Agência Nacional de Proteção de Dados
Superintendência de Fiscalização
Coordenação-Geral de Fiscalização
Coordenação de Proteção de Dados Pessoais

Nota Técnica nº 4/2026/CPDP/CGF/SFI/ANPD

1. INTERESSADO

1.1. Secretaria de Estado da Educação do Paraná (SEED/PR).

2. ASSUNTO

2.1. Tratamento de dados pessoais biométricos de crianças e adolescentes pela Secretaria de Educação do Estado do Paraná-PR, por meio da utilização de Tecnologia de Reconhecimento Facial (TRF).

3. REFERÊNCIAS

3.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);

3.2. Regimento Interno da Autoridade Nacional de Proteção de Dados (RI-ANPD), aprovado pela Portaria nº 01, de 08/03/2021;

3.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD (Regulamento de Fiscalização), aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021;

3.4. Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528) (Instauração de Procedimento de Fiscalização);

3.5. Despacho Decisório nº 27/2024/FIS/CGF (0159980).

4. RELATÓRIO

4.1. Em 13/12/2024, foi instaurado o presente processo de fiscalização por meio do Despacho Decisório nº

27/2024/FIS/CGF (0159980), com base na Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528). Esta, por sua vez, foi elaborada a partir de denúncia recebida pela Divisão de Monitoramento (DIM) da Coordenação-Geral de Fiscalização (0131827), no âmbito do Processo de monitoramento nº 00261.004865/2024-50, por meio do qual o denunciante informou emprego de tecnologia de reconhecimento facial (TRF) na rede pública de educação do Estado do Paraná.

4.2. A Divisão de Monitoramento, em 11/09/2024, nos termos do Despacho DIM/CGF/ANPD (0143550), destacou que o Governo do Paraná deixou de encaminhar os documentos solicitados pela Divisão no âmbito do processo nº 00261.004865/2024-50.

4.3. Diante da falta de cooperação da regulada, somado ao fato de que o tratamento de dados pessoais biométricos de crianças e adolescentes consta das prioridades elencadas no Mapa de Temas Prioritários do biênio 2024-2025[1], foi constatada a necessidade de instauração de processo administrativo de fiscalização para apurar os fatos narrados na denúncia.

4.4. Instaurado o processo, foi enviado Ofício nº 5/2025/FIS/CGF/ANPD (0164965) e Anexo (0164967) ao Secretário de Educação do Estado do Paraná em 20/01/2025. Em resposta, a SEED/PR encaminhou e-mail (0174714) e o Processo 23.348.296-0- SEED/PR (0174716) no dia 07/02/2025.

4.5. Tendo os documentos acima mencionados respondido apenas parcialmente as questões da Coordenação de Fiscalização (FIS)[2], foi enviado novo Ofício (0174790) e Anexo (0174918) solicitando complementação de dados à regulada, no dia 14/03/2025. Após insistência dessa Coordenação, a SEED/PR enviou o complemento das respostas via peticionamento eletrônico no sistema SEI/ANPD no dia 02/07/2025, por meio do Processo 23.734.118-0- SEED/PR (0195330).

4.6. É o relatório.

5. ANÁLISE

A) *Objeto da fiscalização*

5.1. Inicialmente, cabe ressaltar que o objeto do presente processo é o tratamento de dados pessoais biométricos (tecnologia de reconhecimento facial - TRF) de alunos da rede pública de ensino do Estado do Paraná, grupo este composto por

crianças e adolescentes em idade escolar.

5.2. O tratamento de dados pessoais biométricos, no contexto da utilização de sistemas de reconhecimento facial para o controle da entrada de pessoas em espaços públicos, já foi objeto de análise pela Coordenação de Fiscalização (FIS). Destaca-se trecho da Nota Técnica nº 5/2025/FIS/CGF/ANPD (0165389), que analisou o tratamento de dados biométricos de torcedores, inclusive de crianças e de adolescentes, por clubes de futebol, em razão do cumprimento de obrigações legais contidas na Lei nº 14.597, de 14 de junho de 2023 - Lei Geral do Esporte (LGE):

> 5.4.1. Os atributos biométricos de determinada pessoa natural, conforme definição do art. 2º, II, do Decreto nº 10.046/2019, podem ser definidos como as **características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar**. Os atributos biométricos dos indivíduos, por definição legal, constituem dados pessoais sensíveis, que, nos termos do artigo 5º, II, da LGPD, se referem ao dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou **biométrico**, quando vinculado a uma pessoa natural.
>
> 5.4.2. A tutela dos dados pessoais sensíveis, ao estar vinculada à tutela da liberdade, da igualdade, e integridade tanto dos indivíduos quanto da coletividade, mostra-se especialmente relevante para a garantia dos direitos e liberdades fundamentais de seus titulares, devendo ser protegidos de forma mais específica e cuidadosa[13], visto que eventual má utilização dessa categoria de dados pode gerar riscos significativos à pessoa humana, podendo ser fonte para preconceitos e discriminações ilícitas e abusivas em face dos titulares[14].
>
> 5.4.3. As tecnologias de reconhecimento facial (TRF), por sua vez, são um dos principais mecanismos utilizados para o tratamento de atributos biométricos, especialmente com vistas ao desenvolvimento de sistemas de identificação que auxiliam no controle e monitoramento de pessoas para diversas finalidades, inclusive segurança pública e o combate a fraudes financeiras[15].
>
> 5.4.4. A análise técnica de atributos biométricos é realizada por meio de ferramenta tecnológica que

permite a *detecção* (descobrir e localizar faces nas imagens e vídeos), a *classificação* (categorizar o indivíduo por meio de atributos como gênero, etnia, raça, idade, alegre, feliz, nervoso etc.), a *verificação* (se a pessoal existe ou está cadastrada?) e a *identificação* (quem é a pessoa da imagem?) de indivíduos específicos ou grupos de pessoas de forma mais rápida e confiável, com base em um conjunto de dados reconhecíveis e verificáveis, que são únicos e específicos sobre seus titulares[16]. O processo de reconhecimento facial é explicado por Canavez da seguinte maneira[17]:

> Para atingir esses objetivos, o mecanismo de processamento das imagens, então, passa por alguns subprocessos, como: (i) aquisição de imagem: captura da face através de uma câmera e sua conversão em formato digital; (ii) detecção de rosto: localização de um rosto na imagem capturada e sua demarcação; (iii) normalização: suavização das variações na imagem, como conversão em tamanho padrão, rotação para adequar o ângulo e distribuição de cores; (iv) extração de características atributo: isolamento e extração de leituras repetíveis e distintas, sendo que o conjunto de características chave pode ser armazenado para ser modelo de referência em uma comparação posterior; (v) registro: se for a primeira vez que um indivíduo mostra o rosto em um sistema de reconhecimento, a imagem e/ou modelo de referência pode ser armazenado como um registro para comparação posterior; por fim, (vi) comparação/análise: medição da similaridade entre o conjunto de características extraídas (amostra) com outro conjunto previamente cadastrado. Essa fase de comparação irá variar conforme a finalidade da tecnologia.
>
> (...)
>
> **É no momento de extração dos atributos (item iv) que são retiradas as informações úteis da face da pessoa para a análise desejada. As informações seriam as características geométricas de forma, localização e distância da boca, olhos, nariz, orelhas, entre outras.** Após esse passo, existem duas possibilidades a depender da finalidade do emprego da tecnologia de reconhecimento facial: (a) descarte imediato dos dados coletados do rosto; ou (b) armazenamento desses dados. A primeira situação seria apenas para os casos em que o objetivo seja gerar relatórios estatísticos sobre os

indivíduos, o que poderia ser usado, por exemplo, para o direcionamento de propagandas para consumidores em tempo real. O não armazenamento dos dados inviabilizaria a comparação entre imagens (sexto subprocesso), portanto, impediria a verificação ou identificação de uma pessoa.

5.4.5. O uso dessa tecnologia, assim, permite que indivíduos sejam automaticamente reconhecidos a partir da criação de uma representação digital da sua face, obtida por meio de fotos ou imagens previamente armazenadas, de maneira a facilitar processos de *verificação* e de *identificação* de determinada pessoa ou grupos[18]. Além disso, ao ser integrada a sistemas de vídeo e vigilância, a tecnologia de reconhecimento facial permite a identificação de indivíduos à distância, sem que as pessoas saibam, inclusive, que estão sendo monitoradas ou tenham que cooperar com o processo de identificação[19]. Para de Teffé[20], os processos de identificação, por meio do uso de dados biométricos, transformam o corpo das pessoas em senhas, como se as suas características físicas únicas fossem o meio de sua individualização.

5.4.6. Embora a LGPD não proíba o uso de sistemas de reconhecimento facial para a identificação de indivíduos, **o emprego dessa tecnologia pelos controladores deve ser feito em estrita consonância com as normas e princípios que regulamentam o tratamento de dados pessoais sensíveis, sempre com o objetivo de assegurar o exercício dos direitos e garantias fundamentais constitucionalmente protegidas.** Isto se deve ao fato de que a categoria de dados pessoais sensíveis se refere a dados pessoais que, em razão de seu conteúdo, podem implicar em risco ou vulnerabilidade potencialmente mais gravosas para o exercício dos direitos e garantias fundamentais pelos seus titulares[21]. Nesse sentido, o uso das tecnologias de reconhecimento facial, em virtude de sua natureza mais invasiva, especialmente quando utilizada em ambientes de controle e monitoramento do público, em que as pessoas não sabem que seus dados biométricos estão sendo coletados e processados em tempo real, pode gerar interferências indevidas nos direitos à privacidade e à proteção de dados pessoais dos titulares[22].

5.4.7. Há de se preocupar, do mesmo modo, com os possíveis efeitos discriminatórios no uso da tecnologia, principalmente em relação a determinados grupos sociais vulneráveis, tendo em vista eventuais erros nos

processos de identificação, derivados do uso de algoritmos com vieses discriminatórios e de bases de dados desatualizadas, resultando em limitações a direitos e garantias fundamentais dos titulares. De acordo com o estudo preliminar "Radar tecnológico: biometria e reconhecimento facial"[23], realizado pela Coordenação-Geral de Tecnologia e Pesquisa (CGTP) da ANPD, um dos principais problemas associados ao uso de tecnologia de reconhecimento facial em contextos de ações de controle, especialmente, nas não limitado à segurança pública, é a manutenção de vieses de tendências discriminatórias que permeiam as relações sociais. Isso ocorre uma vez que vieses e normas sociais e culturais no tratamento dos dados biométricos podem se refletir nos algoritmos e nos modelos de aprendizagem utilizados na tecnologia de identificação biométrica, o que pode resultar em efeitos discriminatórios de ordem social, racial, étnica, econômica, entre outros.

5.4.8. Há, nesses casos, o risco de constrangimento às pessoas em decorrência de falhas de identificação, uma vez que tais sistemas podem apresentar erros de análise combinatória, resultando em um falso-positivo ou falso-negativo, o que implicaria em risco ao exercício de direitos civis e políticos pelos titulares dos dados. Do mesmo modo, a falta de atualização das bases de dados usadas para os procedimentos de verificação pode resultar em situações vexatórias para os indivíduos erroneamente identificados, especialmente nos casos em que o sistema de TRF é utilizado para encontrar pessoas evadidas da Justiça.

5.4.9. O estudo realizado pela CGTP, cita ainda questões que devem ser consideradas na análise sobre uso de tecnologias de identificação baseadas no tratamento de dados pessoais biométricos, em especial o seu impacto no exercício dos direitos à privacidade e à proteção de dados pessoais: (i) o uso secundário dos dados pessoais coletados; (ii) a coleta não informada ao titular; (iii) o uso inadequado do consentimento como hipótese legal; (iv) efeitos discriminatórios e naturalização da vigilância; (v) a acurácia dos sistemas de reconhecimento facial; e (vi) os desafios à segurança da informação.

5.3. Como dito na Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528), a Lei Geral de Proteção de Dados Pessoais (LGPD) não proíbe, à princípio, o tratamento de dados pessoais sensíveis de crianças e adolescentes por agentes de tratamento, mas estabelece regras e princípios específicos para garantir a proteção dos direitos de personalidade desse grupo de titulares vulneráveis. Assim sendo, os agentes de tratamento (controlador

e operador) devem atuar observando os princípios gerais de proteção de dados pessoais, os direitos dos titulares e os mecanismos técnicos, organizacionais e administrativos necessários para a segurança dos dados pessoais.

5.4. Outrossim, **o controlador precisa, antes do início do tratamento, necessariamente, definir a hipótese legal mais adequada à atividade que pretende realizar**. Observe-se, nesse sentido, trecho da Nota Técnica nº 28/2025/FIS/CGF/ANPD (0175984):

> 6.14. (...), ao controlador competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, da LGPD), de maneira que é o agente de tratamento responsável pela definição dos elementos centrais das operações de tratamentos de dados; ou seja, ele é responsável, em última instância, por definir os critérios que orientaram toda a cadeia de tratamento de dados pessoais em uma determinada operação. No contexto da definição da hipótese legal, por exemplo, é possível que um mesmo tratamento possa, em tese, ser embasado em mais de uma das hipóteses legais listadas no art. 7º ou no art. 11 da LGPD. Desse modo, caberá ao controlador ponderar qual hipótese legal será mais adequada à finalidade específica do tratamento.
>
> 6.15. A definição de hipótese legal, desse modo, é uma das decisões mais substanciais a ser tomadas, uma vez que é vedado o tratamento de dados pessoais sem o amparo em uma das hipóteses legais definidas na Lei. Isso ocorre uma vez que a definição da hipótese legal restringe os casos de utilização de dados pessoais pelo controlador, de maneira a proteger preventivamente os direitos e as liberdades dos titulares[3]. É importante ressaltar, nesse sentido, que tal definição tem relação direta com o dever de lealdade que o controlador deve ter para com os titulares de dados afetados, especialmente quando o tratamento estiver amparado na hipótese legal do consentimento.
>
> 6.16. O controlador, além disso, deve definir a hipótese legal mais adequada à finalidade do tratamento proposto antes do início da respectiva operação de tratamento[4], visto que o caráter ex ante do modelo regulatório de proteção de dados pessoais adotado pela legislação brasileira caracteriza-se essencialmente pela exigência prévia de requisitos para o tratamento de dados (racionalidade preventiva)[5]. Isso porque cada hipótese legal possui condições de validade específicas que podem ser determinantes para se avaliar, por exemplo, eventual imposição de limites ao exercício de direitos pelos titulares no caso concreto, bem como condições

específicas para a realização do tratamento.

6.17. A definição da hipótese legal antes do início da operação de tratamento, como já ressaltado, ademais, é fundamental para atender as legítimas expectativas dos titulares de dados na sua relação com o agente de tratamento[6]. O controlador, desse modo, ao estabelecer as condições de validade de determinada operação de tratamento, por meio da definição da hipótese legal que a fundamentará, atrai para si, em sua relação jurídica com o titular, as responsabilidades associadas aos requisitos legais de validade inerentes à hipótese legal escolhida. Apenas a título de exemplo, iria de encontro ao princípio da boa-fé, conforme o art. 6º, caput, da LGPD, se o controlador negasse pedido do titular de revogação do consentimento anteriormente concedido para determinado tratamento alegando que a mesma operação, na verdade, também estaria fundamentada no seu legítimo interesse. A identificação da hipótese legal mais adequada, antes do início da operação de tratamento, assim, deve estar fundamentada na finalidade do tratamento e na relação de confiança estabelecida pelo controlador com o titular[7].

5.5. Em relação a dados pessoais sensíveis, o art. 11 da LGPD define expressamente as hipóteses legais que autorizam o tratamento de dados dessa natureza:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

5.6. A seção III da LGPD, por sua vez, é dedicada ao tratamento de dados pessoais de crianças e adolescentes. Seu art. 14[3], caput, explicita que o tratamento dos dados desses titulares deverá ser realizado sempre em seu melhor interesse e, em se tratando de dados pessoais sensíveis, deve ter por base o art. 11 da LGPD.

5.7. Além da definição de hipótese legal adequada, para que determinada atividade de tratamento de dados pessoais seja considerada legítima, o agente de tratamento deve observar os princípios gerais de tratamento de dados pessoais, como finalidade, adequação, necessidade, transparência, prestação de contas, dentre outros.

5.8. Para mais, o art. 23, I e III, da LGPD impõe à Administração Pública deveres adicionais de transparência e de vinculação do tratamento de dados ao interesse público. O tratamento de dados pessoais sensíveis pelos órgãos estatais deve ser orientado à execução de competências legais, observando-se a finalidade pública, a necessidade e a proporcionalidade da medida. A lei estabelece, ainda, que a entidade pública deve disponibilizar em veículos de fácil acesso informações claras e atualizadas acerca da previsão legal, da finalidade e dos procedimentos utilizados para o tratamento, de modo a assegurar controle social e *accountability*.

5.9. Deve-se, igualmente, ressaltar que o tratamento de dados pessoais biométricos de alunos da rede pública do Estado do Paraná pode ser considerado como uma atividade de tratamento de alto risco[4], de acordo com o art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte aprovado pela Resolução CD/ANPD nº 2/2022, já que se configura como tratamento em larga escala[5], que pode afetar significativamente interesses e direitos fundamentais dos titulares pela utilização de dados pessoais sensíveis de crianças e adolescentes[6].

B) Hipótese legal do tratamento

B.1) Da definição de hipótese legal pelo

controlador

5.10. A ANPD tem se posicionado sobre a necessidade de o controlador definir **apenas uma hipótese legal para uma mesma finalidade do tratamento**[7]. Assim, deve o agente, antes de iniciar qualquer operação de tratamento de dados pessoais, definir a hipótese legal mais adequada para a consecução das finalidades pretendidas, já que cada hipótese legal possui condições próprias de validade, bem como requisitos específicos para a realização do tratamento.

5.11. Embasar o tratamento em apenas uma hipótese legal para uma mesma finalidade é essencial para proteger a legítima expectativa do titular na sua relação com o agente de tratamento. Isto porque, cada hipótese legal traz em si características que podem ser determinantes para se avaliar, no caso concreto, eventual imposição de limites ao exercício de direitos pelos titulares. Seria desarrazoado, por exemplo, que o titular revogasse o consentimento em determinado tratamento e, em seguida, o controlador rejeitasse tal negativa, informando que possui outra hipótese legal que justifique o tratamento[8]. A definição da hipótese legal pelo controlador estabelece o contexto em que ele se relacionará com os titulares de dados, essa escolha vincula tanto o titular de dados quanto o controlador, respectivamente no que concerne aos direitos do primeiro e os deveres do segundo.

5.12. Dessa forma, a identificação da hipótese legal deve estar fundamentada na finalidade do tratamento e na relação estabelecida pelo controlador com o titular[9], de forma clara e transparente, desde o início da relação entre as partes.

5.13. No caso em análise, conforme informado pela SEED-PR, o tratamento de dados pessoais biométricos de crianças e adolescentes no âmbito escolar público daquele estado foi determinado pela Resolução GS/Seed nº 2.865, de 08/05/2023, publicada no Publicado no Diário Oficial nº 11.415 de 10/05/2023 (0195330, p. 12).

5.14. Inicialmente, e mesmo antes de adentrar na análise do referido texto normativo, tem-se possível conflito de informações, uma vez que, segundo a denúncia que deu origem a esse processo (0133059), o tratamento de dados pessoais de crianças e adolescentes pela SEED-PR teria se iniciado no ano de 2021, e não em 2023, como afirmado pela regulada.

5.15. Segundo a denúncia (0133059), a Resolução SEED nº

2.953, de 07/07/2021, teria sido utilizada para iniciar o tratamento de dados biométricos dos alunos das escolas estaduais do Paraná, ao estabelecer “uma primeira fase” em “instituições-piloto”, atrelada ao sistema “Registro de Classe Online (RCO)”.

5.16. Ainda segundo a denúncia (0133059), o sistema teria sido instituído definitivamente por meio do “Livro Registro de Classe (LRC)” e “Livro Registro de Classe Online (LRCO)”, com a edição da Resolução SEED 3.550, de 23/06/2022, que, por seu turno, não mencionava o registro de frequência por TRF[10].

5.17. A regulada, ao ser questionada sobre a hipótese legal de tratamento, apenas apresentou que o uso da TRF teria sido estabelecido de modo permanente — e não mais como “piloto” — em maio de 2023, a partir da Resolução GS/SEED nº 2.865, quando os docentes passaram a ser “obrigados” a registrar a frequência escolar pelo “cadastro biométrico facial dos estudantes utilizando o aplicativo Escola Paraná Biometria”. Em outro momento, a regulada afirmou que a coleta de dados pessoais biométricos de crianças e adolescentes pela SEED-PR se iniciou a partir do Aditivo Contratual assinado com a Celepar (Companhia Paranaense de Informática), em 26/08/2023, e que o lapso temporal apresentado na denúncia se referia ao “processo de Contratação entre Celepar e Valid, como sendo de 2020” (0195330, p. 43).

5.18. Ainda sobre o tópico, foi informado que **o escopo do tratamento é o processamento das imagens dos estudantes para fins de Registro de Frequência Escolar**, por meio da captura de 3 fotos de cada estudante (cadastro) e registro de frequência diário, capturadas pelo professor por meio de fotos da turma. Além das imagens, afirmou a regulada que a Celepar tem acesso a dados como Código Geral de Matrícula do aluno (CGM), frequência escolar, fotos individualizadas e fotos da turma capturadas em sala de aula, além dos dados gerais da escola e da turma (0174716, p. 32). Além da SEED-PR e Celepar, uma terceira empresa – Valid - foi contratada para atuar no processamento de dados pessoais biométricos dos estudantes, por meio de processo licitatório. Esta empresa teria acesso aos seguintes dados pessoais: imagem individual do estudante; Código Geral de Matrícula (CGM) que identifica o estudante no Sistema Estadual de Registro Escolar (SERE); e registro de frequência na turma (0174716, p. 32).

5.19. Em termos numéricos, foi afirmado que a operação

de tratamento de dados pessoais abrangia, em 2021, 2.136 Instituições de Ensino, aproximadamente (01) um milhão de estudantes na escolarização básica e mais de 100 mil colaboradores (0174716, p. 33). Não foi apresentado, porém, o quantitativo de dados tratados no ano de 2023 ou atualmente, não tendo sido também explicada ou detalhada a fase-piloto e sua transição para o modelo atual.

5.20. No Relatório de Impacto à Proteção de Dados Pessoais – RIPD (0174716 p. 27/40) enviado pela SEED-PR, elaborado em janeiro de 2021, a finalidade do tratamento foi definida como "*estrito cumprimento de obrigação legal ou regulatória, assim como à execução de políticas públicas educacionais, neste caso em específico para cumprimento da regulamentação de registro de frequência escolar, primando pela segurança e direito à escolarização de todos os estudantes*" (0174716, p. 34). Enfatiza, contudo, que a "*finalidade principal do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*" (0174716, p. 34).

5.21. Continuando, o mesmo documento (RIPD) reafirma, em seguida, que a "*automatização da chamada escolar visa cumprir uma obrigação legal e regulatória do controlador*", o que dispensaria o consentimento do titular de dados (0174716, p. 35). Assevera, ainda, que a partir do ano de 2021, o requerimento de matrícula serviria como "*ciência das ações de tratamento de dados*" aos pais e responsáveis:

> Venho, através deste, requerer matrícula para o(a) aluno(a) supracitado(a) declarando estar de acordo com as disposições do Regimento Escolar do Estabelecimento e demais normas complementares. Declaro que em atendimento a Lei n.º 13.709/2018, **estou de acordo e autorizo o uso da imagem e dos registros do(a) aluno(a) nos Sistemas Estaduais de Educação** para fins pedagógicos e estatísticos da SEED, para declaração do Censo Escolar, para planejamento e execução de políticas públicas e atendimento à rede de proteção (0174716, p. 35) Grifo nosso.

5.22. Após o que, o RIPD aponta como hipótese legal do tratamento o art. 7º, II e III da LGPD (0174716, p. 36). Quando questionada diretamente por esta ANPD sobre o tópico, a regulada disse que:

> o tratamento de dados biométricos realizado pela SEED fundamenta-se nas seguintes hipóteses legais previstas na LGPD:

> a) Execução de políticas públicas (Art. 7º, inciso III e Art. 11, inciso II, alínea "a" da LGPD): o reconhecimento facial é utilizado para otimizar a gestão educacional e garantir a precisão no registro de frequência dos estudantes;
>
> b) Proteção da criança e do adolescente (Art. 14 da LGPD): a tecnologia contribui para um acompanhamento mais eficaz da assiduidade escolar, permitindo que gestores adotem medidas para a permanência dos alunos na escola;
>
> c) Cumprimento de obrigação legal ou regulatória (Art. 11, inciso II, alínea "a" da LGPD): os registros de frequência são fundamentais para o cumprimento de normas educacionais, incluindo programas de assistência estudantil e prestação de contas. (0174716, p. 86)

B.2) Da inadequação da hipótese legal definida pela SEED/PR com a LGPD

5.23. A partir do apresentado no item B.1, vê-se algumas desconformidades a respeito da definição da hipótese legal que autoriza o tratamento de dados biométricos de alunos da rede de educação pública do Paraná com as normas de proteção de dados pessoais brasileiras.

5.24. Primeiramente, a controladora definiu mais de uma hipótese legal para justificar o tratamento de dados para uma mesma finalidade, sem qualquer justificativa; em seguida, deixou de apresentar definição precisa dos normativos que imporiam a ela a necessidade do tratamento de dados pessoais biométricos para o cumprimento de obrigação legal ou regulatória do controlador (art. 11, II, a, da LGPD); por fim, apresentou hipótese legal não aplicável ao tratamento de dados pessoais sensíveis, bem como hipótese legal inexistente (art. 7º, III, e art. 14 da LGPD).

5.25. Como exposto nesta Nota, e de acordo com o art. 5º, II, da LGPD, os dados pessoais biométricos são considerados como dados pessoais sensíveis, requerendo hipótese de tratamento **necessariamente** baseada no art. 11 da LGPD. A regulada, neste sentido, afirmou que a aplicação da Resolução GS/SEED nº 2.865, de 08/05/2023, entre outros, se apoia na hipótese legal de tratamento prevista no art. 11, II, a, da LGPD, ou seja, quando o tratamento de dados pessoais seria indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador.

5.26. De acordo com o “Guia orientativo: tratamento de dados pessoais pelo Poder Público”, editado pela ANPD, a

aplicação do art. 11, II, a, da LGPD pode decorrer de dois contextos normativos distintos, cuja diferenciação reside na natureza da norma que estabelece a obrigação a ser cumprida.

5.27. O primeiro contexto é o das **normas de conduta**, que impõem obrigações específicas de comportamento, acompanhadas de sanções em caso de descumprimento. Nessas hipóteses, o tratamento de dados pessoais é necessário para viabilizar o cumprimento de uma determinação legal expressa ou de obrigação regulatória, ainda que não haja relação direta e necessária com o exercício das atribuições típicas do órgão controlador.

5.28. O segundo contexto é o das **normas de organização**, que estruturam órgãos e entidades públicas e definem suas competências e atribuições. Nesses casos, o tratamento de dados pessoais é intrinsecamente ligado à própria execução de prerrogativas estatais e ao cumprimento das finalidades públicas da entidade. Diferentemente das normas de conduta, que disciplinam obrigações pontuais e preveem consequências jurídicas para seu descumprimento, as normas de organização condicionam o tratamento de dados à realização das funções típicas da Administração, sendo pressuposto necessário para a execução de políticas públicas.

5.29. Examinando o conteúdo da Resolução GS/SEED nº 2.865/2023, observa-se que o ato normativo, subscrito pelo Secretário de Educação do Estado do Paraná, determina que o registro de frequência escolar seja realizado, prioritariamente, por meio de reconhecimento facial biométrico, e estabelece o cadastramento obrigatório dos estudantes no aplicativo “Escola Paraná Biometria”. Vejamos:

> Art. 1.º Determinar que a frequência dos estudantes das instituições de ensino da rede estadual seja registrada no horário da aula, no Livro Registro de Classe Online – LRCO, mediante reconhecimento facial biométrico.
>
> Parágrafo único. O reconhecimento facial biométrico é um sistema de identificação que, a partir da captura de imagem do rosto, permite comprovar a identidade do estudante e sua frequência escolar.
>
> Art. 2.º Alterar o § 4.º do art. 2.º da Resolução GS/SEED n.º 3.550, de 23 de junho de 2022, que passa a constar conforme segue:
>
> > § 4.º O docente tem acesso a 1 (um) Livro Registro de Classe Online por turma/componente curricular, com listagem de estudantes matriculados no

> Sistema Estadual de Registro Escolar – SERE, no qual deve registrar a frequência mediante reconhecimento facial biométrico no horário da aula, assim como o conteúdo por aula e por componente curricular, de acordo com o planejamento inserido pela mantenedora, além de notas ou pareceres descritivos, em conformidade com o sistema de avaliação da instituição de ensino.
>
> Art. 3.º As instituições de ensino da rede estadual deverão efetuar o cadastro biométrico facial dos estudantes utilizando o aplicativo Escola Paraná Biometria.
>
> Parágrafo único. A forma de utilização do reconhecimento facial e do cadastro biométrico facial dos estudantes será disciplinada por orientação própria.
>
> Art. 4.º Em caso de instabilidade de rede lógica e de internet ou de outras excepcionalidades técnicas identificadas no momento da aula, será possível ao docente realizar o registro manual da frequência escolar no LRCO.
>
> Parágrafo único. O registro manual no LRCO permanecerá liberado, por tempo determinado, exclusivamente para atender às instituições de ensino que apresentarem limitações técnicas, até que sejam disponibilizadas todas as condições necessárias para o registro da frequência escolar mediante reconhecimento facial.

5.30. Trata-se, portanto, de ato administrativo normativo que **cria dever específico aos alunos** da rede estadual de ensino: submeter-se ao cadastramento biométrico como condição para a realização da matrícula[11]. No entanto, não existe norma que tenha criado obrigação legal ou regulatória à Secretaria de Educação, ou mesmo ao Estado do Paraná, a respeito da coleta e tratamento de dados pessoais biométricos de crianças e adolescentes como condição para matrícula escolar. Consequentemente, não se pode falar em “cumprimento de obrigação legal ou regulatória pelo controlador”, mas sim de eventual “tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos” (art. 11, II, b, da LGPD).

5.31. Ressalte-se que a própria Resolução GS/SEED nº 2.865/2023 reconhece a possibilidade de registro manual da frequência em situações de instabilidade técnica, o que indica que o uso do reconhecimento facial não é indispensável ao cumprimento do dever de controle de presença em sala de aula.

Esse dado é relevante para a análise de proporcionalidade, uma vez que, se há meios menos invasivos para se alcançar a finalidade administrativa, o tratamento biométrico pode ser considerado excessivo ou desnecessário, violando o princípio da minimização de dados, conforme o disposto no art. 6º, III, da LGPD, especialmente nos casos que envolvem a proteção conferida pelo art. 14 da própria LGPD aos dados de crianças e adolescentes.

5.32. De mais a mais, a regulada também afirmou que realiza o tratamento de dados biométricos dos alunos da rede pública de ensino com fundamento no art. 7º, inciso III, da LGPD. Nesse sentido, o reconhecimento facial seria utilizado para otimizar a gestão educacional e garantir a precisão no registro de frequência dos estudantes no âmbito da execução de política pública estadual.

5.33. O legislador, ao dispor no art. 7º, III, da LGPD, conferiu hipótese legal de maior amplitude para o tratamento de dados pessoais, permitindo que os entes públicos realizem esse tipo de tratamento sempre que necessário à implementação de políticas públicas **previstas em leis ou regulamentos**, bem como quando respaldadas em **contratos, convênios ou instrumentos congêneres**. Trata-se, portanto, de hipótese de legitimação que admite como fundamento não apenas a lei em sentido formal, mas também atos normativos secundários e instrumentos de cooperação administrativa, desde que voltados à persecução do interesse público.

5.34. Diversamente, **o tratamento de dados pessoais sensíveis encontra-se submetido a regime jurídico mais restritivo**. O art. 11, II, b, da LGPD, ao disciplinar o tratamento desses dados para a execução de políticas públicas, condiciona sua legitimidade à **existência de lei ou regulamento**, vedando, portanto, a utilização de instrumentos meramente negociais ou de atos administrativos destituídos de caráter normativo como fundamento jurídico suficiente. Essa diferenciação legislativa revela a opção do ordenamento por uma tutela reforçada aos dados pessoais sensíveis, exigindo que a Administração Pública disponha de um fundamento legal robusto, específico e previamente estabelecido, apto a conferir previsibilidade e segurança jurídica aos titulares. Nesse sentido, observe-se o trecho de doutrina especializada[12]:

> Para os dados sensíveis, existe a exigência adicional de que apenas políticas públicas baseadas em leis ou

> regulamentos podem justificar o tratamento, o que mostrar o maior rigor com que a LGPD protege tais dados. No caso de dados pessoais 'não sensíveis', basta que a política pública esteja respaldada em contratos (em que há interesses opostos e diversos), convênios (em que interesses paralelos e comuns) ou instrumentos congêneres. (...)
>
> Para os dados sensíveis, a LGPD exige igualmente o cumprimento de uma obrigação adicional: que os órgãos ou entidades públicas deem publicidade à dispensa de consentimento para o seu tratamento, informando os titulares, de forma clara e atualizada, em veículos de fácil acesso, preferencialmente em seus sites, a respeito da previsão que autoriza o tratamento, da finalidade para a qual ele é realizado (art. 11, § 2º), bem com os procedimentos e práticas utilizados para tanto.

5.35. Nesse contexto, o tratamento de **dados biométricos**, especialmente de crianças e adolescentes, para a execução de políticas públicas pela Administração, não pode estar ancorado exclusivamente em atos administrativos secundários de caráter infralegal, cuja natureza precária seria incapaz de oferecer o mesmo nível de proteção aos direitos fundamentais dos titulares, conforme definido pelo Congresso Nacional. A utilização de tais instrumentos como base exclusiva poderia ensejar discricionariedade excessiva por parte de autoridades públicas que, atuando simultaneamente como legisladores e como controladores de dados em estruturas descentralizadas, poderiam ampliar ou restringir de forma desproporcional o espectro de dados sensíveis tratados, afetando de forma desarrazoada o exercício de direitos fundamentais pelos administrados.

5.36. Impõe-se, assim, que o tratamento de dados pessoais sensíveis, quando justificado pelo art. 11, II, b, seja ancorado em **normas hierarquicamente superiores**[13], preferencialmente lei formal ou regulamento editado por autoridade competente nos estritos limites da delegação legislativa. Apenas dessa forma será possível assegurar o equilíbrio entre a execução eficiente de políticas públicas e a proteção do núcleo essencial dos direitos fundamentais à intimidade, à privacidade e à autodeterminação informativa.

5.37. A Resolução GS/SEED nº 2.865/2023, portanto, não é instrumento legal adequado para legitimar o tratamento em larga escala de dados pessoais biométricos de crianças e adolescentes com fundamento na execução de política pública

governamental, nos termos do art. 11, II, b, da LGPD, por se tratar de ato administrativo secundário de caráter infralegal.

5.38. Por outro lado, ainda que se considerasse que a Resolução GS/SEED nº 2.865/2023, enquanto ato administrativo secundário de caráter infralegal, poderia fundamentar o tratamento de dados pessoais sensíveis com base no art. 11, II, b, da LGPD, a medida se mostra claramente desproporcional para a finalidade que se pretende alcançar. Assim, ainda que a Resolução GS/SEED nº 2.865/2023 seja formalmente válida e derive de competência atribuída pela Lei Estadual nº 21.352/2023, permanece a necessidade de verificar se o ato é proporcional, necessário e adequado ao fim almejado, e se existe previsão legal suficiente para autorizar o tratamento em larga escala de dados biométricos de estudantes, visto a exigência do art. 11, II, b, da LGPD de haver lei ou regulamento que crie uma política pública que exija o tratamento compartilhado de dados pela Administração Pública.

5.39. O princípio da necessidade (minimização de dados), nos termos do art. 6º, II, da LGPD, dispõe que o tratamento deve se ater ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Nesse sentido, o princípio da necessidade impõe ao controlador o dever de limitar o tratamento somente aos dados indispensáveis e verdadeiramente pertinentes ao tratamento que realiza[14].

5.40. Assim, caso a hipótese legal informada pelo agente de tratamento seja **inadequada** para o cumprimento da finalidade específica para a qual os dados pessoais foram coletados, a atividade de tratamento poderá ser considerada incompatível com a LGPD. Nesse sentido, é questionável a obrigatoriedade da coleta de dados biométrico quando da existência de sistemas de registro de frequência menos intrusivos para a privacidade dos alunos (DE TEFFÉ, 2022). Além disso, a coleta indiscriminada de dados biométricos de crianças e adolescentes, quando havia meios menos invasivos para se chegar à mesma finalidade do tratamento, pode resultar em riscos desproporcionais para o público infanto-juvenil. Nesse sentido, observe-se trecho da Nota Técnica nº 5/2025/FIS/CGF/ANPD (0168655):

> 5.9.15. Conforme adverte de Teffé, o processo de datificação das pessoas naturais, por meio da coleta de

seus dados biométricos desde o nascimento, permite que seja possível realizar o rastreio, o monitoramento e uma profunda análise das pessoas tanto pelo setor público quanto pelo privado. Assim, seria possível implementar sofisticados sistemas de vigilância e controle sob a população, o que levantaria preocupações quanto à possibilidade de rastreamento das pessoas e discriminações. Ademais, os dados pessoais biométricos da face correspondem a um dos principais atributos da personalidade desses titulares, por justamente distingui-los de outras pessoas. A coleta indevida desses dados, portanto, não apenas viola o direito fundamental à privacidade, mas também contraria os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), que visam garantir a integridade, a identidade e a dignidade dos titulares dos dados, especialmente aqueles pertencentes a grupos vulneráveis.

5.9.16. Por conseguinte, ainda que se considere a aplicabilidade de outra hipótese legal para o tratamento de dados biométricos de crianças e adolescentes menores de 16 (dezesseis) anos de idade, deve-se questionar a proporcionalidade de eventual obrigatoriedade do cadastramento biométrico desse grupo de titulares como condição à entrada e permanência em estádios de futebol.

5.9.17. O Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), órgão competente para, dentre outros, editar orientações e recomendações sobre a aplicação do Estatuto da Criança e do Adolescente, recentemente publicou a Resolução CONANDA nº 245, de 5 de abril de 2024, que dispõe sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital. De acordo com o art. 16 da Resolução, qualquer tipo de **mecanismo de vigilância**, como é o caso de sistemas de **monitoramento com uso de reconhecimento facial, e monitoramento digital de crianças e adolescentes**, associado a ferramentas de automação e tratamento de dados pessoais, deve respeitar o direito desse grupo à privacidade e **não deve ser utilizado de forma indiscriminada e injustificável**. Ademais, o parágrafo único do dispositivo aduz que **devem ser priorizados sempre os meios menos invasivos de tratamento de dados pessoais quando utilizados mecanismos de segurança**. Tais dispositivos vão ao encontro dos princípios da adequação e da necessidade, previstos no art. 6º, II e III, LGPD:

(...)

5.9.18. Portanto, para além da inexistência de obrigação

> legal específica para tal prática, em análise preliminar, **entende-se que o cadastramento biométrico deste grupo vulnerável se mostra desnecessário**, tendo em vista a existência de alternativas menos invasivas que possam assegurar, simultaneamente, os direitos à proteção de dados pessoais e à privacidade de crianças e adolescentes e a sua segurança nos eventos esportivos. Nesse sentido, **é de extrema relevância que sejam pensadas alternativas alinhadas com os princípios da minimização de dados e proporcionalidade estabelecidos pela LGPD, reduzindo os riscos de violação de privacidade e uso indevido de dados pessoais de crianças e adolescentes.**

5.41. Em outro, a regulada apresentou como hipótese legal de tratamento de dados biométricos o art. 14 da LGPD. Como já ressaltado nesta Nota Técnica, a definição das hipóteses legais que autorizam o tratamento de dados pessoais encontra-se disposta de forma **taxativa** nos arts. 7º e 11 da LGPD. O art. 14 da LGPD, por sua vez, estabelece um regime jurídico especial para o tratamento de dados pessoais de crianças e adolescentes, reforçando a tutela conferida a esse grupo vulnerável e condicionando o tratamento ao atendimento do **melhor interesse** da criança ou do adolescente. O dispositivo não cria, por si só, uma hipótese legal autônoma de tratamento, mas impõe requisitos adicionais e complementares às hipóteses legais previstas nos arts. 7º e 11 da LGPD.

5.42. Diferentemente de uma hipótese legal de tratamento - que constitui fundamento jurídico direto e independente para legitimar a atividade de tratamento - o art. 14 funciona como uma cláusula de proteção reforçada, impondo salvaguardas adicionais para o tratamento de dados pessoais de crianças e adolescentes. Assim, para tratar dados de crianças ou adolescentes, o controlador deverá identificar previamente uma hipótese legal adequada, mas também comprovar que observou os requisitos específicos do art. 14, especialmente a demonstração de que o tratamento atende ao melhor interesse do menor.

5.43. É nesse sentido que a ANPD publicou o **Enunciado CD/ANPD nº1/2023**, com o objetivo de uniformizar a interpretação da LGPD quanto às hipóteses legais que autorizam o tratamento de dados pessoais de crianças e adolescentes. De acordo com o Enunciado,otratamento de dados pessoais de crianças e adolescentes pode ser realizado com base nas hipóteses legais previstas na LGPD, como nos casos de

consentimento fornecido pelo titular, de cumprimento de obrigação legal, de proteção à vida ou de atendimento a interesse legítimo do controlador. Em qualquer situação, **omelhor interesse da criança e do adolescente deve prevalecer, exigindo avaliação cautelosa por parte do controlador.** Vejamos:

> Enunciado CD/ANPD nº1/2023
>
> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

5.44. **O art. 14 da LGPD, desse modo, não é uma hipótese legal, mas um parâmetro normativo de validade e legitimidade do tratamento, funcionando como filtro interpretativo e limitador da atuação do controlador.** A inobservância desses requisitos, ainda que haja base legal invocada, pode tornar o tratamento ilícito, por violação ao regime jurídico protetivo diferenciado conferido a crianças e adolescentes pelo ordenamento.

5.45. Por fim, vale ressaltar que a regulada exige dos pais ou responsáveis de seus alunos a assinatura de um "Termo de Consentimento"[15]. Porém, deve-se questionar o fato de que a SEED/PR impõe o consentimento de pais ou responsáveis para a coleta biométrica, sendo que, na verdade, ela se baseia em hipótese legal que prescinde do consentimento parental. Esta atitude do controlador descumpre o dever de lealdade para com os titulares, pois presta informações sabidamente equivocadas, a despeito do princípio da boa-fé objetiva que deveria guiar os atos da Administração Pública. Nesse sentido, é importante destacar que o cumprimento das obrigações de transparência perante os pais ou responsáveis dos alunos não deve se confundir com a hipótese legal do consentimento.

C) Medidas de segurança

5.46. Apesar de se ter determinado, no tópico acima, a respeito da irregularidade do tratamento por ausência de hipótese legal adequada, é importante que seja observado se o tratamento de dados pessoais biométricos de crianças e adolescentes no âmbito escolar do estado do Paraná atende aos demais requisitos impostos pela LGPD, especialmente em relação ao cumprimento dos seus princípios e medidas mínimas de

segurança a serem respeitadas.

5.47. Deve-se ressaltar, inicialmente, que a existência de riscos é algo inerente ao tratamento de dados pessoais, especialmente em se tratando de dados pessoais sensíveis. Tal característica impõe aos agentes de tratamento o dever de adotar medidas técnicas, administrativas e de governança de dados suficientes para proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, consoante os artigos 46 e 47 da LGPD.

5.48. As medidas a serem adotadas pelo controlador devem ser proporcionais aos riscos associados às atividades de tratamento que desenvolve, justamente com o objetivo de mitigar eventuais danos sofridos pelos titulares afetados que sejam decorrentes de incidentes de segurança[16], mau uso dos dados etc. A regulada reconhece tal fato em seu RIPD, ao dizer que “não se pode garantir a eliminação total dos riscos” de tratamento (0174716, p. 29).

5.49. Em termos práticos, diante do alto risco da atividade de tratamento em análise, compreende-se que, entre os requisitos mínimos de segurança que devem ser observados pela regulada, inclui-se a adoção de controles de acesso lógico rigorosos aos dados biométricos, como senhas robustas e autenticação multifator para operadores autorizados.

5.50. Deve-se, do mesmo modo, assegurar a criptografia dos dados biométricos tanto em repouso quanto em trânsito, prevenindo interceptações ou vazamentos. É essencial manter registros detalhados e mecanismos de auditoria recorrente de todos os acessos e operações realizados sobre os dados biométricos, viabilizando o rastreamento e a responsabilização em caso de incidentes. Uma política de retenção de dados clara também deve ser definida, prevendo a eliminação segura dos dados assim que a finalidade for atingida ou deixarem de ser estritamente necessários.

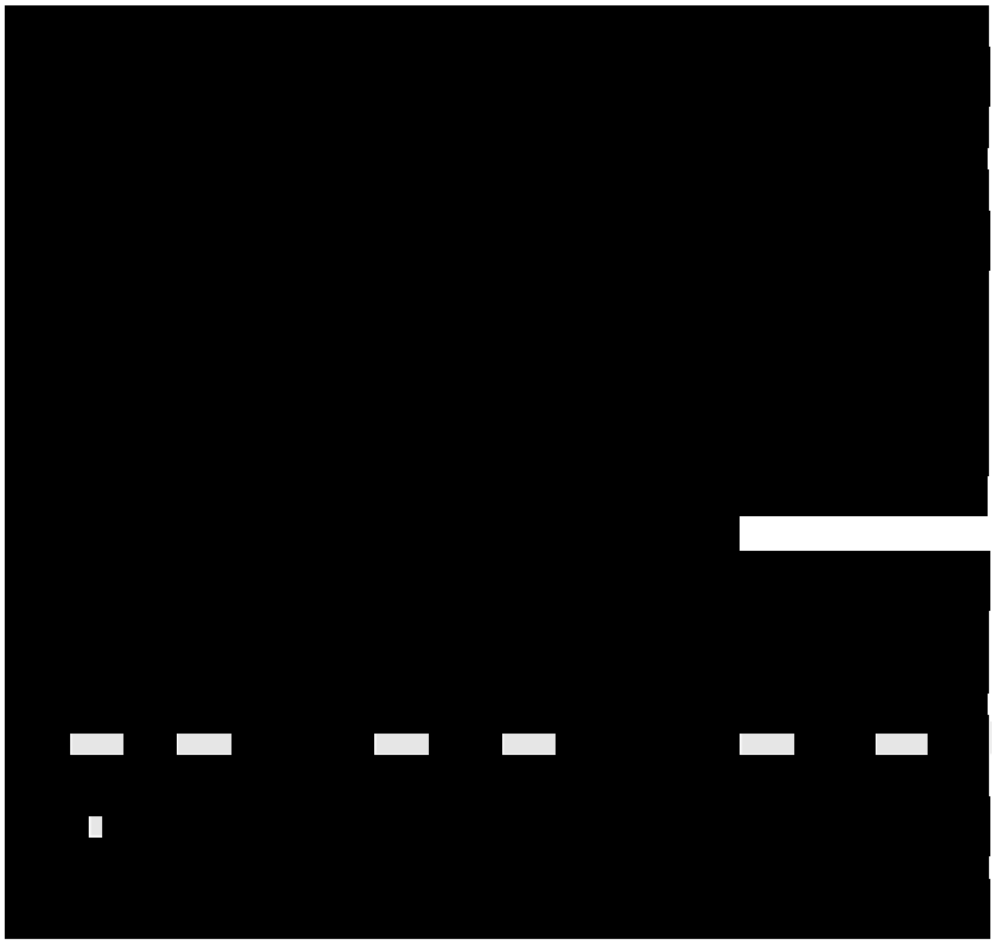
5.51. Assim sendo, uma política de segurança da informação baseada nas melhores medidas técnicas, administrativas e de gestão disponíveis é imperativa, devendo ser ela revisada constantemente, a partir das atualizações de ferramentas de proteção de dados, bem como dos dados obtidos pelas necessárias auditorias a serem realizadas nas operações de tratamento.

5.52. Sobre esse ponto, chama-se atenção para o fato de que a Política de Segurança da Informação da Secretaria de Estado da Educação do Paraná (SEED) tenha sido inteiramente baseada na "Política de Tratamento de Incidentes à Privacidade de Dados Pessoais da Celepar" (0174716, p. 30). Mesmo que a Celepar seja, no caso em análise, a operadora dos dados da SEED-PR, cabe à controladora (SEED-PR) garantir a segurança dos direitos individuais das crianças e adolescentes sob sua guarda, conforme o disposto no art. 39 da LGPD[17].

5.53. É importante destacar que o controlador, nos termos do art. 5º, VI, e 39 da LGPD, é o agente de tratamento responsável por definir as decisões centrais relativas ao tratamento de dados pessoais, bem como de estabelecer as finalidades específicas para as quais esse tratamento será realizado, cabendo a ele orientar os operadores de dados contratados, mediante o fornecimento de instruções claras, quanto à execução de determinadas atividades de tratamento de dados pessoais.

5.54. A respeito do fluxo de informações do processo de reconhecimento facial para fins de frequência escolar, assim se posicionou a regulada (0174716, p. 33):

Aplicativo de cadastramento biométrico dos alunos – Escola Paraná – Biometria:



Restrição de acesso a informação, nos termos do art. 13, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito.

Aplicativo de chamada – Escola Paraná – Professores:

informação, nos termos do art. 13, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito.

Medidas operacionais de segurança

[redacted]

estrição de acesso à informação, 13, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito.

5.55. Foram, ainda, informadas as seguintes medidas de segurança e privacidade:

[redacted]

3, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito.

5.56. Entende-se que a regulada procurou descrever medidas técnicas razoáveis para atender aos requisitos de segurança da informação, aos padrões de boas práticas e de

governança dos dados pessoais tratados. Contudo, diante das declarações e documentos juntados pela regulada ao processo, verifica-se que sua política de tratamento de dados ainda requer alterações e complementações para estar em acordo com os ditames do art. 49 da LGPD, uma vez que são tratados dados pessoais biométricos de crianças e adolescentes em larga escala. Em outro, a regulada apenas descreveu medidas de forma genérica, não tendo comprovado as alegações feitas.

5.57. Inicialmente, não foi verificada, em nenhum dos documentos entregues pela SEED/PR, demonstração de como funcionam os controles de acesso aos dados pessoais, especialmente em relação às pessoas autorizadas e aos mecanismos de segurança para sua utilização. O RIPD limita-se a informar que adotará “Controle de Acesso Lógico às bases de dados e aplicação, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física do ambiente central e monitoramento constante contra ameaças e indisponibilidades dos sistemas”, sem descrever, de forma técnica, precisa e suficiente, a arquitetura dos controles de segurança referentes ao tratamento de dados biométricos.

5.58. No documento (RIPD) não constam informações sobre a existência de ambientes segregados para os dados biométricos; a localização física e lógica dos dados; a distribuição das responsabilidades entre os agentes de tratamento; com é feita a implementação de controles de acesso; compartilhamentos entre sistemas; e mecanismos de monitoramento e auditoria.

5.59. A ausência de descrição adequada da arquitetura dos controles de segurança impede a identificação de pontos críticos de exposição dos dados pessoais, limita a compreensão dos fluxos de informação e compromete a avaliação da suficiência das medidas mitigatórias.

5.60. Desse modo, pode-se afirmar que o controlador não trouxe aos autos evidências documentais que comprovem a existência de governança sobre o controle de acesso aos dados biométricos dos estudantes, em desrespeito ao princípio da responsabilização e prestação de contas. De acordo com o art. 6º, inciso X, da LGPD, cabe ao agente de tratamento comprovar que adotou a medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

5.61. Em segundo lugar, deve-se apontar estudo da Agência Espanhola de Proteção de Dados (AEPD) sobre o uso de

funções de *hash* como técnica de pseudoanonimização de dados pessoais[18]. Nele, foi registrado que, embora o *hash* possua propriedades criptográficas importantes, sua aplicação exige cuidados técnicos e jurídicos para garantir a conformidade com os princípios da proteção de dados. O uso de *hash*, por si só, não descaracterizaria um dado como pessoal, sendo necessário avaliar o contexto e os riscos de reidentificação.

5.62. Ainda segundo o estudo, a gestão segura do ciclo de vida dos dados e a eliminação dos elementos que permitam a reidentificação (isolamento informacional para evitar correlações que facilitem a reidentificação) são essenciais para transformar a pseudoanonimização em anonimização. Assim sendo, a adoção d o *hash* como técnica de pseudoanonimização deveria ser acompanhada de avaliação de risco de reidentificação, considerando o algoritmo, a entropia de dados e a existência de dados correlatos, o que não foi demonstrado no caso em tela.

5.63. Da mesma forma, a utilização de *hash* biométrico é apresentada como mecanismo suficiente para impedir a reversão da imagem original, sem qualquer demonstração técnica sobre as características desse identificador, seu potencial de vinculação entre bases distintas, seus riscos de reidentificação ou sua capacidade de funcionar, na prática, como identificador biométrico persistente. É necessário esclarecer se se trata efetivamente de função *hash* criptográfica aplicada a determinado artefato, de template biométrico, de vetor de características ou de outro identificador derivado.

5.64. Ainda que a reconstrução visual integral da face não seja tecnicamente viável, o artefato poderá continuar apto a distinguir ou autenticar o titular, ser comparado com novos registros, vinculado a outras bases de dados ou utilizado para inferências. Nessas condições, a pseudoanonimização reduz determinados riscos, mas não descaracteriza o tratamento de dados biométricos nem elimina a necessidade de controles reforçados de governança, supervisão e responsabilização.

5.65. Em terceiro lugar, seja na utilização de *hash* como técnica de pseudoanonimização de dados pessoais, seja para o tratamento em larga escala de dados pessoais sensíveis, é indispensável que o tratamento seja documentado e revisado periodicamente, com auditorias técnicas e organizacionais. O RIPD apresentado, entretanto, não indicou a realização de qualquer análise técnica que demonstrasse a existência de procedimento de revisão periódica das medidas de mitigação de

riscos. Na verdade, verifica-se que a última versão do RIPD apresentado é datada de 25 de janeiro de 2021 (versão 1.6).

5.66. Conforme a Nota Técnica nº 5/2025/FIS/CGF/ANPD (0165389), a CGF consignou que o RIPD deve conter descrição detalhada dos processos de tratamento capazes de gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação adotados.

5.67. Conforme assinalado na análise técnica, o RIPD deve proporcionar uma organização sistemática das operações de tratamento que permita visualizar processos e procedimentos internos, identificar riscos e verificar a correspondência entre esses riscos e as medidas destinadas a preveni-los ou reduzi-los. O documento não se presta, portanto, a registrar fórmulas genéricas ou categorias abstratas de controles, mas a evidenciar como cada salvaguarda incide sobre determinado risco, em qual etapa do fluxo de dados, sob responsabilidade de qual agente e mediante quais parâmetros de desempenho, supervisão e verificação.

> 5.5.7. A LGPD não impõe aos controladores e operadores a necessidade de produção de RIPD para toda e qualquer operação de tratamento de dados pessoais. O art. 38 da LGPD, nesse sentido, confere à ANPD competência para determinar aos controladores que elaborem relatório de impacto à proteção de dados pessoais referentes a suas operações de tratamento, observados os segredos comercial e industrial. Entretanto, baseada numa abordagem principiológica, tem-se que a LGPD adotou uma regulação baseada em risco, que presume a responsabilidade dos agentes de tratamento na avaliação dos riscos de sua atividade. Assim, ao pensar melhores práticas em relação ao tratamento de dados, os agentes de tratamento devem levar em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> 5.5.8. Desse modo, embora a ANPD não tenha regulamentado a matéria, compreende-se que **os controladores, em respeito aos princípios da prevenção, da segurança, e da responsabilização e prestação de contas, previstos no art. 6º, incisos VII, VIII e IX, da LGPD, devem elaborar o respectivo RIPD quando a operação de tratamento de dados pessoais suscitar nível de risco elevado para a garantia dos direitos dos titulares.** Essa avaliação deve ser realizada antes mesmo do início da operação de tratamento, de maneira que o controlador

> possa avaliar previamente os riscos que sua atividade poderá gerar aos titulares aferrados e as possíveis ações mitigatórias.
>
> (...)
>
> 5.5.12. (...) Os documentos devem conter, de forma detalhada, informações sobre (i) a identificação dos agentes de tratamento; (ii) o escopo do tratamento; (iii) a descrição do tratamento, especificando-se a natureza dos dados coletados, o fundamento legal que autoriza a sua coleta, as finalidades específicas, a análise da adequação e da necessidade de coleta dos dados, o uso compartilhado dos dados; o período de retenção dos dados; e as medidas de transparência previstas; (iv) os mecanismos de exercício dos direitos previstos na LGPD pelos titulares; (v) a descrição das medidas técnicas e administrativas para assegurar a proteção dos dados pessoais; e (vi) a análise quanto à identificação e avaliação dos riscos inerentes à operação de tratamento e as medidas mitigadoras previstas.

5.68. Ademais, a regulada foi diretamente questionada sobre a existência de procedimentos de auditoria ou mecanismos de controle das operações já realizadas, não tendo sido fornecida qualquer documentação que evidenciasse adoção efetiva desta medida de governança. Inclusive, no tocante à falta de envio de informações e documentos importantes para o bom andamento do processo de fiscalização, deve-se ressaltar que, mesmo diante de pedidos reiterados, o controlador deixou de apresentar o Registro de Operações de Tratamento de Dados Pessoais (ROT) referente à operação de tratamento em análise.

5.69. A manutenção dos registros das operações de tratamento de dados pessoais não é uma faculdade dos agentes de tratamento, uma vez que o art. 37 da LGPD impõe a produção deste documento como uma obrigação legal, tanto de controladores quanto de operadores[19]. À título de esclarecimento, um ROT deve descrever, de forma clara e organizada, todas as atividades de tratamento de dados pessoais realizadas sob a responsabilidade do operador. Esta obrigação legal, ademais, precisa ser compreendida à luz do princípio da responsabilização e prestação de contas, inscrito no inciso X do art. 6º da LGPD[20], que impõe aos agentes de tratamento o dever de demonstrar a adoção de medidas capazes de comprovar a observância, o cumprimento e a eficácia das normas de proteção de dados pessoais[21].

5.70. O ROT, nesse sentido, tem como uma de suas

principais finalidades a comprovação de que o controlador realizou o mapeamento integral das cadeias de tratamento de dados pessoais, com a identificação documentada das fontes originárias dos dados coletado, finalidades específicas de tratamento, hipóteses legais, agentes envolvidos, prazos de retenção e eventual compartilhamento de dados, indicando-se os agentes destinatários. **A apresentação deste documento à ANPD no âmbito de procedimentos de fiscalização, além de constituir uma obrigação, é fundamental para a demonstração da regularidade das operações de tratamento do regulado.**

5.71. Por esse motivo, o art. 5º, inciso I, da Resolução CD/ANPD nº 1/2021[22][23], que aprovou o Regulamento de Fiscalização e do Processo Administrativo Sancionador no âmbito desta Agência Reguladora, estabelece como prerrogativa da ANPD, no âmbito de sua atividade fiscalizatória, determinar aos agentes regulados a apresentação de cópia dos documentos relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas.

5.72. A recusa dos agentes regulados em atender às determinações da ANPD, inclusive, poderá caracterizar a conduta de obstrução à atividade de fiscalização, sujeitando o infrator a medidas repressivas, nos termos do art. 6º do Regulamento de Fiscalização[24]. A conduta que incorre em obstrução à atividade de fiscalização da ANPD constitui infração de natureza grave, nos termos do art. 8º, §3º, inciso II, da Resolução CD/ANPD nº 4/2023, que aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas[25].

5.73. Desse modo, a recusa do órgão público regulado em encaminhar para a Coordenação-Geral de Fiscalização o registro de operação de tratamento, após reiteradas solicitações, **constitui conduta de natureza grave**, pois caracteriza obstrução da atividade fiscalizatória da ANPD, que impõe constrangimento ilegal ao exercício das competências exaradas pelo art. 55-J, inciso IV, da LGPD c/c os artigos 5º, inciso I, e 6º da Resolução CD/ANPD nº 1/2021.

5.74. Para mais, a revisão dos mecanismos e da política de proteção de dados é essencial quando se fala de tratamento em larga escala de dados pessoais sensíveis, ainda mais em se tratando de titulares menores de idade. Contudo, a regulada deixou de trazer aos autos documentos que comprovem a

realização de estudos ou análises de verificação de riscos de danos aos direitos à privacidade e à proteção de dados pessoais dos titulares, bem como de sua atualização.

5.75. Na verdade, algumas das medidas mitigadoras são apresentadas no RIPD de maneira bastante genérica, sem a devida delimitação das ações a serem tomadas em caso da ocorrência dos riscos identificados. Observe-se, nesse sentido, os exemplos abaixo:

Risco referente ao tratamento de dados pessoais	Medidas mitigadoras
Uso indevido da imagem coletada por usuário do sistema (usando a própria chave ou de outro).	[redacted]
Risco de vazamento das imagens (acesso indevido às imagens) diretamente na infraestrutura de TI (storage NAS).	
Vazamento de informações em trânsito, entre dispositivo onde foi coletada a imagem e ambiente central, ou entre ambiente central e Contratada.	
Tratamento indevido das imagens pela Contratada (armazenamento não autorizado, ou uso para outras finalidades).	
Tratamento das imagens sem consentimento do titular.	Restrição de acesso a informação, nos termos do art. 13, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito.

5.76. O RIPD da SEED/PR foi assinado em janeiro de 2021 e a atividade de tratamento de dados pessoais se iniciou em 2023, sem que houvesse atualização do RIPD ou a comprovação de elaboração de ROT, mesmo diante de vários avanços tecnológicos em relação ao tratamento de dados pessoais por meio de

tecnologia de biometria facial. Assim, deve-se entender que a declaração da regulada de que “a SEED recomenda e direciona suas ações para que a revisão das avaliações de impacto e riscos seja conduzida pelo menos uma vez ao ano ou sempre que houver eventos que alterem significativamente o cenário de riscos” não foi corretamente aplicada.

5.77. A análise conjunta do Relatório de Impacto à Proteção de Dados (RIPD) e das informações complementares apresentadas evidencia que o controlador não demonstrou, de forma técnica, precisa e auditável, que as medidas de segurança adotadas sejam adequadas à natureza, à escala e à gravidade dos riscos inerentes ao tratamento de dados biométricos de crianças e adolescentes no ambiente escolar.

5.78. As informações apresentadas concentram-se predomin

foram efetivamente implementados, quais parâmetros técnicos foram adotados, quais mecanismos asseguram sua eficácia nem como são continuamente monitorados e auditados. (Restrição de acesso a informação, nos termos do art. 13, inciso II, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) no Poder Executivo Federal, uma vez que o trecho ocultado traz informações referentes a aspectos técnicos de sistema de informação de acesso restrito).

5.79. Observa-se que as medidas mitigatórias apresentadas se concentram, em grande parte, na redução de riscos de segurança da informação, deixando de enfrentar riscos específicos inerentes ao reconhecimento facial em ambiente escolar. Não há avaliação técnica acerca da taxa de falsos positivos e falsos negativos do algoritmo, da possibilidade de identificação equivocada de estudantes, dos riscos de viés algorítmico em relação a diferentes grupos demográficos, dos impactos decorrentes de recusas indevidas de acesso, da possibilidade de reidentificação a partir dos identificadores biométricos, nem da eventual memorização ou reutilização dos templates biométricos.

5.80. Consequentemente, a irreversibilidade alegada não

afasta sua natureza de dado pessoal sensível, nos termos do art. 5º, inciso VI, nem elimina os riscos de correlação, reprodução, comprometimento ou uso incompatível. Em razão da permanência e da baixa substituibilidade das características biométricas, eventual comprometimento desses identificadores pode produzir consequências duradouras, superiores às associadas ao vazamento de credenciais convencionais.

5.81. Da mesma forma, inexistem evidências de que tenham sido realizados testes independentes de robustez, auditorias periódicas do algoritmo, avaliações de acurácia em população infantojuvenil ou mecanismos contínuos de monitoramento destinados a identificar degradação de desempenho, vieses discriminatórios ou alterações no comportamento do sistema ao longo do tempo. Tais elementos são relevantes porque, em sistemas biométricos, a efetividade das medidas mitigatórias depende não apenas da segurança da infraestrutura tecnológica, mas também da confiabilidade do próprio processo de identificação biométrica.

5.82. Ademais, embora o compartilhamento das fotografias dos estudantes com os operadores ocorra desacompanhado da identificação direta do estudante e exista previsão contratual de eliminação das imagens após o processamento, o RIPD não demonstra como o controlador verifica o efetivo cumprimento dessa obrigação, tampouco descreve mecanismos de auditoria técnica, inspeções, certificações independentes, registros verificáveis de eliminação ou controles destinados a impedir reutilização, retenção indevida ou treinamento secundário dos algoritmos pelo fornecedor.

5.83. Verifica-se, ainda, que a matriz de riscos permanece excessivamente centrada em riscos operacionais de vazamento ou acesso indevido, deixando de contemplar riscos diretamente relacionados ao exercício de direitos e liberdades fundamentais dos estudantes. Não foram identificados, por exemplo, riscos associados ao monitoramento permanente de crianças e adolescentes, ao efeito de normalização da vigilância biométrica no ambiente escolar, à limitação da autodeterminação informativa, à utilização compulsória da biometria como condição para acesso à educação, à ampliação das finalidades do sistema, à eventual integração com outras bases governamentais, em especial, de órgãos de segurança pública, ou à utilização secundária dos dados biométricos.

5.84. A Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528),

ademais, reconhece que o tratamento de dados biométricos dos alunos da rede pública estadual constitui atividade de alto risco, pois combina tratamento em larga escala, potencial afetação significativa de direitos fundamentais, utilização de tecnologia inovadora, possível vigilância ou controle de ambientes escolares e tratamento de dados sensíveis de crianças e adolescentes.

> 4.32. É importante destacar, desse modo, que a coleta massiva de dados pessoais tem imbuída em si grandes riscos, em termos de vazamento ou uso abusivo. Aqui se fala não somente da tecnologia do reconhecimento facial para identificação das crianças presentes em sala de aula, mas de todo o processo de coleta, armazenamento, uso e compartilhamento de dados que envolvem, entre outros: escolas, professores, servidores, empresa pública e privada, os governos estadual e municipal e todos os órgãos públicos listados como aptos a possível compartilhamento de dados (conselho tutelar, Ministério Público, etc.).
>
> 4.33 O tratamento de dados pessoais biométricos de alunos da rede pública do Estado do Paraná, desse modo, pode ser considerada uma ***atividade de tratamento de alto risco***, já que cumpre os requisitos do art. 4º do Regulamento aprovado pela Resolução CD/ANPD nº 2/2022 (“Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte”)

5.85. A análise de riscos não poderia, por conseguinte, restringir-se a hipóteses técnicas e convencionais de vazamento, indisponibilidade ou acesso indevido à infraestrutura. Seria necessário avaliar, de maneira específica, riscos relacionados ao exercício de direitos e garantias fundamentais pelos estudantes, como a exclusão ou constrangimento durante o procedimento de identificação, vieses relacionados a características fenotípicas, idade, deficiência (PCD) ou condições ambientais, bem como aqueles resultantes de reidentificação a partir de templates, vinculação entre bases de dados, ampliação das finalidades de tratamento, vigilância persistente e normalização do monitoramento biométrico no espaço escolar.

5.86. Por fim, o princípio da responsabilização e prestação de contas exige mais do que a afirmação de que determinadas providências foram adotadas. Cabe ao controlador demonstrar, mediante evidências verificáveis, que as medidas são adequadas, foram efetivamente implementadas e produzem os resultados esperados. No contexto do RIPD, a documentação exerce dupla função. Primeiro, reconstrói o processo decisório que conduziu à identificação dos riscos, à seleção das salvaguardas e à aceitação

do risco residual; em seguida, viabiliza o controle independente pela autoridade supervisora e por outras instâncias de auditoria ou controle social. A ausência de documentação organizada, coerente e tecnicamente verificável amplia a assimetria informacional, impede a rastreabilidade das decisões e enfraquece a demonstração de conformidade.

5.87. Diante desse conjunto de elementos, conclui-se que as medidas relacionadas no RIPD não são suficientes para demonstrar a mitigação adequada dos riscos elevados associados ao reconhecimento facial de crianças e adolescentes como mecanismo de gestão de presença escolar. Permanecem não comprovadas a eficácia dos controles de segurança, a governança sobre os acessos e compartilhamentos, a supervisão do fornecedor, a confiabilidade e não discriminação do algoritmo, a existência de alternativas menos invasivas e o atendimento concreto ao melhor interesse dos estudantes.

5.88. A insuficiência das ações do controlador compromete: (i) o dever de observância do melhor interesse de crianças e adolescentes no tratamento de dados pessoais, nos termos do art. 14, caput, da LGPD e (ii) o dever de estruturação dos sistemas utilizados para o tratamento de dados pessoais de forma a atender aos requisitos de segurança[26], aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD, em especial os princípios da necessidade, prevenção, segurança e responsabilização e prestação de contas, nos termos dos arts. 6º, incisos III, VII, VIII e X, e 49 da LGPD.

5.89. Conforme pontua Bioni (BIONI, 2022), uma das principais funções do RIPD é antever impactos e estabelecer medidas mitigadoras quando o risco do tratamento não for demasiadamente elevado para a finalidade que se pretende alcançar:

> De acordo com a LGPD, caberia a tal agente de tratamento de dados descrever os riscos a direitos e liberdades civis e fundamentais ao titular de dados pessoais resultantes da sua atividade de tratamento de dados, bem como as medidas de salvaguardas e mecanismos de mitigação. Todo esse processo de gerenciamento de risco deveria, ao final, ser documentado, que é justamente no que consiste o relatório de impacto.

5.90. Ademais, quando questionada sobre a realização de auditorias sobre as operações de tratamento de dados pessoais biométricos, a SEED apenas informou que caberiam...

> ... à Diretoria de Tecnologia e Inovação – DTI, os procedimentos relacionados ao constante monitoramento e adequações das regras e sistemas utilizados pela Secretaria de Estado da Educação do Paraná, quanto à compatibilidade e promoção da segurança das bases de dados dos sistemas estaduais. Ao Departamento de Planejamento da Rede – DPR e ao Encarregado de Tratamento de Dados Pessoais – DPO, entre suas competências, respondem pelos procedimentos administrativos e boas práticas com vistas à minimização e à proteção dos dados conforme prevê o artigo 46 da LGPD, a partir do s constante monitoramento e auditorias permanentes diretamente nas bases de dados do Sistema Educacional do Paraná, e sempre que identificadas situações adversas ao prospectado, ou para averiguação de denúncias, emissões de notificações, realização de verificações *in-loco* que conforme apuração dos fatos podem ser enquadradas no artigo 52 da LGPD. (0195330, p. 53)

5.91. Diante da ausência de resposta objetiva da regulada, bem como do não fornecimento de qualquer registro de operações de tratamento, **deve-se entender que não foram realizadas as ações de monitoramento ou atualização das normas de mitigação de riscos**, o que levaria à SEED-PR a não atender as medidas mínimas de segurança para poder continuar a realizar operação de tratamento de dados pessoais sensíveis de crianças e adolescentes de forma massiva, como faz hoje.

D) Do tratamento desnecessário, desproporcional e excessivo de dados biométricos de crianças e adolescentes

5.92. Além da definição da hipótese legal adequada e de medidas de segurança eficazes, para que determinada atividade de tratamento de dados pessoais seja considerada legítima, o agente de tratamento deve observar os princípios gerais de tratamento de dados pessoais, como finalidade, adequação, necessidade, transparência, prestação de contas, dentre outros, bem como garantir que os titulares de dados possam exercer os direitos previstos na norma durante toda a cadeia de tratamento, isto é, desde a coleta dos dados pessoais até o seu eventual descarte.

5.93. No caso em tela, onde são tratados dados pessoais sensíveis de crianças e adolescentes, deve ser ressaltada a importância de que o tratamento seja realizado de forma minimamente invasiva, sendo proporcional à real necessidade da

política pública vinculada. Neste contexto, falamos, por exemplo, do princípio da necessidade ou da "minimização" de coleta de dados pessoais[27], para que sejam tratados apenas os dados **estritamente necessários** para alcançar o objetivo pretendido, sem que haja retenção prolongada ou uso distinto da finalidade coletada.

5.94. Sobre o tópico, a regulada alegou que a automatização do registro de frequência do aluno, por meio de reconhecimento facial fotográfico, geraria ganho de tempo em sala de aula, com duração variável (em 100%) dependendo da familiaridade do docente com a tecnologia (0174716, p. 33), além de possível redução de falhas de registro geradas por "possíveis fraudes que estejam relacionadas à frequência de alunos em sala de aula" (0174716, p. 34).

5.95. Quando questionada sobre a necessidade e proporcionalidade do uso da TRF para aferição de frequência escolar, a regulada se limitou a dizer que "o tratamento de dados é limitado ao vínculo do código da imagem ao CGM (Código Geral de Matrícula), mínimo necessário para a realização da finalidade prevista de Registro de Frequência Escolar" (0174716, p. 36), bem como pela necessidade de se "alcançar os objetivos educacionais delineados pela Secretaria de Educação, sob a administração consciente do Gestor Público da Pasta" (0195330, p. 40).

5.96. Em outro momento, a regulada afirmou que "implementar essa tecnologia nas escolas reflete um compromisso em alinhar as práticas educacionais com soluções modernas e eficientes. A política pública estabelecida visa não apenas a otimização dos processos internos, como o registro de frequência, mas também melhorar substancialmente a eficácia do acompanhamento educacional" (0174716, p. 49). Ao ser questionada se haveria meio menos gravoso para se atingir as mesmas finalidades, a regulada declarou que "o registro de identificação por reconhecimento facial é altamente eficiente", não havendo "meio gravoso", mas "alternativas que permitam alcançar as mesmas finalidades com igual eficácia e precisão" (0195330, p. 40 e 41).

5.97. Diante das respostas da regulada, **não se antevê que tenha havido análise da real necessidade e proporcionalidade do uso da TRF para aferição de frequência escolar,** especialmente no que se refere aos eventuais impactos dessa prática nos direitos e garantias

fundamentais das crianças e adolescentes, mas tão somente interesse em reduzir o tempo gasto em sala de aula com tal atividade, o que não foi evidenciado por estudos aplicados posteriormente à entrada em vigor da medida.

5.98. A regulada menciona, ainda, que o modelo de TRF para gerenciamento das frequências minimiza a oneração financeira decorrente da manutenção de formatos impressos (0174716, p. 49), mas posteriormente alega que o registro de frequência escolar já havia sido outrora modernizado pela implementação do Livro de Registro de Classe Online (0174716, p. 82). Neste ponto, vê-se que um sistema de registro online ou o uso de cartões magnéticos particulares, capaz de registrar a presença via sistema eletrônico, poderia substituir a TRF no que tange à oneração financeira decorrente da manutenção de formatos impressos, com menos riscos de exposição de dados pessoais dos alunos.

5.99. A adequação ao princípio da finalidade do tratamento também pode ser questionada, uma vez que a regulada associou à redução de tempo possivelmente obtida pelo uso da TRF na aferição de frequência escolar a um benefício de “segurança da comunidade escolar e tomada de decisões mais ágeis, pois possibilita o registro automático e o reconhecimento de pessoas não autorizadas de imediato, além do registro de incidentes, objetos perigosos, ou comportamento de risco, ajudando a criar um ambiente mais seguro e agradável para os estudantes, justificando o legítimo interesse público” (0195330, p. 51).

5.100. Neste ponto, vemos finalidades completamente divergentes em natureza sendo “confundidas” com o interesse público da medida. Ora, se a operação de tratamento foi pensada e estruturada como uma ferramenta de aferição de frequência escolar, a utilização da mesma operação de tratamento para registro de incidentes (com pessoas ou objetos) e identificação de “comportamentos de risco” se traduz em utilização dos dados pessoais para finalidades totalmente distintas daquela informada aos responsáveis pela criança ou adolescente, em claro desrespeito aos princípios da finalidade (art. 6ª, I, da LGPD[28]) e da transparência. Por força da LGPD, ao controlador, não se admite o tratamento de dado pessoais para finalidades não declaradas, dever que é reforçado pelo disposto no art. 23, I, quando se trata do poder público.

5.101. De mais a mais, deve-se mencionar o período de retenção e atualização dos dados pessoais biométricos coletados

pela regulada, já que foi informado que esses dados “são armazenados enquanto o estudante estiver regularmente matriculado na rede estadual de ensino” (0174716, p. 89).

5.102. No Brasil, os anos escolares obrigatórios (dos 4 aos 17 anos) incluem a Educação Infantil, o Ensino Fundamental e o Ensino Médio, totalizando 14 anos de educação básica. Assim sendo, caso a regulada mantenha sua política de retenção de dados, ficarão registrados em seu sistema o equivalente a 14 anos de dados biométricos de cada aluno. Uma coisa é a retenção de dados acadêmicos não biométricos necessários para fins legais e institucionais, como registros de identificação nominal e de avaliações escolares. Outra é a guarda de dados biométricos até a finalização do vínculo escolar, que pode significar risco desnecessário aos direitos fundamentais dos titulares, sem que sejam indispensáveis à precisão da política pública que promoveu o tratamento.

5.103. A título de exemplo, ressalta-se que há significativa preocupação doutrinária quanto à acurácia das tecnologias de reconhecimento facial em crianças, adolescentes e grupos raciais diferentes[29]. No contexto escolar, resultados que ensejam falsos positivos ou falsos negativos podem implicar imputações indevidas de condutas irregulares, exclusões injustas de ambientes escolares, medidas sociais de auxílio, ou ainda medidas disciplinares desproporcionais, com reflexos duradouros na trajetória de vida do estudante.

5.104. Isso porque, o uso de dados biométricos de crianças e adolescentes possui múltiplas camadas de sensibilidade: os sujeitos envolvidos (cuja proteção foi significativamente ampliada a partir da Lei nº 15.211/2025); a natureza dos dados biométricos (art. 5º, II da LGPD) e a necessidade de observância à transparência e a responsabilidade no tratamento de dados pessoais de pessoas em fase de desenvolvimento (art. 4º, IX da Lei nº 15.211/2025).

5.105. Outro ponto que merece atenção, relacionado à adequação entre necessidade e finalidade do tratamento, versa sobre a acurácia dos dados biométricos de crianças e adolescentes. Durante o fim da infância e ao longo da adolescência, as mudanças na face são significativas, alterando seus padrões em um ritmo de aproximadamente quatro a seis meses em relação à alteração de posicionamento de pontos nodais fundamentais aos mecanismos de biometria facial para fins de reconhecimento, especialmente os que empregam

ferramentas 2D, 3D e imagens dinâmicas[30].

5.106. O principal pilar que sustenta a inadequação dessas tecnologias para crianças e adolescentes, especialmente no contexto escolar, reside na mencionada dinâmica acelerada e não-linear do crescimento facial. Ao contrário da relativa estabilidade morfológica observada na idade adulta, a face infantil está em constante processo de transformação. Um estudo longitudinal conduzido ao longo de oito anos, com coletas de dados semestrais de crianças de 3 a 18 anos, demonstrou de forma contundente a degradação temporal da acurácia dos sistemas de reconhecimento facial[31][32].

5.107. Essa variabilidade no ritmo de desenvolvimento facial, intrínseca ao processo pubertário, torna qualquer tentativa de padronização para reconhecimento biométrico uma tarefa de alta imprecisão. Os modelos de progressão etária testados no estudo apresentaram erros médios que, embora possam parecer pequenos (em torno de 2 mm), são suficientes para comprometer a confiabilidade da identificação em sistemas automatizados, especialmente quando se considera que as áreas de maior desvio, ainda que não sejam as mais importantes para o reconhecimento facial humano, podem afetar os algoritmos de *machine learning* de forma imprevisível.

5.108. Se a tecnologia não é capaz de garantir um nível aceitável de acurácia ao longo do tempo, sua utilidade prática e a relação custo-benefício (considerando os riscos envolvidos) tornam-se questionáveis, pois as possíveis falhas de identificação podem afetar direitos constitucionalmente protegidos, como a honra, imagem e dignidade, além do direito à educação. Mais grave seria o caso de eventual compartilhamento dos dados biométricos, coletados para finalidades relacionadas ao ambiente escolar, com forças de segurança, sem que haja transparência sobre como, quando e por que esse compartilhamento ocorreria.

5.109. Para além das questões de acurácia, emergem riscos éticos, sociais e psicológicos. A coleta de dados biométricos em ambiente escolar pode acabar por inserir a criança em uma lógica de vigilância constante, normalizando a captura de sua experiência e a conversão de seus comportamentos em dados, o que se convencionou chamar de "vigilância do berço", onde os indivíduos crescem condicionados à aceitação do monitoramento como algo natural. Como as crianças e adolescentes se encontram em fase de desenvolvimento cognitivo e socioemocional, a vigilância biométrica pode minar o

desenvolvimento de sua autonomia e privacidade, podendo gerar ambientes de maior ansiedade e hostilidade, especialmente em uma relação de hipervigilância e hierarquia[33], além de poder gerar efeito de autocensura e redução da espontaneidade, essenciais ao aprendizado e ao exercício da liberdade de expressão.

5.110. Em outro, deve-se apontar que mesmo os algoritmos mais avançados dependem de verificação humana para confirmação de correspondências. Em sua ausência, cria-se ambiente onde erros podem ser constantes e aceitos. Na sua presença, tem-se retrabalho e possível aumento de tempo para uma atividade que poderia ser realizada de outra forma (como uma chamada nominal realizada em ambiente computadorizado).

5.111. Outro ponto crítico, frequentemente negligenciado, é o risco de finalidade. A coleta e o armazenamento de dados biométricos de milhões de crianças criam um acervo que pode vir a ser utilizado por cibercriminosos ou em parcerias com vieses (as vezes obscuros) de mercantilização de dados pessoais. Além disso, a retenção desses dados por plataformas que já estão "acumulando dados em antecipação a futuras demandas de aplicação da lei”[34] agrava exponencialmente esse risco. A justificativa para a coleta, portanto, precisa ser não apenas robusta e baseada em evidências de eficácia, mas também proporcional ao dano potencial em caso de incidente de segurança, um dano que, para uma criança, pode se estender por toda a sua vida adulta.

5.112. Como visto na Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528)[35], mesmo que tratamento de dados pessoais de crianças e adolescentes, inclusive dados sensíveis, não seja proibido em abstrato, ele exige demonstração concreta de que a operação atende ao melhor interesse desse grupo vulnerável, nos termos do art. 14 da LGPD. Não basta ao controlador apontar uma hipótese legal de tratamento ou afirmar genericamente que a solução aprimora o controle de frequência escolar.

5.113. O controlador deve demonstrar que a tecnologia escolhida é efetivamente necessária, adequada e proporcional; que seus benefícios específicos superam os riscos produzidos; que inexistem alternativas menos intrusivas com eficácia comparável; e que os impactos sobre privacidade, igualdade, liberdade, dignidade e desenvolvimento dos estudantes foram

considerados no desenho da solução. A documentação apresentada, contudo, não revela avaliação suficientemente aprofundada dessas questões.

5.114. Assim sendo, mesmo que o uso da TRF não seja, de início, ilícito, sua adoção, na forma atualmente adotada pela SEED-PR, não parece ser condizente com o melhor interesse das crianças e adolescentes que precisam frequentar o ambiente escolar público para o seu desenvolvimento. Ademais, também não parecem estar adequadas com vários dos princípios da LGPD, como o da minimização de dados, adequação, finalidade, prevenção e prestação de contas/responsabilização, visto que o objetivo da coleta e tratamento de dados não parece ser proporcional à finalidade destinada: realização de controle de frequência escola em sala de aula, que pode ser aferida com meios menos gravosos. A conveniência fundamentada na praticidade não é capaz de sustentar a necessidade exigida pelo inciso II do art. 11 da LGPD.

E) Da possibilidade de fiscalização da ANPD frente aos possíveis ilícitos praticados

5.115. A LGPD, art. 5º, I, considera dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável". Os dados envolvidos no presente processo – dados biométricos de crianças e adolescentes – são dados pessoais, pois consistem em informação relacionada a pessoa natural identificada ou identificável. Desta forma, cabe à ANPD, de acordo com o art. 55-J da LGPD:

> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

5.116. A inteligência do supracitado dispositivo (art. 55-J, inciso IV, LGPD) faz com que a ANPD tenha centralidade na verificação da aplicação das normas de proteção de dados pessoais pelos agentes de tratamento. E, no âmbito da ANPD, coube à Superintendência de Fiscalização (SFI)[36] identificar as infrações à LGPD, de acordo com o Regimento Interno da ANPD, art. 17:

> Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:
>
> I - fiscalizar e aplicar as sanções previstas no artigo 52 da

> Lei nº 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> II - proferir decisão em primeira instância nos processos administrativos sancionadores da ANPD;

5.117. Para o correto exercício de sua competência fiscalizatória e sancionadora, foram aprovadas pelo Conselho Diretor da ANPD a Resolução CD/ANPD nº 01/2021, que regulamentou o Processo de Fiscalização e o Processo Administrativo Sancionador (Regulamento de Fiscalização), e a Resolução CD/ANPD nº 04/2023, que estabeleceu os parâmetros e os critérios para aplicação de sanções administrativas, bem como as formas e dosimetrias para o cálculo do valor-base das sanções de multa (Regulamento de Dosimetria).

5.118. Tendo sido identificados possíveis atos antijurídicos praticados pela regulada em relação ao disposto na LGPD – ausência de base legal adequada para o tratamento (art. 11 da LPGD),descumprimento dos princípios da finalidade, adequação, necessidade e melhor interesse (art. 6º, I, II, III, VI; e o art. 14 da LGPD) e falta de apresentação do registro das operações de tratamento de dados pessoais (art. 37) e diante dos possíveis riscos que o tratamento pode causar à aproximadamente (01) um milhão de estudantes na escolarização básica, deve-se entender pela necessidade de aplicação de medida preventiva de natureza cautelar, já que presentes os institutos do *fumus boni iuris* e *periculum in mora*.

5.119. No presente caso, o *fumus boni iuris* está relacionado a possível ausência de hipótese legal para o tratamento, bem como da observância dos princípios orientadores da LGPD, o que levaria a um tratamento de dados pessoais sem embasamento legal, caracterizando-se como ato antijurídico. O risco aos titulares seria especialmente relevante por tratar-se de dado pessoal sensível. Materialmente, vê-se a necessidade de que o tratamento de dados sensíveis esteja amparado em uma hipótese legal válida (art. 11 da LGPD) e, em se tratando de crianças e adolescentes, do estrito atendimento ao princípio do melhor interesse (art. 14 da LGPD).

5.120. O *periculum in mora* fica evidenciado por tratar-se de lesão a direito fundamental que se renova e se repete todos os anos, e a cada dia, aumentando o dano em função do acúmulo de tratamentos de dados biométricos a cada novo semestre ou no caso de migrações escolares, por exemplo. Adicionalmente, a cada ano, novos alunos são recebidos pelo sistema educacional

público estadual, ficando eles sujeitos a esse modelo de verificação de frequência, e ampliando a base de crianças de adolescentes expostos aos riscos desse tratamento inadequado.

5.121. De acordo com o caput do art. 30 do Regulamento de Fiscalização da ANPD, as medidas preventivas podem ter duas naturezas: a primeira refere-se às medidas que explicitam a atuação responsiva da ANPD, visando reconduzir o agente de tratamento à plena conformidade"; a segunda refere-se às medidas preventivas de natureza acautelatória, que visam proteger os titulares de dados de tratamentos que possam lhes causar riscos ou danos eminentes[37]. Vejamos:

> Art. 30. A atividade preventiva visa reconduzir o agente de tratamento à plena conformidade ou evitar ou remediar situações que acarretem risco ou dano aos titulares de dados pessoais.

5.122. As medidas preventivas que podem ser adotadas pela ANPD em tais situações estão listadas no art. 32 do Regulamento de Fiscalização. Ademais, diante da complexidade dos casos que possam ser apresentados a esta Autoridade e da multiplicidade de medidas potencialmente adequadas e proporcionais a cada caso concreto, o § 1º do supracitado art. 32 autoriza a ANPD a recorrer a medidas preventivas atípicas, quando necessário à proteção dos titulares de dados. Citamos:

> Art. 32. São consideradas medidas preventivas:
>
> I - divulgação de informações;
>
> II - aviso;
>
> III - solicitação de regularização ou informe; e
>
> IV - plano de conformidade.
>
> §1º Poderão ser adotadas outras medidas não previstas neste artigo, se compatíveis com o disposto nos arts. 30 e 31. (grifo nosso)

5.123. Como dito acima, no caso em tela, a ausência de hipótese legal de tratamento, combinada com a ausência de adoção de princípios e medidas técnicas suficientes para resguardar os dados pessoais biométricos de mais de um milhão de crianças e adolescentes, é suficiente para motivar ação preventiva por parte da ANPD.

5.124. Conforme dito outrora por esta ANPD, **as medidas preventivas de natureza acautelatória são distintas de medidas sancionatórias (e, portanto, punitivas)** – ou seja: aplicar medidas cautelares não é o mesmo que aplicar, de

maneira imediata, uma sanção. Especialmente no contexto da fiscalização de natureza responsiva, adotada pela ANPD, uma medida preventiva confere ao regulado a oportunidade de adotar as providências necessárias para regularizar a sua conduta, visando à plena conformidade com a legislação de proteção de dados pessoais[38].

6. CONCLUSÃO E ENCAMINHAMENTOS

6.1. Com fundamento nos documentos colacionados aos autos do presente processo de fiscalização, entende-se que o controlador incidiu nas seguintes condutas irregulares à luz da Lei Geral de Proteção de Dados Pessoais - LGPD:

6.1.1. Realizar o tratamento em larga escala de dados pessoais sensíveis (biométricos) de estudantes da rede pública de ensino, em sua maioria crianças e adolescentes, sem hipótese legal adequada, em desrespeito ao disposto no art. 11 da LGPD. A hipótese legal do cumprimento de "obrigação legal ou regulatória do controlador", conforme o art. 11, II, a, da LGPD, é inadequada ao contexto do tratamento, visto que a imposição do cadastramento biométrico pela Resolução GS/SEED nº 2.865/2023 cria **dever específico aos alunos** da rede estadual de ensino, não ao controlador. A hipótese legal de "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos", nos termos do art. 11, II, b, da LGPD, do mesmo modo, também se mostra inadequada, uma vez que a Resolução GS/SEED nº 2.865/2023, por se tratar de ato administrativo secundário de caráter infralegal, não se mostra aderente ao critério restritivo imposto pelo legislador ao tratamento de dados pessoais sensíveis pelo Poder Público nesse contexto. Por fim, a definição de duas hipóteses legais de tratamento para a consecução da mesma finalidade afronta os princípios da boa-fé objetiva e da transparência, ao dificultar o exercício de direitos pelos titulares afetados.

6.1.2. Realizar o tratamento em larga escala desnecessário, desproporcional e excessivo de dados pessoais sensíveis (biométricos) de

estudantes da rede pública de ensino, em sua maioria crianças e adolescentes, para a consecução da finalidade de registro de frequência escolar, em desrespeito ao art. 6º, inciso III, da LGPD, tendo em vista a existência de meios menos invasivos à privacidade dos titulares afetados que, se utilizados, alcançariam resultados similares aos pretendidos pelo controlador. Nesse sentido, o controlador não apresentou evidências de que tenha realizado uma análise efetiva da necessidade e da proporcionalidade da utilização da tecnologia de reconhecimento facial para o controle de frequência escolar, especialmente quanto aos potenciais impactos dessa prática sobre os direitos e as garantias fundamentais de crianças e adolescentes. Em vez disso, limitou-se a justificar a medida com o objetivo de reduzir o tempo despendido em sala de aula para essa atividade, sem, contudo, demonstrar, por meio de estudos ou avaliações realizados após a implementação da tecnologia, que esse benefício tenha sido efetivamente alcançado.

6.1.3. Deixar de demonstrar que os sistemas utilizados para o tratamento de dados pessoais biométricos dos alunos da rede pública de ensino do Estado do Paraná, para fins de registro de frequência escolar, nos termos da Resolução GS/SEED nº 2.865/2023, foram estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais de proteção de dados pessoais, em desconformidade com os arts. 6º, incisos VII, VIII e X, e 49 da LGPD. As medidas relacionadas no Relatório de Impacto à Proteção de Dados (RIPD) não são suficientes para demonstrar a mitigação adequada dos riscos elevados associados ao reconhecimento facial de crianças e adolescentes como mecanismo de gestão de presença escolar. Permanecem não comprovadas, nesse sentido, a eficácia dos controles de segurança, a governança sobre os acessos e compartilhamentos, a supervisão do fornecedor, a confiabilidade e não discriminação do algoritmo, a avaliação de alternativas menos invasivas e o atendimento

concreto ao melhor interesse dos estudantes.

6.1.4. Realizar o tratamento em larga escala de dados pessoais sensíveis (biométricos) de estudantes da rede pública de ensino sem considerar o melhor interesse deste grupo de titulares, em desrespeito ao art. 14, caput, da LGPD c/c o Enunciado CD/ANPD nº 1/2021. O controlador, nesse sentido, não apresentou evidências que demonstrassem que a implementação da tecnologia foi realizada após a consideração do melhor interesse das crianças e adolescentes afetados pela medida, em especial no que se refere aos eventuais benefícios alcançados em detrimento da interferência nos direitos de proteção de dados pessoais, privacidade e acesso à educação decorrentes do tratamento de dados biométricos.

6.1.5. Obstrução às atividades fiscalizatórias da ANPD em razão da seguida omissão em fornecer cópias de documentos e informações necessários para a avaliação das atividades de tratamento investigadas, em desrespeito aos arts. 5º, inciso I, e 6º do Regulamento de Fiscalização.

6.2. Diante do exposto, sugere-se que, nos termos dos arts. 30 e 32, inciso III, do Regulamento de Fiscalização, e do art. 17, I e III, do Regimento Interno da ANPD (Portaria nº 1, de 8 de março de 2021), seja adotada medida preventiva de **Informe** para determinar à SEED/PR que:

6.2.1. **Suspenda imediatamente** o tratamento de dados pessoais biométricos de crianças e adolescentes da rede pública de ensino do Estado do Paraná, conforme estabelecido pela Resolução GS/Seed nº 2.865, de 08/05/2023, publicada no Publicado no Diário Oficial nº 11.415 de 10/05/2023 (0195330, p. 12), realizado com a finalidade de verificação e **registro de frequência escolar,** por meio da utilização de tecnologia de reconhecimento facial, em seus sistemas e no dos seus operadores e suboperadores, ficando sob sua responsabilidade a comprovação da suspensão do tratamento em todos os âmbitos.

6.3. Recomenda-se, ainda, o envio do presente processo à

Coordenação-Geral de Sanção, para avaliar a possibilidade de abertura de processo administrativo sancionador em face do regulado, de acordo com o art. 35, § 4º, da Resolução CD/ANPD nº 1, de 28/10/2021.

6.4. Sugere-se encaminhar cópia desta Nota Técnica ao Denunciante e ao Ministério Público Estadual do Paraná, para conhecimento.

6.5. Por fim, intime-se a regulada a respeito da presente Nota Técnica para conhecimento e adoção das providências cabíveis.

À consideração superior.

PRISCILA LINI
Chefe da Divisão de Fiscalização 2

RENATA DE ASSIS CALSING
Coordenadora de Proteção de Dados Pessoais

De acordo. Encaminha-se ao Superintendente de Fiscalização.

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA
Coordenador Geral de Fiscalização

Referências:

1. ^ Resolução CD/ANPD nº 10, de 5 de dezembro de 2023, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528.
2. ^ Em atenção à restruturação da ANPD, em decorrência de sua conversão em Agência Reguladora, a então Coordenação-Geral de Fiscalização foi sucedida pela Superintendência de Fiscalização (SFI), nos termos do Despacho Decisório CD/ANPD nº 68/2026 (0278971). A atual Coordenação-Geral de Fiscalização, sucessora da Coordenação de Fiscalização, por sua vez, é a unidade administrativa da SFI

responsável por conduzir investigações, sendo a Coordenação de Proteção de Dados Pessoais, CPDP, a responsável pelos casos de adequação de tratamentos de dados conforme a LGPD.

3. ^ Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
4. ^ Esse tópico já foi abordado no presente processo, na Nota Técnica nº 55/2024/FIS/CGF/ANPD (0159528).
5. ^ Segundo o § 1º do citado artigo, o tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.
6. ^ Itens a, b e d do artigo destacado.
7. ^ Nota Técnica 5 /2025/FIS/CGF/ANPD (0165389), item 5.6.1.
8. ^ Nota Técnica 5 /2025/FIS/CGF/ANPD (0165389).
9. ^ CRUZ, S. N.; MONTEIRO, Renato Leite. Como identificar a base legal adequada na LGPD?. In: Obra coletiva. (Org.). Comentários à Lei Geral de Proteção de Dados Pessoais. 1ed.São Paulo: Migalhas, 2021, v. 1, pp. 90-100. Ver, também, Nota Técnica nº 5/2025/FIS/CGF/ANPD, item 5.6.1.
10. ^ A denúncia (0133059) cita o relatório: ISRAEL, Carolina Batista; FIRMINO, Rodrigo (coords.), *Reconhecimento facial nas escolas públicas do Paraná*. Curitiba: UFPR, que contém vários indícios do início do tratamento de dados pessoais biométricos pela SEED-PR já no ano de 2021, como entrevistas com professores estaduais.
11. ^ Embora a Secretaria de Educação disponha de competência para disciplinar os procedimentos internos de apuração de frequência escolar, a escolha de tecnologia de alto impacto sobre direitos fundamentais, como o reconhecimento facial, configura decisão administrativa que amplia a esfera de deveres dos cidadãos afetados, pois gera clara restrição a direitos fundamentais das crianças e adolescentes que devem se submeter ao cadastramento biométrico como condição para a realização da matrícula e o registro de frequência.
12. ^ FRAZÃO, Ana; CARVALHO, Ângelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados Pessoais: fundamentos da LGPD. 1º ed. Rio de Janeiro: Forense, 2022. p. 128.
13. ^ As resoluções de secretários estaduais são atos administrativos secundários por derivarem sua validade e fundamento de atos primários, como leis e decretos, e por se limitarem a detalhar e explicar a legislação existente dentro de suas áreas de competência.
14. ^ FRAZÃO, Ana; CARVALHO, Ângelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados Pessoais: fundamentos da LGPD. 1º ed.

Rio de Janeiro: Forense, 2022. p.87.

15. ^ Processo 23.348.296-0 SEED/PR - p. 43 (0174716)
16. ^ Incidente de segurança, nos termos do art. 3º, XII, da Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança, é “qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais”.
17. ^ Art. 39. O operador deverá realizar o tratamento **segundo as instruções fornecidas pelo controlador**, que verificará a observância das próprias instruções e das normas sobre a matéria.
18. ^ Agencia Española de Protección de Datos – AEPD. Introducción al hash como técnica de seudonimización de datos personales. Disponível em: https://www.aepd.es/guias/estudio-hash-anonimidad.pdf, acesso em 16/10/2025.
19. ^ Art. 37. O controlador e o operador **devem** manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
20. ^ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
21. ^ FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de Proteção de Dados - Fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. ISBN 9786559645831.p 109
22. ^ Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.
23. ^ Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros: I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;
24. ^ Art. 6º O não cumprimento dos deveres estabelecidos no art. 5º poderá caracterizar obstrução à atividade de fiscalização, sujeitando o infrator a medidas repressivas, sem prejuízo da adoção das medidas necessárias com o objetivo de concluir a ação de fiscalização obstruída por parte da ANPD.
25. ^ Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf.
26. ^ No que se refere à segurança, entende-se o dever de adoção de

medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos do art. 46 da LGPD.

27. ^ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
28. ^ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
29. ^ BARRETT, Lindsey. *Ban Facial Recognition Technologies for Children—And for Everyone Else* (July 24, 2020). Boston University Journal of Science and Technology Law. Volume 26.2, Available at SSRN: https://ssrn.com/abstract=3660118
30. ^ Koudelová *et al*, Simulation of facial growth based on longitudinal data: Age progression and age regression between 7 and 17 years, 2019.
31. ^ A pesquisa revelou que, ao comparar uma imagem de matrícula inicial com imagens coletadas ao longo do tempo, a Taxa de Precisão de Verificação (TAR) sofre uma queda progressiva e acentuada. Enquanto para um intervalo de dois anos a TAR era de 98,52% (com uma Taxa de Falsa Aceitação de 0,1%), esse índice caiu para 95,68% em quatro anos, reduzindo para 87,24% após seis anos e atingindo apenas 71,32% em um intervalo de oito anos. A pesquisa identificou que a maior queda de acurácia ocorre justamente no período de transição para a vida escolar, onde tais tecnologias são frequentemente propostas para controle de acesso e monitoramento. Ver mais em: Mobilio, When the Kids Aren't Alright: The Use of Facial Recognition Technologies at School, 2024; e Singh, *et al.* Longitudinal Evaluation of Child Face Recognition and the Impact of Underlying Age, 2024.
32. ^ Outras evidências quantitativas são corroboradas por estudos que mapeiam as trajetórias de envelhecimento facial. A modelagem tridimensional do crescimento facial entre 7 e 17 anos de idade revela que o processo não é uniforme, apresentando picos de crescimento associados ao início da puberdade, que ocorrem em idades diferentes entre meninos e meninas. A pesquisa identificou taxas de crescimento semelhantes entre os sexos dos 7 aos 10 anos, seguidas por um aumento na velocidade de crescimento com máximas entre 11 e 12 anos nas meninas e 11 e 13 anos nos meninos. Em: Koudelová, *Idem,*

2019.

33. ^ Zuboff, *Idem.*
34. ^ Godsell, Communication Minister Anika Wells' age-check scheme for social media ban raises privacy, data hoarding fears, 2025.
35. ^ A Nota Técnica nº 55/2024/FIS/CGF/ANPD (SEI nº 0159528) serviu de fundamento para o Despacho Decisório nº 27/2024/FIS/CGF (SEI nº 0159980), que determinou a instauração do presente processo de fiscalização.
36. ^ Em atenção à restruturação da ANPD, em decorrência de sua conversão em Agência Reguladora, a então Coordenação-Geral de Fiscalização foi sucedida pela Superintendência de Fiscalização (SFI), nos termos do Despacho Decisório CD/ANPD nº 68/2026 (0278971). A atual Coordenação-Geral de Fiscalização, sucessora da Coordenação de Fiscalização, por sua vez, é a unidade administrativa da SFI responsável por conduzir a investigação.
37. ^ Nota Técnica nº 10/2025/FIS/CGF/ANPD (0167203).
38. ^ Nota Técnica nº 10/2025/FIS/CGF/ANPD (0167203).

Documento assinado eletronicamente por **Priscila Lini**, **Servidor(a) Requisitado(a)**, em 31/07/2026, às 18:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Renata de Assis Calsing**, **Coordenador(a)**, em 31/07/2026, às 18:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima**, **Coordenador(a)-Geral**, em 31/07/2026, às 19:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

[redacted]