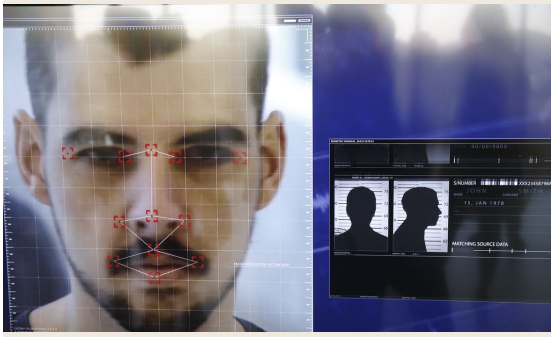
Dados biométricos de alunos: o que gestores e advogados públicos precisam saber antes de contratar

Um debate que ocorreu na Europa há alguns anos chegou discretamente ao Brasil. A tecnologia em questão é o reconhecimento facial em escolas públicas. O objetivo é legítimo: controlar frequência, reduzir evasão, notificar pais em tempo real.

Fernando Frazão/Agência Brasil



Em 2021, *Mata de São João*, município baiano, inovou ao implantar o sistema nas suas 27 escolas de ensino fundamental e virou destaque no *Jornal Nacional*. A iniciativa merece reconhecimento: a gestão identificou problemas reais. Evasão escolar, controle de acesso, desperdício na merenda e tempo perdido com chamadas manuais. A solução tecnológica respondia a cada um deles. Na Europa, projetos semelhantes foram barrados pelas autoridades de proteção de dados. A diferença não estava na intenção. Estava no que a lei exigia antes de contratar.

Reconhecimento facial não é uma câmera comum. É um sistema que captura a imagem do rosto, extrai pontos nodais únicos e os converte em um *template* matemático, um código irrepetível vinculado àquela pessoa para sempre. Esse processo transforma uma fotografia em dado biométrico. Sob a LGPD, dado biométrico é dado pessoal sensível. O artigo 11 da Lei 13.709/2018 exige base legal específica para seu tratamento, mais restrita do que a exigida para dados comuns. Quando o titular é criança ou adolescente, o artigo 14 vai além: determina que qualquer tratamento seja realizado no seu melhor interesse.

Vale pausar aqui. A face de uma criança, uma vez convertida em template biométrico e armazenada num sistema, não pode ser trocada se houver vazamento. Uma senha comprometida se redefine em minutos. Um dado biométrico exposto é permanente. Essa assimetria é o centro do problema.

Exemplos europeus de biometria facial

Em 2019, uma escola na Suécia decidiu modernizar o controle de presença dos alunos com reconhecimento facial. A iniciativa parecia razoável. A autoridade sueca de proteção de dados, a IMY, discordou: multou o município em aproximadamente €20.000 e determinou a suspensão imediata do sistema. O argumento foi preciso: estudantes não podem dar consentimento livre numa relação de dependência com a escola. O desequilíbrio de poder, por si só, invalida o consentimento.

Na França, a autoridade de proteção de dados, a Cnil, analisou proposta semelhante e chegou ao mesmo lugar: o reconhecimento facial em escolas viola o princípio da proporcionalidade. Os objetivos pretendidos poderiam ser alcançados por meios menos intrusivos. Crachás, listas digitais, aplicativos de presença. Quando existe alternativa menos invasiva, a coleta de dado biométrico não se justifica. Dois países. Duas autoridades independentes. Mesma conclusão. A tecnologia funcionava. O problema era jurídico.

O artigo 11 da LGPD é o ponto de partida, mas não o único. Ele autoriza o tratamento de dado sensível — categoria em que se enquadra o biométrico — apenas nas hipóteses taxativas do inciso II: consentimento específico e destacado, cumprimento de obrigação legal, execução de políticas públicas previstas em lei ou regulamento, estudos por órgão de pesquisa, exercício regular de direitos, proteção da vida ou tutela da saúde e prevenção à fraude. Fora dessas hipóteses, o tratamento é ilícito. Não há margem interpretativa.

Política pública não é argumento para biometria

O problema começa quando se tenta encaixar o reconhecimento facial escolar em uma dessas bases. A mais tentadora é o inciso II, alínea “b”: execução de políticas públicas previstas em lei ou regulamento. O raciocínio seria: frequência escolar é obrigação legal, logo o sistema serve a uma política pública. O argumento é frágil. A LGPD exige que a política pública esteja prevista em lei ou regulamento específico. Não basta que o objetivo final seja legítimo — é preciso que o meio, o tratamento biométrico, esteja amparado em norma que o autorize expressamente. Resoluções internas da secretaria de

educação, portarias municipais e contratos administrativos não preenchem esse requisito.

Spacca

O consentimento, por sua vez, esbarra num obstáculo estrutural. O artigo 8º, §5º da LGPD determina que o consentimento deve ser livre, informado e inequívoco. O §3º acrescenta que, quando há desequilíbrio de poder entre as partes, a liberdade do consentimento é presumivelmente comprometida. Numa relação entre aluno e escola — onde a presença é compulsória e a autoridade institucional é evidente —, essa presunção opera contra a validade do consentimento. O que as autoridades sueca e francesa identificaram na prática, a lei brasileira já antecipa na teoria.

O artigo 14 merece atenção apartada. Quando o titular é criança ou adolescente, a LGPD introduz uma camada adicional: o tratamento deve ser realizado no melhor interesse do menor. Essa expressão não é retórica. Ela importa um padrão de avaliação substantiva: não basta que o tratamento seja legal — é preciso demonstrar que ele serve, concretamente, ao interesse da criança, e não apenas ao interesse da administração ou do fornecedor. O regulamento deve, idealmente, identificar qual benefício direto o aluno obtém com a coleta do seu dado biométrico. Eficiência operacional da secretaria não equivale a benefício para o titular.

O artigo 6º, III consolida o princípio da necessidade: o tratamento deve se limitar ao mínimo necessário para a finalidade declarada. Esse princípio tem consequência prática imediata: se o objetivo é registrar frequência e existe alternativa técnica menos invasiva — aplicativo com QR code, crachá RFID, lista digital —, a coleta biométrica não é necessária. E o que não é necessário não é proporcional. E o que não é proporcional, sob a LGPD, é ilícito. A cadeia lógica é simples. O processo administrativo que antecede a contratação deveria percorrê-la explicitamente, registrando por que as alternativas foram descartadas. Sem esse registro, a justificativa da escolha tecnológica fica exposta.

Por fim, o artigo 37 impõe ao controlador a obrigação de manter registro das operações de tratamento. Em se tratando de dado biométrico de criança, esse registro não é formalidade — é evidência de que a administração agiu com diligência. Sua ausência, em caso de incidente, agrava a responsabilidade.

Custo reputacional não pode ser subestimado

A Autoridade Nacional de Proteção de Dados não é um órgão consultivo. Tem competência sancionatória prevista no artigo 52 da LGPD: advertência, multa de até 2% do faturamento do grupo econômico no Brasil — limitada a R$ 50 milhões por infração —, publicização da infração, bloqueio e eliminação dos dados tratados ilicitamente. Para entes públicos, a aplicação de multa ainda está em discussão regulatória, mas as demais sanções se aplicam integralmente. Publicização de uma infração envolvendo dados biométricos de crianças tem custo reputacional que nenhum gestor deveria subestimar.

A ANPD já sinalizou interesse no tema. Em 2023, publicou nota técnica sobre o uso de reconhecimento facial em segurança pública, fixando balizas que se aproximam do que as autoridades europeias consolidaram: necessidade de base legal específica, avaliação de impacto prévia e proporcionalidade demonstrada. Embora o documento trate de segurança pública, os princípios são os mesmos que regem qualquer tratamento de dado biométrico — inclusive no ambiente escolar.

O instrumento mais relevante nesse contexto é a DPIA — Data Protection Impact Assessment —, ou, na terminologia da LGPD, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). O artigo 38 da lei autoriza a ANPD a exigi-lo. Para tratamento de dado sensível de criança em larga escala, a elaboração do RIPD antes da contratação não é apenas recomendável — é a medida que demonstra boa-fé institucional e pode, em caso de questionamento, distinguir o gestor diligente do negligente. Um processo licitatório que inclua o RIPD na fase de planejamento contratual está um passo à frente do que a lei exige e um passo atrás do que um incidente pode custar.

Soluções para o processo administrativo

Antes de contratar qualquer solução de reconhecimento facial para escola pública, três pontos merecem atenção no processo administrativo.

O primeiro é a base legal. O processo administrativo deve identificar expressamente a hipótese do artigo 11, II da LGPD que ampara o tratamento. Se a escolha for execução de política pública, é preciso apontar a lei ou o regulamento que a prevê — não a finalidade genérica, mas o ato normativo específico. Se não houver norma, a lacuna deve ser preenchida antes da contratação, não depois. Isso pode significar submeter uma minuta de decreto ou resolução à procuradoria antes de abrir o processo licitatório. Na prática, significa que o advogado público entra no processo mais cedo do que o habitual — e é justamente aí que sua atuação tem maior valor.

O segundo é a proporcionalidade. Não basta que a escolha tecnológica seja razoável na cabeça do gestor. Ela precisa estar registrada. O processo deve conter, preferencialmente na fase de planejamento da contratação, um documento que identifique as alternativas consideradas, explique por que foram descartadas e demonstre que o dado biométrico é o meio menos invasivo disponível para atingir a finalidade. Esse documento não precisa ser extenso. Precisa ser honesto. Se a única razão para escolher reconhecimento facial foi custo ou conveniência operacional, o processo ficará vulnerável. Se a razão foi técnica e documentada, o gestor tem respaldo.

O terceiro é a responsabilidade. A distinção entre controlador e operador no artigo 5º da LGPD tem consequência direta na minuta contratual. O fornecedor que armazena os *templates* biométricos e define como os dados são processados pode ser, na prática, um controlador conjunto — e não apenas um operador. Essa distinção importa porque o controlador responde perante a ANPD. O contrato deve especificar: quem define as finalidades do tratamento, onde os dados são armazenados, por quanto tempo, quem pode acessá-los, o que acontece com os dados ao fim do contrato e qual é o protocolo em caso de incidente. Cláusulas genéricas de confidencialidade não substituem essas definições. Uma rescisão contratual sem previsão de eliminação dos dados deixa o dado biométrico da criança em poder do fornecedor por tempo indeterminado — situação que a LGPD não ampara e que o gestor não consegue justificar.

Respondidas com clareza, essas perguntas tornam o processo mais fundamentado. Ignoradas, elas voltarão, possivelmente num momento menos oportuno.

Vale reforçar que esta verificação não se restringe ao reconhecimento facial em escolas. As mesmas questões surgirão em qualquer contratação pública que envolva dado pessoal sensível: sistemas de monitoramento de saúde de servidores, plataformas de análise comportamental de alunos, câmeras com identificação automática em espaços públicos, soluções de registro biométrico de ponto. Em todos esses casos, base legal, proporcionalidade e definição do controlador continuam sendo as perguntas certas a fazer, antes de assinar.

Fonte: https://conjur.jumps.com.br/2026-mai-28/dados-biometricos-de-alunos-o-que-gestores-e-advogados-publicos-precisam-saber-antes-de-contratar/