Análise de maturidade sobre uso de biometria e adequação normativa da LGPD nos Institutos Federais do Brasil

Pollyana Esteves dos Reis Moreira
Robson de Oliveira Albuquerque
Programa de Pós-Graduação em Engenharia Elétrica (PPEE)
Universidade Federal de Brasília
pollyanaesteves@gmail.com; robson@redes.unb.br

RESUMO

O presente estudo analisa a adoção da tecnologia de biometria facial nos Institutos Federais de Educação, Ciência e Tecnologia do Brasil, com ênfase na relação entre inovação tecnológica e a proteção da privacidade e dos direitos fundamentais de estudantes, sobretudo crianças e adolescentes. Em um cenário de expansão da vigilância digital e de maiores preocupações com a proteção de dados pessoais, torna-se fundamental compreender como essas tecnologias são aplicadas no ambiente escolar. Para tanto, esta pesquisa desenvolve uma investigação empírica a partir de questionários aplicados a gestores institucionais, complementada por análise documental e por informações obtidas por meio da Lei de Acesso à Informação. São abordados os desafios éticos, jurídicos e sociais, além das fragilidades na governança e transparência relacionadas à gestão dos dados biométricos. Os principais resultados destacam a necessidade urgente de políticas públicas que garantam a incorporação responsável dessas tecnologias no ambiente educacional, protegendo direitos fundamentais. Nesse sentido, este artigo contribui para o debate sobre o equilíbrio entre inovação tecnológica e a proteção de populações vulneráveis no contexto escolar.

Palavras-Chave

Biometria Facial, Privacidade, LGPD, Institutos Federais, Inteligência Artificial.

ABSTRACT

This study analyzes the adoption of facial biometrics technology at Brazilian Federal Institutes of Education, Science, and Technology, with an emphasis on the relationship between technological innovation and the protection of the privacy and fundamental rights of students, especially children and adolescents. In a context of expanding digital surveillance and heightened concerns about personal data protection, understanding how these technologies are applied in the school environment is crucial. To this end, this research develops an empirical investigation based on questionnaires administered to institutional administrators, complemented by document analysis and information obtained through the Access to Information Law. The ethical, legal, and social challenges, as well as weaknesses in governance and transparency related to the management of biometric data, are addressed. The main results highlight the urgent need for public policies that ensure the responsible incorporation of these technologies into the educational environment, protecting fundamental rights. In this sense, this article contributes to the debate on the balance between technological innovation and the protection of vulnerable populations in the school context.

Keywords

facial biometrics, privacy, LGPD, Federal Institutes, Artificial Intelligence.

1. INTRODUÇÃO

O avanço das tecnologias digitais e, em particular do uso de inteligência artificial (IA), tem impulsionado a adoção de sistemas biométricos em diversos setores, e isso inclui a educação básica e superior (Leaton Gray, 2018; Necochea-Chamorro, 2024; Hoo et al., 2019). Entre essas tecnologas, o reconhecimento facial se destaca por sua capacidade de automatizar processos de identificação a partir de características únicas do rosto humano, permitindo, por exemplo, registrar presenças, controlar acessos e monitorar deslocamentos de estudantes. No Brasil, o uso desse tipo de tecnologia em escolas públicas tem sido justificado por gestores como estratégia para otimizar a gestão administrativa, prevenir a evasão escolar e reforçar a segurança do ambiente escolar (Tavares et al., 2023).

Apesar dessas justificativas, múltiplos estudos apontam preocupações éticas, jurídicas e sociais na adoção de reconhecimento facial em ambientes escolares (Mead & Park, 2014; Schropp, 2015). O relatório "TECNOLOGIAS DE VIGILÂNCIA E EDUCAÇÃO: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras", elaborado pelo InternetLab, identificou que, nos quinze casos mapeados em escolas públicas brasileiras, não foram realizados estudos prévios de impacto à proteção de dados pessoais ou aos direitos humanos antes da implementação, mesmo quando envolviam crianças e adolescentes (Tavares et al., 2023, p. 17). Além disso, pesquisas sobre racismo algorítmico indicam que sistemas de reconhecimento facial apresentam taxas significativamente maiores de erro para pessoas negras, especialmente mulheres negras, o que pode resultar em situações de exclusão, constrangimento ou criminalização indevida (Buolamwini & Gebru, 2018; Santos et al., 2023; Queiroz, 2023).

Esses riscos se somam a um contexto mais amplo de "plataformização" da educação, fenômeno caracterizado pela crescente dependência de soluções tecnológicas proprietárias, muitas vezes controladas por empresas transnacionais, que coletam, armazenam e processam grandes volumes de dados, principalmente em países em desenvolvimento que não são detentoras dessas tecnologias (UNCTAD, 2019; 2021). Esse caso é, claramente, mais grave no caso de dados de comunidades escolares como os de estudantes e professores (NIC.BR, 2023). Conforme ressalta o estudo do Comitê Gestor da Internet no Brasil, tal modelo pode comprometer a soberania digital e a autonomia educacional, além de fragilizar a proteção de dados sensíveis, especialmente em instituições públicas que têm como missão

atender populações historicamente vulnerabilizadas (NIC.BR, 2023).

No caso dos Institutos Federais de Educação, Ciência e Tecnologia (IFs), a discussão se torna ainda mais relevante. Criados pela Lei nº 11.892, de 29 de dezembro de 2008, essas instituições oferecem educação profissional, científica e tecnológica integrada, atendendo majoritariamente adolescentes e jovens. Trata-se, portanto, de um público protegido pelo Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), o que impõe obrigações legais rigorosas quanto à coleta e ao tratamento de dados biométricos.

Considerando o contexto apresentado, este estudo tem como foco principal realizar uma análise do uso de biometria com reconhecimento facial, nos IFs, examinando suas finalidades, formas de implementação, riscos e implicações éticas, jurídicas e sociais. Para isso, o artigo é organizado conforme se segue. Primeiramente é apresentada uma caracterização dos IFs, incluindo a justificativa para a escolha desse recorte para a pesquisa (Seção 2); em seguida, aborda-se a aplicação da inteligência artificial no âmbito educacional, com ênfase nos sistemas biométricos de reconhecimento facial, destacando os principais riscos e desafios associados (Seção 3). Posteriormente, apresentam-se e discutem-se os resultados de uma pesquisa empírica acerca da aplicação dessa tecnologia nos Institutos Federais (Seção 4). Por fim, são elaboradas as considerações finais e recomendações resultantes do estudo (Seção 5).

2. OS INSTITUTOS FEDERAIS

Os IFs foram instituídos pela Lei nº 11.892, de 29 de dezembro de 2008, que criou a Rede Federal de Educação Profissional, Científica e Tecnológica. Conforme dispõe o art. 2º da referida lei, os IFs configuram-se como "instituições de educação superior, básica e profissional, pluricurriculares e multicampi, especializados na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas" (Brasil, 2008).

De acordo com dados oficiais publicados pelo Ministério da Educação (MEC), a Rede Federal de Educação Profissional, Científica e Tecnológica é composta por 686 unidades, incluindo 38 IFs, dois Centros Federais de Educação Tecnológica (Cefets), a Universidade Tecnológica Federal do Paraná (UTFPR), 22 escolas técnicas vinculadas a universidades federais e ao Colégio Pedro II. Adicionalmente, por meio do Novo Programa de Aceleração do Crescimento (Novo PAC), o governo federal encontra-se em processo de implantação de 102 novos campi dos Institutos Federais em todo o território nacional (Basil, 2025).

A organização institucional dos IFs apresenta singularidades relevantes para a análise do uso de tecnologias biométricas. Primeiramente, destacam-se pela integração vertical de ensino, abrangendo desde a educação básica, notadamente o ensino médio técnico integrado, até cursos de graduação e pós-graduação. Essa estrutura permite que uma mesma instituição atenda públicos diversos, incluindo crianças e adolescentes matriculados em cursos técnicos integrados, concomitantes ou subsequentes, jovens adultos em graduações e especializações, bem como adultos em cursos de formação inicial e continuada (FIC) ou programas de qualificação profissional (Brasil, 1996; 2008).

Essa diversidade etária e formativa implica desafios particulares para a gestão institucional, especialmente no que se refere à proteção de dados pessoais. Crianças e adolescentes são sujeitos de direitos com proteção especial prevista no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), enquanto todos os discentes, independentemente da faixa etária, estão amparados pelas garantias da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que estabelece regras específicas para o tratamento de dados pessoais e pessoais sensíveis, como aqueles de natureza biométrica.

Além da diversidade do público atendido, os IFs possuem capilaridade territorial e compromisso social expressivos. Presentes em todas as unidades federativas, com campi distribuídos em capitais e municípios de médio e pequeno porte, essas instituições desempenham papel estratégico na promoção do desenvolvimento regional e na democratização do acesso à educação profissional e tecnológica. Ademais, a missão institucional prevê a articulação entre ensino, pesquisa e extensão, fomentando não apenas a formação técnica, mas também a formação cidadã crítica e a inserção qualificada no mundo do trabalho (Senado Federal, 2024).

A escolha dos IFs como objeto de análise no presente estudo fundamenta-se em três aspectos principais:

a. Pluralidade etária e formativa – a coexistência de diferentes perfis de estudantes impõe cuidados diferenciados na implementação de tecnologias de identificação, especialmente aquelas que envolvem coleta e processamento de dados biométricos;
b. Natureza pública e federal – a adoção de tecnologias como o reconhecimento facial nesses espaços adquire relevância para a formulação e avaliação de políticas públicas educacionais de alcance nacional;
c. Missão educacional ampliada – a proposta de formação integral, aliando conhecimentos técnicos, científicos e humanísticos, exige que a incorporação de novas tecnologias seja compatível com princípios pedagógicos, direitos fundamentais e marcos regulatórios de proteção de dados.

Diante desse cenário, compreender como e em que medida os IFs têm incorporado ou avaliado a possibilidade de utilizar reconhecimento facial é essencial para avaliar não apenas a eficácia administrativa da tecnologia, mas também seus impactos pedagógicos, éticos e jurídicos, considerando a complexidade e heterogeneidade da comunidade escolar que essas instituições atendem.

3. APLICAÇÃO DA IA EM SISTEMAS BIOMÉTRICOS DE RECONHECIMENTO FACIAL NO CONTEXTO EDUCACIONAL

O reconhecimento facial é uma tecnologia biométrica capaz de identificar ou verificar a identidade de indivíduos a partir de características únicas do rosto, como distâncias relativas entre olhos, nariz e boca, contornos faciais e estrutura óssea. Esse processo envolve a captura de imagens digitais e a extração de padrões faciais, posteriormente comparados por algoritmos treinados. O avanço recente dessa tecnologia está diretamente ligado ao uso de inteligência artificial (IA), em especial de técnicas de machine learning e redes neurais profundas, que permitem aprimorar continuamente os modelos por meio do treinamento em grandes volumes de dados (Hernández-De-Menéndez *et al*., 2021). No campo educacional, essa combinação tem sido empregada com

o objetivo de automatizar processos como controle de frequência, autenticação de acesso a áreas restritas, apoio a avaliações eletrônicas e monitoramento de segurança (Hernández-De-Menéndez *et al*., 2021), sob o argumento de otimizar rotinas administrativas e aumentar a segurança no ambiente escolar.

No entanto, a adoção dessa tecnologia em instituições de ensino apresenta desafios técnicos, éticos, jurídicos e sociais que exigem análise criteriosa. Questiona-se ainda se tecnologicamente já é possível adotar reconhecimento fácil para crianças, que estão em fase de crescimento. Hossain & Schuckers (2025) discutem as taxas de erros de algoritmos, e contesta-se o custo-benefício dessa aplicação quando se trata de crianças e adolescentes, já que as dificuldades aumentam, pois mudanças fisiológicas decorrentes do crescimento podem alterar parâmetros faciais, comprometendo a precisão ao longo do tempo (Moolla et al., 2021).

A dimensão ética da aplicação dessa tecnologia é igualmente sensível. O reconhecimento facial lida com dados biométricos sensíveis, que exigem alto nível de proteção e transparência. Muitos sistemas, no entanto, operam de forma opaca, sem que os usuários compreendam plenamente como seus dados são coletados, processados e armazenados, situação apontada por Roundtree (2021) em estudos sobre reconhecimento facial em jovens. No contexto brasileiro, isso pode representar uma violação do direito à autodeterminação informativa previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece regras específicas para o tratamento de dados pessoais sensíveis. Quando o público-alvo inclui crianças e adolescentes, a complexidade aumenta, pois esses indivíduos não têm capacidade plena para fornecer consentimento informado, transferindo essa decisão para os responsáveis legais. Conforme argumenta Badawy (2025), o consentimento de menores é dinâmico e pode precisar ser revisto ou revogado quando atingem a maturidade, o que exige mecanismos que permitam essa revisão. Além disso, o uso de imagens de crianças traz riscos adicionais, como o possível uso indevido desses dados, a formação de perfis digitais permanentes e a maior vulnerabilidade a ataques cibernéticos, sobretudo em um cenário marcado por recorrentes vazamentos de informações.

O Radar Tecnológico – Biometria e Reconhecimento Facial da Autoridade Nacional de Proteção de Dados (ANPD, 2024) corrobora a necessidade dessa cautela ao relatar experiências internacionais e nacionais em que a aplicação de sistemas biométricos sem adequada avaliação prévia de impacto resultou em violações de direitos fundamentais. Em 2020, a autoridade de proteção de dados da Holanda advertiu formalmente um supermercado que utiliza reconhecimento facial ao vivo para prevenir furtos, por entender que essa finalidade não se enquadra nas situações excepcionais autorizadas por lei (Autoriteit Persoonsgegevens, 2020). Em 2022, autoridades da Itália, França (EDPB, 2022) e Reino Unido (ICO, 2022) aplicaram sanções milionárias à empresa *Clearview AI* pela coleta massiva e não autorizada de imagens de cidadãos para extração de dados biométricos, em desacordo com a GDPR e princípios de transparência, finalidade e base legal.

No Brasil, o mesmo relatório destaca que, diferentemente de outros países, não há legislação federal específica para regulamentar o uso de reconhecimento facial na educação. O estudo do InternetLab (2023), citado pela ANPD, mapeou quinze iniciativas em escolas públicas, identificando falhas recorrentes: ausência de normas orientativas, inexistência de estudos de impacto à proteção de dados, consentimento inadequado e, em alguns casos, erros de registro de frequência — como no município de Xaxim (SC), onde alunos presentes foram indevidamente marcados como ausentes. O caso da rede estadual do Paraná, implantado em 2023, foi apontado como exemplo crítico, por condicionar o acesso à educação à cessão compulsória de imagem e por não reconhecer formalmente que dados biométricos são dados sensíveis, em desacordo com os arts. 11 e 14 da LGPD (ANPD, 2024).

Esses exemplos reforçam que a adoção de reconhecimento facial no contexto educacional, especialmente envolvendo crianças e adolescentes, exige a implementação de mecanismos referentes de governança, transparência e supervisão independente, alinhados ao princípio do melhor interesse do menor e às recomendações da ANPD. Além disso, demonstram que falhas na regulação e no controle dessas tecnologias podem replicar, no Brasil, problemas já identificados em outros países, ampliando riscos de discriminação, uso desproporcional e violação de direitos, além de impactos no desenvolvimento integral da criança, como já ressaltam estudos recentes da UNICEF (2025) sobre vulnerabilidade digital na infância. Fora isso, questiona-se ainda se a tecnologia já avançou o suficiente, para que sua adoção seja de fato vantajosa, do ponto de vista de uma avaliação de custo-benefício.

Diante desse cenário, torna-se essencial investigar como os IFs estão incorporando, ou se planejam incorporar, sistemas de reconhecimento facial e outras aplicações que utilizam a inteligência artificial, identificando se essa é uma realidade já presente na rede e de que forma estão sendo tratados os aspectos técnicos, jurídicos e éticos envolvidos. Tal investigação revela-se fundamental para identificar lacunas regulatórias, bem como para revelar possíveis fragilidades ou irregularidades que possam colocar em risco os direitos fundamentais não apenas de crianças e adolescentes, mas também de toda a comunidade escolar. Essa análise fornecerá subsídios para a compreensão do cenário atual e servirá de base para a interpretação dos achados apresentados na seção seguinte, onde são discutidos os resultados da pesquisa realizada.

4. PROBLEMA DE PESQUISA E METODOLOGIA

4.1 Discussão do problema

Apesar do crescente interesse na adoção de sistemas de reconhecimento facial em instituições educacionais, pouco se conhece sobre sua implementação e gestão efetiva no contexto escolar. Riscos relacionados à proteção de dados e à transparência do tratamento, especialmente no que se refere a crianças e adolescentes, ainda não foram suficientemente investigados.

Há escassez de estudos empíricos que examinem detalhadamente as práticas institucionais, as finalidades da tecnologia e os mecanismos de governança adotados. Essa lacuna impede avaliar se tais sistemas estão alinhados aos marcos regulatórios nacionais e se garantem a proteção efetiva dos direitos fundamentais dos titulares.

Diante desse cenário, o problema central desta pesquisa investiga como os Institutos Federais têm incorporado sistemas biométricos, e quais impactos éticos, jurídicos e sociais essas tecnologias produzem sobre a comunidade escolar. A investigação busca analisar tanto as finalidades e condições de implementação quanto a existência de mecanismos institucionais de governança, transparência algorítmica e proteção de dados, de modo a

compreender os riscos, limites e implicações da adoção dessas tecnologias no contexto da educação pública federal.

4.2 Métodos aplicados

Para compreender o panorama atual do uso de tecnologias biométricas, nos IFs, este tópico apresenta e discute o método utilizado no estudo. Nossa coleta de dados foi realizada a partir de dados oficiais coletados via solicitações fundamentadas na Lei de Acesso à Informação (Lei nº 12.527/2011), realizadas entre os meses de novembro de 2024 e março de 2025 aos 38 IFs que compõem a Rede Federal, complementados por buscas sistemáticas nos portais da transparência e nos sites das referidas instituições, conforme constante no Apêndice I.

A análise buscou identificar a extensão da adoção dessas tecnologias, seus processos administrativos, bem como os cuidados relacionados à proteção de dados pessoais sensíveis no ambiente educacional.

Também foi elaborado um questionário estruturado (Apêndice I) com perguntas objetivas e dissertativas, visando investigar práticas institucionais da adoção de tecnologias biométricas, governança e proteção de dados, com atenção especial a crianças e adolescentes. Todos os 38 IFs responderam ao questionário.

O método considerado nesta pesquisa é, portanto, misto, com aspectos qualitativos a partir de análise documental e quantitativo a partir de estruturação de dados. A investigação foi organizada em duas dimensões temáticas, que orientaram a coleta e análise dos dados:

- **1a Dimensão: Identificação Institucional.** Visou mapear as características institucionais, como a estrutura física e normativas internas relacionadas à privacidade, proteção de dados e segurança da informação, além da governança do tratamento de dados.
- **2a Dimensão: Utilização de Dados Biométricos**. Buscou compreender o grau de implantação ou planejamento para uso de tecnologias biométricas, suas finalidades e a existência de análises de impacto de proteção de dados pessoais.

Para nortear nossa análise, nós construímos duas hipóteses de pesquisa, descritas a seguir:

- **Hipótese de pesquisa 1**: Descobrir se IFs maiores apresentam maior maturidade normativa em relação à segurança da informação e à proteção de dados pessoais.
- **Hipótese de pesquisa 2**: Descobrir se as IFs que adotam iniciativas de biometria e reconhecimento facial são as instituições com maior maturidade normativa em relação à segurança da informação e à proteção de dados pessoais.

5. RESULTADOS E DISCUSSÕES

5.1 Análise de Maturidade Normativa

O primeiro passo é analisar a maturidade normativa em relação à segurança da informação e à proteção de dados pessoais. Para isso, investigamos se os IFs apresentavam política ou normativo relacionado à privacidade ou proteção de dados aprovado internamente ou em construção. A Tabela 1 mostra quantos IFs apresentam política ou normativo relacionado à proteção de dados pessoais aprovado internamente ou em construção e as quantidades média de cursos e de matrículas de cada uma das categorias, enquanto a Figura 1 mostra as instituições que apresentam esses normativos por região do país.

Tabela 1 - Normativos relacionados à privacidade ou à proteção de dados

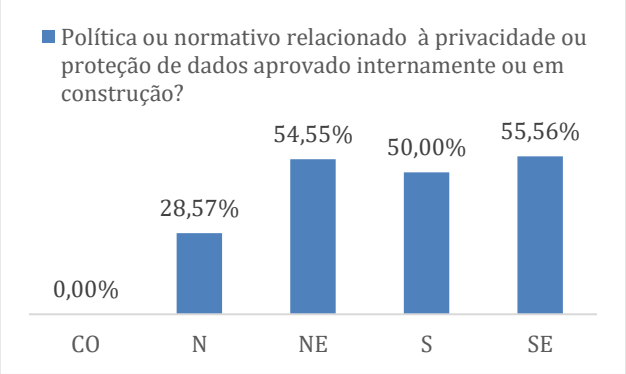
	Política ou normativo relacionado à **privacidade ou proteção de dados** aprovado internamente ou em construção?			
	Número de instituições	Em percentual	Quantidade média de cursos	Quantidade média de matrículas
Não	22	57,9%	57,6	7039,6
Sim	16	42,1%	82,9	9769,3
Total	38	100,0%	64,5	8188,9

Elaboração própria. Fonte: pesquisas via LAI.

Menos da metade dos 38 IFs têm apresentavam política ou normativo relacionado à privacidade ou proteção de dados aprovado internamente ou em construção, sinalizando assim baixa maturidade normativa em relação à proteção de dados pessoais. Parece haver uma correlação entre tamanho de instituição e a maturidade normativa, uma vez que as instituições que apresentam normativos ou políticas têm, em média, um número maior de cursos e de matrículas, o que sugere que não devemos rejeitar nossa Hipótese de pesquisa 1, pelo menos no que diz respeito à proteção de dados pessoais.

Observa-se também que nenhum IF da região CO apresenta política de proteção de dados e que na região norte também parece haver uma baixa maturidade. Nossos dados não permitem explorar essa relação de forma mais aprofundada, mas como estudos futuros, sugere-se investigar a relação entre a maturidade normativa de instituições mais ao interior do país em relação à proteção de dados pessoais.

Figura 1 – Distribuição dos IFs por região do Brasil considerando aspectos normativos relacionados à privacidade ou à proteção de dados



Elaboração própria. Fonte: pesquisas via LAI.

Prosseguindo com nossa investigação, a Tabela 2 mostra quantos IFs apresentam política ou normativo relacionado à segurança da informação aprovado internamente ou em construção e as quantidades média de cursos e de matrículas de cada uma das categorias, enquanto a Figura 2 mostra as instituições que apresentam esses normativos por região do país.

Tabela 2 - Normativos relacionados à segurança da informação

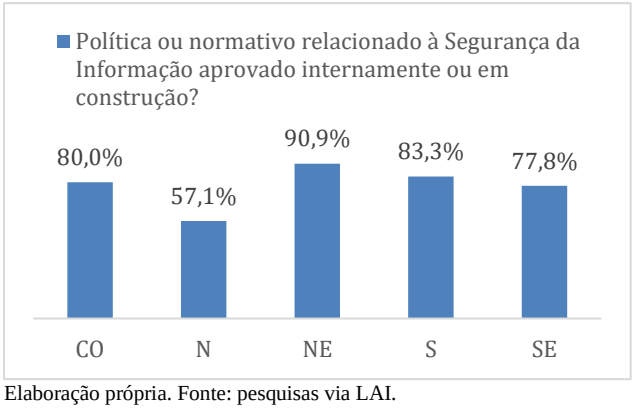
	Política ou normativo relacionado à **Segurança da Informação** aprovado internamente ou em construção?			
	Número de instituições	Em percentual	Quantidade média de cursos	Quantidade média de matrículas
Não	8	21,1%	57,9	6272
Sim	30	78,9%	71,3	8700,1
Total	38	100,0%	64,5	8188,9

Elaboração própria. Fonte: pesquisas via LAI.

Pelos dados apresentados, há uma maior maturidade normativa em relação à segurança da informação do que em relação à proteção de dados pessoais. Essa diferença pode ser explicada pelo fato de que os regulamentos de segurança da informação começaram a ser consolidados ainda nos anos 2000, impulsionados por diretrizes federais voltadas à governança de TI, à proteção de ativos digitais e à gestão de incidentes, promovendo padrões técnicos de confidencialidade, integridade e disponibilidade da informação. Contudo, tais normativos possuem um viés essencialmente institucional, voltado à preservação de sistemas e à continuidade organizacional, sem considerar de forma abrangente os direitos individuais e a transparência no uso de informações pessoais. Essa assimetria revela uma limitação estrutural: a maturidade em segurança da informação não implica, necessariamente, maturidade em proteção de dados pessoais, já que esta exige também uma abordagem jurídica, ética e social que só foi consolidada no Brasil com a LGPD.

Mais uma vez, parece haver uma correlação entre tamanho de instituição e a maturidade normativa, uma vez que as instituições que apresentam normativos ou políticas relacionados à segurança da informação também têm, em média, um número maior de cursos e de matrículas, o que sugere que não devemos rejeitar nossa Hipótese de pesquisa 1.

Figura 2 - Normativos relacionados à segurança da informação por região do país



Elaboração própria. Fonte: pesquisas via LAI.

5.2 Análise sobre encarregados de tratamento de dados

A Tabela 3 mostra quantos IFs nomearam seus encarregados pelo tratamento de dados, um dos requerimentos da LGPD e indicadores de maturidade normativa em relação à privacidade e à proteção de dados pessoais.

Tabela 3 - Nomeação de encarregado pelo tratamento de dados

	Nomeou o **encarregado pelo tratamento de dados**?			
	Número de instituições	Em percentual	Quantidade média de cursos	Quantidade média de matrículas
Não	7	18,4%	52	6799,4
Sim	31	81,6%	72,2	8502,7
Total	38	100,0%	64,5	8188,9

Elaboração própria. Fonte: pesquisas via LAI.

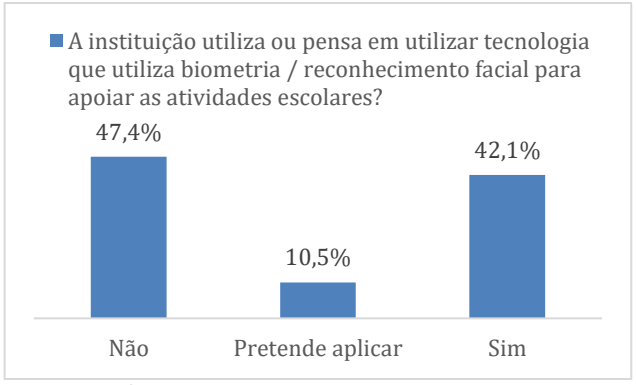
Dado que se trata de uma obrigação legal, chama a atenção que 18,4% dos IFs ainda não tenha nomeado seu encarregado pelo tratamento de dados pessoais. Mas, mais uma vez, a Hipótese de pesquisa 1 de pesquisa se mantém não rejeitada, dado que isso ocorre em instituições que são, em média menores e que, possivelmente, têm maiores dificuldades institucionais para isso.

Dos IFs que apresentavam política ou normativo relacionado à privacidade ou proteção de dados aprovado internamente ou em construção, somente 1 instituição ainda não nomeou seu encarregado de tratamento de dados pessoais, o que sugere que ter uma política é um primeiro passo nesse processo de maturidade normativa.

5.3 Análise sobre uso de tecnologias biométricas

Partindo agora para nossa investigação específica acerca do uso de tecnologias biométricas e/ou de reconhecimento facial, dos 38 IFs, aproximadamente 42,1% já utilizam tecnologias biométricas em suas atividades institucionais, enquanto cerca de 10,5% encontram-se em processo de avaliação para a implantação dessas tecnologias. Por outro lado, 47,4% declararam não utilizar tais sistemas. Esses dados estão representados no Figura 3.

Figura 3 - Uso de tecnologias biométricas e/ou de reconhecimento facial nos IFs



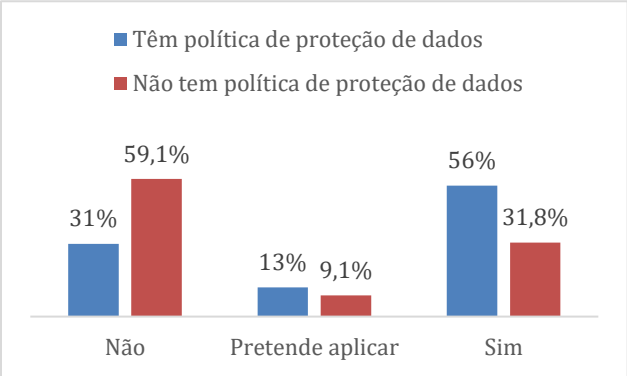
Elaboração própria. Fonte: pesquisas via LAI.

A Figura 4, por sua vez, relaciona o uso/desejo de uso de tecnologias biométricas com a existência ou não de política de proteção de dados pessoais.

Os dados do Figura 4 mostram que 31,8% usam tecnologias biométricas e de reconhecimento facial sem ter política ou normativo relacionado à proteção de dados pessoais aprovado internamente ou em construção, em total desacordo com a legislação. Isso é bastante alarmante e chama a atenção para a falta

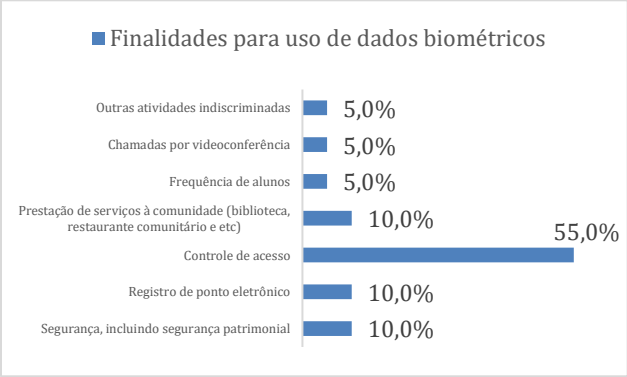
de maturidade normativa dessas instituições e de como ainda há muito a se construir em termos de proteção de dados no país.

Figura 4 - Uso de tecnologias biométricas e/ou de reconhecimento facial nos IFs por instituição com ou sem política de proteção de dados



Elaboração própria. Fonte: pesquisas via LAI.

Figura 5 - Finalidades para o uso de biometria



Elaboração própria. Fonte: pesquisas via LAI.

Em relação às finalidades de uso das tecnologias biométricas, a maioria das instituições indicou que a principal aplicação está no controle de acesso físico às unidades, realizado por meio de catracas e cancelas, abrangendo servidores, colaboradores e estudantes, como mostram as informações do Figura 5. Ao serem questionadas sobre os procedimentos realizados antes da aquisição e implementação das tecnologias biométricas, como a realização da análise de impacto e riscos, a inclusão de cláusulas contratuais que definam responsabilidades em conformidade com a LGPD, e a verificação da adequação das empresas fornecedoras à referida legislação, foram identificadas importantes lacunas.

5.4 Discussões considerando o problema e as hipóteses

Os resultados obtidos permitem uma análise crítica da relação entre a adoção de tecnologias biométricas nos IFs e o nível de maturidade normativa das instituições, especialmente no que se refere à segurança da informação e à proteção de dados pessoais.

Apesar da crescente adoção dessas tecnologias, constatou-se baixa conformidade com as exigências legais da Lei nº 13.709/2018 (LGPD). Apenas 3% das instituições declararam ter realizado Relatórios de Impacto à Proteção de Dados (RIPD), instrumento fundamental para identificar e mitigar riscos associados ao tratamento de dados sensíveis. Além disso, a maioria das contratações ocorreu sem a inclusão de cláusulas contratuais específicas que delimitassem responsabilidades entre controlador e operador, revelando fragilidades de governança. Outro aspecto relevante foi a reduzida verificação da conformidade das empresas fornecedoras com a LGPD no momento da contratação, o que compromete a segurança jurídica e a efetividade da proteção de dados pessoais.

No plano das políticas internas, poucas instituições apresentaram normativos específicos para o tratamento de dados biométricos, limitando-se a regulamentos gerais de segurança da informação. Em muitos casos, os gestores não souberam informar detalhes sobre armazenamento, transferência ou eventual processamento internacional dos dados, evidenciando lacunas de transparência e controle. Essas deficiências configuram um desafio relevante para a implementação responsável da biometria, expondo os IFs a riscos legais, operacionais e éticos.

No tocante à fiscalização externa, a maioria das instituições declarou não ter recebido questionamentos por parte de órgãos de controle. Contudo, foi identificado ao menos um inquérito civil em tramitação no Ministério Público Federal, indicando que o tema começa a atrair atenção de instâncias de controle e que a governança de dados deve constituir prioridade estratégica.

Diante desse panorama, as hipóteses de pesquisa formuladas orientam a análise crítica a seguir.

5.4.1 Hipótese de Pesquisa 1

Hipótese: Instituições Federais maiores apresentam maior maturidade normativa em relação à segurança da informação e à proteção de dados pessoais.

Os resultados das Tabelas 1, 2 e 3 confirmam a existência de uma associação entre o porte institucional — medido pelo número médio de cursos e matrículas — e a adoção de normativos de proteção de dados e de segurança da informação. Verificou-se que os IFs de maior porte apresentam políticas aprovadas ou em elaboração, além de maior consolidação na nomeação de encarregados pelo tratamento de dados pessoais.

Esse cenário sugere que a complexidade organizacional e o volume de dados processados impulsionam a formalização de práticas de governança, refletindo em maior maturidade normativa. Assim, os achados permitem não rejeitar a Hipótese 1, dado que há evidências consistentes de que instituições maiores apresentam níveis mais avançados de adequação normativa.

5.4.2 Hipótese de Pesquisa 2

Hipótese: As Instituições Federais que adotam iniciativas de biometria e reconhecimento facial são aquelas com maior maturidade normativa em relação à segurança da informação e à proteção de dados pessoais.

A análise empírica evidencia um cenário heterogêneo. De um lado, verificou-se que parte dos IFs que possuem políticas consolidadas de proteção de dados, encarregados formalmente designados também figura entre aqueles que mais avançaram na implementação de tecnologias biométricas, o que confirma parcialmente a relação proposta. Esses achados sugerem que a maturidade normativa pode atuar como fator facilitador ou mesmo como pré-condição para a adoção de tecnologias de maior complexidade regulatória.

Por outro lado, identificou-se que uma parcela significativa das instituições implementa sistemas biométricos sem dispor de

políticas específicas de proteção de dados pessoais, demonstrando que essa associação não é absoluta. Tal situação é particularmente preocupante diante da natureza sensível dos dados biométricos e do perfil do público atendido, majoritariamente composto por crianças e adolescentes, cujos direitos demandam salvaguardas adicionais.

Dessa forma, os achados reforçam que a Hipótese 2 deve ser compreendida como um parâmetro normativo desejável: a maturidade em segurança da informação e em proteção de dados pessoais deve ser condição prévia para a implementação de sistemas de biometria e reconhecimento facial. A lacuna observada entre esse ideal e a prática institucional evidencia fragilidades regulatórias e de governança de dados que precisam ser sanadas, seja por meio de políticas públicas, seja por atuação mais rigorosa de órgãos de controle e de fiscalização.

Portanto, a Hipótese 2 contribui para evidenciar que a mera adoção tecnológica não pode ser confundida com maturidade normativa. Pelo contrário, os dados sugerem que há instituições avançando em soluções de reconhecimento facial de forma prematura, sem respaldo adequado em políticas internas, o que amplia riscos jurídicos, éticos e sociais. Esse contraste demonstra não apenas a relevância da hipótese, mas também a urgência de alinhar a inovação tecnológica às exigências legais e regulatórias de uso de inteligência artificial no contexto da educação pública brasileira.

6. CONCLUSÕES

Este estudo analisou a implementação de tecnologias biométricas, em especial o reconhecimento facial, nos IFs, destacando a relação entre adoção tecnológica e maturidade normativa em segurança da informação e proteção de dados pessoais. Os resultados indicam que, embora instituições maiores e com normativos consolidados avancem mais rapidamente na implementação dessas tecnologias, ainda há um número expressivo de IFs que as utilizam sem políticas formais ou mecanismos adequados de governança, o que gera vulnerabilidades jurídicas e operacionais, especialmente no tratamento de dados de crianças e adolescentes.

A análise evidencia que a maturidade em segurança da informação não garante, por si só, a proteção efetiva de dados pessoais sensíveis, reforçando a necessidade de políticas internas de proteção de dados pessoais, avaliação de impacto e fiscalização contínua. Além disso, os achados suscitam uma reflexão crítica sobre a real adequação do uso de reconhecimento facial em contextos educacionais. Considerando as limitações técnicas, como taxas de erro em crianças em crescimento, e os riscos associados à criação de perfis digitais permanentes, questiona-se se a adoção dessa tecnologia é realmente necessária ou se alternativas menos invasivas poderiam atender aos objetivos administrativos e de segurança.

Sob essa perspectiva, o estudo sugere que o uso de biometria em instituições de ensino deve ser cuidadosamente ponderado, com limites claros quanto ao tratamento de dados pessoais realizados, especialmente quando envolve públicos vulneráveis. A implementação deveria ocorrer apenas em ambientes com maturidade normativa consolidada, monitoramento constante e mecanismos transparentes de supervisão, garantindo que os benefícios não se sobreponham aos direitos fundamentais dos titulares.

Outro achado relevante diz respeito às diferenças regionais. Observou-se que determinadas regiões do país apresentam menor consolidação normativa, como no caso do Centro-Oeste, em que não foram identificadas políticas de proteção de dados pessoais nos IFs respondentes, e da região Norte, que também revela baixos níveis de maturidade. Embora os dados obtidos não permitam aprofundar a análise dessa disparidade, trata-se de um aspecto que merece investigação futura, sobretudo para compreender em que medida fatores territoriais e estruturais podem influenciar o grau de adequação normativa das instituições federais de ensino.

Por fim, os resultados indicam a importância de trabalhos futuros que investiguem não apenas os impactos pedagógicos, sociais e psicológicos do uso dessas tecnologias, mas também a avaliação sistemática dos riscos e impactos associados ao tratamento de dados biométricos, incluindo aspectos de segurança, privacidade e conformidade legal. Esse tipo de análise permitirá compreender de forma mais aprofundada os efeitos da adoção de reconhecimento facial em ambientes educacionais e fornecerá subsídios para a formulação de políticas e práticas institucionais mais efetivas.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Radar Tecnológico – Biometria e Reconhecimento Facial*. 1. ed. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 3 ago. 2025.

AUTORITEIT PERSOONSGEGEVENS, Dutch DPA issues formal warning to supermarket for use of facial recognition technology, 2020. Disponível em: https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognition-technology. Acesso em: 01 ago. 2024.

BADAWY, Wael. The ethical implications of using children's photographs in artificial intelligence: challenges and recommendations. AI and Ethics, p. 1-12, 2025.

BUARQUE, Gabriela. Artificial intelligence and algorithmic discrimination: a reflection on risk and vulnerability in childhood. Brazilian Journal of Law, Technology and Innovation, v. 1, n. 2, p. 63-86, 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Diário Oficial da União, Seção 1, Edição Extra, 18 nov. 2011, p. 1

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 11.892, de 29 de dezembro de 2008. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 30 dez. 2008.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União: Brasília, 20 dez. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 10 ago. 2025.

BRASIL. Ministério da Educação. Educação Profissional e Tecnológica. Disponível em:https://www.gov.br/mec/pt-br/100-novos-ifs. Acesso em: 10 ago. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender

classification. Proceedings of Machine Learning Research, v. 81, p. 1-15, 2018.

EUROPEAN DATA PROTECTION BOARD - EDPB, Facial recognition in school renders Sweden's first GDPR fine, 2019. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf. Acesso em: 01 ago. 2024.

HERNANDEZ-DE-MENENDEZ, Marcela et al. Biometric applications in education. International Journal on Interactive Design and Manufacturing (IJIDeM), v. 15, n. 2, p. 365-380, 2021.

Hossain, A., & Schuckers, S. (2025, May). Fusion of Face and Ear Biometrics for Robust Child Recognition: Insights into Age-Dependent Recognition Trends. In 2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG) (pp. 1-8). IEEE

HOO, S. C., & IBRAHIM, H. (2019). Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements. Journal of Sensors, 2019(1), 7410478.

INFORMATION COMMISSIONER'S OFFICE – ICO, ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted, 2022. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 01 ago. 2024.

INTERNETLAB, Tutela antidiscriminatória na Lei Geral de Proteção de Dados: problemáticas e alternativas, 2021. Disponível em: https://revista.internetlab.org.br/tutela-antidiscriminatoria-na-lei-geral-de-protecao-de-dados-problematicas-e-alternativas/. Acesso em: 01 ago. 2024.

LEATON GRAY, S. H. (2017). Biometrics in schools: The role of authentic and inauthentic social transactions.

LEATON GRAY, S. (2018). Biometrics in schools. In The Palgrave international handbook of school discipline, surveillance, and social control (pp. 405-424). Cham: Springer International Publishing.

LIANG, Yunji et al. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal, v. 7, n. 9, p. 9128-9143, 2020.

MEAD, E. L., & PARKS, R. F. Privacy and Security Implications of Biometrics in Schools: Should Parents be Concerned?. Proceedings of 2014 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop

MOBILIO, Giuseppe. When the kids aren't alright: the use of facial recognition technologies at school. In: Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. The Hague: TMC Asser Press, 2024. p. 41-63.

MOOLLA, Yaseen et al. Biometric recognition of infants using fingerprint, iris, and ear biometrics. IEEE access, v. 9, p. 38269-38286, 2021.

NECOCHEA-CHAMORRO, J. I., Sotelo Asalde, C. M., Loli Nuñez, M. E., & del Rosario Vasquez Valencia, Y. (2024). Systematic Literature Review: Biometric Technology Applied to Educational Institutions. TEM Journal, 13(1).

NIC.BR – Núcleo de Informação e Coordenação do Ponto BR. Educação em um cenário de plataformização e de economia de dados: soberania e infraestrutura. São Paulo: CGI.br, 2023. Disponível em: https://nic.br. Acesso em: 10 ago. 2025.

QUEIROZ, Guilherme Matheus. A inteligência artificial e o reconhecimento facial: impactos à população negra no Brasil. 2023. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, São Paulo, 2023.

ROUNDTRREE, Aimee. *Testing Facial Recognition Software for Young Adults and Adolescents: An Integrative Review*. 2021. Disponível em: https://dl.acm.org/doi/abs/10.1007/978-3-030-77392-2_4. Acesso em: 31 ago. 2025.

SANTOS, Lucas Gabriel de Matos; COSTA, Arthur Barbosa da; DAVID, Jessica da Silva; PEDRO, Rosa Maria Leite Ribeiro. Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. Psicologia & Sociedade, v. 35, e277141, 2023.

SCHROPP, S. P. (2015). Biometric Data Collection and RFID Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy. NCL Rev., 94, 1068.

SENADO FEDERAL. Com 1,6 milhão de vagas gratuitas, institutos federais são mistura de colégio com universidade. Senado Notícias, 9 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2024/10/com-1-6-milhao-de-vagas-gratuitas-institutos-federais-sao-mistura-de-colegio-com-universidade. Acesso em: 10 ago. 2025

SIMON, Judy et al. Design and Development of Novel Artificial Intelligence Assisted Children's Fingerprint Recognition System using Enhanced Biometrical Strategy. In: 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). IEEE, 2023. p. 1-8.

TAVARES, Clarice; SIMÃO, Bárbara; MARTINS, Fernanda K.; SANTOS, Blenda; ARAÚJO, Anna Martha. Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras. São Paulo: InternetLab, 2023.

TRENTIN, Pedro Henrique de Viveiros. Aplicação de redes neurais convolucionais na extração de minúcias de impressões digitais de recém-nascidos. 2024. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Pato Branco, 2024.

UNCTAD - Conferência das Nações Unidas sobre Comércio e Desenvolvimento (2019). Relatório sobre Economia Digital 2019 – Criação e captura de valor: implicações para os países em desenvolvimento.

UNCTAD - Conferência das Nações Unidas sobre Comércio e Desenvolvimento (2021). Relatório sobre Economia Digital 2021 - Fluxos de dados transfronteiriços e desenvolvimento: para quem os dados fluem. Disponível em: https://unctad.org/publication/digital-economy-report-2021 Acesso em maio de 2024 .

UNICEF. *Childhood in a Digital World*. Florence: UNICEF Office of Research – Innocenti, 2025. Disponível em: https://www.unicef.org/innocenti/reports/childhood-digital-world. Acesso em: 28 ago. 2025.

APÊNDICE I

QUESTIONÁRIO

1 - IDENTIFICAÇÃO DA INSTITUIÇÃO

1) Qual o nome da instituição e quantos campi possuem?

2) Este órgão possui política ou normativo relacionado à privacidade ou proteção de dados aprovado internamente?
3) Este órgão possui política ou normativo relacionado à privacidade ou proteção de dados em construção?
4) Este órgão possui política ou normativo relacionado à Segurança da Informação aprovado internamente?
5) Este órgão possui política ou normativo relacionado à Segurança da Informação em construção?
6) A instituição já nomeou o encarregado pelo tratamento de dados?
7) Existe comitê ou comissão para apoiar o encarregado?

2- IDENTIFICAÇÃO SOBRE O USO DE DADOS BIOMÉTRICOS

1) A instituição utiliza ou pensa em utilizar tecnologia que utiliza biometria / reconhecimento facial para apoiar as atividades escolares?
2) Caso utilizem dados biométricos/ reconhecimento facial, quais finalidades as tecnologias foram adquiridas?(exemplo: registro de presença, acesso a instituição)
3) Antes da compra e implementação da tecnologia mencionada na questão anterior, foi realizada análise de impacto dos riscos ao titular de dados? Se sim, a análise está disponível ao público?

3 - PROCESSO DE CONTRATAÇÃO DA TECNOLOGIA

1) Qual foi o processo de contratação realizado pela instituição para adquirir essas tecnologias, e qual foi o valor total da compra?
2) Qual o nome da empresa contratada e por qual período de tempo?
3) Foram estipuladas cláusulas contratuais sobre as responsabilidades e obrigações relacionadas a LGPD referente ao controlador e operador?
4) Foram observados se a empresa contratada estava adequada a LGPD?

4 - TRATAMENTO DOS DADOS

1) Como é realizada a coleta, armazenamento e uso dos dados das pessoas - em especial, crianças e adolescentes - que utilizam essas tecnologias?
2) Como e com quem é feito o compartilhamento desses dados biométricos?
3) Como é realizado o tratamento de dados após a saída do aluno da instituição de ensino? Eles continuam armazenados ou são descartados? Quais são as hipóteses de exclusão dos dados de um aluno?
4) Há práticas de segurança previstas em relação ao tratamento dos dados colhidos pelo sistema de reconhecimento facial? Se sim, quais?
5) Existe normativo interno que aborda o tratamento dos dados biométricos?
6) Houve questionamento por parte de alguma outra instituição, como Ministério Público, Defensoria Pública, Tribunal de Contas, na implementação do reconhecimento facial nas escolas?