



MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

AO JUÍZO DE DIREITO DA VARA DA FAZENDA PÚBLICA DA COMARCA DE CAMPO MOURÃO – PR

A ação se baseia no uso indevido de sistemas de reconhecimento facial em escolas da rede estadual do Paraná para registro de frequência de alunos. A petição argumenta que o uso do reconhecimento facial viola o regramento sobre a proteção dos dados pessoais. O Ministério Público pede a remoção do ilícito e a indenização por danos morais coletivos.

MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ, por intermédio do seu Agente Ministerial que esta subscreve, com fundamento nos artigos 37, *caput* e parágrafo 4º, artigos 127 e 129, inciso III, todos da Constituição Federal; no artigo 1º inciso IV da Lei Federal nº 7.347/1985, no artigo 25, alínea “a” e “b” da Lei nº 8.625/1993 e na Lei 13.709/2018, além de outros dispositivos legais aplicáveis à espécie, com base nos documentos do Inquérito Civil nº 0024.24.000014-1, vem, perante este r. juízo, propor:

AÇÃO CIVIL PÚBLICA DE REMOÇÃO DE ILÍCITO CUMULADA COM INDENIZAÇÃO POR VIOLAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS COM PEDIDO DE TUTELA PROVISÓRIA DE URGÊNCIA

contra o **ESTADO DO PARANÁ**, pessoa jurídica de direito público interno, ente representado, para fins judiciais, pelo Excelentíssimo Senhor Procurador-Geral do Estado, a ser citado na Rua Paula Gomes, 145, Curitiba-PR; **COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PARANÁ - CELEPAR**, sociedade de economia mista, inscrita no CNPJ nº 76.545.011/0001-19, com sede na Rua Mateus Leme, 1561, Bom Retiro, CEP 80.520-174, Curitiba/PR, representada por seu Diretor Presidente, Sr. André Gustavo Souza Garbosa, e seu Diretor Administrativo Financeiro e Jurídico, Sr. Guilherme de Abreu e Silva; **VALID SOLUÇÕES S.A.**, inscrita no CNPJ nº 33.113.309/0001-47, com sede na Rua Alameda Rio Claro, 241, Bela Vista, São Paulo/SP, CEP 01332-010, representada por seu Diretor Comercial e Marketing, Sr. Ilson Roque Bressan, CPF nº 478.661.950-72, e seu procurador, Sr. André Luiz Cutrim Gallózio, CPF nº 106.732.947-14, pelos seguintes fatos e fundamentos jurídicos.





3ª Promotoria de Justiça de Campo Mourão

1. DOS FATOS

A Administração Pública do Estado do Paraná começou a utilizar, em novembro de 2022¹, sistemas de reconhecimento facial por inteligência artificial em instituições de ensino da rede estadual para o registro de frequência dos alunos do Ensino Fundamental II (6º ao 9º ano) e do Ensino Médio (1º ao 3º ano)². No município de Campo Mourão, 11 (onze) instituições implementaram esta tecnologia.

O Estado do Paraná, por meio da Secretaria da Educação e do Esporte (SEED), autorizou a Companhia de Tecnologia da Informação e Comunicação do Paraná (Celepar) a realizar a coleta e o tratamento da biometria facial e de imagens dos estudantes da rede estadual de ensino para fins de registro de frequência escolar utilizando reconhecimento facial.

A partir disso, a Celepar publicou edital de licitação na modalidade Pregão Eletrônico nº 1349/2020, com o seguinte objeto: *“Contratação de empresa para prestação de serviços de reconhecimento biométrico facial por meio da análise de imagens; serviços de processamento e armazenamento em nuvem para sustentação deste ambiente e suporte técnico para a integração de informações com sistemas legados”*.

A justificativa para a contratação dos sistemas de reconhecimento facial³ foi que a implementação *“permitirá ao professor uma redução no tempo para a realização das chamadas e permitirá aos pais e responsáveis ter maior segurança quanto à presença e frequência dos seus filhos à escola, com acompanhamento por meio do aplicativo”*⁴.

No arquivo “Justificativa da Aquisição”, elaborado pela Celepar, foi esclarecido que o reconhecimento facial se trata de recurso para identificar rostos humanos em imagens por meio de sistemas de Inteligência Artificial⁵.

O item 8.1.1.21 do Termo de Referência nº 46/2020 constou previsão expressa de que “o motor biométrico” deveria ser capaz de: (i) identificar o gênero; (ii) detectar emoções;

¹O contrato de nº 4313/2022 celebrado entre a Companhia de Tecnologia da Informação e Comunicação do Paraná (Celepar) e a Valid Soluções S. A foi assinado em 16 de setembro de 2022 e começou a ser executado em novembro de 2022 (seq. 27.2 do Inquérito Civil).

²A matrícula no Ensino Fundamental é obrigatória para alunos com seis anos completos ou a completar até o dia 31 de março do ano em que ocorrer a matrícula, conforme art. 32, da Lei 9.394/1996 (Lei das Diretrizes e Bases da Educação Nacional) e artigo 3º da Resolução CNE/CBE 6/2010. Assim, os alunos ingressam no 6º ano do Ensino Fundamental com 10 anos (nos casos de início do ensino fundamental com seis anos incompletos) ou 11 anos (no caso de ingresso com 6 anos completos).

³O vídeo explica como a chamada por reconhecimento facial é feita: <https://www.youtube.com/watch?v=APtzE5QxKnk&>

⁴Conforme item “2 Justificativa e objetivos da contratação” do Termo de Referência nº 46/2020, anexo ao edital de licitação (fls. 234, mov. 18 do Protocolo nº 16.994.392-3).

⁵Conforme fls. 234, mov. 18 do Protocolo nº 16.994.392-3. Na justificativa apresentada pela Celepar que antecedeu a contratação da Valid S/A, A Celepar divulgou uma notícia de que o uso de reconhecimento facial em registros de presença da Valid Soluções S/A seria realizada por meio de inteligência artificial (seq. 27.2 do Inquérito Civil) Disponível em: <https://encurtador.com.br/U70dx>





3ª Promotoria de Justiça de Campo Mourão

(iii) idade aproximada; (iv) atributos faciais: sorriso, boca aberta, olhos fechados; e (v) acessórios: óculos, chapéu e bigode⁶.

A pessoa jurídica Valid Soluções S. A. venceu a licitação, apresentando uma proposta de R\$4.501.760,00 (quatro milhões, quinhentos e um mil e setecentos e sessenta reais) sendo que, hoje, com os aditivos, o valor contratado é de R\$12.133.290,45. O contrato foi assinado em 16 de setembro de 2022 e começou a ser executado em novembro de 2022, conforme informações do Portal da Transparência do Estado do Paraná⁷.

O sistema de registro de frequência por reconhecimento facial é feito por meio do aplicativo Escola Paraná Professores, que foi desenvolvido pela Celepar. Por outro lado, a coleta da biometria facial dos alunos ocorre por meio de outro aplicativo, o Escola Paraná Biometria. O processamento do reconhecimento facial biométrico é realizado pela pessoa jurídica Valid Soluções S. A.

De acordo com o Relatório de Impacto à Proteção de Dados Pessoais⁸ apresentado pela SEED, o fluxo de informações ocorre da seguinte forma.

A coleta da biometria facial dos alunos é realizada pelo docente ou profissional autorizado pela SEED (são tiradas três fotos por aluno, para fins de cadastro).

A seguir, as fotos e a identificação do aluno são enviadas para a Celepar. Elas ficam gravadas em um servidor *Network-Attached Storage* (NAS)⁹, sem identificação, e um link para a imagem é associado ao aluno em seu cadastro dentro do banco de dados.

Em seguida, as imagens são enviadas para a Valid Soluções S. A em arquivo JPEG acompanhadas de um código de agrupamento gerado na Celepar. Após o processamento da imagem, a Valid, pelo contrato, gera uma chave de identificação (*hash*) e exclui a foto. A chave gerada pela Valid é enviada e armazenada pela Celepar, que, por sua vez, a vincula ao Código Geral de Matrícula do aluno correspondente.

Abaixo, segue fluxograma para melhor compreensão da fase de cadastro do aluno:

⁶Conforme item "8.1.1.21" do Termo de Referência nº 46/2020 (seq. 19 do Inquérito Civil - ref. Protocolo nº 16.994.392-3).

⁷Informações disponíveis no Portal da Transparência, juntadas no seq. 27.3 a 27.5 do Inquérito Civil.

⁸Disponível nas fls. 730 e seguintes (mov. 109) do Protocolo nº 16.994.392-3.

⁹Tradução: armazenamento conectado à rede. É um servidor de armazenamento de dados de computador em nível de arquivo (em oposição ao armazenamento em nível de bloco) conectado a uma rede de computadores que fornece acesso a dados a um grupo heterogêneo de clientes. Disponível em <https://pt.wikipedia.org/wiki/Armazenamento_conectado_%C3%A0_rede>





PROCEDIMENTO DE CADASTRO DO ALUNO



Na chamada do aplicativo Escola Paraná - Professores, é disponibilizada a opção de chamada por reconhecimento facial, que utiliza a câmera do próprio celular do docente. São realizados os registros da imagem da turma e transmitidos imediatamente para a Celepar, junto com a identificação da turma.

Ao receber a imagem da turma, a Celepar armazena a foto no servidor NAS sem identificação, criando um link em um banco de dados.

Na sequência, a imagem é enviada para o reconhecimento dos alunos à Valid, que retorna uma lista de chaves identificadas na foto. Com essa lista, são identificados os Códigos Gerais de Matrícula dos alunos na base de dados da Celepar e enviados ao



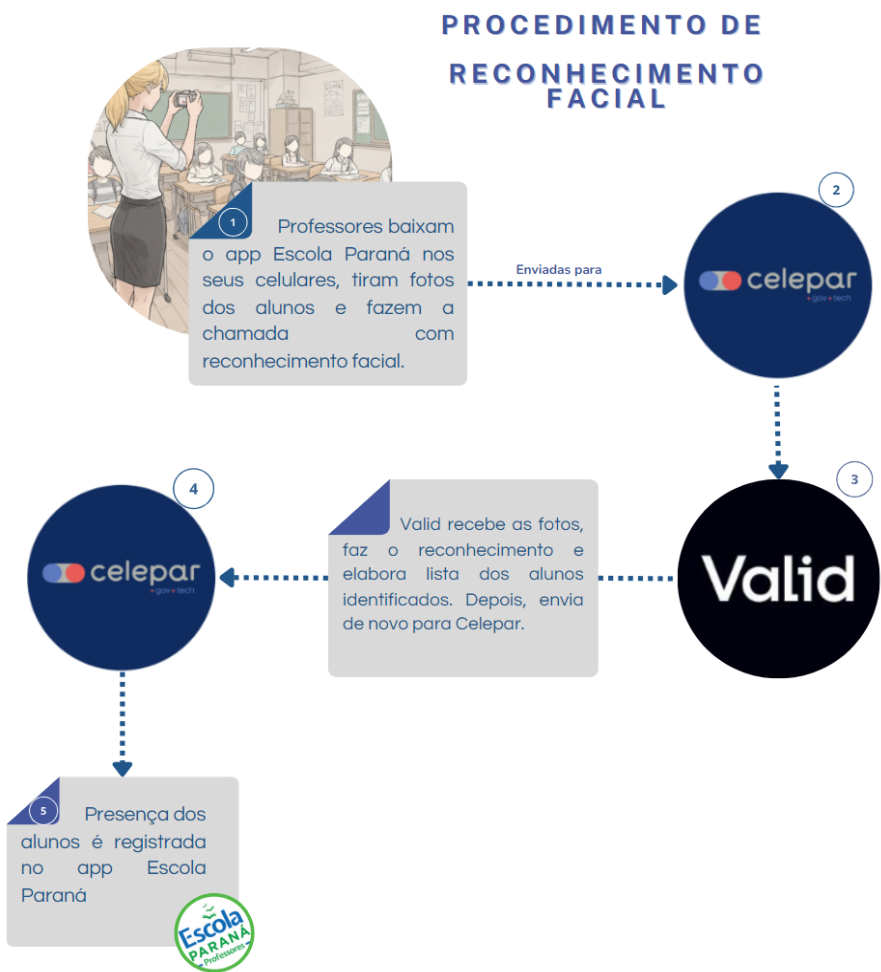


MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

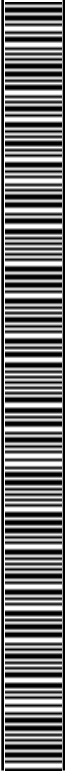
aplicativo para o registro da presença.

Abaixo, segue fluxograma para melhor compreensão da fase de reconhecimento facial dos alunos:



No relatório de impacto à proteção de dados pessoais, consta que é feito o reconhecimento facial de aproximadamente um milhão de alunos.

Como será visto, este comportamento é ilegal porque violou diversas normas da Lei Geral de Proteção de Dados e causou danos de natureza coletiva, que devem, por meio desta ação, ser reparados.





3ª Promotoria de Justiça de Campo Mourão

2. DA TUTELA COLETIVA NA PROTEÇÃO DOS DADOS PESSOAIS

Rafael Zanatta, em sua obra *A proteção coletiva dos dados pessoais no Brasil: vetores de interpretação*, assinala que: “[...] a LGPD foi pensada, desde o início, a partir de amplos mecanismos de acesso à justiça e de tutela coletiva à proteção de dados pessoais”¹⁰.

Foi neste contexto que a Lei 13.709/2018 (Lei Geral de Proteção de Dados), em seu artigo 22, deixou explícito que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

O legislador também deixou clara a possibilidade da tutela coletiva na proteção de dados ao prever a responsabilização pelo dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados (art. 42).

No caso em julgamento, é evidente a necessidade da tutela coletiva, tendo em vista que os direitos violados são de natureza coletiva, ou seja, a situação narrada atinge todos os alunos da rede estadual de ensino matriculados e sujeitos ao reconhecimento facial utilizado para a chamada nas escolas estaduais do Paraná.

Ademais, a ilicitude está sendo praticada em prejuízo ao patrimônio público, uma vez que estão sendo despendidos recursos do Estado para a execução de um contrato administrativo cujo objeto viola frontalmente o direito à proteção dos dados pessoais. Observa-se que, até o presente momento, o contrato celebrado entre as requeridas Celepar e Valid Soluções, com os aditivos, alcançou o patamar de R\$12.133.290,45.

O caso abrange escolas públicas de ensino fundamental e ensino médio de todo o Paraná, incluindo as escolas da Comarca de Campo Mourão-PR. Diante do art. 2º da Lei nº 7.347/1985, é competente para julgar o feito o foro do local onde ocorrer o dano¹¹, e a propositura da ação prevenirá a jurisdição do juízo para todas as ações posteriormente intentadas que possuam a mesma causa de pedir ou o mesmo objeto.

Além disso, a sentença fará coisa julgada *erga omnes* para todas as escolas do Paraná, conforme disposição do art. 16, da Lei de Ação Civil Pública, sem o vício de inconstitucionalidade da expressão “*nos limites da competência territorial do órgão*”

¹⁰ZANATTA, Rafael A. F. *A proteção coletiva dos dados pessoais no Brasil: vetores de interpretação* - Belo Horizonte: Letramento, 2023, p. 259.

¹¹No mesmo sentido, o Superior Tribunal de Justiça definiu, em decisão vinculante proferida no Incidente de Assunção de Competência nº 10, que prevalecem sobre quaisquer outras normas locais, primárias ou secundárias, legislativas ou administrativas, a competência do local do dano para ação civil pública, conforme fixado na tese “A”, item “j”.





prolator”, conforme reconhecido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 1.101.937/SP¹².

3. DA VIOLAÇÃO À LEI GERAL DE PROTEÇÃO DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados representa um marco significativo na legislação brasileira, estabelecendo diretrizes para o tratamento de dados pessoais. O objetivo central da lei reside na proteção do dado pessoal, que pode ser definido como qualquer informação relacionada a pessoa natural identificada ou identificável (art. 5º, inciso I, LGPD).

A proteção de dados pessoais foi incluída expressamente no rol de direitos fundamentais previstos na Constituição da República, em seu art. 5º, inciso LXXIX, pela Emenda Constitucional nº 115/2022, consolidando sua importância no ordenamento jurídico brasileiro como direito fundamental autônomo.

No âmbito da Administração Pública, a LGPD estabelece regras específicas para o tratamento de dados pessoais, conforme previsto no artigo 23. A Administração Pública deve tratar os dados pessoais para atendimento de sua finalidade pública, na persecução do interesse público, visando executar as competências legais ou cumprir as atribuições legais do serviço público.

Para tanto, deve informar as hipóteses em que realiza o tratamento de dados pessoais, com informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, e devem indicar o encarregado¹³.

A exigência prevista no artigo 23 de que o tratamento dos dados pessoais pela Administração Pública deve atender à finalidade pública, na persecução do interesse público, está relacionada aos princípios da supremacia e da indisponibilidade do interesse público.

O princípio da supremacia do interesse público significa que o Estado deve atuar na busca da justiça social, do bem comum e do bem estar coletivo. Isso tanto no momento da elaboração de uma lei como na sua execução pela Administração Pública. Por outro lado, a indisponibilidade do interesse público significa que a Administração Pública não é titular dos

¹²O Recurso Extraordinário foi afetado ao Tema de repercussão geral nº 1.075, que envolvia a discussão da constitucionalidade do artigo 16 da Lei da Ação Civil Pública, com a redação dada pela Medida Provisória nº 1.570/1997, que previa a limitação dos efeitos da sentença civil, julgada erga omnes, aos limites da competência territorial do órgão prolator.

¹³Art. 5º Para os fins desta Lei, considera-se: [...] VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).





direitos da coletividade e, por isso, não tem disponibilidade sobre eles, devendo atuar de modo a protegê-los¹⁴.

No caso em questão, as condutas dos requeridos infringiram a Legislação de Proteção dos Dados Pessoais em quatro aspectos, são eles: violação aos princípios expressos no art. 6º, da LGPD; violação ao direito à autodeterminação informativa, garantido como fundamento da proteção de dados pessoais no artigo 2º, inciso II, da LGPD; violação ao direito dos titulares dos dados de terem seus dados tratados alicerçados em bases legais válidas (aquelas previstas nos artigos 7º e 11); e a ilegalidade do consentimento fornecido pelos pais ou responsáveis legais dos titulares dos dados pessoais.

3.1. VIOLAÇÃO AO ARTIGO 6º DA LEI GERAL DE PROTEÇÃO DE DADOS: PRINCÍPIOS

A observância aos princípios previstos no art. 6º da Lei Geral de Proteção de Dados é elemento fundamental para uma interação legítima entre agentes de tratamento e titulares de dados pessoais.

Contudo, no presente caso, os requeridos violaram os princípios da finalidade, transparência e necessidade, previstos no art. 6º da Lei Geral de Proteção de Dados. Esses princípios, de observância obrigatória por aqueles que controlam e operam dados pessoais, foram desrespeitados pelas ações dos requeridos.

3.1.1. VIOLAÇÃO AO PRINCÍPIO DA FINALIDADE E DA TRANSPARÊNCIA

O princípio da finalidade, nos termos do art. 6º, inciso I, consiste na realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

O princípio da transparência, por sua vez, garante aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, conforme art. 6º, inciso VI, da Lei 13.709/2018.

Este princípio impõe obrigações de cunho geral e demanda uma postura ativa do agente de tratamento, que tem o dever de disponibilizar as informações exigidas pela lei, independentemente de solicitação do titular¹⁵.

Ambos os princípios estão intrinsecamente ligados, pois o princípio da finalidade somente será respeitado se as informações forem fornecidas de forma clara e precisa ao

¹⁴DI PIETRO. Maria Sylvia Zanella. *Direito Administrativo*, 29ª Ed. Rio de Janeiro, Forense, 2016. p. 97-98. apud MELLO. Celso Antônio Bandeira de. *Curso de Direito Administrativo*. São Paulo: Malheiros, 2004. p. 69.

¹⁵Conforme o [Guia orientativo da ANPD](#) "Tratamento de dados pessoais pelo Poder Público", versão 2.0, Junho/2023 (p. 26-27).





titular, conforme pressupõe o princípio da transparência.

Se os titulares dos dados não forem informados de maneira clara e inequívoca sobre os propósitos específicos para os quais seus dados estão sendo coletados e utilizados, não poderão consentir de forma livre, informada e inequívoca, conforme exigido pela LGPD. Isso porque a falta de transparência impede que o titular compreenda a real finalidade do tratamento, comprometendo sua capacidade de tomar decisões conscientes sobre seus dados pessoais.

No caso concreto, uma das afrontas ao princípio da finalidade decorreu do fato de que os propósitos do tratamento de dados biométricos não foram explícitos e informados aos titulares dos dados. Tal fato ficou evidente nos requerimentos de matrícula e de renovação de matrícula¹⁶, em que constaram autorizações para:

“tratar e utilizar os dados e imagens do estudante para fins institucionais, estatísticos, frequência escolar, coleta do Censo Escolar, planejamento e execução de ações, programas e políticas públicas e quando necessário, o compartilhamento com a rede proteção, Ministério Público, sistema público de segurança, sistema público de saúde e demais setores da administração pública que possuam acordo de cooperação.”

“autorizo o uso da imagem e dos registros educacionais nos Sistemas Estaduais de Educação do(a) aluno(a) citado para fins estatísticos da SEED/PR, Censo Escolar, comunicação oficial da SEED, planejamento e execução de políticas e/ou programas públicos, atendimento à rede proteção e da imagem para fins de frequência escola.”

Apesar de constar menção à “frequência escolar” nas autorizações transcritas, não foi devidamente informado que o registro da frequência seria realizado por meio de reconhecimento facial, tampouco que os dados pessoais utilizados seriam a biometria facial dos alunos.

Outro fato que viola diretamente o princípio da finalidade é a falta de informação do motivo para que serão detectadas as emoções, de atributos faciais como sorriso, boca aberta, olhos fechados e o uso de acessórios como óculos, chapéu e bigode, cuja exigência constou expressamente no Termo de Referência nº 46/2020¹⁷.

Tais informações são consideradas dados pessoais, nos termos do art. 5º, inciso I, da LGPD, uma vez que estão relacionadas à pessoa natural identificada ou identificável¹⁸. Por essa razão, somente poderiam ser tratados para uma finalidade legítima e devidamente informada aos titulares, o que não aconteceu no caso concreto.

¹⁶ Documentos de seq. 15.3 a 15.6 do Inquérito Civil, enviados pela Celepar em resposta ao Ofício nº 225/2024-3º.

¹⁷ Conforme item “8.1.1.21” do Termo de Referência nº 46/2020 (seq. 19 do Inquérito Civil - ref. Protocolo nº 16.994.392-3).

¹⁸ Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.





A requerida Celepar, ao ser questionada pela Valid Soluções S. A. se poderia fornecer um sistema de reconhecimento facial sem a funcionalidade de detecção de *emoções, sorriso, chapéu e bigodes*, afirmou que estas funcionalidades são mínimas e obrigatórias, ainda que “*não associado a nenhum acordo de nível de serviço*”¹⁹. Na mesma ocasião, a Celepar informou que esses dados devem ser coletados para futuras análises estatísticas e de interesse da contratante.

Ou seja, não há propósito legítimo para a coleta de tais dados pessoais dos alunos paranaenses, de modo que o tratamento destes dados pessoais configura clara violação ao princípio da finalidade.

Além disso, não houve menção ao tratamento dos dados pessoais relacionados às emoções dos alunos no Relatório de Impacto à Proteção de Dados. Verificou-se, portanto, que existem outros dados pessoais coletados além dos informados no Relatório de Impacto, configurando também violação ao princípio da transparência.

O princípio da transparência também foi violado pelos requeridos por não terem informado, de forma específica, como ocorreria a coleta e armazenamento dos dados pessoais dos alunos, e por não terem identificado quais dados sensíveis dos alunos seriam tratados, assim como a sua finalidade específica.

Os dados pessoais informados como tratados no processo de reconhecimento facial no Relatório de Impacto à Proteção de Dados foram: (i) Código Geral de Matrícula do aluno (CGM), (ii) frequência escolar, (iii) fotos individualizadas e (iv) fotos da turma capturadas em sala de aula, além dos dados gerais da escola e da turma.

Contudo, embora informado que são tratadas no processo de reconhecimento facial fotos individualizadas, é notório que o dado pessoal tratado no sistema de reconhecimento facial para registro de frequência é a biometria facial, cuja diferenciação será melhor compreendida no tópico destinado à violação do direito à autodeterminação informativa.

Assim, a conduta praticada pelos requeridos violou tanto o princípio da transparência, por não fornecer todas as informações necessárias sobre o tratamento dos dados pessoais, quanto o princípio da finalidade, vez que não expuseram aos titulares dos dados e a seus responsáveis o propósito do tratamento dos dados sensíveis dos alunos.

¹⁹Conforme fls. 358, do Protocolo nº 16.994.392-3. Transcreve-se o seus termos: *Estas funcionalidades são mínimas e obrigatórias, porém não está associado a nenhum acordo de nível de serviço mas deve existir e funcionar. Portanto o serviço fornecido deve atender ao item 8.1.1.21 - Para futuras análises estatísticas e de interesse da CONTRATANTE, o motor biométrico deve ser capaz de gerar as seguintes informações a partir das imagens capturadas nos eventos de identificação automatizada de rostos: a) Identificação de gênero; b) Detecção de emoções; c) Idade aproximada; d) Atributos faciais: Sorriso, boca aberta, olhos fechados; e) Acessórios: Óculos, chapéu e bigode”.*





3.1.2. VIOLAÇÃO AO PRINCÍPIO DA NECESSIDADE

O princípio da necessidade, por seu turno, diz respeito à 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 (art. 6º, inc. III, LGPD).

A violação ao princípio da necessidade no caso dos autos é clara, pois o registro de frequência poderia ser feito de outras formas, sem precisar utilizar dados faciais biométricos de crianças e adolescentes. É patente a desproporcionalidade quanto ao uso desses dados para tal fim, ainda mais tratando-se de crianças e adolescentes, pessoas com vulnerabilidade tutelada pelo Estatuto da Criança e do Adolescente²⁰.

É evidente que a Administração Pública poderia estudar e viabilizar formas menos invasivas para buscar "melhor eficiência" na chamada para *"permitir ao professor uma redução no tempo para a realização das chamadas e permitir aos pais e responsáveis ter maior segurança quanto à presença e frequência dos seus filhos à escola, com acompanhamento por meio do aplicativo"*²¹.

O fato de a chamada escolar via reconhecimento facial envolver direitos tão sensíveis e fortemente tutelados pelo ordenamento jurídico, de titulares de dados com vulnerabilidade acentuada, coloca em cheque a razoabilidade e a legalidade do tratamento dos dados pessoais.

Tanto é que o tratamento dos dados faciais biométricos para o registro de frequência em sala de aula viola diversos princípios do direito brasileiro e, também, tratados de direito internacional dos quais o Brasil é signatário, como o Pacto Internacional sobre Direitos Civis e Políticos e a Declaração Universal dos Direitos Humanos.

Primeiro, o procedimento de reconhecimento facial por inteligência artificial na chamada reduz a subjetividade e a identidade de cada aluno a um *hash*, em um padrão de objetificação temerário, ou mesmo de perfilização, o que coloca em risco a dignidade da pessoa humana. Isso porque a dignidade da pessoa humana pressupõe a autonomia vital da pessoa, a sua autodeterminação relativamente ao estado, às demais entidades públicas e às outras pessoas²².

Segundo, a expectativa dos alunos de que serão fotografados diariamente cria um

²⁰ Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais.

²¹ Conforme item "2 Justificativa e objetivos da contratação" do Termo de Referência nº 46/2020, anexo ao edital de licitação. Conforme fls. 353, mov. 23 do Protocolo nº 16.994.392-3 - Celepar.

²² MIRANDA, Jorge. Manual de Direito Constitucional, 6 ed., Coimbra: Almedina, t. IV, p. 169.





ambiente de vigilância que afeta sua espontaneidade e comportamento, inibindo, até mesmo, o sadio desenvolvimento da personalidade, desrespeitando sua condição peculiar de pessoa em desenvolvimento em transgressão ao art. 71, do ECA²³.

Terceiro, no procedimento de coleta e uso dos dados, haverá o risco de falhas. Possíveis falhas na identificação com o uso do reconhecimento facial para registrar presença em sala de aula potencializa o risco de exposição dos alunos a situações constrangedoras, invasivas e discriminatórias, afetando sua dignidade. Tal exposição confronta com o disposto no art. 18²⁴, que estabelece como dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor.

Além disso, pesa no mesmo lado do princípio da dignidade da pessoa humana em posição contrária à alegada eficiência da administração pública no procedimento de chamada por reconhecimento facial, os princípios da igualdade e o direito à não discriminação, que estão assegurados no artigo 5º, caput e inciso I, da Constituição da República e no artigo 26 do Pacto Internacional sobre Direitos Civis e Políticos.

Quarto, o procedimento de coleta de dados para a chamada escolar via reconhecimento facial não viola somente o direito à proteção dos dados pessoais, mas a própria imagem das crianças e adolescentes, que deve ser tutelada conforme art. 20 do Código Civil e art. 17 do Estatuto da Criança e do Adolescente. As proteções ao direito de imagem também estão previstas no artigo 5º, inciso X, da Constituição da República Federativa do Brasil e no artigo 12 da Declaração Universal dos Direitos Humanos.

Quinto, pesa ainda que no caso concreto é utilizado sistema de inteligência artificial. A adequada utilização de sistemas de inteligência artificial pressupõe a observância dos princípios de direitos humanos e, mesmo diante da ausência de regramento específico sobre o tema - Marco Legal da Inteligência Artificial, que ainda é um Projeto de Lei -, existem normas suficientes para impedir o uso da inteligência artificial quando violar outras regras do ordenamento jurídico, sobretudo normas protetoras dos direitos humanos. Nesse sentido, destaca-se a visão de Alessandro Mantelero de que os sistemas de inteligência artificial já podem ser avaliados considerando os impactos nos direitos humanos²⁵.

Aliás, em uma eventual ponderação de princípios, que poderia, em tese, ser realizada

²³Art. 71. A criança e o adolescente têm direito à informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento.

²⁴Art. 18. É dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor.

²⁵MANTELERO, Alessandro. Além dos Dados: Direitos Humanos, Avaliação Ética e de Impacto Social em IA (Beyond Data - Human Rights, Ethical and Social Impact Assessment in AI) Alemanha: Ed. Springer, 2022.





3ª Promotoria de Justiça de Campo Mourão

entre o princípio da eficiência da administração pública e os princípios da dignidade da pessoa humana, aqueles previstos no art. 6º da LGPD e os acima expostos, a balança, no caso concreto, pesa fortemente para este último lado.

Para corroborar o argumento de desproporcionalidade entre o tratamento dos dados faciais biométricos e a finalidade de registro de frequência nas escolas, o Parlamento Europeu proibiu o reconhecimento de emoções no local de trabalho e nas escolas por meio do Regulamento de Inteligência Artificial²⁶.

A título de ilustração, em 2023, o Tribunal de Justiça de São Paulo determinou, no contexto de reconhecimento facial no Metrô de São Paulo, a abstenção de captação de imagens, sons e quaisquer outros dados pessoais dos usuários sem consentimento prévio do consumidor²⁷, argumentando invasão à intimidade pela captação indevida de imagem (sem prévia autorização). Essa decisão destaca a preocupação com o uso dessa tecnologia em espaços públicos e a necessidade de proteção de dados sensíveis.

Por fim, a coleta massiva de dados biométricos faciais dos alunos e a utilização destes pela inteligência artificial o expõem a riscos de segurança como vazamento de dados, contrariando o direito das crianças às medidas de proteção que a sua condição de infante requer por parte do Estado, previsto no artigo 24 do Pacto Internacional sobre Direitos Civis e Políticos.

Portanto, o tratamento dos dados pessoais sensíveis de crianças e adolescentes não se mostra proporcional e razoável para o propósito pretendido - redução de poucos minutos no registro de frequência escolar - uma vez que os potenciais riscos superam as "vantagens" de sua utilização, configurando clara violação ao princípio da necessidade previsto no art. 6º, inciso III, da Lei Geral de Proteção de Dados.

3.2. VIOLAÇÃO AO ARTIGO 9º DA LEI GERAL DE PROTEÇÃO DE DADOS: DIREITO À AUTODETERMINAÇÃO INFORMATIVA

A autodeterminação informativa é um dos fundamentos da proteção de dados pessoais, nos termos do art. 2º, inciso II, da LGPD. Apesar de não ter seu conceito definido pela legislação, pode ser entendido como a garantia devida ao titular dos dados para que tenha controle sobre seus dados pessoais, de modo que figure na posição de protagonista das decisões sobre o uso de seus dados²⁸.

²⁶Disponível em: <<https://shre.ink/bl4U>> Acesso em 26 de fevereiro de 2025.

²⁷TJSP; Apelação Cível 1090663-42.2018.8.26.0100; Relator (a): Antonio Celso Faria; Órgão Julgador: 8ª Câmara de Direito Público; Foro Central Cível - 37ª Vara Cível; Data do Julgamento: 10/05/2023; Data de Registro: 12/05/2023

²⁸MENDES; Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, v. 120, nov.-dez. 2018. p. 576).





Os direitos previstos no Capítulo III “Dos Direitos do Titular”, assim como aquele previsto no artigo 9º, demonstram a aplicação prática e a forma de exercício da autodeterminação informativa, uma vez que permitem ao titular dos dados ter domínio e acesso facilitado às informações sobre o tratamento de seus dados.

No caso narrado, a autodeterminação informativa dos titulares dos dados não foi respeitada pelos requeridos, uma vez que, por diversas condutas que serão expostas neste tópico, os alunos paranaenses da rede estadual de ensino e seus responsáveis não puderam exercer controle e domínio sobre seus dados pessoais.

A primeira conduta praticada pelos requeridos em desrespeito ao direito à autodeterminação informativa foi a de fornecer informações genéricas no momento da matrícula ou rematrícula dos alunos e não especificar, nos formulários das autorizações, os dados pessoais sensíveis tratados e a finalidade específica para justificar o tratamento deles.

No Relatório de Impacto à Proteção dos Dados Pessoais constou que, na confirmação de vaga, que ocorre *online*, e na efetivação da matrícula anual, o responsável legal é informado acerca do uso dos dados do estudante e a finalidade desse uso no momento que preenche o Requerimento de Matrículas.

Contudo, conforme verificou-se das autorizações supratranscritas no subtópico “3.1.1. VIOLAÇÃO AO PRINCÍPIO DA FINALIDADE E DA TRANSPARÊNCIA”, as informações são genéricas e não há menção aos dados pessoais sensíveis tratados e à finalidade específica que justifica o tratamento, nem mesmo daqueles que exigem o consentimento do titular dos dados, desrespeitando o art. 9º e 23, da Lei Geral de Proteção de Dados (este aplicado ao Estado do Paraná e à Celepar, por força do art. 24, parágrafo único).

A autorização genérica para o tratamento de “*dados e imagens do estudante*” não legitima o tratamento dos dados faciais biométricos de crianças e adolescentes, uma vez que o termo “imagem” não se confunde com o dado facial biométrico.

Isso porque a biometria é a análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo. Segundo Stan Z. Li, a característica biométrica é a característica biológica e comportamental de um indivíduo que pode ser detectada e da qual podem ser extraídas características biométricas distintivas e repetíveis para fins de reconhecimento automatizado de indivíduos. As características biológicas e comportamentais são propriedades físicas de partes do corpo, processos





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

fisiológicos e comportamentais criados pelo corpo e combinações de qualquer um deles²⁹.

O dado pessoal “imagem”, por sua vez, não possui capacidade distintiva e repetível de promover o reconhecimento automatizado de indivíduos. Por essa razão, a suposta autorização para tratamento do dado pessoal “imagem” não legitima o tratamento do dado biométrico, vez que a natureza jurídica deles não se confunde: o dado facial biométrico é dado pessoal sensível, enquanto a imagem é dado pessoal comum.

Além disso, o termo imagem é amplo e, segundo a doutrina de Cristiano Chaves de Faria e Nelson Rosendal³⁰, ela compreende todas as características que tornam uma pessoa singular, podendo ser: imagem-retrato, imagem-atributo ou imagem-voz. Eles conceituam cada uma delas da seguinte forma:

Essa elasticidade conceitual, decorrente da proteção constitucional da imagem (CF, art. 5º, incisos V e X), faz compreender, no conceito de imagem, diferentes aspectos: a imagem-retrato (referindo-se às características fisionômicas do titular, à representação de uma pessoa pelo seu aspecto visual, enfim, é ao seu pôster, à sua fotografia, encarada tanto no aspecto estático – uma pintura – quanto no dinâmico – um filme – art. 5º, X, CF); a imagem-atributo (que é o consectário natural da vida em sociedade, consistindo no conjunto de características peculiares da apresentação e identificação social de uma pessoa, referindo aos seus qualificativos sociais; aos seus comportamentos reiterados. Não se confunde com a imagem exterior, cuidando, na verdade, de seu retrato moral) e a imagem-voz (caracterizada pelo timbre sonoro, que também serve para identificação de uma pessoa, até mesmo porque não poderia imaginar que a personalidade não se evidencia menos na voz que nas características fisionômicas).

Portanto, além da natureza jurídica distinta dos dados tratados (biometria facial) e dos dados informados (imagem), diante da amplitude de abrangência conceitual do termo imagem, a autorização genérica para o tratamento de “dados e imagens do estudante” não é suficiente para legitimar o tratamento de dados biométricos faciais de crianças e adolescentes.

A segunda conduta praticada em afronta ao direito à autodeterminação informativa consistiu em restringir o exercício dos direitos previstos no art. 18 da LGPD, limitando os titulares de dados pessoais a apenas dois canais eletrônicos: Sistema de Ouvidoria e Sistema e-Protocolo³¹.

²⁹Encyclopedia of Biometrics: I - Z., Volume 2, página 80: Biometric characteristic: biological and behavioral characteristic of an individual that can be detected and from which distinguishing, repeatable biometrics features can be extracted for the purpose of automated recognition of individuals. Biological and behavioral characteristics are physical properties of body parts, physiological and behavioral processes created by the body and combinations of any of these.

³⁰FARIA, Cristiano Chaves de; ROSENVALD, Nelson. Direito Civil, Teoria Geral. 6ª ed. Rio de Janeiro: Lumen Juris, 2007. p. 140

³¹ Conforme consta do relatório de impacto (fls. 741-742 - mov. 109 - Protocolo nº 16.994.392-3).





Constou no Relatório de Impacto, também, que os titulares dos dados pessoais podem demandar as solicitações previstas pelo art. 18 da LGPD ou, caso identifiquem alguma falha ou vulnerabilidade de segurança no sistema, pelo Sistema de Ouvidoria ou via Sistema e-Protocolo e que não serão atendidas solicitações dessa natureza por e-mail, contato telefônico ou presencialmente.

No entanto, a imposição dessas restrições para o exercício dos direitos previstos no art. 18 não se compatibiliza com o que propõe a Lei Geral de Proteção de Dados.

Isso porque uma das solicitações previstas neste artigo é justamente a revogação do consentimento (LGPD, art. 18, inciso IX), que, nos termos do §5º do art. 8º, pode ser revogado a qualquer momento mediante manifestação expressa do titular, *por procedimento gratuito e facilitado*.

Neste contexto, Danilo Doneda afirma que restrições à revogação do consentimento implicam injustificada diminuição do poder do titular dos dados pessoais de autodeterminação³². Assim, a limitação do exercício dos direitos previstos no art. 18 a apenas dois canais eletrônicos (Sistema de Ouvidoria e Sistema e-Protocolo) distancia-se do procedimento facilitado exigido pela LGPD.

Além disso, essa conduta viola o princípio do livre acesso, previsto no art. 6º, inciso IV, da LGPD, que garante aos titulares consulta facilitada e gratuita sobre a forma, a duração do tratamento e a integridade de seus dados pessoais. Isto é, de acordo com este princípio, o agente de tratamento tem o dever de disponibilizar mecanismos efetivos para que o titular possa solicitar e ter acesso facilitado e gratuito a determinadas informações referente ao tratamento de seus dados pessoais³³.

A terceira e quarta conduta dos requeridos que violaram o direito à autodeterminação informativa consistiram, respectivamente, na ausência de oferta aos pais e responsáveis, no momento de efetivação da matrícula ou rematrícula, de opção de não consentir com o tratamento de dados pessoais sensíveis para o registro de frequência via reconhecimento facial prevista no Relatório de Impacto à Proteção de Dados Pessoais e na exigência de justificativa para a recusa de fornecimento do consentimento.

No Relatório de Impacto à Proteção de Dados Pessoais constou o seguinte:

Cabe ressaltar que para casos específicos de não consentimentos de captação da imagem do estudante, o docente procederá o Registro de Frequência deste estudante de forma tradicional no Livro de Registro de Classe Online – LRCO, podendo haver

³²DONEDA, Danilo; Da Privacidade à Proteção de Dados Pessoais. Revista dos Tribunais, 2021. P. RB-4.9. Disponível em: <<https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-4.9>> Acesso em 10/03/2025

³³Guia orientativo da ANPD "Tratamento de dados pessoais pelo Poder Público", versão 2.0, Junho/2023.





3ª Promotoria de Justiça de Campo Mourão

alteração nos quantitativos apresentados nesse item.

Também foi informado no Relatório de Impacto que a negativa de captação de imagem exige justificativa datada e assinada pelo responsável legal do estudante e conferida pelo gestor escolar, oportunidade em que seria comunicado aos docentes da turma onde o aluno está matriculado para que ele não faça parte da foto coletiva da turma e que seu registro de frequência seja executado manualmente.

Porém, apesar de constar no Relatório de Impacto, essa opção não foi fornecida aos pais e responsáveis legais nos requerimento de matrícula ou de renovação de matrícula, tampouco na confirmação da vaga perante a instituição de ensino. Na verdade, não há opção de recusa disponível, uma vez que a “não autorização” não garantiria a vaga do aluno na instituição de ensino.

E, ainda que essa alternativa fosse oferecida aos pais e responsáveis, a recusa em fornecer o consentimento não precisa de justificativa. Portanto, tal medida é incompatível com a autodeterminação informativa garantida pela Lei Geral de Proteção de Dados.

A quinta prática dos requeridos em violação à autodeterminação informativa foi a de prestar informação equivocada no que diz respeito às bases legais para justificar o tratamento dos dados faciais biométricos.

Isso porque foram informadas as bases legais constantes do art. 7º, inciso II e III³⁴, tanto no Relatório de Impacto quanto na Política de Privacidade de Dados Pessoais do Aplicativo Escola Paraná - Biometria³⁵. Todavia, os dados pessoais tratados para o reconhecimento facial são dados sensíveis, de modo que as bases legais previstas no art. 7º não são capazes de legitimar o tratamento destes dados, mas sim aquelas previstas no art. 11 da LGPD.

A principal diferença entre elas é que o tratamento de dados pessoais sensíveis pela Administração Pública para a execução de políticas públicas (art. 11, inciso II, alínea “b”) somente é legítimo quando estas estiverem previstas em leis ou regulamentos³⁶, enquanto o tratamento dos dados pessoais comuns para execução de políticas públicas (art. 7º, inciso III) será legítimo também quando respaldadas em contratos, convênios ou instrumentos

³⁴ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

³⁵ Disponível em: <https://pia.paas.pr.gov.br/termos/app/escola_parana_biometria/politica_privacidade>. Acesso em 06/03/2025.

³⁶ Art. 11 [...] b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

congêneres³⁷.

Essa conduta de não informar a base legal adequada - e, mais grave ainda, de não ter base legal que respalda o tratamento dos dados, conforme será demonstrado adiante - afronta diretamente o direito à autodeterminação informativa, visto que o controle sobre os dados pessoais pelos titulares só existe quando eles tiverem pleno conhecimento das informações necessárias para amparar o tratamento dos dados pessoais.

Por fim, a sexta conduta praticada pelos requeridos que afrontou o direito à autodeterminação informativa foi a de prestar informações incorretas sobre os agentes de tratamento dos dados, ou seja, sobre quem realiza o tratamento de dados pessoais e a quem competem as decisões referentes ao tratamento dos dados pessoais.

Foi informado, no Relatório de Impacto à Proteção de Dados Pessoais, que o controlador é a Secretaria de Estado da Educação e do Esporte do Paraná. No entanto, conforme disposição expressa da Lei Geral de Proteção de Dados, o controlador é pessoa natural ou jurídica (art. 5º, inciso VI).

Tal determinação decorre da possibilidade de responsabilização do controlador. Por esta razão, os órgãos públicos despersonalizados não podem ser considerados controladores, uma vez que, salvo algumas exceções autorizadas pela jurisprudência, não possuem capacidade de ser parte.

É o que orienta a Autoridade Nacional de Proteção de Dados no “*Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*”³⁸:

Assim, em conclusão: nas operações de tratamento de dados pessoais conduzidas por órgãos públicos despersonalizados a pessoa jurídica de direito público a que os órgãos sejam vinculados é a controladora dos dados pessoais e, portanto, responsável pelo cumprimento da LGPD.

As informações sobre o operador também não estão em conformidade com a lei. A LGPD define operador como pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador³⁹.

Foi informado apenas a Companhia de Tecnologia da Informação e Comunicação do Paraná (CELEPAR) como operadora. No entanto, o tratamento de dados também é realizado pela empresa vencedora da licitação para implementação do reconhecimento facial pelo uso

³⁷Art. 7º [...] III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

³⁸Em anexo.

³⁹Art. 5º Para os fins desta Lei, considera-se: VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;





3ª Promotoria de Justiça de Campo Mourão

da inteligência artificial. No caso, a Valid Soluções S/A.

As informações imprecisas sobre o controlador e os operadores também afrontam o direito à autodeterminação informativa, pois uma das premissas deste direito consiste em assegurar que “os dados corretos serão usados pelas pessoas certas para os propósitos certos”⁴⁰. Deste modo, ter conhecimento de quem realizará o tratamento e a quem competem as decisões referentes ao tratamento dos dados é fundamental para que o titular dos dados tenha total domínio sobre seus dados pessoais.

Diante das condutas expostas neste tópico, restou demonstrado que o direito à autodeterminação informativa dos titulares dos dados pessoais não foi observado no tratamento dos dados biométricos para o uso da tecnologia de reconhecimento facial no registro de frequência escolar.

3.3. VIOLAÇÃO AO ARTIGO 11 DA LEI GERAL DE PROTEÇÃO DE DADOS: AUSÊNCIA DE BASE LEGAL PARA TRATAMENTO DOS DADOS PESSOAIS

Além dos princípios mencionados e a autodeterminação informativa, o tratamento dos dados pessoais biométricos das crianças e adolescentes da forma como foi realizado violou o direito dos titulares dos dados pessoais de terem seus dados tratados alicerçados em bases legais válidas.

As bases legais informadas pelos requeridos para o tratamento dos dados pessoais dos alunos paranaenses foram aquelas constantes do art. 7º, incisos II e III, da LGPD, quais sejam: “*cumprimento de obrigação legal ou regulatória pelo controlador*” e a “*execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*”, conforme é possível verificar no Relatório de Impacto à Proteção de Dados Pessoais⁴¹ e na Política de Privacidade de Dados Pessoais⁴² do aplicativo “Escola Paraná - Biometria”.

As bases legais previstas no art. 7º não são capazes de legitimar o tratamento dos dados faciais biométricos por se tratarem de dados pessoais sensíveis⁴³, pois o tratamento de dados pessoais sensíveis somente poderá ocorrer com base nas hipóteses descritas no art. 11, da LGPD. E, mesmo utilizando o artigo 11, somente se adequaria ao caso concreto a base legal do consentimento, prevista no inciso I (que, também, como será visto no tópico

⁴⁰ “Right data are used by the right people for the right purposes” (Paul Siehgart, *Privacy and Computer*, Londres: Latimer, 1976)

⁴¹ Página 234-246 do Inquérito Civil nº 0024.24.000014-1

⁴² Disponível em: https://pia.paas.pr.gov.br/termos/app/escola_parana_biometria/politica_privacidade. Acesso em 06/03/2025. Juntado no seq. 24.8 do Inquérito Civil.

⁴³ A biometria facial é considerada dado pessoal sensível, nos termos do art. 5º, inciso II, da LGPD.





3.4, não ocorreu de forma válida).

Nota-se que o texto do artigo 7º e 11 tem similaridade quanto às bases legais.

A base legal prevista no art. 7º, inciso II, corresponde à hipótese de dispensa de consentimento prevista no art. 11, inciso II, alínea “a”, qual seja: *para o cumprimento de obrigação legal ou regulatória pelo controlador*.

Já a hipótese do art. 7º, inciso III, corresponde à base legal para o *tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*. Enquanto que a base legal do art. 11, inciso II, alínea “b”, exige que a política pública esteja prevista em lei ou regulamento para o tratamento dos dados pessoais sensíveis.

Contudo, ainda que as bases utilizadas e informadas fossem aquelas previstas no art. 11º, II, alíneas “a” e “b”, da LGPD, o tratamento dos dados faciais biométricos não estaria alicerçado em base legal válida.

Isso porque as bases legais previstas no art. 11º, II, alíneas “a” e “b”, somente legitimariam o tratamento dos dados faciais biométricos caso estes fossem indispensáveis para a execução de políticas públicas previstas em leis ou regulamentos ou para o cumprimento de obrigação legal ou regulatória pelo controlador.

Ou seja, se não existir vinculação direta do dado pessoal sensível coletado ao cumprimento de obrigação legal ou regulatória (art. 11, II, alínea “a”) ou se a “política pública” (art. 11, II, alínea “b”) não tiver respaldo em lei ou regulamento, a Administração Pública somente poderá tratar os dados pessoais sensíveis mediante o consentimento dos titulares dos dados ou de seus pais ou responsável legal.

Em relação à base legal informada de “*cumprimento de obrigação legal ou regulatória pelo controlador*”, apesar de aplicável para alguns dados pessoais tratados (como o histórico escolar, por exemplo), não se aplica aos dados faciais biométricos, uma vez que não há nenhuma obrigação que somente pode ser cumprida por meio do reconhecimento facial.

Por essa razão, ainda que informado no Relatório de Impacto à Proteção dos Dados Pessoais que a “chamada escolar” é obrigação legal da instituição de ensino, não há vinculação direta do dado facial biométrico ao cumprimento da obrigação de registro de frequência. Ou seja, não há imprescindibilidade da utilização do dado pessoal sensível para o cumprimento da obrigação, de modo que o tratamento dos dados faciais biométricos não pode se fundamentar na base legal disposta no art. 11, II, alínea “a”.

Por sua vez, a base legal prevista no art. 11, inciso II, alínea “b”, LGPD, está





condicionada à existência de leis ou regulamentos que respaldam a política pública em questão. Assim, caso a política pública não esteja prevista em lei ou regulamento, a coleta e o tratamento de dados pessoais sensíveis de crianças estariam sujeitos à regra do art. 11, inciso I, e art. 14, §1º, da LGPD, a qual exige o consentimento específico e em destaque para finalidades específicas.

No caso concreto, como a utilização de sistemas de reconhecimento facial por inteligência artificial para a finalidade de registro de frequência em escolas não está prevista em leis ou regulamentos, seria absolutamente necessário o consentimento dos pais ou responsáveis para o tratamento dos dados sensíveis das crianças e adolescentes, mesmo se tratando de uma iniciativa da Administração Pública.

Além disso, o tratamento de dados pessoais sensíveis de crianças e adolescentes possuem regras ainda mais rígidas, demandando, também, a observância ao seu melhor interesse, nos termos do art. 14 da LGPD, e respeito à condição peculiar de pessoa em desenvolvimento, conforme disposição do art. 71, do Estatuto da Criança e do Adolescente.

Portanto, em uma remota hipótese de implantação dos sistemas de reconhecimento facial por inteligência artificial para chamada escolar em conformidade com a legislação de proteção de dados, antes de sua implementação, deveria ter sido obtido o consentimento expresso e em destaque, informando os pais e responsáveis, de forma clara e acessível, sobre a finalidade específica do tratamento dos dados faciais biométricos.

Por fim, ainda que o caso concreto se amoldasse a alguma hipótese de dispensa de consentimento prevista no inciso II do art. 11 - o que, repisa-se, não aconteceu no presente caso, os agentes de tratamento continuariam obrigados às demais obrigações previstas na Lei Geral de Proteção de Dados, conforme disposição expressa do §6º do art. 7º.

3.4. VIOLAÇÃO AO ARTIGO 11, INCISO I, DA LEI GERAL DE PROTEÇÃO DE DADOS: ILEGALIDADE QUANTO AO CONSENTIMENTO

Nos termos do artigo 11, o tratamento de dados pessoais sensíveis somente poderá ser realizado nas hipóteses elencadas em seus incisos. Veja-se, a propósito, transcrição do referido artigo:

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:





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

- 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, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
- 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 (Redação dada pela Lei nº 13.853, de 2019)*
- 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.*

Como as bases legais informadas pelo Estado do Paraná para o tratamento dos dados faciais biométricos dos alunos não são cabíveis no caso em questão, conforme fundamentado no tópico imediatamente superior, o Estado do Paraná somente poderia tratar os dados pessoais das crianças e adolescentes mediante o consentimento dos pais ou responsáveis legais e em observância ao melhor interesse da criança e do adolescente, fato que não ocorreu, conforme será demonstrado.

Nesse contexto, a lei conceitua o consentimento em seu artigo 5º, inc. XII, como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Nos casos de dados pessoais sensíveis, o consentimento precisa ser específico, destacado e para finalidades específicas (art. 11, inciso I, LGPD), exigência comum aos dados pessoais de crianças, em que se faz necessário que o consentimento seja específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, §1º, LGPD).

Para o tratamento de dados pessoais de crianças e adolescentes, além das exigências acima, é imprescindível que o tratamento seja realizado em seu melhor interesse (art. 14, caput, LGPD).

No caso dos autos, o “consentimento” foi supostamente colhido durante a matrícula e rematrícula dos alunos. Nos requerimentos de matrícula e de renovação de matrícula constaram as seguintes autorizações⁴⁴:

⁴⁴ Documentos de seq. 15.3 a 15.6 do Inquérito Civil, enviados pela Celepar em resposta ao Ofício nº 225/2024-3º.





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

“Eu, responsável legal pela(o) estudante citado neste requerimento de renovação de matrícula, venho através deste, requerer a sua matrícula nesta Instituição de Ensino, declarando estar ciente dos deveres inerentes ao poder de família junto à criança e/ou ao adolescente em especial quanto ao que se refere à matrícula, acompanhamento da frequência e aproveitamento escolar previstos na Constituição Federal e Lei n.º 8069/1990 – Estatuto da Criança e do Adolescente, e de acordo com as disposições do Regimento Escolar da Instituição de Ensino e demais normas complementares. Estou ciente da Lei n.º 13.709/2018 – LGPD, e portanto concordo e autorizo a Secretaria de Estado da Educação do Paraná, a tratar e utilizar os dados e imagens do estudante para fins institucionais, estatísticos, frequência escolar, coleta do Censo Escolar, planejamento e execução de ações, programas e políticas públicas e quando necessário, o compartilhamento com a rede proteção, Ministério Público, sistema público de segurança, sistema público de saúde e demais setores da administração pública que possuam acordo de cooperação.”

“Declaro ainda estar de acordo com as disposições do Regimento Escolar da Instituição de Ensino, demais normas educacionais complementares e à Lei Federal n.º 13.709/2018 e em cumprimento à essas legislações, autorizo o uso da imagem e dos registros educacionais nos Sistemas Estaduais de Educação do(a) aluno(a) citado para fins estatísticos da SEED/PR, Censo Escolar, comunicação oficial da SEED, planejamento e execução de políticas e/ou programas públicos, atendimento à rede proteção e da imagem para fins de frequência escola.”

Não há adequada menção de coleta de dados biométricos faciais e a sua natureza de dado pessoal sensível nas autorizações supostamente concedidas pelos pais ou responsáveis legais, tampouco informações claras e detalhadas sobre a finalidade específica da coleta de tais dados e sua real necessidade.

Segundo Danilo Doneda, como consequência do princípio da finalidade, “a informação, dada para fins de obtenção de consentimento, deve ser completa a respeito do rumo dos dados, incluindo destinatário, usos, tempo de tratamento, possibilidade de transmissão a terceiros, sem prejuízo de outras informações necessárias;”. A informação, portanto, segundo Doneda, é o que legitima todo consentimento para tratamento de dados.⁴⁵

A autorização genérica para o tratamento de “dados e imagens do estudante” não legitima o tratamento dos dados faciais biométricos de crianças e adolescentes, uma vez que o termo “imagem” não se confunde com o dado facial biométrico.

Isso porque a biometria é a análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo. Segundo Stan Z. Li, a característica biométrica é a característica biológica e comportamental de um indivíduo que pode ser detectada e da qual podem ser extraídas características biométricas distintivas e repetíveis para fins de reconhecimento automatizado de indivíduos. As características

⁴⁵DONEDA, Danilo. Da privacidade à proteção de dados, 2. ed. São Paulo: Thomson Reuters, 2020, cap. 4.2.6.





biológicas e comportamentais são propriedades físicas de partes do corpo, processos fisiológicos e comportamentais criados pelo corpo e combinações de qualquer um deles⁴⁶.

O dado pessoal “imagem”, por sua vez, não possui capacidade distintiva e repetível de promover o reconhecimento automatizado de indivíduos. Por essa razão, a suposta autorização para tratamento do dado pessoal “imagem” não legitima o tratamento do dado biométrico, vez que a natureza jurídica deles não se confunde: o dado facial biométrico é dado pessoal sensível, enquanto a imagem é dado pessoal comum.

Em outras palavras, quando a imagem é posta em movimento para a finalidade além da exposição da imagem, ela se torna um dado pessoal sensível.

Contudo, ainda que se tratasse apenas da imagem de crianças e adolescentes, o Código Civil prevê proteção no capítulo destinado aos direitos da personalidade. O referido código estabelece, em seu art. 20, que a utilização da imagem de uma pessoa só é possível se autorizada e, ainda assim, poderá ser proibida, a seu requerimento e sem prejuízo da indenização que couber, se atingir a honra, a boa fama ou a respeitabilidade, ou se destinadas a fins comerciais.

Além disso, há sujeição entre a garantia da vaga na instituição pública de ensino à cessão compulsória da imagem dos estudantes, conforme consta até mesmo na Instrução Normativa nº 001/2022/DPGE⁴⁷, fato que evidencia a ausência de manifestação livre para fins de consentimento.

Neste ponto, vale ressaltar que a medida adotada pelas escolas estaduais do Paraná possui duas faces de coerção que viciam o “consentimento” supostamente fornecido: a primeira decorre do fato de que a ausência das autorizações mencionadas impediria o acesso ao direito à educação, garantido pelo art. 6º, da Constituição da República⁴⁸; a segunda reside no fato de que, sem a vaga garantida na instituição pública por ausência de autorização, os pais ou responsáveis legais podem ser responsabilizados pelo não cumprimento da obrigação de matricular seus filhos ou pupilos na rede regular de ensino, prevista no art. 55, do Estatuto da Criança e do Adolescente⁴⁹.

⁴⁶Encyclopedia of Biometrics: I - Z., Volume 2, página 80: Biometric characteristic: biological and behavioral characteristic of an individual that can be detected and from which distinguishing, repeatable biometrics features can be extracted for the purpose of automated recognition of individuals. Biological and behavioral characteristics are physical properties of body parts, physiological and behavioral processes created by the body and combinations of any of these.

⁴⁷Ao concordar com a vaga e com a instituição de ensino, propostas pela SEED, o responsável legal deverá ler e assinar eletronicamente o termo uso de imagem e requerimento de matrícula, disponibilizados automaticamente pela “Área do Aluno”, e optar em receber uma cópia do comprovante de matrícula, no endereço de e-mail informado, ou imprimir-la.

⁴⁸Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.

⁴⁹Art. 55. Os pais ou responsável têm a obrigação de matricular seus filhos ou pupilos na rede regular de ensino.





Em buscas de maiores detalhes sobre a situação narrada nos autos, localizou-se o seguinte comentário publicado no dia 24 de outubro de 2022, sem maiores informações de identificação⁵⁰: *“No Paraná, sem consulta aos pais e levando em consideração autorização do uso da imagem para fins de divulgação institucional, estão forçando alunos da rede pública, mesmo contra a vontade dos mesmos, a cadastrarem suas biometrias faciais com a justificativa de fazer chamada, assediando aqueles que se recusam sob ameaça de falta, mesmo estando em aula. Há algo que possa ser feito para impedir isso?”*

Este relato reforça a ausência de liberdade para o fornecimento do consentimento para o tratamento dos dados pessoais biométricos coletados.

Deve ser ressaltado, ainda, que as crianças e adolescentes encontram-se em situação de hipervulnerabilidade, à medida em que já são vulneráveis pela condição de pessoas em desenvolvimento e acabam por serem colocados novamente em situação de vulnerabilidade por figurarem na posição de titulares de dados, uma vez que quem colhe os dados conhece o titular, mas quem tem os dados colhidos não faz a menor ideia do que fazem com eles, e quem lhes detêm⁵¹.

Por esta razão, todas as informações precisam ser disponibilizadas de forma clara e suficiente no momento do ato de consentir, para, então, não restar eivado de vícios de consentimento.

Note-se que a própria legislação se encarregou de definir que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, de modo que cabe ao controlador o ônus da prova de que foi obtido em conformidade com o acima exposto (art. 8º, caput e §2º, LGPD).

O artigo 8º ainda esclarece que é vedado o tratamento de dados pessoais mediante vício de consentimento e que as autorizações genéricas para o tratamento de dados pessoais serão nulas, eis que o consentimento deverá referir-se a finalidades determinadas (art. 8º, §§ 3º e 4º, LGPD).

Ademais, o artigo 9º, §1º, dispõe que, nas hipóteses em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenha conteúdo enganoso, abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca, exatamente como ocorreu (e ainda ocorre) na coleta de dados pelos agentes de tratamento.

Portanto, o “consentimento” pelos pais ou responsável legal concedido na matrícula

⁵⁰Disponível em: <https://www.lgpdbrasil.com.br/lgpd-na-aplicacao-do-reconhecimento-facial>. Acesso em 10/03/2025.

⁵¹FERREIRA, Dâmares. LGPD aplicada à educação. Curitiba: CRV, 2021, p. 96.





ou rematrícula é considerado nulo, pelos fundamentos acima. O “consentimento” no caso em questão consistiu, na prática, em mera obediência dos pais ou responsável legal do titular dos dados pessoais à vontade da Administração Pública e não em uma decisão informada e racional, fato que impossibilita, por consequência, o tratamento dos dados faciais biométricos pelo Estado do Paraná, Celepar e Valid Soluções S. A.

4. DA RESPONSABILIZAÇÃO CIVIL: TRATAMENTO ILÍCITO DOS DADOS PESSOAIS

As ilegalidades narradas na presente inicial podem ser sintetizadas em: violação aos princípios expressos no art. 6º, da LGPD; violação ao direito à autodeterminação informativa, garantido como fundamento da proteção de dados pessoais no art. 2º, inciso II, da LGPD; violação ao direito dos titulares dos dados de terem seus dados tratados alicerçados em bases legais válidas (aquelas previstas nos artigos 7º e 11); e ilegalidade do consentimento fornecido pelos pais ou responsáveis legais dos titulares dos dados pessoais.

O *caput* do artigo 44 da LGPD prevê duas condutas que tornam o tratamento dos dados pessoais irregular. Veja-se:

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Da leitura do citado dispositivo, verifica-se que tanto a conduta de “deixar de observar a legislação” quanto a conduta de “não fornecer a segurança que o titular dele pode esperar” configuram condutas sujeitas a responsabilização.

Ana Luisa Tarter Nunes⁵² classifica os três enquadramentos possíveis de responsabilidade civil previstos na LGPD da seguinte forma: (i) a conduta de violação à legislação como *tratamento ilícito* (art. 42, *caput*, LGPD); (ii) a conduta de não atender a expectativa de segurança do titular dos dados pessoais como *tratamento inadequado* (art. 44, *caput*, parte final); e (iii) a violação da segurança dos dados pela ausência de adoção das medidas de segurança previstas como *tratamento indevido* (art. 44, parágrafo único, c/c art. 46, *caput* e § 1º, LGPD).

A conduta narrada nos autos se enquadra perfeitamente à primeira modalidade do

⁵²Vários autores. 5 anos de LGPD [livro eletrônico]: estudos em homenagem a Danilo Doneda / coordenação Claudia Lima Marques - 1. ed. São Paulo: Thomson Reuters Brasil, 2023.





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

caput do art. 44, uma vez que houve clara violação à legislação.

O artigo 42, *caput*, da LGPD define os requisitos para a configuração da responsabilidade civil na modalidade de tratamento ilícito (em violação à legislação de proteção de dados pessoais):

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Extrai-se, desta norma, que é necessária a prática de ato próprio que cause dano por descumprimento de um dever legal (observância da LGPD). Nunes⁵³ aduz que um exemplo dessa hipótese é o tratamento de dados pessoais fora das bases legitimadoras previstas nos arts. 7º e 11, exatamente como narrado no presente feito.

Além da ausência de base legitimadora, as condutas dos requeridos narradas nos autos também violaram a LGPD no que diz respeito ao direito à autodeterminação informativa, ao consentimento coletado e também em relação aos princípios previstos no art. 6º da legislação mencionada.

Deste modo, é possível inferir que as condutas dos agentes de tratamento configuram o tratamento ilícito dos dados pessoais, legitimando a responsabilização civil pelos danos causados, conforme será argumentado no tópico subsequente.

4.1. DO DANO MORAL COLETIVO

As condutas narradas nos autos causaram danos a aproximadamente um milhão de estudantes paranaenses⁵⁴, sendo eles crianças e adolescentes.

Conforme fundamentado no tópico acima, o art. 42 da Lei Geral de Proteção de Dados prevê que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Os danos causados aos alunos devem ser compreendidos como danos coletivos.

Isso porque a situação envolve um grande volume de dados pessoais sensíveis, cuja finalidade do tratamento é a implementação de uma ferramenta de registro de frequência escolar para uso coletivo, de forma generalizada.

⁵³Vários autores. 5 anos de LGPD [livro eletrônico]: estudos em homenagem a Danilo Doneda / coordenação Claudia Lima Marques - 1. ed. São Paulo: Thomson Reuters Brasil, 2023.

⁵⁴Conforme informado pelos agentes de tratamento no relatório de impacto à proteção de dados pessoais.





O dano, sob a ótica da responsabilidade civil, é definido como a lesão a qualquer bem jurídico⁵⁵. O dano moral coletivo, por sua vez, é uma categoria autônoma de dano relacionado à violação injusta e intolerável de valores fundamentais da coletividade.

Para Carlos Alberto Bittar Filho⁵⁶, o dano moral coletivo é a *"injusta lesão da esfera moral de dada comunidade, ou seja, é a violação antijurídica de um determinado círculo de valores coletivos"*.

Deste modo, deve ser compreendido que os danos morais coletivos atingem valores e interesses fundamentais da sociedade por violação ao ordenamento jurídico e aos princípios éticos da sociedade. No caso da presente demanda, o direito fundamental violado foi o direito à proteção dos dados pessoais de aproximadamente um milhão de crianças e adolescentes.

Neste contexto, deve ser ressaltado que, a partir da Emenda Constitucional nº 115 de 10 de fevereiro de 2022, o direito à proteção dos dados pessoais passou a integrar o rol do artigo 5º, da Constituição Federal, precisamente no inciso LXXIX, sendo considerado direito fundamental autônomo do ser humano e, portanto, inviolável e indisponível, figurando a privacidade apenas como uma de suas referências axiológicas no regime instituído pela LGPD⁵⁷.

Sobre a configuração do dano moral coletivo, o Ministro Luis Felipe Salomão afirma que ele é aferível *in re ipsa*, ou seja, sua configuração decorre da mera constatação da prática de conduta ilícita que, de maneira injusta e intolerável, viola direitos de conteúdo extrapatrimonial da coletividade, revelando-se despcienda a demonstração de prejuízos concretos ou de efetivo abalo moral⁵⁸.

Assim decidiu o Superior Tribunal de Justiça no REsp 1517973/PE, em caso de ofensa coletiva à dignidade de crianças e adolescentes:

RECURSO ESPECIAL. AÇÃO CIVIL PÚBLICA. DIGNIDADE DE CRIANÇAS E ADOLESCENTES OFENDIDA POR QUADRO DE PROGRAMA TELEVISIVO. DANO MORAL COLETIVO. EXISTÊNCIA. 1. O dano moral coletivo é aferível in re ipsa, ou seja, sua configuração decorre da mera constatação da prática de conduta ilícita que, de maneira injusta e intolerável, viole direitos de conteúdo extrapatrimonial da coletividade, revelando-se despcienda a demonstração de prejuízos concretos ou de efetivo abalo moral. Precedentes. [...] 3. A análise da configuração do dano moral coletivo, na espécie, não reside na identificação de seus telespectadores, mas sim nos

⁵⁵ ALVIM, Agostinho. Da inexecução das obrigações e suas consequências. Ed. Jurídica e Universitária. 3ª.ed. p. 171.

⁵⁶ Bittar Filho, C. A. Responsabilidade Civil. 20ª ed. São Paulo: Atlas, 2018.

⁵⁷ TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p:99-130.

⁵⁸ REsp 1517973/PE, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 16/11/2017, DJe 01/02/2018.





prejuízos causados a toda sociedade, em virtude da vulnerabilização de crianças e adolescentes, notadamente daqueles que tiveram sua origem biológica devassada e tratada de forma jocosa, de modo a, potencialmente, torná-los alvos de humilhações e chacotas pontuais ou, ainda, da execrável violência conhecida por bullying. 4. Como de sabença, o artigo 227 da Constituição da República de 1988 impõe a todos (família, sociedade e Estado) o dever de assegurar às crianças e aos adolescentes, com absoluta prioridade, o direito à dignidade e ao respeito e de lhes colocar a salvo de toda forma de discriminação, violência, crueldade ou opressão. 5. No mesmo sentido, os artigos 17 e 18 do ECA consagram a inviolabilidade da integridade física, psíquica e moral das crianças e dos adolescentes, inibindo qualquer tratamento vexatório ou constrangedor, entre outros. [...] 8. Recurso especial não provido.

As violações narradas à legislação de proteção de dados pessoais brasileira e aos direitos de crianças e adolescentes, assim como as afrontas aos princípios multidisciplinares expostos na presente petição, configuram hipervulnerabilização da coletividade de alunos da rede estadual de ensino paranaense e revelam uma conduta ilícita, injusta e intolerável.

Em situação de violação à Lei Geral de Proteção de Dados, o Superior Tribunal de Justiça reconheceu a responsabilização dos agentes de tratamento de dados por danos morais coletivos *in re ipsa*⁵⁹:

RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. [...] 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.[...] 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa [...].

Demonstrada, portanto, a configuração do dano moral coletivo no presente caso, resta discorrer sobre os demais requisitos da responsabilidade civil dos agentes de tratamento.

4.2. DA RESPONSABILIDADE CIVIL DE CADA AGENTE DE TRATAMENTO

Considerando que o dano por violação à legislação de proteção de dados pessoais foi demonstrado no tópico anterior, torna-se imprescindível a elucidação das condutas de cada agente de tratamento.

⁵⁹ REsp n. 1.758.799/MG, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 12/11/2019, DJe de 19/11/2019.





O Estado do Paraná, na condição de controlador, autorizou a Companhia de Tecnologia da Informação e Comunicação do Paraná - Celepar - a realizar o tratamento e compartilhamento dos dados pessoais para a realização da chamada escolar por meio de reconhecimento facial⁶⁰.

Além disso, realizou a coleta dos dados faciais biométricos sem base legal válida⁶¹, colheu o consentimento de maneira ilegal⁶², elaborou o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em desacordo com a LGPD, violou o direito à autodeterminação informativa⁶³ e os princípios da finalidade, transparência e necessidade, todos previstos no art. 6º, da LGPD⁶⁴.

A Companhia de Tecnologia da Informação e Comunicação do Paraná, por sua vez, realizou o processo licitatório para contratação da empresa para prestação do serviço de reconhecimento biométrico facial (Pregão Eletrônico nº 1349/2020), elaborou justificativa para aquisição dos serviços de automatização do registro de frequência⁶⁵ e celebrou o contrato administrativo de nº 4313/2022 com a Valid Soluções S. A.

Ainda, na condição de operadora, elaborou a Política de Privacidade de Dados Pessoais do aplicativo Escola Paraná - Biometria em violação à LGPD, realizou o tratamento ilícito dos dados pessoais sem estarem alicerçados em base legal válida e, com isso, violou os princípios da finalidade, transparência e necessidade, previstos no art. 6º, da LGPD, e o direito à autodeterminação informativa.

A pessoa jurídica Valid Soluções S. A. foi a vencedora do Pregão Eletrônico nº 1349/2020 e, mesmo tendo conhecimento de ilegalidades na coleta dos dados pessoais na fase inicial do processo licitatório⁶⁶, celebrou o contrato administrativo de nº 4313/2022. Na condição de operadora, realizou o tratamento ilícito dos dados pessoais sem estarem alicerçados em base legal válida, violando os princípios da finalidade, transparência e necessidade, previstos no art. 6º, da LGPD, e o direito à autodeterminação informativa.

Da leitura do art. 42 da Lei Geral de Proteção de Dados, extrai-se que, para a responsabilização civil dos agentes de tratamento, é necessária a prática de ato próprio que

⁶⁰Conforme Despacho Secretarial do Protocolo nº 17.281.176-0, de fls. 728 (página 575 do arquivo "Processo_16.994.392-3_1%20.pdf")

⁶¹Conforme fundamentado no tópico "3.3. VIOLAÇÃO AO ARTIGO 11 DA LEI GERAL DE PROTEÇÃO DE DADOS: AUSÊNCIA DE BASE LEGAL PARA TRATAMENTO DOS DADOS PESSOAIS"

⁶²Conforme fundamentado no tópico 3.4. VIOLAÇÃO AO ARTIGO 11 DA LEI GERAL DE PROTEÇÃO DE DADOS: ILEGALIDADE QUANTO AO CONSENTIMENTO"

⁶³Conforme fundamentado no tópico "3.2. VIOLAÇÃO AO ARTIGO 9º DA LEI GERAL DE PROTEÇÃO DE DADOS: DIREITO À AUTODETERMINAÇÃO INFORMATIVA"

⁶⁴Conforme fundamentado no tópico "3.1. VIOLAÇÃO AO ARTIGO 6º DA LEI GERAL DE PROTEÇÃO DE DADOS: PRINCÍPIOS"

⁶⁵Conforme Justificativa da Aquisição de fls. 234 (página 61 do arquivo "Processo_16.994.392-3_1%20.pdf")

⁶⁶Teve ciência da coleta das emoções sem finalidade específica e questionou sobre a necessidade de realizar a coleta deste dado, conforme questionamento nº 4 da Valid Soluções S/A (página 345 do Processo_16.994.392-3_1.pdf).





cause dano por violação à legislação de dados pessoais.

Como regra⁶⁷, a LGPD é mais consentânea com a responsabilidade subjetiva, na medida em que condiciona a responsabilização dos agentes de tratamento à violação de deveres do art. 42 da LGPD. Por essa razão, não parece adequado adotar-se um regime de responsabilidade objetiva que impute a todo e qualquer agente de tratamento todo dano decorrente de sua atividade, especialmente se este puder demonstrar que adotou cuidados relevantes para evitar eventuais violações⁶⁸.

A avaliação da suposta violação deverá ser feita no contexto dos princípios reitores de sua aplicação, com especial atenção para o chamado princípio da responsabilização e prestação de contas, ao exigir a 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 destas medidas⁶⁹.

Apesar disso, o Estado do Paraná e a Celepar apresentam exceção à regra da responsabilidade subjetiva.

O Estado do Paraná responde de forma objetiva, nos termos do art. 37, §6º da Constituição da República⁷⁰. Da mesma forma, a Celepar responde objetivamente, por ser integrante da administração pública indireta (sociedade de economia mista) e prestadora de serviços públicos⁷¹.

Ambas respondem de maneira solidária por estarem diretamente envolvidos no tratamento do qual decorreram os danos aos titulares dos dados pessoais, nos termos do art. 42, inciso II, da Lei 13.709/2018.

Com relação à Valid Soluções S/A, o artigo 42, inciso I, da LGPD, estabelece a responsabilização solidária do operador pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.

⁶⁷Embora não mencionado pela LGPD, a responsabilidade do Poder Público é inerente ao art. 37 §6º da Constituição Federal. Ainda, o art. 45 da LGPD ressalta que: "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

⁶⁸FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovana. *Curso de Proteção de Dados Pessoais. Fundamentos da LGPD*. 1ª Ed. Rio de Janeiro, 2022. p. 436.

⁶⁹FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovana, op. cit., p. 438.

⁷⁰Art. 37 [...] § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

⁷¹O Supremo Tribunal Federal no julgamento do ACO nº 3.640, ao reconhecer a imunidade tributária recíproca entre a Celepar e a União, asseverou que a Celepar é: "uma sociedade de economia mista que executa serviço público essencial e atua em regime não concorrencial na área de tecnologia da informação, visando fomentar os objetivos institucionais dos bens do estado". (STF. Ação Cível Originária (ACO) nº 3.640. Rel. Min. Dias Toffoli. Plenário. D.J. 19/12/2023).





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

No presente caso, houve descumprimento das obrigações da legislação de proteção de dados pessoais por todos os agentes de tratamento de dados, incluindo a Valid Soluções S. A.

Ademais, apesar de o regime da responsabilidade civil ser subjetivo, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil⁷².

Isso porque, a despeito da exigência do preenchimento do requisito culpa/dolo, o artigo 43, inciso II, da LGPD, atribuiu aos agentes de tratamento a prova de que não houve violação à legislação de proteção de dados para afastar a responsabilidade civil.

Assim, em relação à Valid Soluções S. A., a responsabilidade de reparação no caso de tratamento ilícito dos dados pessoais é subjetiva, cujos requisitos para sua configuração são: (i) atividade de tratamento de dados pessoais; (ii) dano patrimonial, moral, individual ou coletivo; (iii) violação à legislação de proteção de dados pessoais; (iv) culpa ou dolo e (v) nexo de causalidade.

A atividade de tratamento de dados pessoais, a violação à legislação de proteção de dados pessoais e o dano moral coletivo para todos os requeridos já foram demonstrados nos tópicos anteriores.

Com relação ao nexo de causalidade da conduta dos requeridos, é possível estabelecer que o dano moral coletivo acima delineado vincula-se direta e adequadamente ao tratamento ilícito de dados, motivo pelo qual reputa-se presente também o pressuposto do liame causal para todos os requeridos.

O requisito culpa ou dolo, não exigido para a responsabilização do Estado do Paraná e para a Celepar, está presente na conduta da ré Valid Soluções S. A.

Isso porque a requerida Valid é uma empresa que lida constantemente com grande volume de dados pessoais⁷³ e, por consequência, detém conhecimento técnico especializado sobre a legislação de proteção de dados.

Esse conhecimento implica na adequada compreensão do princípio da responsabilização e prestação de contas (art. 6º, inciso X, LGPD) e na ciência inequívoca dos deveres estabelecidos na Lei Geral de Proteção de Dados, cuja negligência em cumprir esses deveres configura, no mínimo, culpa.

⁷²BIONI, Bruno; DIAS, Daniel. *Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor*. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: <<http://civilistica.com/responsabilidade-civil-na-protacao-de-dados-pessoais/>>. Data de acesso: 05/03/2025.

⁷³Informação extraída do site institucional da Valid Soluções S. A: "Sempre que a solução é complexa, com alta volumetria e envolve dados sensíveis, pode ter certeza de que tem a Valid por trás". Disponível em: <https://valid.com/quem-somos>; Acesso em 10/03/2025.





3ª Promotoria de Justiça de Campo Mourão

Além disso, o fato de a Valid ter questionado no processo licitatório a necessidade de coleta de emoções dos alunos e indagado se seria possível uma oferta de solução sem essa funcionalidade⁷⁴ demonstra que ela tinha plena ciência da ilegalidade da coleta dos dados e, ainda assim, decidiu prosseguir com a contratação e o tratamento dos dados pessoais. Tal atitude, mesmo diante do questionamento realizado, indica, pelo menos, a assunção do risco.

Portanto, todos os requisitos para a responsabilização de todos os requeridos estão demonstrados.

Além disso, no caso em análise não está presente nenhuma das hipóteses de excludente de responsabilidade previstas no art. 43, da Lei Geral de Proteção de Dados.

O mencionado artigo estabelece que os agentes de tratamento de dados somente não serão responsabilizados quando provarem: (i) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (iii) que o dano é decorrente da culpa exclusiva do titular dos dados ou de terceiro.

Portanto, todas as requeridas são responsáveis solidárias pela reparação dos danos causados aos titulares dos dados pessoais.

4.3. DO VALOR DA REPARAÇÃO DO DANO MORAL COLETIVO

Após reconhecida a ocorrência do dano e o dever de repará-lo, torna-se imprescindível quantificar a reparação que se mostre suficiente, tendo em vista que a indenização deve buscar pelo menos três funções: compensação, prevenção e punição⁷⁵.

Por este motivo, a aplicação dos valores indenizatórios devem ser suficientes por parte do Judiciário, compatíveis com a extensão do dano - nos termos do art. 944, CC -, capazes de desencorajar práticas ilícitas nesta esfera.

Por conta da extensão e da natureza do dano moral coletivo, a fixação da reparação civil não se limita ao sofrimento individual de cada uma das vítimas, tampouco lhes cabe a destinação da indenização.

Nesse contexto, importante, desde já, frisar que o artigo 13, da Lei da Ação Civil Pública, disciplina que a condenação deve ser revertida em depósito para fundo específico, com pertinência temática, a ser aproveitado de forma difusa pela sociedade.

⁷⁴Conforme questionamento nº 4 da Valid Soluções S/A (página 345 do Processo_16.994.392-3_1.pdf).

⁷⁵KERN, Bernd-Rüdiger. A função de satisfação no indenização do dano pessoal: um elemento penal na satisfação do dano? Trad. de Lélío Candiota de Campos. RDC 33/9-32, São Paulo: Ed. RT, jan.-mar. 2000.





Para alcançar o valor indenizatório justo, o método bifásico - método adotado pelo Superior Tribunal de Justiça em suas recentes decisões - mostra-se como um meio eficaz para a finalidade almejada. O ministro do STJ, Paulo de Tarso Sanseverino, ao discorrer sobre o método bifásico, destacou a necessidade de se ponderar a indenização na linha dos precedentes da corte, considerando duas etapas para o correto arbitramento do valor:

Na primeira etapa, deve-se estabelecer um valor básico para a indenização, considerando o interesse jurídico lesado, com base em grupo de precedentes jurisprudenciais que apreciaram casos semelhantes.

Na segunda etapa, devem ser consideradas as circunstâncias do caso, para fixação definitiva do valor da indenização, atendendo à determinação legal de arbitramento equitativo pelo juiz.

Deste modo, na primeira etapa deve-se operar a justiça comutativa, em que se busca uma razoável igualdade de tratamento para casos semelhantes. Nesse sentido, ante a escassez de julgados sobre ressarcimento de danos por violação dos direitos à proteção dos dados pessoais nos tribunais brasileiros, a primeira etapa será realizada por meio de multas administrativas aplicadas pelos órgãos responsáveis pela fiscalização de outros países.

Assim, colacionam-se multas administrativas aplicadas em relação a violações à legislação de proteção de dados pessoais para aferição do valor médio de condenações em casos “semelhantes”.

- A empresa Meta (controladora do Facebook) foi multada em € 1,2 bilhão pela Comissão de Proteção de Dados da Irlanda (DPC), em maio de 2023, por violar a privacidade dos dados ao transferir dados pessoais dos usuários do Facebook da União Europeia para servidores nos Estados Unidos⁷⁶.
- A empresa Amazon foi multada em € 746 milhões, em julho de 2021, pela Comissão Nacional de Proteção de Dados (CNPD), de Luxemburgo, por violações relacionadas ao tratamento de dados pessoais para fins de publicidade direcionada⁷⁷.
- A empresa Google foi multada em € 50 milhões pela Comissão Nacional de Informática e Liberdades da França (CNIL), em janeiro de 2019, por violar regras de privacidade online da União Europeia⁷⁸.

⁷⁶Disponível em: <https://www.cnnbrasil.com.br/tecnologia/meta-recebe-multa-recorde-de-us-13-bilhao-da-ue-por-violar-privacidade-de-dados/> e <https://www.estadao.com.br/link/meta-facebook-multa-12-bilhao-euros-uniao-privacidade-nprei/>. Acesso em 07/03/2025.

⁷⁷Disponível em: <https://www.correiobraziliense.com.br/mundo/2021/07/4940755-luxemburgo-multa-amazon-em-746-milhoes-por-nao-proteger-dados.html>. Acesso em 07/03/2025.

⁷⁸Disponível em: <https://www.cnnbrasil.com.br/tecnologia/tribunal-frances-confirma-multa-ao-google-por-violacao-de-privacidade/>. Acesso em 07/03/2025.





3ª Promotoria de Justiça de Campo Mourão

Portanto, o valor de R\$10.000.000,00 (dez milhões de reais) mostra-se como o valor mínimo de indenização, devendo a análise prosseguir para a segunda etapa do método.

Na segunda etapa, partindo-se do valor obtido anteriormente, são analisadas as circunstâncias particulares do caso, como a gravidade do fato em si, a culpabilidade do agente, a culpa concorrente da vítima e a condição econômica das partes, para, enfim, obter o montante definitivo.

Em atenção ao caso em tela, deve-se ter em vista que não houve culpa concorrente da vítima, não havendo que se falar em diminuição do montante neste ponto.

Em seguimento, a culpabilidade do agente é notória, conforme já exaustivamente argumentado, e a gravidade do fato em si diz respeito à violação de direito fundamental de aproximadamente um milhão de alunos da rede estadual de ensino paranaense.

Nesta perspectiva, a gravidade do fato se justifica pela própria natureza do dano e, por este motivo, deve o montante ser majorado a fim de adequar a média obtida anteriormente a um valor razoável.

No que tange à condição econômica das partes, é imperioso ponderar que um dos requeridos é o Estado do Paraná e, por ser um ente federativo, detém capacidade econômica de arcar com o valor acima estipulado.

As requeridas Celepar e Valid Soluções celebraram contrato administrativo que, com os aditivos, alcançou o patamar de R\$12.133.290,45 (doze milhões, cento e trinta e três mil, duzentos e noventa reais e quarenta e cinco centavos). Tal fato demonstra a capacidade econômica de ambas em suportar o valor da reparação no patamar proposto.

Assim, em observância aos princípios da razoabilidade e proporcionalidade, entende este órgão ministerial que a condenação em R\$15.000.000,00 (quinze milhões de reais) gerará os efeitos almejados.

Por meio deste método, tem-se um arbitramento efetivamente equitativo, que respeita as peculiaridades do caso, motivo pelo qual requer-se a condenação da parte ré à reparação do dano moral coletivo em R\$15.000.000,00 (quinze milhões de reais), a ser revertido em depósito para fundo específico, nos termos do artigo 13, da Lei nº 7.347/1985.

5. DA REMOÇÃO DO ILÍCITO

O Estado do Paraná implementou um sistema de reconhecimento facial por inteligência artificial para registrar a frequência dos alunos em escolas estaduais, que coletou dados faciais biométricos sem base legal válida e sem observar os princípios da Lei Geral de Proteção de Dados. Essa conduta configura um ilícito que viola os direitos





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

fundamentais dos estudantes, especialmente o direito à proteção de seus dados pessoais, e cujos efeitos precisam ser removidos.

Além disso, a ilicitude está sendo praticada pela Administração Pública, em prejuízo ao patrimônio público, uma vez que estão sendo despendidos recursos do Estado para a execução de um contrato administrativo cujo objeto viola frontalmente o direito à proteção dos dados pessoais. Observa-se que, até o presente momento, o contrato celebrado entre as requeridas Celepar e Valid Soluções, com os aditivos, alcançou o patamar de R\$12.133.290,45 (doze milhões, cento e trinta e três mil, duzentos e noventa reais e quarenta e cinco centavos).

O Código de Processo Civil elencou duas formas de tutelas jurisdicionais contra o ilícito: (a) a tutela inibitória, voltada contra a prática, a repetição ou a continuação de um ilícito e (b) a tutela de remoção do ilícito, direcionada à remoção dos efeitos concretos da conduta ilícita.

O art. 497 do Código de Processo Civil dispõe:

Art. 497. [...] Parágrafo único. Para a concessão da tutela específica destinada a inibir a prática, a reiteração ou a continuação de um ilícito, ou a sua remoção, é irrelevante a demonstração da ocorrência de dano ou da existência de culpa ou dolo.

No presente caso, a tutela adequada é a de remoção do ilícito, uma vez que a ilicitude perpetrada pela coleta de dados faciais biométricos sem base legal válida e sem observância aos princípios da LGPD, assim como os efeitos dela decorrentes (tratamento ilícito dos dados pessoais), precisam ser removidos.

Para a concessão dessa tutela, são necessários dois requisitos: i) ação contrária ao direito; ii) efeitos ilícitos derivados da ação praticada, que estejam em ato no momento da propositura da ação judicial⁷⁹.

Ambos os requisitos estão preenchidos no presente caso.

A coleta dos dados faciais biométricos (dados pessoais sensíveis) foi realizada em desacordo com a Lei Geral de Proteção de Dados. Foram identificadas inúmeras ilicitudes na coleta dos dados biométricos, dentre as quais se destaca: desrespeito aos princípios da finalidade, transparência e necessidade (art. 6º, incisos I, III e VI, LGPD); violação ao direito à informação previsto no art. 9º, da LGPD; ausência de consentimento válido e, por consequência, de base legal para justificar o tratamento dos dados faciais biométricos; e inobservância ao melhor interesse da criança e do adolescente, conforme exigido pelo art.

⁷⁹MARINONI, Luiz Guilherme; ARENHART, Sergio Cruz; MITIDIERO, Daniel. Novo Curso de Processo Civil: Tutela dos direitos mediante procedimento comum. 2. 2. ed. São Paulo: Revista dos Tribunais, 2016. p. 892.





14 da LGPD.

Da coleta ilícita dos dados biométricos decorrem os seguintes efeitos ilícitos: o tratamento ilícito dos dados pessoais, com violação ao direito fundamental de proteção dos dados pessoais dos alunos (art. 5º, inciso LXXIX, Constituição da República) e afronta à autodeterminação informativa, assegurada pelo artigo 2º, inciso II, e art. 17 da Lei Geral de Proteção de Dados Pessoais.

Diante das ilicitudes praticadas e dos efeitos ilícitos delas decorrentes, que estão presentes na data da propositura desta ação e continuam expondo os alunos a riscos de segurança, deve ser determinada a remoção do o ilícito, proibindo-se o Estado e os demais requeridos de coletar e tratar dados biométricos de alunos com a finalidade de uso do sistema de reconhecimento facial por inteligência artificial para a chamada escolar.

6. TUTELA PROVISÓRIA DE URGÊNCIA

Sobre a possibilidade de tutela provisória de urgência em ação civil pública, o art. 12 da Lei nº 7.347/1985⁸⁰ esclarece que poderá ser concedido mandado liminar, com ou sem justificação prévia.

Diante do exposto, e com base nos fatos e fundamentos jurídicos apresentados nesta petição, fica evidente a necessidade da concessão de tutela provisória de urgência. Tal medida, amparada pelo art. 300 do Código de Processo Civil, visa a imediata remoção do ilícito e se justifica pela presença dos requisitos legais, conforme será demonstrado.

A probabilidade do direito está evidenciada pelas ilicitudes narradas na petição inicial, com destaque para a coleta de dados faciais biométricos dos alunos sem base legal válida e em desacordo com os princípios da Lei Geral de Proteção de Dados.

Tal ilicitude se comprova pelos documentos anexos, notadamente pelo Relatório de Impacto à Proteção de Dados Pessoais, pelos formulários de requerimento de matrícula e renovação de matrícula e pela Política de Privacidade de Dados Pessoais do Aplicativo Escola Paraná - Biometria.

O perigo de dano também está configurado, pois o tratamento ilícito de dados pessoais de crianças e adolescentes causa dano contínuo a todos os alunos a ele submetidos. Além disso, a cada dia que se passa, mais recursos públicos são destinados à execução de um contrato administrativo que gera efeitos ilícitos, agravando o prejuízo ao patrimônio público. Pois, até o presente momento, o contrato celebrado entre as requeridas Celepar e Valid Soluções, com os aditivos, alcançou o patamar de R\$12.133.290,45 (doze

⁸⁰ Art. 12. Poderá o juiz conceder mandado liminar, com ou sem justificação prévia, em decisão sujeita a agravo.





milhões, cento e trinta e três mil, duzentos e noventa reais e quarenta e cinco centavos).

Reforçando a necessidade da concessão da tutela de urgência nas ações com pedido de remoção de ilícito, Luiz Guilherme Marinoni defende, ainda, que a probabilidade de o ilícito ter ocorrido configura, por si só, a probabilidade de dano futuro, uma vez que a própria norma de proteção (provavelmente violada) possui o objetivo de evitar danos⁸¹.

Portanto, a demora na remoção do ilícito agrava os danos, tornando imperativa a concessão da tutela de urgência para evitar maiores prejuízos e assegurar a efetividade da prestação jurisdicional.

Por fim, verifica-se que a medida pleiteada não oferece perigo de irreversibilidade dos efeitos da decisão, conforme art. 300, §3º, do CPC, uma vez que a suspensão da coleta e tratamento de dados faciais biométricos para a finalidade de reconhecimento facial para registro de frequência dos alunos pode ser revertida caso, ao final do processo, sejam julgados improcedentes os pedidos da presente ação.

Diante do exposto, requer-se a concessão de tutela provisória de urgência, nos termos do art. 300 do CPC, para determinar a imediata suspensão da coleta e tratamento de dados faciais biométricos para a finalidade de reconhecimento facial para registro de frequência dos alunos.

7. DA INVERSÃO DO ÔNUS DA PROVA

Nos termos do art. 42, §2º, da LGPD, nas ações em que se busca a responsabilidade pelo exercício de atividade de tratamento de dados pessoais, o juiz poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de provas pelo titular resultar-lhe excessivamente onerosa.

Desta forma, por se tratar de crianças e adolescentes na condição de titulares dos dados pessoais e o Estado do Paraná na condição de controlador, é nítida a hipervulnerabilidade em relação à parte ré, fato que dificulta a produção de provas pelos titulares. Deste modo, configura-se a espécie legal e imperativa de inversão do ônus da prova.

⁸¹No caso de remoção, o *periculum in mora* é inerente à própria probabilidade de o ilícito ter sido praticado. Ou melhor: como a tutela final, na ação de remoção, objetiva eliminar o próprio ilícito ou a causa do dano, não há como supor que a tutela antecipada de remoção exija, além da probabilidade da prática do ilícito (*fumus*), a probabilidade da prática do dano (que seria o perigo nas ações tradicionais). Isso por uma razão óbvia: a simples prática do ilícito abre oportunidade à tutela final, sem que seja preciso pensar em dano, que já é pressuposto pela regra de proteção e, assim, descartado para a efetividade da tutela jurisdicional, seja final ou antecipada" MARINONI. Luiz Guilherme. Tutela Inibitória e Tutela de Remoção do Ilícito. Academia Brasileira de Direito Processual Civil. Disponível em <<http://www.abdpc.org.br/abdpc/artigos>>. Acesso em 27/02/2025.





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

Assim, requer seja reconhecida a inversão do ônus da prova no presente caso pelo acima fundamentado.

8. DOS PEDIDOS

Face os fundamentos acima mencionados, requer o Ministério Público do Estado do Paraná:

- O recebimento e a autuação da presente petição inicial, bem como dos documentos digitalizados do Inquérito Civil nº 0024.24.000014-1;
- O deferimento do pedido de tutela provisória de urgência para suspensão da coleta e tratamento de dados pessoais dos alunos para a finalidade de reconhecimento facial no procedimento de chamada dos alunos previsto no contrato nº 4313.2022 de prestação de serviços celebrado entre as rés Celepar e Valid Soluções S. A.;
- A citação dos requeridos para que, querendo, no prazo de 15 (quinze) dias, ofereça contestação, nos termos do art. 335 do Código de Processo Civil;

A procedência do pedido de provimento jurisdicional para o fim de:

1. Condenar as requeridas Companhia de Tecnologia da Informação e Comunicação do Paraná (CELEPAR), Valid Soluções S. A e Estado do Paraná, solidariamente, ao pagamento de danos morais coletivos no valor de R\$15.000.000,00 (quinze milhões de reais), a ser revertido em depósito para fundo específico, nos termos do artigo 13, da Lei nº 7.347/1985.
2. Condenar as requeridas Companhia de Tecnologia da Informação e Comunicação do Paraná (CELEPAR), Valid Soluções S. A e Estado do Paraná à remoção do ilícito para que se abstenham de coletar e tratar dados faciais biométricos dos alunos para finalidade de reconhecimento facial no procedimento de chamadas dos alunos.

Protesta pela produção de todos os meios lícitos de provas em direito admitidas, notadamente a juntada de novos documentos, caso necessário, a oitiva de testemunhas, cujo rol será apresentado oportunamente, e realização das perícias judiciais eventualmente necessárias, observando-se ainda o disposto no artigo 42, §2º, da Lei Geral de Proteção de





MPPR
Ministério Público do Paraná

3ª Promotoria de Justiça de Campo Mourão

Dados, no que tange à inversão do ônus da prova em favor dos titulares dos dados pessoais.

Dá-se a causa o valor de R\$15.000.000,00 (quinze milhões de reais).

Campo Mourão, datado e assinado eletronicamente.

Marcos José Porto Soares
Promotor de Justiça

