INPD
INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

Guia para o Uso Responsável da Biometria no Ambiente Educacional

INPD – Instituto Nacional de Proteção de Dados
Martha Leal – **Vice-presidente**
Rafael Reis – **Presidente**
Atilio Braga – **Secretário**

Coordenação:
Izabela Lehn e Martha Leal
Fellowship:
Adriana Azevedo e Maísa González Rodríguez Dassie

Apresentação

O Instituto Nacional de Proteção de Dados (INPD) é uma entidade que se consolidou como referência nacional na promoção da cultura de proteção de dados pessoais, da privacidade e da governança responsável do uso de tecnologias emergentes. Composto por especialistas de diferentes áreas, o INPD atua de forma independente e colaborativa na produção de conhecimento, capacitação e orientação de boas práticas, sempre em sintonia com os parâmetros estabelecidos pela Lei Geral de Proteção de Dados (LGPD), pela legislação internacional e pelas diretrizes da Autoridade Nacional de Proteção de Dados (ANPD).

Neste cenário, o INPD coloca-se como um agente fundamental na reflexão e na orientação sobre o uso da inteligência artificial de forma responsável, como os sistemas de autenticação biométrica no ambiente educacional. A biometria, ainda que ofereça ganhos em eficiência, segurança e gestão, envolve o tratamento de dados pessoais sensíveis de adultos e de crianças e adolescentes, grupo que merece especial tutela jurídica e social.

A missão do INPD, ao desenvolver guias como este, é justamente fornecer orientações práticas e normativas para que as instituições de ensino possam conciliar inovação tecnológica com o respeito aos direitos fundamentais, assegurando, especialmente no caso de menores, a proteção integral da infância e adolescência.

Ao apresentar este material, o INPD reafirma seu compromisso de ser um parceiro estratégico das escolas, gestores e comunidades, oferecendo uma abordagem multidisciplinar que combina fundamentos jurídicos, regulatórios, técnicos e pedagógicos.

O objetivo é demonstrar e fornecer subsídios para que a adoção de tecnologias de biometria no contexto educacional ocorra de forma ética, transparente e segura, fortalecendo a confiança entre instituições, famílias e estudantes, e promovendo um espaço que respeite tanto os avanços tecnológicos quanto a dignidade humana.

INPD – Instituto Nacional de Proteção de Dados
Martha Leal – **Vice-presidente**
Rafael Reis – **Presidente**
Atilio Braga – **Secretário**

Coordenação:
Izabela Lehn e Martha Leal
Fellowship:
Adriana Azevedo e Maísa González Rodríguez Dassie

Versão 02 – Novembro/2025

Índice

1. **INTRODUÇÃO** 5
2. **O TRATAMENTO DE DADOS BIOMÉTRICOS NO AMBIENTE EDUCACIONAL** 6
   2.1. Definição de biometria e suas aplicações 6
   2.1.1. O que é biometria? 7
   2.1.2. Possíveis usos da biometria – autenticação e identificação 7
   2.2. Contextualização do uso de autenticação biométrica no ambiente educacional (controle de acesso e frequência). 8
   2.3. Algumas considerações necessárias 10
   2.3.2. Limites do uso da biometria para evitar invasão de privacidade 10
   2.3.3. Garantias de não discriminação ou estigmatização de estudantes 10
3. **FUNDAMENTOS LEGAIS E REGULATÓRIOS** 12
   3.1. Lei Geral de Proteção de Dados (LGPD) 12
   3.2. Estatuto da Criança e do Adolescente 12
   3.3. Marco Civil da Internet 13
   3.4. Resolução CD/ANPD nº. 2/2022 13
   3.5. Normas ISO/IEC 13
   3.6. Outras normas internacionais importantes 13
   3.7. Princípios 14
4. **BASE LEGAL PARA TRATAMENTO DE DADOS BIOMÉTRICOS EM INSTITUIÇÕES DE ENSINO** 15
   4.1. O Consentimento como base legal adequada, conforme a LGPD e o ECA 15
   4.2. Requisitos do consentimento 16
   4.3. Direito de oposição ao tratamento por estudantes menores de 18 anos de idade 17
   4.4. Requisitos do consentimento segundo a Norma ISO/IEC 24745/2022 18
   4.5. A importância da transparência quanto ao uso da biometria 19
5. **PROTEÇÃO, ARMAZENAMENTO E DESCARTE SEGURO DE INFORMAÇÕES BIOMÉTRICAS** 20
   5.1. Dados Pessoais Biométricos: 20
   5.2. Requisitos para garantir a segurança dos dados biométricos em instituições de ensino 22
   5.2.1.Confidencialidade 22
   5.2.2. Integridade 22

5.2.3. Cancelamento e renovação 22
5.2.4. Disponibilidade 23
5.3. Requisitos para garantir a privacidade dos dados biométricos 23
5.3.1. Irreversibilidade 23
5.3.2. Desvinculação (unlinkability) 23
5.3.3. Confidencialidade 24
5.4. Gestão da privacidade durante o ciclo de vida das informações biométricas 24
5.4.1. Compartilhamento de dados biométricos 25
5.4.2. Uso secundário de informações biométricas 26
5.4.3. Armazenamento 27
5.4.4. Prazo de retenção das informações biométricas 29
5.4.5. Descarte de dados biométricos 30
5.4.6. Ciclo de vida encerrado e prestação de contas 31
6. **RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS** 33
6.1. Relatório de Impacto à proteção de Dados de Crianças e de Adolescentes 34
7. **RECOMENDAÇÕES PROVENIENTES DAS DEMAIS NORMAS ISO** 36
8. **TRATAMENTO DE INCIDENTES E COMUNICAÇÃO À ANPD** 36
9. **ALTERNATIVAS AO TRATAMENTO DEDADOS BIOMÉTRICOS** 37
9.1. O uso de cartões de identificação com a Frequency IDentification (RFID) ou Identificação por Rádio Frequência 38
9.2. O uso de registro manual 39
9.3. Soluções baseadas em aplicativos e QR Codes 38
9.4. Quando e por que optar por biometria em vez de outras soluções? 39
10. **CONSIDERAÇÕES FINAIS** 39
ANEXO I - Modelo de Termo de Consentimento 42
ANEXO II - Modelo de Política de Tratamento de Dados Biométricos no Ambiente Escolar 45
ANEXO III - Vídeo Informativo sobre o Uso de Biometria 48

1. INTRODUÇÃO

O avanço das tecnologias de identificação biométrica tem transformado diversas esferas da vida social, alcançando também o ambiente educacional. Instituições de ensino têm adotado soluções biométricas, como reconhecimento facial e leitura de digitais, para fins de controle de frequência, segurança, acesso a dependências escolares e autenticação em sistemas.

Ainda que tais aplicações possam trazer vantagens operacionais, seu uso no contexto de instituições de ensino exige uma análise crítica e multidisciplinar, especialmente sob as perspectivas jurídica e pedagógica.

Do ponto de vista jurídico, o uso de dados biométricos no ambiente escolar envolve o tratamento de dados pessoais sensíveis, conforme previsto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD). Tais dados demandam um grau elevado de proteção, sobretudo quando se referem a crianças e adolescentes, cuja condição de desenvolvimento impõe obrigações específicas de cuidado, nos termos do Estatuto da Criança e do Adolescente (ECA).

O princípio do melhor interesse da criança, consagrado na Convenção sobre os Direitos da Criança da Organização das Nações Unidas, ratificada pelo Brasil, deve orientar toda e qualquer decisão que envolva o tratamento de dados de menores, reforçando a necessidade de proporcionalidade, finalidade legítima e base legal apropriada.

A regulação internacional também oferece parâmetros relevantes. O Regulamento Geral de Proteção de Dados da União Europeia (GDPR), referência em proteção de dados, oferece orientações adicionais para o tratamento de dados de menores, reconhecendo sua maior vulnerabilidade frente às tecnologias digitais.

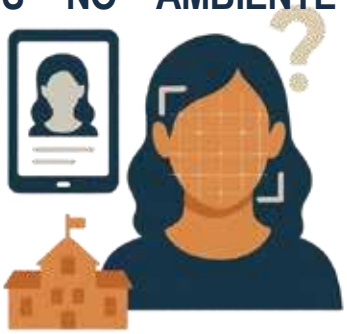
Nesse contexto, as orientações da Agência Nacional de Proteção de Dados

(ANPD), no Brasil, e de outros organismos internacionais, podem ser utilizadas como referência para políticas institucionais e decisões administrativas sobre o assunto.

Sob a ótica pedagógica, é essencial que a adoção de tecnologias biométricas seja compatível com os princípios educacionais que regem a formação cidadã e o desenvolvimento ético dos estudantes. Assim, considerando que as instituições de ensino têm um papel formativo no contexto digital, devem promover o letramento em proteção de dados e o uso responsável da tecnologia como parte de sua missão pedagógica.

Este guia, sem a pretensão de esgotar o assunto, apresenta subsídios práticos e normativos para instituições educacionais que estejam considerando ou já utilizando soluções biométricas. Ao integrar fundamentos jurídicos, regulatórios e pedagógicos, pretende-se contribuir para decisões fundamentadas, seguras e éticas, que respeitem os direitos fundamentais dos estudantes e estejam alinhadas à legislação nacional e internacional.

2. O TRATAMENTO DE DADOS BIOMÉTRICOS NO AMBIENTE EDUCACIONAL



2.1. Definição de biometria e suas aplicações

2.1.1. O que é biometria?

A biometria é uma tecnologia que utiliza características físicas, fisiológicas ou comportamentais de um indivíduo para sua identificação ou autenticação de maneira automática. A tecnologia emprega dados como impressões digitais, reconhecimento facial, padrões de voz, íris, palma da mão, assinatura, entre outros, para conferir e validar a identidade de um indivíduo.

Após a coleta dos dados biométricos, ocorre um processamento técnico que analisa as informações capturadas e cria um padrão matemático exclusivo para cada pessoa, denominado de template biométrico. Esse padrão único possibilita a identificação precisa do indivíduo que se dá mediante a

comparação dos dados, permitindo ou não, a sua validação.

Os templates biométricos não permitem a reconstrução direta das características originais, mas são projetados para serem comparados com dados capturados em tempo real para autenticar ou identificar uma pessoa. Por serem únicos e imutáveis, oferecem alta precisão, mas também demandam proteção rigorosa devido ao impacto de um possível vazamento, já que características biométricas são consideradas dados sensíveis.

O processamento de dados biométricos ocorre de acordo com as seguintes etapas:

1º. Captura das características individuais: coleta da informação do indivíduo, por exemplo, uma foto do rosto ou coleta das impressões digitais.

2º. Extração de características: por meio da tecnologia, se extrai os padrões exclusivos da característica capturada, por exemplo, a voz, cor do cabelo, digitais, íris, etc.

3º. Criação de um template biométrico: uma vez extraídos os padrões, convertem-se tais características únicas do indivíduo em um padrão matemático digital exclusivo que representa aquele indivíduo.

2.1.2. Possíveis usos da biometria – autenticação e identificação

Após a criação do template, inicia-se a utilização dos dados biométricos, sendo a autenticação e a identificação os dois principais processos de validação.

A **autenticação** é um processo de verificação em que os dados biométricos coletados de um indivíduo são comparados a uma amostra biométrica previamente armazenada, confirmando se a pessoa é quem afirma ser. Por exemplo, em uma instituição de ensino, é o que acontece quando estudantes utilizam as suas impressões digitais para acessar o ambiente escolar, garantindo que apenas quem está autorizado tenha acesso.

Já a **identificação** consiste em comparar os dados biométricos de uma pessoa com todos os templates armazenados em um banco de dados, a fim de determinar a sua identidade. A identificação biométrica responde à pergunta "Quem é você?". Assim, por exemplo, numa escola, o aluno se posiciona frente à câmera de captura e o software compara a imagem com todos os templates biométricos cadastrados para encontrar uma correspondência. Se encontrar, informará "este é o aluno tal" e permitirá a entrada.

Importante registrar que as finalidades de tratamento acima referidos, autenticação e identificação, devem ser devidamente compreendidas, pois atraem riscos diferenciados.

A autenticação processa menos dados, pois a consulta é direcionada e limitada (acontece apenas a comparação da pessoa que está acessando o ambiente escolar com o template biométrico previamente armazenado).

Entretanto, a identificação de um indivíduo requer que a coleta da amostra biométrica (impressão digital, reconhecimento facial, íris, etc) seja comparada com todos os templates armazenados no sistema. Ou seja, o tratamento envolve maior quantidade de dados, elevando os riscos.

Feita a distinção entre autenticação e identificação, sugere-se, por envolver menos riscos, o uso da tecnologia com o intuito de **autenticar** o titular de dados pessoais.

2.2. Contextualização do uso de autenticação biométrica no ambiente educacional (controle de acesso e frequência).

A implementação de sistemas biométricos no ambiente educacional, incluindo escolas e universidades, vem sendo utilizada com diferentes finalidades, principalmente para combinar eficiência operacional e segurança, conforme justificado pelas instituições de ensino que estão adotando esse tipo de tecnologia.

Os principais usos incluem:

● Controle de Acesso:

A autenticação biométrica vem sendo utilizada para garantir que apenas pessoas autorizadas, como alunos, responsáveis legais, professores e funcionários, acessem as instalações escolares, aumentando a segurança e mitigando as chances de situações de risco.

Uma das principais vantagens apontadas por instituições de ensino em defesa do acesso ao espaço físico escolar por biometria, é dificultar fraudes e acessos não autorizados.

Como esse tipo de autenticação se baseia em características únicas de cada pessoa — como impressões digitais, reconhecimento facial ou padrões de voz —, a falsificação se torna extremamente difícil, oferecendo segurança superior aos métodos tradicionais; enquanto cartões de acesso podem ser clonados, perdidos ou manipulados, a biometria reduziria significativamente esses riscos, tornando o controle de entrada e saída do ambiente de ensino mais seguro.

Além disso, as instituições de ensino estão usando esse tipo de tecnologia para controlar o acesso de pessoas a determinados espaços dentro do ambiente escolar, como laboratórios, reforçando a proteção de estudantes e funcionários.

● Controle de Frequência:

O registro biométrico também vem sendo empregado para facilitar o registro de frequência dos alunos, reduzindo o risco de falhas e fraudes no controle de presença manual.

Com o uso de sistemas de reconhecimento facial, o tempo gasto para registrar a presença é reduzido e a precisão do processo aumenta.

A vantagem de usar autenticação biométrica para o controle de presença também estaria na possibilidade de geração de relatórios automáticos capazes de identificar faltas recorrentes e atrasos, permitindo que pais e responsáveis

legais mantenham maior controle mediante recebimento de alertas em portais educacionais.

2.3. Algumas considerações necessárias

2.3.1. Aspectos éticos e de privacidade

A utilização da autenticação biométrica no ambiente escolar traz benefícios, mas também levanta importantes questões legais e éticas, especialmente porque pode envolver dados sensíveis de crianças e adolescentes, sendo fundamental garantir a privacidade através de um nível elevado de proteção, bem como a não discriminação dos titulares.

2.3.2. Limites do uso da biometria para evitar invasão de privacidade

O uso de dados biométricos, como impressões digitais e reconhecimento facial, deve ser pautado por limites claros para evitar invasões de privacidade. A biometria é considerada um dado sensível e, portanto, seu tratamento deve seguir os princípios legais, como necessidade, adequação e transparência. Além disso, a coleta de dados biométricos deve ser restrita a finalidades específicas e legítimas fundamentadas em base legal adequada. Portanto, é fundamental que as instituições de ensino adotem medidas rigorosas de segurança cibernética para proteger essas informações contra vazamentos ou acessos não autorizados.

2.3.3. Garantias de não discriminação ou estigmatização de estudantes

A garantia de que o uso da biometria não resulte em discriminação ou estigmatização de estudantes é imprescindível, pois as tecnologias de reconhecimento facial (autenticação e identificação) podem apresentar vieses que afetam negativamente determinados grupos raciais ou de gênero.

É aqui importante destacar os possíveis problemas que o uso biométrico pode gerar, a depender da tecnologia utilizada, que são o falso positivo e falso negativo.

Um falso positivo ocorre quando o sistema autentica erroneamente uma pessoa como outra, o que pode comprometer a segurança ao permitir o acesso de um indivíduo não autorizado.

Por outro lado, um falso negativo acontece quando o sistema não consegue reconhecer ou autenticar corretamente uma pessoa legítima, resultando em frustrações para os usuários e possíveis bloqueios e indiscriminação indevidos.

Portanto, falsos positivos ou falsos negativos podem resultar em discriminação contra pessoas ou contra um grupo. Tais erros podem ser influenciados por fatores como qualidade dos dados biométricos capturados, condições ambientais (como iluminação ou ruído) e limitações nos algoritmos de correspondência.

Para mitigar essas situações, para além de ajustes nos parâmetros do sistema, deve-se oferecer a possibilidade de tal autenticação ser verificada por uma pessoa, caso o sistema resulte num falso positivo ou falso negativo.

Para evitar esses riscos, é necessário que as instituições de ensino escolham fornecedores que sigam padrões éticos no desenvolvimento de seus algoritmos e realizem auditorias regulares para identificar e corrigir possíveis distorções, garantindo a transparência algorítmica. Além disso, a promoção de uma cultura inclusiva e o respeito à diversidade devem ser pilares fundamentais no ambiente escolar.

Em suma, a biometria pode trazer benefícios significativos para as instituições de ensino, mas a sua implementação deve ser acompanhada de responsabilidade ética e legal.

O equilíbrio entre inovação tecnológica e respeito aos direitos dos estudantes e da comunidade escolar é essencial para garantir um ambiente educacional seguro, inclusivo e respeitoso.

Enfim, como os dados biométricos são classificados como dados sensíveis pela Lei Geral de Proteção de Dados Pessoais (LGPD), seu tratamento exige

atenção especial à legislação aplicável, inclusive orientações de organismos nacionais e internacionais sobre o assunto, conforme será abordado adiante.

3. FUNDAMENTOS LEGAIS E REGULATÓRIOS

3.1. Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é a principal legislação que regula o tratamento de dados pessoais no Brasil, estabelecendo princípios, direitos e obrigações. Isso inclui os dados biométricos, que são classificados como dados sensíveis (art. 5, inciso II) devido ao impacto sobre a privacidade dos indivíduos se forem alvo de incidentes de segurança.

No contexto educacional, a LGPD estabelece diretrizes para o uso de biometria, determinando que o tratamento e processamento desses dados seja realizado de forma lícita, transparente e segura.

3.2. Estatuto da Criança e do Adolescente

O Estatuto da Criança e do Adolescente (ECA) - Lei nº 8.069/1990 é aplicável quando a biometria envolver crianças e adolescentes.

Referida norma estabelece que devem ser aplicadas medidas de proteção às crianças e aos adolescentes em caso de ameaças a direitos, levando-se em conta alguns princípios, como o da privacidade e da obrigatoriedade de informação (art. 100, §único, V e XI, ECA).

Portanto, o uso da biometria nas escolas deve observar, sempre que envolver esse grupo de pessoas, o melhor interesse da criança e adolescente, de forma que os sistemas biométricos não deverão criar ou reforçar desigualdades, discriminação ou vulnerabilidades (art. 5º, ECA).

3.3. Marco Civil da Internet

A Lei no. 12.965/2014 – Marco Civil da Internet- aplica-se em sistemas biométricos online, prevendo a necessidade de proteção e privacidade dos dados pessoais (Art. 3º, II e III).

3.4. Resolução CD/ANPD nº. 2/2022

A Resolução CD/ANPD nº. 2/2022, que regula agentes de tratamento de pequeno porte considera de alto risco o processamento de dados sensíveis ou de crianças e de adolescentes (art. 4º, I, d).

3.5. Normas ISO/IEC

Quanto às normas técnicas (NBR, ISO/IEC), listamos as principais referências relacionadas ao tema em questão:

- ABNT NBR ISO/IEC 19792/2012 – trata de normas sobre avaliação de segurança de sistemas biométricos;
- ABNT ISO/IEC 30107-1:2023 – trata da detecção de ataques de apresentação (PAD), como tentativas de enganar sensores biométricos;
- ABNT ISO/IEC 24745/2022 – trata de norma de proteção de informação biométrica e proteção contra reidentificação.

3.6. Outras normas internacionais importantes

E, por fim, cumpre registrar a relevância das seguintes as normas internacionais:

- Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia: O GDPR, no Artigo 9(1), proíbe, como regra geral, o tratamento de dados biométricos para identificar uma pessoa de forma inequívoca. Contudo, não obstante uma das exceções para o tratamento seja o consentimento explícito do titular de dados, conforme Artigo 9(2)-a, o mesmo tem sido invalidado por Autoridades de Proteção de Dados sob o argumento de não ser

livremente dado, tendo em vista a relação desequilibrada entre instituições de ensino e seus alunos e pais.

- Convenção 108+ do Conselho de Europa: A Convenção 108+, em seu Artigo 6º, estabelece uma categoria especial de dados que exige tutela jurídica reforçada. O tratamento destes dados é considerado mais arriscado devido ao seu potencial para lesar os direitos e liberdades fundamentais dos titulares de dados, em particular através da criação de estigmas ou da facilitação de práticas discriminatórias. As categorias especiais de dados, ou "dados sensíveis", conforme definidos no Artigo 6º da Convenção, incluem dados biométricos que identifiquem uma pessoa de forma inequívoca. A Convenção reconhece que características físicas, fisiológicas ou comportamentais, quando processadas por meios técnicos para permitir a identificação única de um indivíduo, transcendem a categoria de dados pessoais comuns. A natureza imutável e a ligação intrínseca à identidade física do indivíduo justificam a classificação como sensíveis e, consequentemente, a aplicação de um regime de proteção mais rigoroso.

- Convenção sobre os Direitos da Criança da ONU (1989): com o objetivo de garantir a proteção máxima e o bem-estar das crianças e adolescentes, a Convenção reconhece o direito das crianças à privacidade e proteção de seus dados pessoais no contexto internacional. Entre as principais diretrizes, a Convenção estabelece que o melhor interesse da criança deve ser a prioridade em qualquer ação (art. 3), de modo a proteger sua privacidade e vida particular (art. 16).

3.7. Princípios

Dentre os princípios estabelecidos no art. 6 da LGPD, ressaltamos a transparência, finalidade e a necessidade.

As instituições de ensino devem ser transparentes sobre a coleta e o uso de dados biométricos, informando claramente aos alunos e seus responsáveis legais sobre as finalidades, que devem ser específicas, legítimas e explícitas, bem como os procedimentos envolvidos, o período de retenção e os direitos dos titulares sobre os dados coletados.

A divulgação das políticas de privacidade e o acesso facilitado à informação sobre a finalidade do tratamento dos dados biométricos garante maior transparência do processo, de modo que os dados só serão utilizados para o objetivo inicialmente definido. Assim, por exemplo, se a finalidade do tratamento dos dados biométricos é o acesso a um campus universitário, não há possibilidade de tratamento posterior de forma incompatível com essa finalidade inicialmente estabelecida.

Para além disso, a coleta dos dados biométricos deve ser restrita ao mínimo necessário, de modo a evitar armazenamento excessivo e desnecessário de informações.

4. BASE LEGAL PARA TRATAMENTO DE DADOS BIOMÉTRICOS EM INSTITUIÇÕES DE ENSINO

4.1. O Consentimento como base legal adequada, conforme a LGPD e o ECA

O tratamento de dados biométricos em instituições de ensino somente poderá acontecer mediante o consentimento dos estudantes, se maiores de 18 anos, ou de seus pais ou representantes legais, se o titular não tiver atingido 18 anos completos (art. 11, I, e art. 14, II, ambos da LGPD c/c art. 2º do Estatuto da Criança e do Adolescente).

Poderá, contudo, ser utilizada outra base legal, caso exista legislação específica que exija a adoção de autenticação biométrica num determinado caso em específico, bem como, em se tratando de escolas públicas em que a referida tecnologia faça parte de um programa governamental para segurança ou controle de acesso.

Entretanto, no cenário das instituições de ensino privadas, a hipótese legal que nos parece adequada para amparar o tratamento de dados biométricos de adultos, crianças e adolescentes é o consentimento.

Optamos por não utilizar a base legal da prevenção à fraude (art. 11, II, g, da LGPD), adotando posição mais conservadora e cuidadosa porque o tratamento no âmbito de instituições de ensino pode envolver dados de crianças e de adolescentes, considerados vulneráveis.

4.2. Requisitos do consentimento

Segundo dispõe a LGPD, o consentimento para o tratamento de dados pessoais sensíveis deverá ser específico e destacado, ou seja, colhido em separado, por termo independente de outras cláusulas contratuais ou termos gerais de uso; deve, enfim, demonstrar uma ação positiva do titular concordando com o tratamento desses dados.

Os titulares ou seus responsáveis legais, se incapazes, devem também ser explicitamente informados sobre a categoria de dados que será tratada (íris, digital, reconhecimento facial, etc.), a finalidade clara e justificada (por exemplo, controle de acesso ao ambiente escolar) e o período de tratamento dos dados.

Para garantir que o consentimento preencha os requisitos legais, ele deve ser livre, exercido sem qualquer tipo de coerção, pressão ou consequência pelo não consentimento.

Além disso, o consentimento deve ser formalizado antes da captura do dado biométrico do estudante e, portanto, da geração do template biométrico, garantindo transparência ao titular de dados: primeiro ele recebe todas as informações correspondentes ao tratamento de dados e depois consente.

Também é necessário informar quais as consequências para o titular que não consentir e o meio alternativo para acesso ao ambiente escolar. Essas

alternativas devem garantir igualdade de tratamento, evitando qualquer tipo de discriminação. Assim, se os dados biométricos foram usados para acessar as dependências de uma instituição de ensino (entrada e saída do ambiente escolar), se o titular de dados não consentir, devem ser garantidos meios de acesso alternativos, através de cartões de identificação, por exemplo. A alternativa é essencial para que o consentimento seja realmente livre (o titular somente consentirá se puder também não consentir, sem prejuízo).

Além disso, deve ser esclarecido aos estudantes e outros titulares de dados que o consentimento pode ser revogado a qualquer tempo com informações sobre o canal de comunicação que deverá ser acessado para que isso aconteça. Lembrando que a LGPD dispõe que a revogação do consentimento deve ser facilitada, significando que a instituição de ensino não deverá dificultar a revogação.

Se o titular revogar o consentimento durante a fase de uso dos templates biométricos, os dados devem ser descartados, independentemente de ainda estar dentro do prazo definido de retenção.

Também deve ser informado no termo de consentimento que o mesmo canal disponibilizado para revogar o consentimento, poderá ser utilizado pelos titulares de dados para exercer outros direitos previstos no art. 18 da LGPD, relacionados ao tratamento de dados biométricos, tais como acessar, confirmar o tratamento, solicitar correção, etc.

4.3. Direito de oposição ao tratamento por estudantes menores de 18 anos de idade

Sugere-se seja respeitado o direito de estudantes menores de 18 anos de oposição ao tratamento de dados pessoais biométricos, ainda que os pais ou responsáveis legais tenham consentido, pois o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse.

Segundo a ICO, se o aluno se opuser, essa recusa prevalece sobre qualquer consentimento dos pais; portanto, seus dados biométricos não devem ser tratados.

A Autoridade de Proteção de Dados do Reino Unido (ICO), em orientação sobre o tema, sugere que as opiniões de estudantes, pais e responsáveis legais sobre o tratamento dos dados biométricos sejam levadas em consideração para que o consentimento seja livre, ou seja, real.

Em anexo ao presente Guia, estamos disponibilizando um modelo de consentimento livre e informado para auxiliar a comunidade escolar a cumprir tais exigências.

4.4. Requisitos do consentimento segundo a Norma ISO/IEC 24745/2022

De acordo com a Norma ISO/IEC 24745/2022, que dispõe sobre a proteção de dados pessoais biométricos, o consentimento deverá informar:

- Quais informações biométricas serão tratadas;
- Os procedimentos alternativos disponíveis se o titular dos dados não consentir;
- A finalidade da coleta e o período de tratamento das informações biométricas;
- A descrição de como as informações biométricas capturadas serão processadas no sistema biométrico;
- Informações sobre o período de armazenamento e de descarte;
- Informações sobre o encarregado de dados (nome e canal de contato).

Dessa forma, a Norma ISO/IEC complementa e fortalece as disposições da LGPD quanto aos requisitos para obtenção de consentimento válido.

4.5. A importância da transparência quanto ao uso da biometria

A comunicação clara e transparente é essencial para construir confiança e garantir o apoio da comunidade escolar. Isso pode ser feito através de campanhas para a conscientização de estudantes e de seus pais/responsáveis legais, antes e durante o tratamento de dados biométricos.

A introdução da biometria em ambientes de ensino gera preocupações legítimas sobre privacidade, segurança dos dados e uso indevido de informações sensíveis, em especial por envolver também o tratamento de dados de crianças e de adolescentes.

Além disso, o armazenamento de dados biométricos em sistemas externos pode tornar mais vulneráveis as informações a ataques cibernéticos, comprometendo a segurança dos dados sensíveis.

Portanto, embora a biometria possa proporcionar maior segurança, eficiência, otimização da gestão escolar e prevenção de possíveis fraudes, é essencial que a instituição de ensino seja transparente e informe o titular dos dados ou seu responsável legal de maneira clara, objetiva e detalhada sobre o tratamento dos dados biométricos.

Algumas estratégias podem ser implementadas para garantir o engajamento dos pais e responsáveis neste processo, são elas:

- Promover campanhas, consultas e reuniões entre a entidade escolar e os responsáveis legais para esclarecer dúvidas e receber sugestões;

- Disponibilizar em portais online ou murais escolares os detalhes sobre o uso da biometria, incluindo a finalidade, segurança, período de retenção e o direito de revogação;
- Efetuar treinamento com os a professores e a equipe administrativa para lidar com o sistema e com possíveis falhas técnicas;
- Manter a transparência contínua e um canal aberto para comunicação e responder prontamente às dúvidas dos pais e alunos;
- Realizar avaliação periódica para revisar o sistema, os problemas e possíveis melhorias para garantir que o sistema funcione corretamente e não esteja gerando discriminação ou estigmatização.

Em anexo, disponibilizamos um modelo de Política de Tratamento de Dados Biométricos no Ambiente Escolar em formato de vídeo, especialmente elaborada para o público infantil. Nosso objetivo é assegurar que as crianças compreendam, da forma mais clara possível, como seus dados biométricos serão coletados, usados, protegidos e eventualmente compartilhados, sempre respeitando seus direitos e os princípios da proteção de dados. O vídeo funciona como ferramenta educativa, de modo que os alunos possam conhecer suas garantias, saber com quem falar em caso de dúvidas ou reclamações, e entender que a instituição de ensino assume compromisso de transparência, segurança e respeito à privacidade dos menores.

5. PROTEÇÃO, ARMAZENAMENTO E DESCARTE SEGURO DE INFORMAÇÕES BIOMÉTRICAS

5.1. Dados Pessoais Biométricos: considerações relevantes

O uso de biometria em instituições de ensino demanda especial atenção dos agentes de tratamento, tendo em vista que os templates biométricos são

classificados como dados pessoais sensíveis , exigindo medidas adicionais de proteção e uma base legal apropriada para tratamento, desde a coleta até o descarte.

Neste Capítulo do Guia será abordada a necessidade de segurança e privacidade dos dados biométricos tratados em ambientes educacionais, desde o “onboarding digital” até o descarte, apresentando as melhores práticas de acordo com os padrões internacionais previstos na ISO/IEC 24745/2022, tendo em vista a inexistência de regras específicas sobre o assunto relacionados à segurança de informações biométricas no Brasil.

Também trouxemos as regras previstas na Lei Geral de Proteção de Dados Pessoais, além de orientações da ANPD e de Autoridades de Proteção de dados estrangeiras, como EDPB, CNIL e ICO.

5.2. Requisitos para garantir a segurança dos dados biométricos em instituições de ensino

Segundo a Norma ISO/IEC 24745/2022, os requisitos para garantir a segurança das informações biométricas, aplicáveis ao tratamento de dados biométricos em instituições de ensino, são os seguintes:

5.2.1.Confidencialidade

A confidencialidade dos dados biométricos tratados em instituições de ensino deve ser garantida através de mecanismos de controle de acesso e por criptografia.

5.2.2. Integridade

Sistemas biométricos devem empregar proteção para garantir a integridade dos dados tratados. Para tanto, é possível usar técnicas de criptografia combinadas com outras técnicas.

5.2.3. Cancelamento e renovação

Em caso de incidente de segurança envolvendo um template biométrico, o que pode acontecer, por exemplo, por acesso de pessoa não autorizada, a instituição de ensino deverá ter condições técnicas para cancelá-lo e substituí-lo por um novo.

Uma vez cancelado, poderá ser criado um novo template a partir da amostra biométrica original, o que se denomina renovação.

Segundo a ICO, para serem cumpridos os princípios da minimização (necessidade) e da limitação de armazenamento de dados, a instituição de ensino deverá decidir entre manter ou não a amostra original (por exemplo, a foto do estudante que originou o template biométrico). Se decidir mantê-la, deve garantir a segurança das informações armazenadas.

5.2.4. Disponibilidade

Disponibilidade é a possibilidade de acessar, de dispor sobre as informações biométricas sempre que necessário. Assim, se ocorrer a inatividade de um banco de dados com templates biométricos, ele deve estar disponível para ser acessado de outra forma. A Norma ISO 24745/2022 recomenda backups regulares para garantir a disponibilidade do banco de dados biométrico em caso de impossibilidade de acesso.

5.3. Requisitos para garantir a privacidade dos dados biométricos

A Norma ISO/IEC 24745/2022 destaca como requisitos para garantir a privacidade das informações biométricas a irreversibilidade, a desvinculação e a confidencialidade. Vejamos cada um deles, que se aplicam aos casos de tratamento de dados no setor educacional.

5.3.1. Irreversibilidade

Após a extração de um template biométrico, não mais poderão ser obtidas informações sobre o titular de dados, evitando o uso para finalidades diversas das originalmente pretendidas. Isso pode ser alcançado através da criptografia dos dados biométricos.

5.3.2. Desvinculação (unlinkability)

O template biométrico não pode permitir a vinculação à pessoa natural a qual se refere, e, igualmente, não pode ser usado para acessar diferentes sistemas de identificação biométrica.

Assim, por exemplo, se instituições de ensino diferentes usam sistemas de reconhecimento facial distintos, o template de um aluno numa escola não pode ser facilmente associado ao template dele em outra base, garantindo a privacidade das informações.

Essa característica também dificulta que um invasor use um template roubado para encontrar a pessoa em outras plataformas.

5.3.3. Confidencialidade

A confidencialidade no tratamento de dados biométricos em instituições de ensino é fundamental para proteger a privacidade dos estudantes e demais usuários (por exemplo, pais e representantes legais de estudantes, funcionários e visitantes).

Conforme estabelecido pela norma ISO/IEC 24745/2022, confidencialidade implica proteger os dados biométricos contra acessos não autorizados que possam comprometer a privacidade. A mencionada Norma ISO sugere, para garantir a confidencialidade das informações biométricas, a separação de dados e a criptografia

5.4. Gestão da privacidade durante o ciclo de vida das informações biométricas

Tratar dados biométricos com responsabilidade não se resume a protegê-los somente durante seu uso ativo, sendo fundamental gerenciar todo o ciclo de vida dos mesmos dentro de uma instituição de ensino.

A Norma ISO/IEC 24745/2022 traz explicações sobre medidas que devem ser adotadas durante o ciclo de vida dos dados pessoais, ou seja, na coleta, no compartilhamento, no uso, no armazenamento, na retenção, no arquivamento, no backup e no descarte dos dados biométricos.

Embora não mencione expressamente o termo “privacy by design” e “privacy by default”, a Norma ISO incorpora seus princípios fundamentais, exigindo que a privacidade esteja presente em todas as etapas do tratamento de dados biométricos.

Vamos, neste Guia, analisar cada etapa com olhar voltado ao setor educacional.

5.4.1. Compartilhamento de dados biométricos

A Norma ISO/IEC 24745/2022 também traz orientações sobre o compartilhamento de dados pessoais biométricos entre agentes de tratamento, alertando sobre a importância dos contratos envolvendo direitos e obrigações relacionadas à proteção de dados.

Segundo a apontada Norma ISO, o compartilhamento somente poderá acontecer se o titular de dados consentir, ou se o consentimento estiver explícito na prestação de um serviço solicitado pelo titular.

Diz a regra que deverá ser informado ao titular de dados:

- Quem é o terceiro com quem as informações biométricas serão compartilhadas;

- O conteúdo e a quantidade de informações biométricas a serem transferidas;

- A entidade que realiza o compartilhamento;

- A finalidade do compartilhamento e o período de retenção das informações biométricas transferidas.

Enfim, instituições de ensino devem ser transparentes com os titulares de dados, informando sobre o compartilhamento de dados biométricos, o que deverá acontecer através do texto do Termo de Consentimento e, igualmente, estar previsto na Política de Tratamento de Dados Biométricos.

É o caso, por exemplo, de compartilhamento de dados biométricos entre instituições de ensino e empresas fornecedoras de sistemas biométricos, que prestam serviços de assistência técnica.

Diferentemente de dados acadêmicos ou administrativos, que muitas vezes circulam entre órgãos (secretarias de educação, etc.), os dados biométricos devem permanecer sob guarda restrita, não devendo as instituições de ensino repassá-los a ninguém.

5.4.2. Uso secundário de informações biométricas

Deve ser informado ao titular de dados qual a finalidade do tratamento dos dados biométricos e o período de tratamento, conforme já abordado no item que trata sobre o consentimento.

Contudo, caso a instituição de ensino deseje tratar dados biométricos com finalidades distintas daquelas informadas no termo de consentimento, deverá obter novo consentimento do titular de dados, onde deverá descrever a finalidade adicional e o período de retenção dos dados biométricos.

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

5.4.3. Armazenamento

Os templates biométricos devem ser armazenados pelas instituições de ensino com elevado padrão de segurança, para evitar acessos não autorizados.

É também necessário fazer backup das informações biométricas, que também devem ser armazenadas em locais seguros, com acesso controlado e descartados ao término do tratamento.

Para tanto, é preciso adotar cuidados através da implementação de medidas técnicas e organizacionais de segurança, minimizando o risco inerente ao tratamento de dados sensíveis.

A seguir, destacamos algumas práticas recomendadas:

a) Criptografia dos dados

Segundo orientações da CNIL, dados biométricos devem ser criptografados, garantindo uma camada de proteção contra acessos não autorizados. Assim, mesmo que sejam alvo de incidentes de segurança, não será possível identificá-los sem a chave correta.

b) Controle de acesso restrito

Adotar políticas de controle de acesso, garantindo que apenas pessoas autorizadas possam ter acesso à base de dados biométricos. Por exemplo, administradores de TI ou encarregados de dados (DPO) podem ter acesso, enquanto professores ou outros funcionários não devem ter acesso direto a informações sensíveis. Além disso, a manutenção do sistema biométrico deve ser feita por equipes internas treinadas ou por fornecedores que sigam padrões de segurança equivalentes aos da instituição de ensino, tudo ajustado contratualmente, conforme ressaltado nos parágrafos precedentes.

c) Servidores locais e armazenamento em nuvem

Servidores locais devem possuir proteção física e lógica (firewalls, antivírus, atualizações em dia) e, se for utilizado armazenamento em nuvem, o fornecedor de serviços deve demonstrar conformidade com LGPD e boas práticas de proteção de dados.

d) Monitoramento e logs de acesso

Implementar mecanismos de monitoramento contínuo é essencial para detectar e responder rapidamente a acessos indevidos ou atividades suspeitas.

O sistema deve manter logs auditáveis de todas as operações relevantes, registrando quem acessou os dados biométricos, em que momento e para qual finalidade.

Análises regulares desses logs podem revelar tentativas de violação ou uso inadequado.

e) Separação de bases de dados

Uma boa prática para armazenamento seguro dos templates biométricos, recomendada na Norma ISO/IEC 24745/2022, é separar a base de dados biométrica de outras bases contendo dados pessoais.

Isso pode acontecer, por exemplo, se uma instituição de ensino decide implementar controle de acesso por reconhecimento facial para que alunos e demais pessoas acessem as suas dependências. Para isso, precisará tratar dados biométricos (templates de impressão digital) e dados de identidade (nome, matrícula, turma etc.).

Assim, o sistema pode armazenar em separado os templates faciais sem conter o nome, a matrícula ou qualquer dado que permita identificar o estudante diretamente, enquanto num banco de dados em separado são armazenadas informações de identificação do aluno. Dessa forma, mesmo que haja acesso indevido a uma parte, não será possível identificar o titular de dados.

f) Treinamento dos funcionários

De nada adiantarão medidas técnicas se os usuários do sistema não estiverem cientes das boas práticas.

Portanto, a instituição de ensino deve promover treinamentos para funcionários que acessam dados biométricos, enfatizando políticas, protocolos e o caráter sensível dos dados.

Em conjunto, essas medidas atendem ao princípio da segurança previsto nos arts. 6, VII, e 46 da LGPD, que impõe ao agente de tratamento a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado ou ilícito.

5.4.4. Prazo de retenção das informações biométricas

As informações biométricas devem ter prazo determinado para retenção. Portanto, no momento de solicitar o consentimento do titular de dados (estudantes ou pais, por exemplo), a instituição de ensino deve informar e documentar até quando aquele dado será tratado e mantido. Isso demonstra a transparência quanto ao tratamento de dados e permite que os titulares tenham expectativas claras sobre o mesmo.

Os dados podem ser mantidos até o término do contrato de prestação de serviços educacionais ou enquanto o estudante estiver com matrícula vigente, devendo ser excluídos em seguida. E, caso sejam tratados em projeto piloto ou temporário, podem ser tratados até a conclusão do projeto.

Pode ser informado o seguinte aos estudantes: “Os templates faciais serão armazenados enquanto o aluno estiver com matrícula vigente e serão excluídos em até 30 dias após o término do vínculo”.

A retenção sem prazo definido, é evidente, aumenta os riscos relacionados ao tratamento de dados: quanto mais tempo um dado sensível fica armazenado, maiores as chances de incidentes e mais difícil justificar porque ainda permaneciam armazenados numa base de dados.

5.4.5. Descarte de dados biométricos

Para realizar o descarte dos dados biométricos tratados, a instituição de ensino deve agir de maneira segura e comprovável.

O término do tratamento e o descarte dos dados biométricos por instituições de ensino deverá ser realizado:

- Sempre que não houver mais necessidade e desde que cumprida a finalidade do tratamento;

- Após o término do prazo previsto para arquivamento e retenção das informações biométricas;

- Sempre que o titular de dados exercer o direito de revogar o consentimento para o tratamento de dados;

- Após aplicação de penalidade, pela ANPD, por descumprimento da LGPD, se for o caso;

- Se a finalidade para o tratamento de dados for modificada e se o titular, devidamente informado, não consentir quanto ao novo uso[2]

É também aconselhável que sejam estabelecidas políticas claras sobre o ciclo de vida dos dados biométricos, prazos de retenção e procedimentos para que sejam corretamente descartados por instituições de ensino, de modo que não possam ser acessados e recuperados posteriormente.

Portanto, simplesmente “deletar” um registro não é suficiente, pois ele pode persistir no banco de dados ou em backups. Caso a instituição de ensino tenha dúvidas sobre a correta eliminação dos templates biométricos, deverá solicitar que o fornecedor do software biométrico forneça orientações sobre os procedimentos seguros para eliminação dos dados.

A fim de demonstrar conformidade e também para garantir transparência, a instituição de ensino deve registrar internamente o descarte dos dados biométricos. Por exemplo, manter uma planilha ou log com informação do tipo: “Aluno X – data de desligamento: 10/12/2025 – data de exclusão da biometria: 15/01/2026 – responsável pela operação: [nome do administrador]”. Esses registros servem como evidência de que a instituição de ensino cumpriu o prometido e eliminou os dados no prazo. De acordo com boas práticas, as organizações devem manter registros de suas operações de tratamento, incluindo o descarte, o que auxilia em auditorias e inspeções. Importante salientar, quanto ao ponto, que se o titular solicitar, é direito dele saber se seus dados foram eliminados.

Embora não haja, na LGPD, obrigação expressa de informar ao titular sobre o descarte dos seus dados, nada impede que a instituição de ensino realize tal comunicação, adotando-a como boa prática.

A instituição de ensino pode informar, por exemplo, ao entregar o histórico escolar de formatura: “Conforme nossa política de privacidade, os dados biométricos coletados para controle de acesso foram excluídos de nossos sistemas na data ... Caso retorne à instituição, um novo cadastro biométrico será necessário.” Esse tipo de comunicação reforça a confiança e evidencia respeito à autodeterminação do titular.

Caso o descarte aconteça em razão da revogação do consentimento, é recomendável documentar quando isso ocorrer (por exemplo: “Responsável pelo aluno Y revogou o consentimento em [especificar a data]. Os dados foram descartados em [especificar a data]. Foi ativado o método alternativo de acesso via cartão de identificação em [especificar a data]”.

5.4.6. Ciclo de vida encerrado e prestação de contas

Após realizado o descarte, encerra-se o ciclo de vida dos dados biométricos que vinham sendo tratados pela instituição de ensino. Porém, as obrigações não terminam aí, pois a adoção de tecnologias biométricas em instituições de ensino, especialmente aquelas voltadas à autenticação e controle de acesso,

exige mecanismos contínuos de auditoria e monitoramento, com vistas à preservação da segurança, da transparência e da conformidade legal no tratamento de dados pessoais sensíveis, em especial os de crianças e adolescentes.

A Lei Geral de Proteção de Dados (LGPD) determina, em seu art. 6º, que o tratamento de dados pessoais deve observar os princípios da segurança, prevenção, responsabilização e prestação de contas. Isso implica que as escolas e redes de ensino que utilizam sistemas biométricos devem adotar mecanismos regulares de verificação de conformidade, que comprovem a efetiva proteção dos dados pessoais e permitam a detecção de riscos e falhas operacionais.

As auditorias de proteção de dados em sistemas biométricos devem ter como foco:

- Verificar a aderência das práticas escolares aos princípios e bases legais da LGPD, especialmente no tratamento de dados sensíveis;
    - Avaliar a eficácia das medidas técnicas e organizacionais implementadas para garantir a segurança e a integridade dos dados;
    - Detectar vulnerabilidades nos sistemas biométricos, como riscos de vazamento, acessos indevidos, armazenamento excessivo ou falhas de anonimização;
    - Monitorar a ocorrência de erros algorítmicos, como falsos positivos ou falsos negativos;
    - Acompanhar a vigência dos consentimentos obtidos dos responsáveis legais e a existência de alternativas menos invasivas;
- Garantir a adequação dos contratos com fornecedores de tecnologia.

A ANPD recomenda a adoção de boas práticas de governança, que incluem:

- Auditorias periódicas internas e externas;
- Registro de logs de acesso e operação dos sistemas;
- Implementação de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD);

- Estabelecimento de indicadores de desempenho e risco (KPIs);
- Atualização contínua dos sistemas, com foco em cibersegurança;
- Capacitação da equipe escolar e técnica.

Em conclusão, assegurar o descarte seguro e o gerenciamento adequado do ciclo de vida dos dados biométricos resguarda a privacidade dos alunos desde o momento em que eles fornecem seus dados até o ponto em que esses dados deixam de existir nos sistemas.

6. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Antes de implementar o tratamento de dados biométricos é recomendável que a instituição de ensino realize uma Avaliação de Impacto à Proteção de Dados Pessoais, também chamada de Relatório de Impacto à Proteção de Dados (RIPD) na LGPD.

Trata-se de um procedimento para mapear riscos aos direitos dos titulares de dados e benefícios do uso de biometria no ambiente educacional.

O art. 5º, inciso XVII da LGPD define o RIPD como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Conforme previsto no art. 38 da LGPD, a ANPD pode solicitar que a instituição de ensino exiba esse Relatório, que deverá conter, por exemplo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, os potenciais riscos relacionados ao tratamento de dados biométricos e as salvaguardas e os mecanismos de mitigação adotados.

Assim, por exemplo, um risco identificado pode ser “uso indevido dos dados por terceiros” e a medida mitigadora correspondente seria “restringir acesso apenas a pessoal autorizado”.

Outro risco pode ser de “invasão do sistema” e a medida correspondente poderia ser “uso de criptografia”.

O Relatório deve justificar a necessidade e a proporcionalidade do uso de dados biométricos em relação à finalidade proposta. Em resumo, a justificativa deverá ser capaz de demonstrar que os benefícios esperados superam os riscos e que não há alternativa menos intrusiva com eficácia equivalente – atendendo assim ao princípio da proporcionalidade.

Essa análise é importante para fundamentar a base legal do tratamento: no caso de dados sensíveis como biometria, a base mais adequada, ao nosso ver, conforme já ponderado nos itens precedentes, é o consentimento do titular (ou do responsável, no caso de menores).

Se a avaliação concluir que o objetivo poderia ser cumprido de outra forma sem tratar dados biométricos, insistir na biometria poderia violar o princípio da necessidade.

6.1. Relatório de Impacto à proteção de Dados de Crianças e de Adolescentes

Merece especial atenção o RIPD que envolve Avaliação de Impacto do Tratamento de Dados Biométricos de Crianças e de Adolescentes, que possui peculiaridades e deve ser realizado visando o melhor interesse desse grupo de pessoas.

Segundo a ICO, melhor interesse envolve segurança, saúde, bem-estar, relações familiares, desenvolvimento físico, psicológico e emocional,

identidade, liberdade de expressão, privacidade, e liberdade para formar suas próprias opiniões e fazê-las ser ouvidas.

Ou seja, deve ser avaliado se o tratamento afeta o desenvolvimento, a autonomia e o direito da criança de brincar, aprender e estar segura, e não apenas sua privacidade de dados.

Segundo recomenda a ICO, são sugeridas consultas, pesquisas e feedbacks dos titulares, inclusive opiniões das crianças e de seus pais ou representantes legais, que devem ser levados em consideração no RIPD.

O RIPD também deve demonstrar o envolvimento do Encarregado de Dados (DPO) e da alta administração na aprovação do projeto, evidenciando accountability (responsabilização).

Recomenda-se incluir no processo a perspectiva de diversas partes: equipe de TI, jurídico, coordenadores pedagógicos (para avaliar impactos no cotidiano escolar) e representantes legais dos titulares menores de 18 anos, se for o caso, para coletar opiniões sobre a aceitação do uso desse tipo de tecnologia.

Em síntese, a segurança e a proteção de dados biométricos requerem uma abordagem abrangente: entender os riscos particulares da biometria, aplicar múltiplas camadas de proteção tecnológica, instituir políticas internas claras e adotar uma postura proativa de compliance (com auditorias e avaliações contínuas).

Assim, a instituição de ensino resguardará não apenas a conformidade com a LGPD e com os padrões definidos na ISO 24745, mas, principalmente, os direitos e a confiança dos alunos e da comunidade.

7. RECOMENDAÇÕES PROVENIENTES DAS DEMAIS NORMAS ISO

As auditorias e políticas de segurança em sistemas biométricos escolares também podem se beneficiar das diretrizes previstas nas normas internacionais da série ISO/IEC 27000 (especialmente as ISO/IEC 27001 e 27701), que fornecem padrões reconhecidos de gestão da segurança da informação e proteção de dados.

Recomenda-se que as instituições de ensino, além das orientações da Norma ISO/IEC 24475/2022 abordadas no presente Guia:

- Implementem controles previstos na ISO/IEC 27001 (Segurança da Informação), como a gestão de acessos, criptografia de dados biométricos e gestão de incidentes de segurança;
- Utilizem a ISO/IEC 27701 como guia para estruturar um sistema de gestão de privacidade da informação (SGPI), garantindo que a proteção de dados sensíveis (como os biométricos) seja integrada à política institucional;
- Realizem auditorias periódicas com base nos controles das normas ISO, incluindo análise de riscos, revisão de políticas e testes de conformidade;
- Adotem a ISO/IEC 30107 (sobre sistemas biométricos e apresentação de ataques), para mitigar riscos específicos como “spoofing”(tipo de fraude digital baseada na falsificação de identidade) e falsificações.

Dessa forma, a adoção de padrões internacionais e a institucionalização de práticas de auditoria contribuem para fortalecer a confiança da comunidade escolar.

8. TRATAMENTO DE INCIDENTES E COMUNICAÇÃO À ANPD

Em caso de incidentes de segurança com dados biométricos, como vazamentos, acessos não autorizados ou uso indevido, que possam causar riscos e danos relevantes aos titulares de dados, as instituições de ensino devem seguir os procedimentos previstos nos arts. 48 e seguintes da LGPD, incluindo:

● Comunicação imediata à ANPD e aos titulares dos dados afetados para que possam adotar providências;
● Registro e documentação do incidente;
● Revisão dos contratos com fornecedores envolvidos.

Segundo dispõe a Resolução CD/ANPD nº 15/2024, no art. 5º, “O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;
II - dados de crianças, de adolescentes ou de idosos;
III - dados financeiros;
IV - dados de autenticação em sistemas;
V - dados protegidos por sigilo legal, judicial ou profissional; ou
VI - dados em larga escala.”

O apontado dispositivo legal estabelece critérios para determinar quando um incidente de segurança pode acarretar risco ou dano relevante aos titulares de dados. Esses critérios incluem a possibilidade de afetar significativamente interesses e direitos fundamentais dos titulares e envolver, pelo menos, um dos tipos de dados citados em seus incisos, dentre os quais destacamos os dados pessoais sensíveis, dados de crianças, adolescentes e dados de autenticação em sistemas.

9. ALTERNATIVAS AO TRATAMENTO DEDADOS BIOMÉTRICOS

Para além da biometria, é importante considerar que existem outras formas de controle de acesso e frequência no ambiente educacional e que devem ser analisadas antes de uma tomada de decisão, pois o contexto em que a instituição está inserida é de extrema relevância.

9.1. **O uso de cartões de identificação com a Frequency IDentification (RFID) ou Identificação por Rádio Frequência:** Trata-se de tecnologia formada por leitores, antenas e etiquetas. As etiquetas se comunicam com o leitor por meio das ondas de rádio, localizando e identificando diversos tipos de objetos. Estes cartões permitem o registro de entrada e saída dos alunos por meio de leitores instalados na escola. Essa tecnologia permite a associar o cartão a um sistema que envie notificações automáticas aos responsáveis cadastrados, permitindo o monitoramento em tempo real. Outra vantagem é a eliminação das chamadas manuais em salas de aula ao enviar um relatório que apresenta os alunos ausentes. Outra funcionalidade é a de permitir a aferição dos horários que os alunos chegam, quais os alunos que chegam atrasados, os locais por onde os alunos passaram na escola em determinado dia e as médias com os horários de chegada e saída destes.

Apesar de eficiente, o cartão RFID possui limitações, como a possibilidade de perdas ou uso indevido por terceiros, o que requer atenção especial no gerenciamento.

9.2. **O uso de registro manual:** O controle por lista de presença física ou por sistemas digitais, também é uma opção. Essa abordagem, embora simples, pode ser adequada para instituições menores ou em contextos em que o investimento em tecnologia avançada não é viável. No entanto, o método manual é mais suscetível a erros humanos e fraudes, como assinaturas falsas.

9.3. **Soluções baseadas em aplicativos e QR Codes,** também, vêm ganhando popularidade, especialmente em instituições que adotam abordagens tecnológicas acessíveis. Nesse modelo, cada aluno possui um código exclusivo que pode ser escaneado no momento da entrada ou saída. Essa solução é prática e econômica, mas pode enfrentar desafios em situações de falhas técnicas ou falta de conectividade.

Apesar da eficácia dessas alternativas, a biometria pode ser uma escolha preferível em determinados contextos. A principal razão para optar por essa tecnologia é a sua precisão e confiabilidade, pois inibe a possibilidade de

fraudes, como compartilhamento de cartões ou assinaturas falsas.

9.4. Quando e por que optar por biometria em vez de outras soluções?

A decisão por adotar biometria deve ser cuidadosamente avaliada, levando-se em consideração aspectos como custo, privacidade e aceitação da comunidade. Escolher a biometria pode ser a melhor opção em instituições que lidam com grandes fluxos de pessoas ou que precisam garantir níveis elevados de segurança. Por outro lado, alternativas mais simples podem ser adequadas para ambientes menores ou com menor grau de complexidade operacional.

Em resumo, a escolha entre biometria e outras formas de controle de acesso e frequência depende das necessidades específicas de cada instituição educacional, bem como de sua capacidade de implementar e gerenciar a tecnologia selecionada. A solução ideal deve sempre equilibrar eficiência, acessibilidade e respeito aos direitos e à privacidade dos indivíduos envolvidos.

10. CONSIDERAÇÕES FINAIS

A crescente adoção de sistemas biométricos no ambiente escolar reflete uma tendência global de incorporação de tecnologias avançadas com o intuito de aprimorar a segurança, a eficiência administrativa e o controle de acesso às instituições de ensino.
No entanto, a implementação dessas ferramentas demanda atenção redobrada às especificidades legais, éticas e técnicas, sobretudo diante da natureza sensível dos dados tratados e da vulnerabilidade das crianças e dos adolescentes quando o tratamento envolve seus dados.

O presente estudo evidenciou que, embora os benefícios da biometria sejam inegáveis — como a precisão na autenticação de identidade, a prevenção de fraudes e a otimização de processos como o controle de frequência —, seu uso deve ser limitado àquilo que for estritamente necessário e proporcional às finalidades legítimas perseguidas.

A coleta e o tratamento de dados biométricos, por sua natureza sensível, estão submetidos às salvaguardas da Lei Geral de Proteção de Dados (Lei nº

13.709/2018), que estabelece, entre outros, os princípios da finalidade, necessidade, minimização, adequação, segurança e transparência.

Adicionalmente, o uso de biometria no ambiente educacional deve ser observado sob a ótica da proteção integral e do melhor interesse da criança e do adolescente, conforme preceitua o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e a Convenção sobre os Direitos da Criança da ONU. Isso impõe que qualquer tecnologia adotada no contexto escolar deve ter como premissa fundamental a proteção dos direitos dos titulares de dados, com especial atenção para evitar discriminação, estigmatização ou qualquer forma de tratamento que comprometa a dignidade dos estudantes.

A título de recomendação, a implementação de sistemas biométricos em instituições de ensino deve observar, no mínimo, os seguintes requisitos: (i) elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto no art. 38 da LGPD, com orientações especiais para Relatórios de Impacto que envolverem o tratamento de dados de Crianças e de Adolescentes, conforme informado no presente Guia; (ii) obtenção de consentimento livre, específico, destacado, informado e inequívoco dos responsáveis legais, quando aplicável; (iii) adoção de medidas técnicas e organizacionais rigorosas para garantir a segurança da informação; (iv) ampla comunicação com a comunidade escolar, com foco na transparência e na educação digital; e (v) previsão de medidas de mitigação de riscos, como revisão periódica dos sistemas e avaliação de viés algorítmico.

Ainda que as soluções biométricas possam representar avanços na gestão escolar, sua adoção não pode se sobrepor à observância dos direitos fundamentais dos titulares dos dados. Tecnologias que operam com base na identificação física e comportamental de indivíduos em tempo real devem ser evitadas em ambientes de ensino, pois envolvem o risco de danos irreversíveis em caso de violação, especialmente se envolverem o uso indevido, vazamentos ou discriminação automatizada. Assim, a biometria deve ser vista como uma ferramenta complementar e não como um fim em si mesma, devendo sua implementação ser precedida de criteriosa análise de proporcionalidade e impacto.

Neste contexto, recomenda-se que o uso da biometria no ambiente escolar seja restrito, preferencialmente, à autenticação e controle de acesso, evitando-se aplicações mais intrusivas, como o monitoramento em tempo real, que poderia configurar uma forma de vigilância indevida.

Além disso, as instituições de ensino devem considerar alternativas tecnológicas menos invasivas para quem se opuser ao uso de biometria, como QR Codes, RFID ou registros manuais, que também poderão ser adotadas se os riscos superarem os benefícios.

Em síntese, o desafio contemporâneo não está em impedir o avanço tecnológico, mas sim em construir uma governança responsável e ética que assegure que esses avanços se fazem em consonância com os direitos fundamentais, em especial com a autodeterminação informativa dos titulares de dados.

O ambiente escolar, por sua natureza pedagógica e formadora, deve ser um espaço de exemplo quanto ao respeito à privacidade, à transparência no uso de tecnologias e à promoção de uma cultura de proteção de dados desde a infância.

A implementação responsável da biometria nas instituições de ensino deve, portanto, ser precedida de diálogo amplo com toda a comunidade escolar, assessoramento técnico-jurídico qualificado, e monitoramento contínuo quanto ao cumprimento das normas legais e éticas. O equilíbrio entre inovação, segurança e direitos fundamentais deve ser o norte para qualquer projeto que envolva o tratamento de dados sensíveis no contexto educacional.

ANEXO I

MODELO DE TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS BIOMÉTRICOS

Uso de Reconhecimento Facial para Acesso à Escola: Sua Escolha, Sua Privacidade.

Prezados pais, mães e responsáveis,

Para aumentar a segurança de nossos alunos na entrada e saída da escola, estamos oferecendo um novo sistema de acesso por reconhecimento facial. Este documento explica como o sistema funciona e como protegemos a privacidade de sua família.

1. O que estamos propondo e por quê?

Nosso objetivo é tornar o acesso à escola mais seguro e ágil. O sistema de reconhecimento facial identifica rapidamente os alunos e as pessoas autorizadas, garantindo que apenas quem tem permissão entre em nosso ambiente. Isso ajuda a evitar o risco de perda ou esquecimento de cartões de acesso e agiliza o fluxo de pessoas, especialmente nos horários de pico.

2. Você está no controle

Sua escolha e seus direitos são nossa prioridade. Por favor, leia com atenção:

- **A escolha é sua:** você pode escolher entre usar o reconhecimento facial ou utilizar o método de acesso alternativo por cartão, sem qualquer prejuízo para o aluno.
- **Você pode mudar de ideia:** é possível cancelar sua autorização (revogar o consentimento) a qualquer momento, de forma simples e rápida. Basta nos comunicar e voltaremos a usar o cartão de acesso ou a biometria, conforme o caso.
- **A opinião do aluno importa:** respeitamos a vontade dos nossos alunos. Se, a qualquer momento, um estudante se sentir desconfortável e se opuser ao uso da biometria, o consentimento dado pelos responsáveis será cancelado.

3. Como funciona, em termos simples

- **O que é um "dado biométrico"?**

É uma informação única do nosso corpo, como a impressão digital ou os traços

do rosto. A lei brasileira (LGPD) considera esse tipo de dado como "sensível" e exige cuidado redobrado em sua proteção.

- **Como o sistema identifica seu filho(a)?**

1. Com a sua autorização, tiramos uma foto digital do rosto do aluno.
2. Um software especializado mede as distâncias entre pontos-chave do rosto (olhos, nariz, boca) e transforma essa medição em um código numérico único, como uma "impressão digital" do rosto.
3. Importante: a foto original não é o que fica armazenado para comparação diária. O sistema armazena e utiliza apenas este código numérico seguro.

- **A escola vai nos vigiar com câmeras? Não!**

O sistema é usado apenas no momento da entrada e da saída para identificar quem está acessando a escola. Não haverá monitoramento por reconhecimento facial em tempo real nos pátios, corredores ou salas de aula.

4. Nossas promessas de privacidade para você

Assumimos um compromisso sério com a proteção dos dados de sua família.

1. **Finalidade única:** seus dados biométricos serão usados exclusivamente para o controle de acesso à escola. Nada mais.
2. **Segurança:** os dados são armazenados em ambiente seguro, seguindo as melhores práticas de segurança da informação para prevenir acessos não autorizados.
3. **Acesso restrito:** apenas um número limitado de profissionais treinados e empresas parceiras especializadas em manutenção de software terão acesso aos dados, e somente quando estritamente necessário para o funcionamento do sistema. Todos estão sob rigorosos contratos de confidencialidade.
4. **Seus direitos garantidos:** você tem o direito de acessar, corrigir ou solicitar a exclusão dos dados a qualquer momento. Nosso Encarregado de Proteção de Dados (DPO) (...inserir nome completo e e-mail) está à sua disposição para atender a qualquer solicitação.
5. **Descarte Seguro:** os dados biométricos serão permanentemente apagados de nossos sistemas em até 90 dias do término do vínculo do aluno com a escola, ou caso você decida cancelar o Consentimento.

5. Sua declaração de escolha

Por favor, marque sua opção abaixo e assine.

Para o(a) estudante menor de 18 anos:

[ ] SIM, DOU MEU CONSENTIMENTO para uso de biometria facial do estudante sob minha responsabilidade para o acesso à escola.
[ ] NÃO DOU MEU CONSENTIMENTO, prefiro que ele use o método alternativo (cartão de acesso).

_____
Nome do Aluno
Nome completo/assinatura do pai, mãe ou do responsável legal
Data: ____/____/_____

Para o estudante maior de 18 anos de idade:

[ ] SIM, DOU MEU CONSENTIMENTO para uso de biometria facial para o acesso à escola.
[ ] NÃO DOU MEU CONSENTIMENTO, prefiro usar o método alternativo (cartão de acesso).

_____
Nome completo e assinatura do aluno maior de 18 anos
Data: ____/____/_____

Nota do INPD para a Instituição de Ensino: *Este documento é um modelo de referência. Antes da sua utilização, é fundamental que a instituição realize uma análise completa de seus próprios processos internos para garantir a plena conformidade com a LGPD, incluindo a elaboração do Registro de Operações de Tratamento de Dados Pessoais e o Relatório de Impacto à Proteção de Dados Pessoais. Enfim, o texto final do termo de consentimento deve ser estruturado com base na realidade de cada instituição de ensino e de acordo com obrigações legais específicas analisadas no presente Guia.*

ANEXO II

Modelo de Política de Tratamento de Dados Biométricos no Ambiente Escolar

1. Objetivo

Esta política tem como objetivo estabelecer diretrizes claras para o tratamento de dados biométricos no ambiente escolar, garantindo a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), a proteção dos direitos dos titulares dos dados e a adoção de medidas técnicas e organizacionais adequadas à segurança da informação.

2. Abrangência

Aplica-se a todos os dados biométricos tratados pela instituição de ensino, incluindo os de alunos, responsáveis, colaboradores, prestadores de serviço e visitantes, para funcionamento dos sistemas de controle de acesso ao espaço escolar.

3. Definições

- Dado biométrico: Informação pessoal sensível que resulta de processamento técnico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa natural.
- Titular: Pessoa natural a quem se referem os dados pessoais.
- Controlador: A instituição de ensino, pois responsável pelas decisões referentes ao tratamento dos dados pessoais.
- Operador: Empresa ou pessoa que realiza o tratamento de dados em nome da instituição de ensino.
- DPO (Data Protection Officer ou Encarregado de Dados): Pessoa indicada pela instituição de ensino para atuar como canal de comunicação com os titulares e a ANPD.

4. Princípios Gerais

O tratamento dos dados biométricos obedecerá aos princípios da finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização.

5. Coleta e Finalidade

A coleta de dados biométricos será realizada exclusivamente para as

finalidades previamente informadas, como controle de acesso às dependências escolares.

Os dados pessoais tratados não poderão ser utilizados para outras finalidades sem o consentimento específico do titular ou responsável legal, salvo hipóteses legais de dispensa.

6. Base Legal

O tratamento de dados biométricos de crianças e adolescentes somente será realizado mediante consentimento específico e em destaque de ao menos um dos pais ou responsável legal, conforme o art. 14 da LGPD.

7. Segurança da Informação

Os dados serão armazenados em sistemas seguros, com criptografia, controle de acesso por autenticação e registro de logs.

O armazenamento local ou em nuvem deverá observar requisitos mínimos de segurança e conformidade com a LGPD.

A instituição de ensino adotará práticas de segurança baseadas nas normas ISO/IEC 27001 e 24745.

8. Armazenamento e Retenção

Os dados serão armazenados apenas pelo tempo necessário para cumprir a finalidade informada, conforme definido em política interna de retenção.

9. Descarte de Dados Biométricos

Ao término da relação com o titular (ex.: desligamento do aluno), os dados serão eliminados de forma segura, mediante técnicas de destruição digital irreversível.

O descarte será documentado, indicando data, método utilizado e responsável pela ação.

10. Compartilhamento

Os dados biométricos não serão compartilhados com terceiros, exceto quando

estritamente necessário para o cumprimento da finalidade, mediante contrato com cláusulas de segurança e confidencialidade, ou por obrigação legal.

11. Direitos dos Titulares

É assegurado aos titulares de dados o exercício dos direitos do art. 18 da LGPD, especialmente:

- Acesso aos dados biométricos;
- Correção ou eliminação;
- Revogação do consentimento;
- Informações sobre compartilhamentos.

12. Treinamento e Conscientização

Todos os colaboradores envolvidos com o tratamento de dados biométricos receberão capacitação contínua sobre boas práticas de segurança e privacidade.

13. Governança e Auditoria

A instituição de ensino manterá registros das operações de tratamento de dados biométricos e realizará auditorias internas e avaliações de impacto à proteção de dados (RIPD).

14. Revisão da Política

Esta política será revisada anualmente ou sempre que houver alterações legislativas, tecnológicas ou operacionais relevantes.

Nota do INPD para a Instituição de Ensino: *Este documento é um modelo de referência. Antes da sua utilização, é fundamental que a instituição realize uma análise completa de seus próprios processos internos para garantir a plena conformidade com a LGPD, incluindo a elaboração do Registro de Operações de Tratamento de Dados Pessoais e o Relatório de Impacto à Proteção de Dados Pessoais. Enfim, o texto final de uma Política somente poderá ser estruturado com base na realidade de cada instituição de ensino e de acordo com obrigações legais específicas analisadas no presente Guia.*

ANEXO III - Vídeo Informativo sobre o Uso de Biometria*

*Produzido com Ferramenta de Inteligência Artificial

REFERÊNCIAS

AUTORITEIT PERSOONSGEGEVENS (AP). Juridisch kader gezichtsherkenning. Autoriteit Persoonsgegevens (AP), 02 maio 2024. Disponível em: https://www.autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning. Acesso em: 10 fev. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Radar Tecnológico: Biometria e Reconhecimento Facial. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 09 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 jan. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 06 jan. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 06 jan. 2025.

BRASIL. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Dispõe sobre o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 01 set. 2025.

CAMPILLO, Rafael. What is a biometric template, and what are its key features? Mobbeel, [s.d.]. Disponível em: https://www.mobbeel.com/en/blog/what-is-a-biometric-template-and-what-are-its-key-features/?utm_source=chatgpt.com. Acesso em: 05 maio 2025.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Comissão Nacional de Informática e Liberdades - autoridade francesa responsável pela proteção de dados e pela liberdade de informação. Disponível em: https://cnil.fr/en. Acesso em: 29 abr. 2025.

CONSELHO DA EUROPA. Convenção 108 +. Decisão do Comité de Ministros da 128ª sessão do Comité de Ministros, Elsinore, 18 de maio de 2018. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 29 abr. 2025.

ESTADO DO PARANÁ. Tecnologia de reconhecimento facial na chamada chega a 1,6 mil colégios da rede estadual. Estado do Paraná, 15 maio 2023. Disponível em: https://www.parana.pr.gov.br/aen/Noticia/Tecnologia-de-reconhecimento-facial-na-chamada-chega-16-mil-colegios-da-rede-estadual. Acesso em: 01 dez. 2024.

EUROPEAN DATA PROTECTION BOARD (EDPB). Orientações 4/2019 relativas ao artigo 25º Proteção de Dados desde a Conceção e por Padrão-Versão 2.0, Adotadas em 20 de outubro de 2020. Disponível em: https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pt.pdf. Acesso em: 15 abr. 2025.

GDPR REGISTER. Biometric Data and GDPR: Key Considerations. GDPR Register, 19 jan. 2025. Disponível em: https://www.gdprregister.eu/gdpr/biometric-data-gdpr. Acesso em: 06 maio 2025.

INFORMATION COMMISSIONER'S OFFICE (ICO). Autoridade de Proteção de Dados Pessoais do Reino Unido. Disponível em: https://ico.org.uk/. Acesso em: 29 abr. 2025.

INFORMATION COMMISSIONER'S OFFICE (ICO). Biometric data guidance: Biometric recognition. ICO, [s.d.]. Disponível em: https://ico.org.uk/media2/uu5jlckw/biometric-data-guidance-biometric-recognition-all-1-0-3.pdf. Acesso em: 20 mar. 2025.

INFORMATION COMMISSIONER'S OFFICE (ICO). Children's code: best interests framework. ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/. Acesso em: 26 jun. 2025.

INFORMATION COMMISSIONER'S OFFICE (ICO). How do we keep biometric data secure? ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/. Acesso em: 06 maio 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Norma ISO/IEC 24745/2022. Segurança da informação, cibersegurança e proteção da privacidade — Proteção de informações biométricas. Disponível em: https://www.iso.org/standard/75302.html. Acesso em: 05 maio 2025.

INTERNATIONAL WORKING GROUP ON DATA PROTECTION TECHNOLOGY. Working Paper on Facial Recognition Technology. International Working Group on Data Protection in Technology, jun. 2023. Disponível em: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2. Acesso em: 30 nov. 2024.

ISRAEL, Carolina Batista; FIRMINO, Rodrigo (coord.). Reconhecimento Facial nas Escolas Públicas do Paraná – Relatório 2023. Curitiba: UFPR, 2023. Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/12/RF_PR_2023.pdf. Acesso em: 01 dez. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). Declaração universal sobre bioética e direitos humanos. Portugal: Unesco, 2006. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000146180_por. Acesso em: 06 jan. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). Relatório do IBC sobre o Princípio da Não Discriminação e Não Estigmatização. Paris: Unesco, 2014. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000221196. Acesso em: 14 dez. 2024.

PREFEITURA DE BETIM. Prefeitura de Betim instala reconhecimento facial nas escolas da rede municipal. Prefeitura de Betim, 02 fev. 2022. Disponível em: https://www.betim.mg.gov.br/portal/noticias/0/3/11327/prefeitura-de-betim-inst ala-reconhecimento-facial-nas-escolas-da-rede-municipal. Acesso em: 10 nov. 2024.

REINO UNIDO. Guia sobre Proteção de Dados biométricos de crianças em escolas e universidades da ICO. Reino Unido, julho de 2022. Disponível em: https://assets.publishing.service.gov.uk/media/62d7d76c8fa8f50c012d14df/Biometrics_Guidance_July_2022.pdf. Acesso em: 10 maio 2025.

TAVARES, C.; SIMÃO, B., MARTINS, F.; SANTOS, B., ARAÚJO, A. Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 06 jan. 2025.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 06 jan. 2025.

UNICEF. Convenção sobre os Direitos da Criança da ONU. Nova Iorque, de 20 de novembro de 1989. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em: 06 jan. 2025.

UNICEF. Guia Data Protection In Schools: Guidance For Legislators, Policy Makers And Schools. Regional Office for Europe and Central Asia: UNICEF, 2024. Disponível em: https://www.unicef.org/eca/media/35876/file/Data%20protection%20in%20schools%20.pdf. Acesso em: 06 jan. 2025.

UODO. Decisão ZSZZS.440.768.2018. Varsóvia, 18 de fevereiro de 2020. Disponível em: https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018. Acesso em: 08 maio 2025.

ZAGONEL, MATEUS VICTORIO; MACHADO, CRISTIAN CLEDER; MÔNEGO, CASSIANO. Tecnologia RFID: Um estudo de caso para controle de acesso em escolas. Revista de Engenharia, Computação e Tecnologia, v. 01, n. 01, p. 31-38, novembro, 2017. Disponível em: https://ppgi.belan.pro.br/iot/Artigos/RFID.pdf. Acesso em: 30 nov. 2024.

INPD
INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS
www.inpd.com.br

Como citar este Guia:

LEAL, Martha; LEHN, Izabela. (Coords.) Guia para uso responsável da biometria no ambiente educacional. Curitiba: Instituto Nacional de Proteção de Dados - INPD, 2025. Disponível em: (citar link) Acesso em: (citar data de acesso ao link).