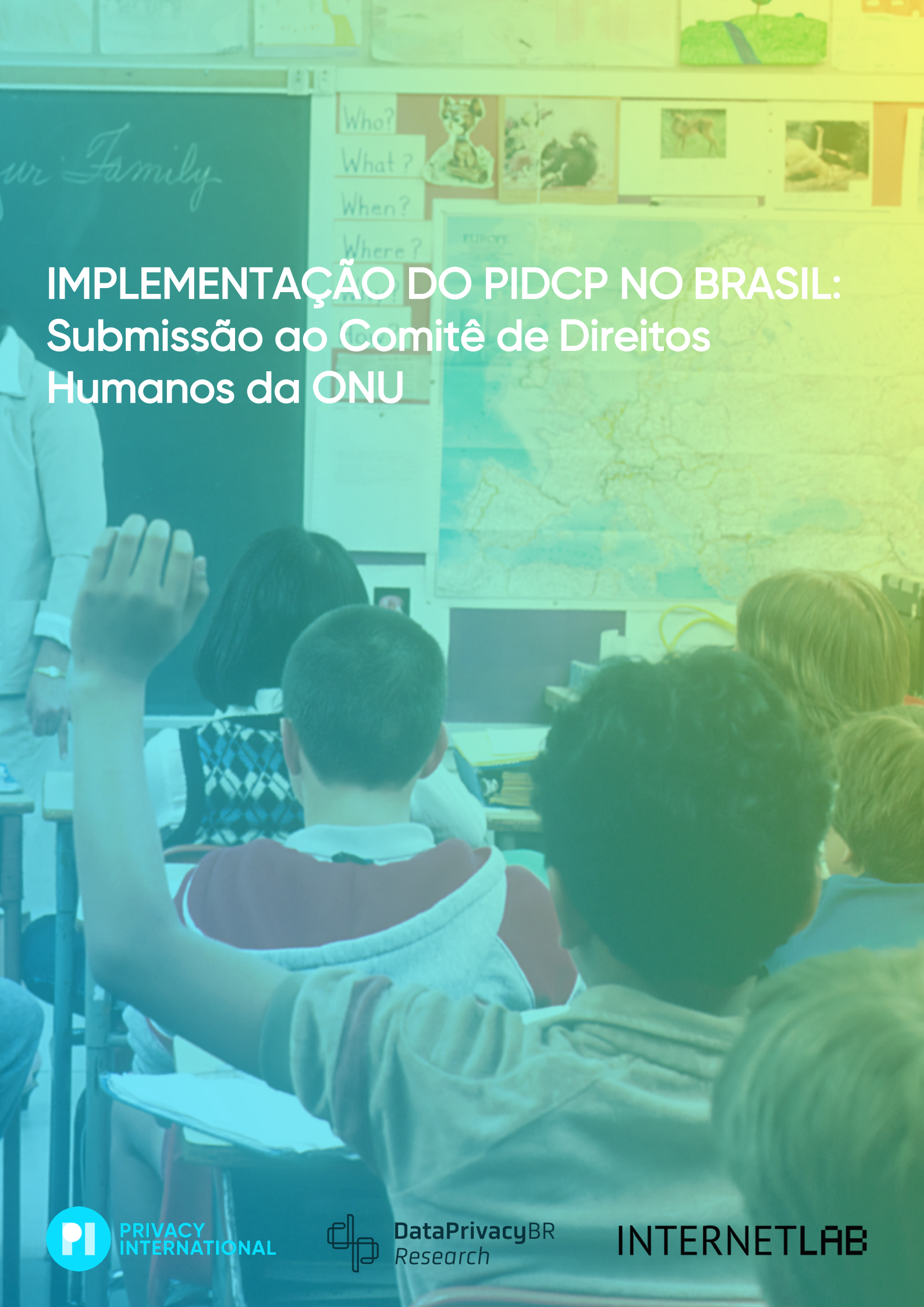

IMPLEMENTAÇÃO DO PIDCP NO BRASIL: Submissão ao Comitê de Direitos Humanos da ONU

PRIVACY INTERNATIONAL
DataPrivacyBR Research
INTERNETLAB

Submissão ao terceiro relatório periódico do Brasil sobre a implementação do Pacto Internacional sobre Direitos Civis e Políticos durante a 138ª sessão do Comitê de Direitos Humanos da ONU

Introdução

Esta submissão conjunta da Privacy International, Associação Data Privacy Brasil de Pesquisa e InternetLab é referente à 138ª Sessão do Comitê de Direitos Humanos da ONU, que ocorrerá entre 26 de junho de 2023 e 28 de julho de 2023, em relação ao cumprimento do Brasil do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP).

A Privacy International (PI) é uma organização internacional não governamental com status consultivo junto ao ECOSOC. A PI pesquisa e atua globalmente contra abusos governamentais e corporativos de dados e tecnologia. Ela expõe danos e abusos, mobiliza aliados globalmente, faz campanhas com o público em busca de soluções e pressiona empresas e governos a mudar. A organização ainda desafia o alcance da vigilância corporativa e do estado para que as pessoas em todos os lugares possam ter maior segurança e liberdade por meio de maior privacidade pessoal.

A Associação Data Privacy Brazil de Pesquisa (DPBR) é uma organização da sociedade civil brasileira sem fins lucrativos que promove a proteção de dados pessoais e outros direitos fundamentais diante do surgimento de novas tecnologias, de desigualdades sociais e de assimetrias de poder. A organização conta com uma equipe multidisciplinar de diferentes regiões brasileiras que desenvolve pesquisas de interesse público, orientações técnicas, textos analíticos sobre temas emergentes e treinamentos com agentes tomadores de decisão e com a sociedade em geral.

O INTERNETLAB (ILab) é um centro de pesquisa independente que visa fomentar o debate acadêmico em torno de questões envolvendo direito e tecnologia, especialmente políticas de internet. O Ilab realiza pesquisas interdisciplinares de impacto e promove o diálogo entre acadêmicos, profissionais e formuladores de políticas. A instituição segue um modelo empresarial sem fins lucrativos, que abrange a busca por produzir pesquisas acadêmicas na forma e no espírito de um think tank acadêmico. Como um nexo de especialização em tecnologia, políticas públicas e ciências sociais, a agenda de pesquisa do ILab abrange

uma ampla gama de tópicos, incluindo privacidade, liberdade de expressão, gênero e tecnologia.

Esta submissão conjunta foca em nossas preocupações em relação ao uso de tecnologias educacionais (EdTech) no Brasil e suas implicações no direito à privacidade sob o Artigo 17 do PIDCP. Considerando isso, a submissão discute o uso de tecnologias de reconhecimento facial em ambientes educacionais, questões de aquisição pertencentes à EdTech, preocupações com inteligência artificial (IA) e falhas regulatórias gerais no Brasil. Também abordamos especificamente as alegações de que sites e aplicativos de tecnologia educacional, que foram endossados e usados pelas autoridades educacionais de Minas Gerais e São Paulo, coletaram e venderam dados coletados no contexto de atividades educacionais online fornecidas a crianças durante a pandemia do COVID-19 levantadas no parágrafo 23 da Lista de Questões.[1]

Recomendações

À luz das informações e análises contidas nas seções abaixo, recomendamos que o Comitê de Direitos Humanos convoque o Brasil a:

- Aderir aos seus padrões internacionais e nacionais de direitos humanos para defender o direito à privacidade e os direitos da criança relativos à EdTech;
- Proibir o uso de tecnologia de reconhecimento facial (TRF) em ambientes educacionais devido à sua desproporcionalidade, riscos de segurança, imprecisões e preconceitos discriminatórios e ilegalidade do processamento de dados biométricos de crianças;
- Proibir o perfilamento e o direcionamento de crianças para fins publicitários usando plataformas EdTech em sala de aula;
- Implementar salvaguardas para evitar a exploração de dados por plataformas e empresas EdTech para garantir a minimização de dados, retenção e exclusão apropriadas de dados de acordo com a lei de proteção de dados do Brasil [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018]);

[1] Comitê de Direitos Humanos, 'List of issues in relation to the third periodic report of Brazil', CCPR/C/BRA/Q/3, 25 de agosto de 2022, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FBRA%2 FQ%2F3&Lang=en, parágrafo 23.

- Certifique-se de que processos robustos de devida diligência em direitos humanos (incluindo de proteção de dados e avaliações de impactos nos direitos da criança) estejam em vigor, que incluam em seu escopo os estágios iniciais de design e desenvolvimento de uma tecnologia EdTech, bem como os estágios de implantação e uso. Os detalhes dos processos em vigor devem ser tornados públicos e disponíveis para revisão;
- Garantir que a EdTech que usa IA seja regulamentada para reduzir os danos associados à IA, inclusive tornando seus algoritmos transparentes e permitindo que os sistemas sejam auditáveis;
- Cumprir os processos formais de aquisição pública ao conceder um contrato a uma empresa EdTech e estabelecer a documentação formal que rege a parceria;
- Capacitar educadores e gestores públicos em legislação de proteção de dados e proteção digital de crianças e adolescentes – incluindo cursos de capacitação continuada para aprimorar o letramento digital dos gestores e capacitá-los para avaliar o uso das tecnologias digitais além da usabilidade;
- Garantir que o uso da EdTech seja regulamentado de acordo com a estrutura de proteção de dados do Brasil [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018] e que a Autoridade de Proteção de Dados regule o uso de dados de crianças de acordo com a LGPD;

Tecnologias Educacionais (EdTech) e sua ascensão no Brasil

EdTech descreve tecnologia ou software que pode ser usado em ambientes educacionais que envolvem o processamento eletrônico de dados de usuários, em particular dados de crianças.[2] Isso inclui software usado para gerenciamento de comportamento, para fins de administração educacional e software usado para auxiliar no ensino de aulas e em materiais educacionais.[3] Também inclui o uso da tecnologia de reconhecimento facial (TRF), que está sendo cada vez mais implementada em ambientes educacionais, como escolas.

O uso de EdTech no Brasil vem se expandindo rapidamente no âmbito do Plano Nacional de Educação (PNE) do Brasil, que incluiu várias metas para incentivar tecnologias a fornecer

[2] Privacy International, 'EdTech Needs Schooling',
https://privacyinternational.org/campaigns/edtech-needsschooling
[3] Ibid.

equipamentos e recursos digitais às escolas e digitalizar a gestão das escolas públicas e das secretarias da educação nos estados, distritos federais e municípios.[4]

Além disso, em resposta à pandemia de Covid-19, com a necessidade de aprendizado remoto e salas de aula virtuais, o uso da EdTech acelerou ainda mais. Antes da pandemia, apenas 21% das escolas no Brasil ofereciam atividades de ensino à distância subindo para 51% em 2020.[5] Ao final de 2020, 45% das escolas públicas e 76% das escolas particulares no Brasil já tinham sistemas de ensino à distância implantados.[6] Desde então, municípios de todo o Brasil estão cada vez mais interessados em adquirir tecnologias para fins educacionais, como ferramentas virtuais de aprendizagem e robótica educacional.[7]

As escolas no Brasil também estão usando cada vez mais sistemas digitais para organizar as informações dos alunos para fins administrativos. Segundo pesquisa, 85% das escolas utilizam sistemas digitais para gerenciar informações associadas ao cadastro do aluno, como nome, endereço, telefone e data de nascimento; 82% das escolas utilizam sistemas digitais para gerenciar os dados de frequência e notas dos alunos; 46% das escolas usam sistemas digitais para gerenciar dados sobre condição física e saúde dos alunos, como peso, altura e alergias; 59% das escolas usam sistemas digitais para gerenciar os resultados da avaliação de desempenho de professores e funcionários e; 71% das escolas usam sistemas digitais para gerenciar dados sobre o orçamento da escola.[8]

Essas são tecnologias extremamente intensivas em dados que dependem da coleta, análise, retenção e processamento de dados de crianças, suas famílias e professores. Quando estão envolvidos dados de crianças ou dados altamente confidenciais, por exemplo, dados biométricos, são necessárias proteções adicionais. No entanto, estamos vendo falhas na estrutura regulatória do estado que rege os dados pertencentes à EdTech, resultando em violações ao Artigo 17 do PIDCP.

---

[4] Plano Nacional de Educação (PNE), 2014, https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13005.htm

[5] Centro Regional para o Desenvolvimento da Sociedade da Informação (Cetic.br)., TIC Educação 2019, Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nas Escolas Brasileiras 12,https://cetic.br/media/docs/publicacoes/2/20201123090444/tic_edu_2019_livro_eletronico.pdf, pg 25.

[6] Ibid.

[7] Open Knowledge Brasil, Querido Diário (2023): Panorama #1: Radar das tecnologias na educação nos municípios, https://queridodiario.ok.org.br/educacao/relatorio/1

[8] Centro Regional para o Desenvolvimento da Sociedade da Informação (Cetic.br), TIC Educação 2020 - Edição COVID-19 metodologia adaptada. Coletiva de Imprensa [Slides], 31 de agosto de 2021, https://cetic.br/media/analises/tic_educacao_2020_coletiva_imprensa.pdf

Além disso, o envolvimento de atores não estatais com os dados do usuário, neste caso, o envolvimento de empresas privadas, também interfere na privacidade do indivíduo de acordo com o Artigo 17 do PIDCP. Por exemplo, a aquisição não está de acordo com os padrões de direitos humanos e estamos vendo acesso irrestrito aos dados individuais para fins além da educação, para atender a seus interesses econômicos.

O uso de tecnologias de reconhecimento facial em ambientes educacionais

O uso do TRF em ambientes educacionais tem sido implantado nas escolas públicas brasileiras, com iniciativas em diferentes regiões do país. O INTERNETLAB (ILab) realizou uma pesquisa para identificar como as escolas públicas brasileiras adotam políticas de reconhecimento facial, mapeando o grau de expansão, formas de uso e prática comum.[9] 9 Quinze casos foram identificados em diferentes regiões do país.[10] A pesquisa explorou semelhanças e diferenças entre esses casos, incluindo a análise de se as políticas estavam em vigor; se foram realizadas avaliações de impacto; se houve participação da sociedade civil; como o reconhecimento facial estava sendo usado; o processo de aquisição de empresas; e práticas de proteção de dados.

Achados de pesquisa

Em relação à implementação do TRF em ambientes educacionais, as autoridades locais alegaram que o propósito era otimizar a gestão escolar, incluindo o combate à evasão escolar, e a segurança.

Eles argumentam que o uso do reconhecimento facial economiza tempo da equipe ao automatizar tarefas como gerenciamento de ausências, rastreamento do número de alimentos e suprimentos necessários nas salas de aula. Os servidores públicos também afirmam que o reconhecimento facial pode impedir a adulteração de registros de frequência, possibilitar denúncias ao Conselho Tutelar sobre os alunos e facilitar a gestão de políticas de

[9] Internet Lab, 'Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras", 2023, https://internetlab.org.br/pt/noticias/em-novo-relatorio-internetlab-mapeia-o-uso-de-reconhecimento-facial-em-escolas-publicas-brasileiras/

[10] (i) Tocantins (TO); (ii) Mata de São João (BA); (iii) Fortaleza (CE); (iv) Jaboatão dos Guararapes (PE); (v) Águas Lindas (GO); (vi) Goiânia (GO); (vii) Morrinhos (GO); (viii) Betim (MG); (ix) Rio de Janeiro (RJ); (x) Angra dos Reis (RJ); (xi) Itanhaém (SP); (xii) Potirendaba (SP); (xiii) Santos (SP); (xiv) Porto Alegre (RS); (xv) Xaxim (SC).

proteção social como o Bolsa Família (Programa Bolsa Família) com base na frequência. A implementação do reconhecimento facial também está sendo usada para impedir que indivíduos não autorizados entrem, protejendoa propriedade escolar.[11]

Em quatorze dos quinze estados brasileiros, a TRF foi implementada por autoridades públicas em nível municipal por meio de contratos públicos assinados com empresas nacionais que oferecem serviços de tecnologia. Na maioria dos casos identificados, a implantação da tecnologia ainda está em fase inicial de testes, não abrangendo toda a rede municipal ou estadual de ensino.[12]

A TRF está totalmente implantado em três municípios: Betim, Jaboatão dos Guararapes e Goiânia. Em outros três casos (Xaxim, Morrinhos e Tocantins), a tecnologia ainda está em fase inicial de testes e não abrange toda a rede municipal ou estadual de ensino. Infelizmente, não há informações suficientes disponíveis sobre o grau de implantação das políticas de reconhecimento facial nos municípios de Angra dos Reis (RJ), Águas Lindas (GO), Itanhaém (SP) e Mata de São João (BA).[13]

Nos três municípios implantados, todas as 69 unidades de ensino fundamental da cidade contam com a TRF. Em Goiânia, o sistema de reconhecimento facial já está em pleno uso nas unidades educacionais municipais, mas ainda são necessários ajustes técnicos para integrar o sistema de reconhecimento facial ao sistema de gestão escolar. Segundo a Secretaria Municipal de Educação e a Agência de Inovação e Tecnologia Educacional, 336 unidades escolares contam com infraestrutura e acesso ao sistema de gestão escolar de reconhecimento facial. Em Jaboatão dos Guararapes, 125 escolas municipais de ensino fundamental (1º ao 9º ano) já possuem sistemas de biometria facial.[14]

O ILab constatou que nenhum município ou estado relatou a realização de estudos de avaliação de impacto sobre os direitos humanos ou a análise de riscos potenciais de discriminação associados ao software de reconhecimento facial antes da implementação dos projetos. Alguns municípios que avançaram na implantação do reconhecimento facial

[11] Internet Lab, 'Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras", 2023, https://internetlab.org.br/pt/noticias/em-novo-relatorio-internetlab-mapeia-o-uso-de-reconhecimento-facial-em-escolas-publicas-brasileiras/
[12] Ibid.
[13] Ibid.
[14] Ibid.

afirmam que a tecnologia tem alto índice de acerto. No entanto, um município destacou casos em que o sistema registrava incorretamente a frequência de um aluno.[15]

Enquanto os administradores públicos afirmam que a implementação do reconhecimento facial foi impulsionada por demandas da comunidade educacional, apenas dois municípios (Itanhaém e Jaboatão dos Guararapes) indicaram algum nível de participação da sociedade civil no desenvolvimento do projeto.[16]

Em relação às práticas de proteção de dados, observou-se que o equipamento coletava dados biométricos dos alunos, armazenava-os no banco de dados do sistema e os utilizava para registro de frequência. O tratamento dos dados na saída dos alunos das instituições de ensino varia entre os municípios: em alguns casos, os dados permanecem armazenados na Secretaria de Educação, enquanto em outros, os dados biométricos são retirados do banco de dados. Como um dos propósitos declarados do reconhecimento facial é prevenir o abandono escolar, os dados são compartilhados, em alguns casos, com o Conselho Tutelar, quando o frequente afastamento do aluno da escola se torna uma preocupação. As autoridades públicas também mencionaram o compartilhamento de dados entre gestores educacionais e com a administração pública para aprimorar a execução de políticas públicas voltadas para a educação.[17]

Implicações para os Direitos Humanos

Acreditamos que o uso da tecnologia de reconhecimento facial em ambientes educacionais no Brasil viola o Artigo 17 do PIDCP. O uso do TRF em ambientes educacionais destina-se a enfrentar os desafios existentes, como salas de aula superlotadas, fundos insuficientes para merenda escolar, evasão escolar e violência. No entanto, usar o TRF para abordar essas questões levanta questões importantes sobre proporcionalidade e necessidade de invasão de privacidade de acordo com o Artigo 17 do PIDCP. Medidas menos invasivas de privacidade poderiam claramente ser adotadas para enfrentar esses desafios sem processar os dados biométricos altamente sensíveis de crianças e adolescentes.

[15] Ibid.
[16] Ibid.
[17] Ibid.

O Comitê dos Direitos da Criança em seu Comentário Geral nº 25 observou especificamente que "qualquer vigilância digital de crianças, juntamente com qualquer processamento automatizado associado de dados pessoais, deve respeitar o direito da criança à privacidade e não deve ser realizada rotineiramente, indiscriminadamente ou sem o conhecimento da criança ou, no caso de crianças muito pequenas, de seus pais ou responsáveis; nem deve ocorrer sem o direito de se opor a tal vigilância, em ambientes comerciais e ambientes educacionais e de assistência, e deve-se sempre levar em consideração os meios menos intrusivos à privacidade disponíveis para cumprir a finalidade desejada".[18]

Além disso, existe potencial para vieses discriminatórios nos sistemas de reconhecimento facial, principalmente em relação a grupos marginalizados. Numerosos estudos destacaram como essas tecnologias são menos precisas quando se trata de indivíduos não-homens ou não-brancos, pois muitas vezes são treinadas em conjuntos de dados sem diversidade de gênero, representação racial e registros culturais.[19] Além das preocupações com a precisão, há outras questões a serem consideradas, como incidentes de segurança que podem levar a acesso não autorizado, roubo, perda ou uso indevido dos dados armazenados que podem levar a violações do Artigo 17 do PIDCP.

Além disso, algumas escolas divulgaram que os dados coletados pelos processos do FRT poderiam ser compartilhados com outras instituições públicas, por exemplo, com o Conselho Tutelar, para questões relacionadas à evasão escolar. Representantes da sociedade civil no Brasil expressaram preocupação sobre a eficácia do reconhecimento facial para enfrentar esses desafios enfrentados pelas escolas públicas brasileiras. As causas de problemas como salas de aula superlotadas estão profundamente enraizadas em questões estruturais do sistema educacional brasileiro, que não podem ser facilmente resolvidas apenas com a tecnologia. O mesmo se aplica à evasão escolar, questão complexa influenciada por fatores como falta de transporte público, violência contra crianças e adolescentes, trabalho infantil e pobreza. Portanto, o uso do TRF não é uma medida proporcional e razoável para lidar com essas questões.

[18] Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', CRC/C/GC/25, 2 de março de 2021, https://www.ohchr.org/en/documents/general-comments-andrecommendations/general-comment-no-25-2021-childrens-rights-relation

[19] Privacy International, 'Facial Recogniton'. https://privacyinternational.org/learn/facial-recognition

Atualmente, não há legislação específica no Brasil, em nível federal, estadual ou municipal, que regule especificamente o uso de tecnologias de reconhecimento facial ou biométrico, particularmente no campo da educação.[20] No nível local, as leis orçamentárias alocam recursos para o setor educacional, mas não há programas ou ações específicas relacionadas ao desenvolvimento, aquisição e manutenção de tecnologias de reconhecimento facial nas escolas. O município de Mata de São João (BA) é a única exceção, pois estabeleceu diretrizes por meio de leis municipais que disciplinam o tratamento de dados pessoais (Decreto Municipal nº 162, de 1º de abril de 2022) e a segurança das informações municipais (Decreto Municipal Política de Segurança da Informação). No entanto, é importante observar que, assim como outras localidades, Mata de São João não forneceu informações sobre a realização de estudos de risco antes ou durante a implementação e uso da tecnologia de reconhecimento facial.

Recomendamos que o Comitê de Direitos Humanos convoque o Brasil a:

• Proibir o uso de tecnologia de reconhecimento facial (TRF) em ambientes educacionais devido à sua desproporcionalidade, riscos de segurança, imprecisões e preconceitos discriminatórios e ilegalidade de processamento de dados biométricos de crianças.

Alegações de que sites e aplicativos de tecnologia educacional, que foram endossados e utilizados pelas autoridades educacionais de Minas Gerais e São Paulo, colheram e venderam dados coletados no contexto de atividades educacionais on-line fornecidas a crianças durante a pandemia da COVID-19.[21]

Em maio de 2022, uma pesquisa realizada pela Human Rights Watch (HRW) descobriu que sete sites educacionais no Brasil estavam extraindo e compartilhando dados infantis com empresas terceirizadas usando tecnologias de rastreamento projetadas para publicidade.[22]

[20] Internet Lab, 'Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras", 2023, https://internetlab.org.br/pt/noticias/em-novo-relatorio-internetlab-mapeia-o-uso-de-reconhecimento-facial-em-escolas-publicas-brasileiras/

[21] Human Rights Committee, 'List of issues in relation to the third periodic report of Brazil', CCPR/C/BRA/Q/3, 25 de agosto de 2022, parágrafo 23, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FBRA%2 FQ%2F3&Lang=en

[22] Human Rights Watch, 'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic', 25 de maio de 2022,

Os sites rastreiam a localização física e as atividades dos usuários fora do site, além de ter acesso à lista de contatos telefônicos do aluno e poder baixar dados pessoais de familiares e amigos. Os sites incluíam Estude em Casa, Centro de Mídias da Educação de São Paulo, Descomplica, Escola Mais, Explicaê, MangaHigh e Stoodi. Um oitavo site, o Revisa Enem, também enviou os dados das crianças para uma empresa terceirizada, sem usar rastreadores específicos de anúncios.

O relatório constatou que sete sites brasileiros recomendados para ensino remoto durante a pandemia por São Paulo e Minas Gerais (os dois estados mais populosos do país): (i) realizaram vigilância das atividades online dos alunos além do uso pretendido da plataforma ; que (ii) nenhum desses sites permitia que os usuários recusassem o rastreamento; e (iii) os dados coletados não eram transparentes para crianças e adolescentes, o que levou a uma violação do Artigo 17 do PIDCP.

Em resposta às descobertas, algumas empresas observaram que seus produtos recomendados pelo governo foram projetados para uso de professores, pais e outros adultos, e não para uso de crianças. Isso sugere que as devidas diligências e avaliações de impacto sobre os direitos humanos não foram realizadas pelas autoridades brasileiras. Antes da publicação do relatório, a Escola Mais não respondeu aos pedidos de comentários e somente após reportagens da mídia a empresa removeu de seu site todos os links direcionados aos alunos para sua plataforma de aprendizado online.[23]

Além disso, em resposta a essas descobertas, a secretaria de educação de Minas Gerais removeu todo o rastreamento de anúncios de seus sites.[24] No entanto, a Secretaria de Educação de São Paulo continua endossando o uso de sites educacionais que coletam dados infantis de forma inadequada e não respondem às perguntas dos HRW. Isso mostra que a Lei Geral de Proteção de Dados Pessoais nacional não fornece proteções suficientes para crianças que usam EdTech e destaca a falta de consideração dos padrões de direitos humanos dos quais o Brasil é signatário.

---

https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violationsgovernments

[23] Human Rights Watch, 'Brazilian Company Moves to Shield Students from Data Surveillance', 4 de abril de 2023, https://www.hrw.org/news/2023/04/04/brazilian-company-moves-shield-students-data-surveillance

[24] Human Rights Watch, 'Brazil: Online Learning Tools Harvest Children's Data, One State Government Removes Ad Tracking, But Others Continue', 3 de abril de 2023, https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data

A Privacy International realizou uma análise técnica dos métodos de pesquisa utilizados pela HRW, incluindo os tipos de análise (estática e dinâmica) que foram realizadas nas plataformas para entender as conclusões que foram tiradas e a extensão dos danos. A PI conduziu anteriormente tipos semelhantes de análise em vários sites e aplicativos para descobrir que as empresas estavam contando com alguma forma de rastreamento em seus serviços.[25]

Uma análise estática de aplicativos usando ferramentas como Exodus Privacy pode fornecer vários insights sobre as práticas de privacidade e segurança de aplicativos, como a coleta de dados confidenciais do usuário; uma lista de terceiros com quem os dados são compartilhados; vulnerabilidades no código do aplicativo e as permissões que o aplicativo solicita no dispositivo do proprietário. Ele analisa o código de um aplicativo e identifica seus recursos e quais funções ou instruções podem ser executadas quando o aplicativo está em execução. Essa análise é realizada sem a necessidade de interação do usuário e é principalmente uma ferramenta útil para ajudar os usuários a tomar decisões informadas sobre o que podem esperar de um aplicativo sem precisar interagir com ele. Quanto mais permissões forem solicitadas de um aplicativo e quanto mais rastreadores ele usar, maior será o risco à privacidade.

Uma análise dinâmica do tráfego de um aplicativo permite que a pessoa que conduz a pesquisa veja todas as trocas de dados sendo feitas dentro do aplicativo em condições realistas. Isso significa que é possível ver quais dados estão saindo do dispositivo analisado e com quem estão sendo compartilhados. Este método fornece informações sobre o que está acontecendo com os dados dentro dos aplicativos, o que é extremamente útil para complementar e cruzar uma análise estática (mais ampla e descontextualizada).

Uma análise estática de sites usando o Blacklight fornece uma visão instantânea dos recursos de um site em relação a sete tipos amplamente documentados de tecnologias de rastreamento: impressão digital de tela, cookies, Meta (anteriormente Facebook), eventos de pixel, registro de chave, rastreadores de terceiros e gravadores de sessão.

[25] A esse respeito, ver Privacy International, "Taking a depression test online? Go ahead, they're listening", 2019, https://www.privacyinternational.org/news-analysis/3188/taking-depression-test-online-go-ahead-theyrelistening; Privacy International, "An unhealthy diet of targeted ads: an investigation into how the diet industry exploits our data", 2021, https://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-adsinvestigation-how-diet-industry-exploits-our-data

O ecossistema Adtech (Advertising Technology) depende de uma rede complexa de corretores de dados, redes de anúncios e outros intermediários, geralmente sem conexão direta e explícita com os aplicativos ou sites onde estão presentes. A inerente opacidade deste ecossistema torna extremamente difícil entender e controlar quais dados estão sendo coletados, como estão sendo processados/usados, por quem e com quem os dados estão sendo compartilhados, interferindo novamente no direito à privacidade.

Na submissão da PI à 41ª sessão da Revisão Periódica Universal do Brasil, destacamos outros exemplos de plataformas e empresas EdTech que estavam coletando e processando dados do usuário causando interferências significativas no Artigo 17 do PIDCP.[26] Esses exemplos incluem IP.TV [27] (empresa responsável pela criação de aplicativos móveis EdTech no Brasil usados nos estados do Amazonas, Paraná, Pará e São Paulo) e Google Workspace (uma ferramenta colaborativa para professores e alunos foi amplamente implementada em todo o sistema educacional brasileiro em escolas de todos os estados e do Distrito Federal).[28]

O Comentário Geral nº 16 sobre o Artigo 17 do PIDCP afirma especificamente que "todo indivíduo também deve ser capaz de determinar quais autoridades públicas ou indivíduos ou órgãos privados controlam ou podem controlar seus arquivos. Se tais ficheiros contiverem dados pessoais incorretos ou tiverem sido recolhidos ou tratados em desacordo com o disposto na lei, todos os indivíduos devem ter o direito de solicitar a sua retificação ou eliminação".[29]

---

[26] Privacy International, 'The Right to Privacy in Brazilian Schools: Universal Periodic Review', https://privacyinternational.org/advocacy/4982/right-privacy-brazilian-schools-universal-periodic-review

[27] Amanda Audi / Pedro Zambarda, 'Aulas online obrigam milhões de alunos a usar app de empresa obscura que criou TV Bolsonaro', The Intercept Brasil, 15 de junho de 2020, https://theintercept.com/2020/06/15/app-empresa-tvbolsonaro-aulas-online-pandemia/

[28] Secretaria de Estado de Educação do Amazonas (SEDUC), 'Professores e alunos da rede estadual podem ativar e-mail institucional para ajudar no ensino remoto', 22 de fevereiro de 2021, http://www.educacao.am.gov.br/gestores-professores-e-alunos-da-rede-estadual-podem-ativar-e-mailinstitucional-para-ajudar-no-ensino-remoto/; Pedido pela Lei de Acesso à Informação, Protocolo nº 00080000386202140, Governo do Estado do Maranhão, 21 de outubro de 2017, Parceria entre Governo e Google Brasil disponibiliza 13 mil vagas para revisão do Enem a estudantes da rede pública. Ouça: https://www.ma.gov.br/agenciadenoticias/?p=202953; SEI Processo nº 030029/002262/2020.

[29] UN Human Rights Committee, 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', 8 de abril de 1988, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FGEC %2F6624&Lang=en, parágrafo 10.

Quando dados pessoais forem processados por uma plataforma EdTech, deve haver transparência em relação às atividades de processamento de dados e salvaguardas sobre como esses dados são usados, incluindo por quanto tempo os dados serão retidos e o que será feito com os dados dos usuários quando a parceria termina.

Isso não apenas interfere no Artigo 17 do ICCPR, mas também interfere em outros direitos, incluindo os direitos contidos na Convenção sobre os Direitos da Criança. O Comitê dos Direitos da Criança da ONU em seu Comentário Geral 25 recomendou que os Estados-partes deveriam "proibir por lei a criação de perfis ou o direcionamento de crianças de qualquer idade para fins comerciais com base em um registro digital de suas características reais ou inferidas, incluindo grupo ou dados coletivos, direcionados por associações ou perfis de afinidade".[30] Também estabelece que "as normas para tecnologias educacionais digitais devem garantir que o uso dessas tecnologias seja ético e adequado para fins educacionais e não exponha as crianças (..) ao uso indevido de seus dados pessoais, exploração comercial ou outras violações de seus direitos, como o uso de tecnologias digitais para documentar a atividade de uma criança".[31]

No geral, nossa análise nos permite apoiar as alegações apresentadas no relatório HRW, que sites e aplicativos de tecnologia educacional, endossados e usados pelas autoridades educacionais de Minas Gerais e São Paulo, e a maioria das plataformas mencionadas eram cúmplices em facilitar alguma forma de rastreamento do aluno, seja intencional ou não.

Recomendamos que o Comitê de Direitos Humanos da ONU convoque o Brasil a:

- Proíbam a criação de perfis e o direcionamento de crianças para fins publicitários usando plataformas EdTech em sala de aula.
- Implemente salvaguardas para evitar a exploração de dados por plataformas e empresas EdTech para garantir a minimização, retenção e exclusão apropriadas de dados de acordo com a lei de proteção de dados do Brasil [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018.

[30] Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', CRC/C/GC/25, 2 de março de 2021, parágrafo 42, https://www.ohchr.org/en/documents/generalcomments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[31] Ibid. Parágrafo 103.

- Certifique-se de que processos robustos de devida diligência em direitos humanos (incluindo proteção de dados e avaliações de impactos nos direitos da criança)[32] estejam em vigor, que incluam em seu escopo os estágios iniciais do projeto e desenvolvimento de uma tecnologia EdTech, bem como os estágios de implantação e uso. Detalhes dos processos em vigor devem ser tornados públicos e disponíveis para revisão.

Inteligência Artificial (IA) em EdTech e ambientes educacionais

A EdTech no Brasil também pode usar inteligência artificial que apresenta riscos adicionais aos direitos humanos.[33] As plataformas EdTech podem usar IA para recomendar aos alunos conteúdo educacional com base em resultados de testes com a intenção de agilizar o aprendizado, bem como software que usa IA para corrigir autonomamente os erros de ensaios dos alunos. A IA também pode ser usada de forma mais geral em ambientes educacionais, por exemplo, dentro do recente programa de segurança que está sendo testado no estado do Paraná, que busca usar a IA para aumentar a segurança nas escolas. A tecnologia de IA será usada para analisar imagens de câmeras de segurança em busca de "comportamento incomum" e, em seguida, comunicar isso às autoridades.[34] Existe um risco real de que o uso de novas ferramentas de IA em ambientes educacionais sem as devidas proteções tenha um impacto negativo sobre direitos humanos, incluindo o direito à privacidade.

Além dos riscos à privacidade dos usuários discutidos acima, por meio do rastreamento, geração e processamento de dados, também há riscos de discriminação por meio de imprecisões e vieses sobre os quais os algoritmos de IA são construídos. Os sistemas de IA

[32] Human Rights Council, 'Report of the Special Rapporteur on the right to education on the impact of the digitalization of education on the right to education,', A/HRC/50/32, 19 de abril de 2022, https://www.ohchr.org/en/documents/thematic-reports/ahrc5032-impact-digitalization-education-righteducation

[33] Privacy International, 'Artificial Intelligence', https://privacyinternational.org/learn/artificial-intelligence

[34] Ver Celepar, "Com inteligência artificial, Celepar torna escolas do Paraná mais seguras", 27 de março de 2023, https://www.celepar.pr.gov.br/Noticia/Com-inteligencia-artificial-Celepar-torna-escolas-do-Parana-maisseguras#:~:text=Com%20intelig%C3%AAncia%20artificial%2C%20Celepar%20torna%20escolas%20do%20Paran% C3%A1%20mais%20seguras,-A%C3%A7%C3%A3o%20integra%20Programa&text=A%20seguran%C3%A7a%20em%20escolas%2C%20no,solu%C 3%A7%C3%A3o%20para%20as%20institui%C3%A7%C3%B5es%20escolares

podem, portanto, exacerbar as desigualdades existentes e causar mais danos a indivíduos em posições vulneráveis. Por exemplo, quando a IA é usada em ambientes educacionais no Brasil, existe o perigo de perpetuar as desigualdades e discriminações existentes, como aquelas ligadas ao menor nível educacional associado a uma maior desigualdade de renda, que é um problema persistente no Brasil.[35] Os riscos da IA quando usados em crianças também são agravados devido ao seu estágio de desenvolvimento físico, psicológico, social e emocional.

A EdTech que usa algoritmos e outros processos de tomada de decisão deve estar aberta ao escrutínio e a contestação por meio de auditoria. A capacidade de auditar tecnologias é essencial para fornecer supervisão e reparação adequadas. Por exemplo, se uma tecnologia levou a um resultado que posteriormente é questionado em tribunal ou usado como prova, a administração adequada da justiça exige que a tecnologia seja totalmente auditável.[36] O projeto atual da Associação Brasileira Data Privacy de Pesquisa (DPBR) 'IA na sala de aula: modelos de participação para a comunidade escolar' explora o emprego de tecnologias que utilizam IA para fins educacionais e tem por objetivo propor um modelo participativo de auditoria de IA em ambientes educacionais que envolva toda a comunidade escolar, principalmente alunos, suas famílias e educadores.[37]

Um marco legal para regulamentar a IA foi recentemente introduzido pela Câmara dos Deputados Brasileira por meio do Projeto de Lei de Inteligência Artificial. No entanto, o projeto de lei recebeu feedback negativo e foi considerado por alguns como um "projeto de lei de desregulamentação" em vez de uma estrutura legal.[38] Em resposta às preocupações, foi estabelecido um grupo de trabalho do Senado formado por um grupo de especialistas jurídicos, membros da academia, empresas e o órgão nacional de proteção de dados do

[35] Committee on the Rights of the Child examines report of Brazil, 22 de stembro de 2015, https://www.ohchr.org/en/press-releases/2015/09/committee-rights-child-examines-report-brazil
[36] Privacy International, 'Safeguard for Public-Private Surveillance Partnerships', Dezembro de 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf
[37] Data Privacy Brasil, "AI in the classroom: models of participation for the school community", https://www.dataprivacybr.org/en/projeto/ai-in-the-classroom-models-of-participation-for-the-schoolcommunity/
[38] Wilson Centre, "AI Regulation Still Lagging in Brazil", 2023, https://www.wilsoncenter.org/blog-post/airegulation-still-lagging-brazil

Brasil.[39] Um processo de consulta pública[40] foi conduzido e foi seguido por um relatório escrito que foi publicado em dezembro de 2022, com recomendações sobre como o Brasil deve regular a IA.[41]41 As recomendações do relatório têm três focos principais: direitos dos cidadãos, a categorização de riscos e a medidas de governança e sanções administrativas que devem ser acionadas quando o regulamento não for cumprido.[42]

Recomendamos que o Comitê de Direitos Humanos da ONU convoque o Brasil a:

• Garantir que a EdTech que usa IA seja regulamentada para reduzir os danos associados à IA, incluindo tornar seus algoritmos transparentes e permitir que os sistemas sejam auditáveis.

Aquisição de EdTech no Brasil

A aquisição de EdTech pelas autoridades brasileiras levanta preocupações significativas que têm implicações para a privacidade do usuário. Pesquisas mostram que durante a pandemia de Covid-19 as escolas escolheram plataformas e recursos para ensino à distância com base no que era mais econômico, o que não garante o melhor interesse da criança ou a proteção dos direitos humanos. Empresas de tecnologia e startups de EdTech têm influenciado o governo local e as escolas a "testar" seus produtos em pequenos municípios.[43]

As plataformas e programas de EdTech no Brasil foram obtidos por meio de acordos de cooperação, licitações ou por meio de doações. Os acordos de cooperação podem ser utilizados no Brasil quando ambas as partes tiverem um interesse comum, que deve estar alinhado ao interesse público e não permite a transferência de recursos. No entanto, as empresas que fornecem plataformas e ferramentas EdTech podem gerar lucro por meio do processamento de dados e, portanto, não exigem pagamento monetário direto para gerar

[39] iapp, "Brazil's AI commission to deliver final report", 2022, https://iapp.org/news/a/brazils-ai-commission-todeliver-final-report/
[40] Privacy International, 'Submission to the Commission of Jurists on the Brazilian Artificial Intelligence Bill', https://privacyinternational.org/advocacy/4984/submission-commission-jurists-brazilian-artificialintelligence-bill
[41] Ver https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4
[42] Ibid.
[43] Ver "Municípios lançam edital para contratar edtechs no ensino público", Folha de S. Paulo, 2 de fevereiro de 2022, https://www1.folha.uol.com.br/empreendedorsocial/2022/02/municipios-lancam-edital-para-contrataredtechs-no-ensino-publico.shtml

lucro. Portanto, neste caso, a transferência de dados deve ser entendida como uma transferência de recursos.[44]

Por exemplo, o Google Classroom foi implementado por meio de uma doação feita pela empresa Empresa Ensinar Tecnologia Educacional LTDA.[45] De acordo com a Secretaria de Educação, o critério utilizado para decidir qual software usar foi que o serviço do Google fosse gratuito.[46]

O Relator Especial da ONU pelo Direito à Educação destacou sobre a mineração de dados de estudantes, famílias e comunidades, bem como educadores e outros funcionários em ambientes educacionais, a privacidade específica da criança e leis de proteção de dados; avaliações de impacto nos direitos da criança antes de adotar tecnologias digitais na educação e due diligence com provedores privados para garantir que a tecnologia recomendada para o aprendizado on-line proteja a privacidade das crianças e os direitos de proteção de dados.[47]

Recomendamos que o Comitê de Direitos Humanos da ONU convoque o Brasil a:

• Aderir aos processos formais de aquisição pública ao conceder um contrato a uma empresa EdTech e estabelecer a documentação formal que rege a parceria.

• Capacitar educadores e gestores públicos em legislação de proteção de dados e proteção digital de crianças e adolescentes – incluindo cursos de capacitação continuada para aprimorar o letramento digital dos gestores e capacitá-los para avaliar o uso das tecnologias digitais além da usabilidade.

[44] É importante destacar que, no plano da defesa do consumidor, o Superior Tribunal de Justiça reconheceu que a relação de consumo existe mesmo quando o serviço prestado é gratuito. Isso porque a remuneração deve ser entendida de forma ampla, de forma a contemplar o ganho indireto do fornecedor. Relator Mín. Nancy Andrighi, Superior Tribunal de Justiça, REsp nº 1.193.764, Diário Oficial Eletrônico, 8 de agosto de 2011.
[45] Privacy International, 'The Right to Privacy in Brazilian Schools: Universal Periodic Review', https://privacyinternational.org/advocacy/4982/right-privacy-brazilian-schools-universal-periodic-review
[46] Pedido de Lei de Acesso à Informação, Protocolo nº 00080000386202140.
[47] Human Rights Council, 'Report of the Special Rapporteur on the right to education on the impact of the digitalization of education on the right to education', A/HRC/50/32, 19 de abril de2022, https://www.ohchr.org/en/documents/thematic-reports/ahrc5032-impact-digitalization-education-righteducation

Falhas legislativas

É evidente que a aquisição da EdTech não é especificamente regulamentada e que os direitos humanos e as normas de proteção de dados não estão sendo respeitados pelo Estado brasileiro. O governo brasileiro e órgãos relevantes, como a Autoridade Nacional de Proteção de Dados, precisam cumprir suas obrigações de defender o direito à privacidade ao usar essas tecnologias.

No plano internacional, o Brasil ratificou diversos tratados internacionais de direitos humanos. A nível nacional, a Constituição da República Federativa do Brasil de 1998 (CF)[48] garante direitos fundamentais, incluindo privacidade e proteção de dados. O Estatuto da Criança e do Adolescente (ECA)[49] (Estatuto da Criança e do Adolescente) de 1990, regulamenta os direitos da criança e do adolescente, o que inclui o direito à privacidade previsto no artigo 17.

A lei de proteção de dados do Brasil, [Lei Geral de Proteção de Dados Pessoais (LGPD) 2018][50] entrou em vigor em 2020 (para disposições gerais) e 2021 (para sanções administrativas). De acordo com o artigo 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado no seu melhor interesse, com consentimento específico e explícito de pelo menos um dos pais ou responsável legal. No Brasil, criança é toda pessoa com menos de 12 anos de idade, enquanto adolescente é toda pessoa entre 12 e 18 anos.[51] Essa distinção é importante na interpretação do artigo 14, § 1º, pois exige que o consentimento seja dado pelos pais ou tutores legais apenas quando os dados das crianças são processados. Este consentimento relativo aos dados das crianças não é exigido quando a recolha de dados é necessária para contactar os pais ou tutores legais, desde que os dados sejam utilizados uma única vez e não armazenados, ou para proteção das crianças. Nesse caso, os dados não devem ser compartilhados com terceiros sem o consentimento dos pais (art. 14, § 3º).

Informações sobre o tipo de dados coletados devem ser divulgadas "de forma simples, clara e acessível" tanto para o entendimento de pais e responsáveis, quanto para o entendimento

[48] Constituição da República Federativa do Brasil de 1988.
[49] Estatuto da Criança e do Adolescente (ECA) 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm
[50] Lei Geral de Proteção de Dados Pessoais (LGPD) 2018, http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm
[51] Artigo 2º, Estatuto da Criança e do Adolescente (ECA) 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

de crianças e adolescentes. A Lei estabelece que os responsáveis pelo tratamento não devem condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais para além do estritamente necessário à atividade (artigo 14.º, n.º 4). Ressalta-se que as diretrizes de implementação ainda deveriam ser publicadas pela Autoridade Nacional de Proteção de Dados, mas sua formulação não constava da agenda regulatória da autoridade para o biênio 2023-2024.

A Política Nacional de Educação Digital, instituída pelo projeto de lei 14.533, foi sancionada em janeiro de 2023 pelo Presidente da República. Como parte dessa política, a educação digital deve ser incluída no currículo escolar, implicando o desenvolvimento de uma visão crítica sobre o uso da tecnologia e a conscientização sobre os direitos digitais (art. 3º, III e IV).

O Comitê dos Direitos da Criança afirma que os governos "devem revisar, adotar e atualizar a legislação nacional" para garantir que o ambiente digital proteja os direitos da criança e que essa legislação "deve permanecer relevante, no contexto dos avanços tecnológicos e práticas emergentes."[52] As leis devem ser atualizadas para apoiar especificamente a aplicação e conformidade em ambientes digitais.[53]

Recomendamos que o Comitê de Direitos Humanos da ONU convoque o Brasil a:

• Aderir aos seus padrões internacionais e nacionais de direitos humanos para defender o direito à privacidade e os direitos da criança pertencentes à EdTech.

• Garantir que o uso de EdTech seja regulamentado de acordo com a estrutura de proteção de dados do Brasil [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018] e que a Autoridade de Proteção de Dados regule o uso de dados de crianças de acordo com a LGPD).

[52] Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', CRC/C/GC/25, 2 de março de 2021, https://www.ohchr.org/en/documents/general-comments-andrecommendations/general-comment-no-25-2021-childrens-rights-relation, parágrafo. 23.
[53] Ibid., parágrafos. 28-29, 35-39.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org