, representa o padrão mínimo necessário para prevenir violações e assegurar o uso ético e legítimo dessa tecnologia.

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 tratamento de dados biométricos de crianças e adolescentes, especialmente em contextos como escolas, espaços recreativos e plataformas educacionais, exige máxima cautela. Por envolver dados pessoais sensíveis de pessoas em condição peculiar de desenvolvimento, a Lei Geral de Proteção de Dados Pessoais (LGPD), no art. 14, estabelece que tal tratamento deve ser realizado sempre em observância ao melhor interesse da criança, conceito que vai além da privacidade e abrange aspectos como segurança, saúde, bem-estar, desenvolvimento e autonomia.

1. Participação informada dos pais ou responsáveis legais

Antes da implementação de qualquer sistema biométrico em ambiente escolar, deve-se garantir uma estratégia clara de conscientização e engajamento dos pais ou responsáveis, incluindo:

Campanhas informativas e reuniões prévias, conforme orienta o Guia da UNICEF (2021, p. 13), explicando a tecnologia, as finalidades do tratamento, os riscos envolvidos e os direitos dos titulares.

Consulta direta às crianças e adolescentes, especialmente se forem mais velhas, com linguagem acessível e proporcional à sua maturidade, conforme o padrão do Children's Code do ICO (UK).

Possibilidade de oposição ao tratamento, conforme previsto no Biometrics Guidance (UK, 2022, p. 10), que reconhece o direito de estudantes se recusarem a fornecer dados biométricos, mesmo com o consentimento dos responsáveis.

2. Base legal

Recomenda-se que o tratamento seja fundamentado em consentimento específico e destacado fornecido pelos pais ou responsáveis legais (art. 14, §1º, LGPD), salvo situações excepcionais que envolvam riscos a proteção dos estudantes ou estabelecimento e políticas públicas, como controle de evasão escolar. No entanto, o consentimento por si só não é suficiente: ele deve ser

precedido de uma avaliação concreta de necessidade, proporcionalidade e impacto, conforme exige a boa-fé e os princípios da lei.

3. Condições para conformidade com o princípio do melhor interesse

Para que o tratamento esteja alinhado ao melhor interesse da criança é fundamental que seja realizado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com foco específico na criança (LGPD, art. 38), avaliando não apenas riscos à privacidade, mas também possíveis efeitos sobre: i) Autonomia e capacidade de escolha;ii) Direito de brincar, aprender e interagir livremente; iii) Desenvolvimento físico, emocional e psicológico; iv) Formação da identidade e expressão pessoal; iv) O tratamento seja proporcional e realmente necessário, evitando coleta excessiva, retenção indevida ou uso secundário dos dados; iv) Haja políticas de exclusão de dados biométricos ao fim da necessidade, com garantias de que os dados não serão utilizados para finalidades de vigilância, controle excessivo ou discriminação.

Recomenda-se que instituições educacionais que pretendam adotar tecnologias biométricas:

- Realizem previamente uma DPIA (Data Protection Impact Assessment), com ênfase nos direitos da criança e nos impactos sociais e psicológicos, conforme o modelo da ICO.
- Criem canais claros de comunicação com famílias, inclusive para manifestação de oposição e exercício dos direitos previstos no art. 18 da LGPD.
- Implementem políticas de "Privacy by Design", que minimizem a coleta de dados sensíveis e priorizem o uso de tecnologias menos invasivas.
- Constituam comissões internas com participação da comunidade escolar (pais, professores e alunos) para acompanhar e fiscalizar o uso dessas tecnologias.
- Respeitem a autodeterminação informativa da criança, evitando práticas coercitivas ou restritivas à participação escolar baseadas na coleta de dados.

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?

O tratamento de dados biométricos de crianças e adolescentes, por envolver dados pessoais sensíveis de indivíduos em condição peculiar de desenvolvimento, está sujeito a requisitos legais e éticos rigorosos. A Lei

Geral de Proteção de Dados Pessoais (LGPD) estabelece, no artigo 14, que o tratamento de dados de crianças e adolescentes deve ser realizado com o consentimento específico e em atenção ao seu melhor interesse.

Hipóteses legais admissíveis

A principal base legal para o tratamento de dados biométricos de crianças é o consentimento específico e destacado dos pais ou responsáveis legais (art. 14, §1º, LGPD). Esse consentimento deve ser: i) Livre, informado e inequívoco; ii) Relacionado a uma finalidade clara, legítima e proporcional; e, iii)Recolhido antes do início do tratamento.

Em situações excepcionais que envolvam políticas públicas e que se faça necessário o uso da biometria para controle de evasão escolar em escolas públicas, ou, em ambientes adversos que representem ameaça a segurança do titular e ou do ambiente, é crível admitir-se a adoção da hipótese legal da política pública e prevenção à fraude no ambiente escolar.

É de extrema relevância a participação informada e o engajamento da comunidade escolar.A proteção efetiva dos direitos de crianças e adolescentes exige transparência e engajamento proativo dos pais, responsáveis e dos próprios estudantes. Entre as boas práticas destacam-se:

- Campanhas de conscientização junto aos responsáveis, com linguagem acessível, promovendo debates e consultas públicas sobre a adoção de sistemas biométricos;
- Informação clara e acessível sobre a finalidade, os riscos, a base legal e os direitos dos titulares, inclusive por meio de reuniões presenciais e materiais educativos;
- Consulta às próprias crianças e adolescentes, conforme sua faixa etária e grau de maturidade, respeitando sua autonomia progressiva.

Essas práticas estão em consonância com diretrizes internacionais como o Children's Code (UK) e o Guia UNICEF sobre proteção de dados em escolas, que orientam a escuta ativa dos menores e o envolvimento dos responsáveis desde as etapas iniciais da decisão.

Medidas técnicas e organizacionais para evitar abusos e vazamentos:

Para garantir a segurança e integridade dos dados biométricos tratados, recomenda-se a adoção das seguintes salvaguardas:

Realização de Relatório de Impacto à Proteção de Dados (RIPD), com foco específico nos impactos sobre os direitos da criança, incluindo aspectos como desenvolvimento, autonomia, segurança e privacidade;

Aplicação das diretrizes da ISO/IEC 24745:2011, que estabelecem requisitos de segurança para sistemas biométricos, com ênfase em:

Confidencialidade, integridade, disponibilidade e revogabilidade dos dados;

Irreversibilidade (não reconstrução da imagem original);

Desvinculação (unlinkability) de registros entre bases distintas;

Controle de acesso rigoroso, com autenticação multifator para operadores do sistema;

Retenção mínima e descarte seguro dos dados ao fim da finalidade;

Treinamento contínuo das equipes técnicas e pedagógicas envolvidas.

O tratamento de dados biométricos de crianças e adolescentes em escolas ou espaços recreativos requer a observância dos seguintes critérios: i) base legal válida, (ii) campanhas transparentes de informação aos pais e alunos,(iii) avaliação prévia dos riscos com foco no melhor interesse da criança, e (iv) implementação de medidas técnicas robustas e proporcionais à sensibilidade dos dados.

Essa abordagem assegura não apenas a conformidade legal, mas também o respeito à dignidade e aos direitos fundamentais de crianças e adolescentes, promovendo uma cultura de proteção de dados no ambiente escolar.

Permanecemos à disposição para contribuir com a regulação da proteção de dados biométricos no país.

Atenciosamente,

Instituto Nacional de Proteção de Dados

Martha Leal – Diretora Vice-Presidente
Izabela Lehn – Diretora Jurídica
Cinthia O. A. Freitas – Conselheira Consultiva
Matheus Passos - Conselheiro Consultivo
Daiane Dantas – Presidente da Comissão de Governança e Compliance
Rafael Mosele – Diretor Financeiro e Presidente da Comissão de Relações do Trabalho
Guilherme Gonçalves – Diretor de Capacitação Técnica
Adriana R. Quinelo - Associada
Adriana Neves Gomes de Azevedo - Fellow
Maysa González Rodriguez Dassie - Fellow