À COORDENADORIA DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD

Procedimento nº 00261.001328/2023-77

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, associação civil sem fins lucrativos, inscrita no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Economia sob o nº 36.942.309/0001-04, com sede na Alameda Santos, 1293, 3º andar, Jardim Paulista, CEP 01419-904, cidade e estado de São Paulo ("**Data Privacy Brasil**"), neste ato representada pelo seu Diretor Executivo **Rafael Augusto Ferreira Zanatta**, inscrito no Cadastro Nacional de Pessoas Físicas (CPF) sob o nº 065660729-77, email zanatta@dataprivacybr.org, vem, respeitosamente, apresentar contribuição como amicus curiae

CONTRIBUIÇÃO - AMICUS CURIAE

no procedimento 00261.001328/2023-77, em epígrafe, o qual apura potenciais infrações à legislação brasileira, sobretudo à Lei Geral de Proteção de Dados Pessoais - LGPD, conforme relatório de pesquisa publicado pela Human Rights Watch que avalia as práticas de tratamento de dados das plataformas de ensino **Centro de Mídias da Educação de São Paulo, Descomplica, Escola Mais, Estude em Casa, Explicaê, Manga High e Stoodi**, recomendadas pelos **estados de São Paulo e Minas Gerais** durante a pandemia de covid-19, nos termos expostos a seguir.

1. DA SÍNTESE DOS FATOS

Em maio de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) iniciou o procedimento de fiscalização sob o **nº00261.001328/2023-77**. A investigação pauta-se pelas revelações apresentadas no relatório da ONG Human Rights Watch, intitulado "Como eles ousam espiar minha privacidade?"[1]. O cerne do caso envolve sete plataformas educacionais no Brasil que **foram identificadas coletando e compartilhando informações de estudantes** com empresas parceiras, fazendo uso de tecnologias de rastreamento originalmente destinadas a fins publicitários. Entre os sites mencionados estão Estude em Casa, Centro de Mídias da Educação de São Paulo, Descomplica, Escola Mais, Explicaê, MangaHigh e Stoodi. Além disso, um oitavo site, Revisa Enem, embora não tenha empregado rastreadores específicos para fins publicitários, também compartilhava dados de estudantes com uma empresa parceira[2].

A natureza intrusiva dessas práticas vai além do simples acompanhamento de atividades online dos alunos, chegando ao acesso de listas de contatos telefônicos dos estudantes, o que levanta **preocupações sérias sobre a obtenção de detalhes pessoais que ultrapassam o escopo educacional, violando a autodeterminação informativa, a dignidade da pessoa humana, a privacidade, a intimidade e a proteção de dados pessoais de sujeitos em condição de hipervulnerabilidade, suas famílias e toda a comunidade escolar**. O relatório também sublinha que essas plataformas foram recomendadas para a aprendizagem remota durante a pandemia nos dois estados mais populosos do Brasil: São Paulo e Minas Gerais. É dizer, para além da responsabilidade de empresas em relação às suas práticas de tratamento de dados pessoais, o caso envolve também uma dimensão de análise da responsabilidade do poder público em relação a potenciais ilícitos de dados.

Em setembro de 2023, a Data Privacy Brasil **solicitou entrada como terceiro interessado no procedimento de fiscalização supramencionado (ID nº0051132)**, em analogia ao disposto no artigo 138 do Código de Processo Civil e no artigo 49 da Resolução CD/ANPD nº 4. A solicitação **foi aceita em seguida (ID nº 0051150),** motivo pelo qual nos manifestamos como terceiro interessado a partir da presente petição.

---

[1] Human Rights Watch, '**Como eles ousam espiar minha privacidade? Violações dos direitos das crianças e adolescentes por governos que endossaram sistemas de aprendizagem on-line durante a pandemia de Covid-19**', 25 de maio de 2022. Disponível em: https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.

[2] Para mais detalhes, consulte o artigo da Human Rights Watch intitulado 'Brasil: ferramentas de educação online coletam dados de crianças', publicado em 3 de abril de 2023, disponível em: https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data.

2. DA LEGITIMIDADE E PERTINÊNCIA DA PARTICIPAÇÃO DO DATA PRIVACY BRASIL

A Data Privacy Brasil é uma associação sem fins lucrativos constituída com a finalidade de desenvolver pesquisas em ciências sociais, humanas, exatas e tecnologia da informação e disponibilização de conteúdo acadêmico consoante com o princípio da participação democrática, conforme o artigo 2º de seu Estatuto Social. Como desdobramento de seu objeto está a promoção e estímulo de discussões com entes públicos e privados sobre temas associados às áreas mencionadas (artigo 2º, f, do Estatuto Social). Diz o Estatuto (Registro n. 63.166 de 25/03/2020, perante 7 Oficial de Registro de Títulos e Documentos e Civil da Pessoa Jurídica da Comarca de São Paulo), *in verbis*:

> Art. 2. Sem finalidade lucrativa e sem distribuir lucros, bonificações ou vantagens a seus mantenedores ou Associados, a Associação tem por finalidade o desenvolvimento de pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico em ciências sociais, humanas, exatas ou tecnologia da informação e disponibilização do conteúdo de cunho acadêmico, dentro dos princípios da participação democrática, da liberdade e da justiça social, sendo os seus objetivos:
>
> a) Difundir a produção de trabalhos científicos e acadêmicos em ciências sociais, humanas, exatas e de tecnologia da informação;
>
> b) Estimular os trabalhos de pesquisa nas áreas de interesse e promover conteúdo de cunho acadêmico;
>
> c) Identificar temas atuais e prioritários para a pesquisa nas áreas de ciências sociais, humanas, exatas e de tecnologia da informação;
>
> d) Promover a pesquisa e trabalhos acadêmicos de interesse;
>
> e) Realizar e participar de congressos, estudos, conferências, cursos, feitas, exposições, seminários sobre os temas de interesse e afins;
>
> f) Promover a estimular discussões com entes públicos e privados sobre temas das áreas afim.

O reconhecimento do papel de promoção de discussão com entes públicos, pela figura do *amicus curiae*, já foi **reconhecido pelo Supremo Tribunal Federal** em três ocasiões. Inicialmente, a

Data Privacy Brasil participou do julgamento da ADI 6387, relatada pela ministra Rosa Weber[3]. Em 07 de janeiro de 2021, em decisão monocrática proferida na Ação Direta de Inconstitucionalidade 6.649-DF, o ministro Gilmar Mendes deferiu o ingresso da Associação Data Privacy Brasil de Pesquisa no feito, na condição de *amicus curiae*[4]. A decisão avaliou a representatividade da postulante, concedendo poderes de participação nos termos da Lei 9.882/1999[5], o que evidencia o reconhecimento estatutário da Associação e sua legitimidade para intervenção em casos complexos que envolvem o direito à proteção de dados pessoais. Em 2024, a Data Privacy Brasil também participou, como *amicus curiae*, da análise do caso ADPF 1143, que tem por objeto a discussão da constitucionalidade do uso de spywares pela Agência Brasileira de Inteligência (Abin)[6].

De modo complementar, a organização é uma **associação civil criada com o objetivo central de produção de pesquisa de interesse público na intersecção entre tecnologia, tratamento de dados pessoais e direitos fundamentais**. Para cumprir com estes objetivos, a associação desenvolveu uma Política de Financiamento Ético e Transparência, para garantir sua autonomia e independência frente aos financiadores, a fim de manter sua liberdade de atuação e a possibilidade de perseguir seus interesses como entender adequado. Resta evidente a compatibilidade do objeto institucional com as temáticas deste procedimento.

Em seu quadro de colaboradores, a Associação Data Privacy de Pesquisa conta com acadêmicos que atuam na temática de governança da Internet e **participam ativamente dos debates nacionais mais relevantes sobre proteção de dados pessoais**.

Para fins de ilustração, o Data Privacy Brasil está, desde sua constituição, inserido em atividades e espaços como os seguintes:

---

[3] Para acessar a intervenção apresentada pela Data Privacy Brasil na Ação Direta de Inconstitucionalidade nº 6.387, visite: https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_amicuscuria_stf_ibge.pdf.

[4] Para consultar a decisão monocrática proferida pelo Ministro Gilmar Mendes, acesse: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=6079238.

[5] O Art. 6º da Lei nº 9.882, de 3 de dezembro de 1999, estabelece que, após a apreciação do pedido de liminar, o relator deve solicitar informações às autoridades responsáveis pelo ato questionado, no prazo de dez dias. O § 2º desse artigo dispõe que, a critério do relator, podem ser autorizadas sustentação oral e a juntada de memoriais, mediante requerimento dos interessados no processo. Para consultar o texto completo da Lei nº 9.882/1999, acesse: https://www.planalto.gov.br/ccivil_03/Leis/L9882.htm.

[6] Para mais informações sobre a participação da Data Privacy Brasil na audiência pública do Supremo Tribunal Federal que discutiu o uso de ferramentas de monitoramento secreto, consulte: dataprivacybr.org +4 dataprivacybr.org +4 dataprivacybr.org +4 https://www.dataprivacybr.org/data-privacy-brasil-participa-de-audiencia-no-stf-de-monitoramento-secreto/.

- Na colaboração com a Autoridade Nacional de Proteção de Dados (ANPD), como nas Consultas Públicas sobre a Norma de Fiscalização[7], sobre as bases legais adequadas para tratamento de dados de crianças e adolescentes[8], bem como na Tomada de Subsídios sobre o Projeto Regulatório Projeto Regulatório sobre o Tratamento de Dados de Crianças e Adolescentes[9], de 2024
- No mesmo contexto de colaboração com a ANPD, é importante destacar que Bruno Bioni, diretor do Data Privacy Brasil, faz parte do Conselho Nacional de Proteção de Dados (CNPD) da Autoridade, como representante da sociedade civil.
- Em debates e eventos promovidos pela própria Autoridade, discutindo Regulação de Inteligência Artificial[10] e os desafios da aplicação da LGPD no Setor Público[11]. Além disso, celebramos os 5 anos da promulgação da Lei Geral de Proteção de Dados Pessoais[12];
- Internacionalmente, no Civil 20 (C20), do G20, junto à entidade paraguaia TEDIC, levantamos a voz sobre os problemas de vigilância na América Latina[13], como também com o Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos

---

[7] DATA PRIVACY BRASIL. **Contribuição à tomada de subsídios da ANPD a respeito de sua Norma de Fiscalização**. 19 jul. 2021. Disponível em: https://dataprivacy.com.br/contribuicao-a-tomada-de-subsidios-da-anpds-a-respeito-de-sua-norma-de-fiscalizacao/. Acesso em: 1 set. 2023.

[8] DATA PRIVACY BRASIL. **Contribuição à tomada de subsídios sobre tratamento de dados de crianças e adolescentes da Autoridade Nacional de Proteção de Dados**. Disponível em: https://dataprivacy.com.br/contribuicao-a-tomada-de-subsidios-sobre-tratamento-de-dados-de-criancas-e-adolescentes-da-anpd/. Acesso em: 1 set. 2023.

[9] DATA PRIVACY BRASIL. **Contribuição à tomada de subsídios sobre o projeto regulatório acerca do tratamento de dados de crianças e adolescentes da Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2024/08/Data-Privacy-Brasil.-Tomada-de-Subsidios-em-Direitos-de-Criancas.-ANPD.-2024.pdf. Acesso em: 2 jan. 2025.

[10] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD fará evento online sobre Regulação de Inteligência Artificial**. Gov.br, 30 jun. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fara-evento-online-sobre-regulacao-de-inteligencia-artificial. Acesso em: 1 set. 2023.

[11] BIONI, Bruno. **govDADOS recebe Bruno Bioni para debater sobre a ANPD e o enforcement da LGPD no setor público**. Disponível em: https://brunobioni.com.br/blog/namidia/govdados-recebe-bruno-bioni-para-debater-sobre-a-anpd-e-o-enforcement-da-lgpd-no-setor-publico/. Acesso em: 1 set. 2023.

[12] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Autoridade anuncia pacote de entregas e destaca avanços na proteção de dados em evento de celebração aos 5 anos da LGPD**. Editora Roncarati, 15 ago. 2023. Disponível em: https://www.editoraroncarati.com.br/v2/Artigos-e-Noticias/Artigos-e-Noticias/Noticias-ANPD-em-15-08-2023.html. Acesso em: 1 set. 2023.

[13] DATA PRIVACY BRASIL. **Associação Data Privacy Brasil de Pesquisa e TEDIC lançam relatório sobre vigilância na tríplice fronteira**. 23 fev. 2022. Disponível em: https://www.dataprivacybr.org/associacao-data-privacy-brasil-de-pesquisa-e-tedic-lancam-relatorio-sobre-vigilancia-na-triplice-fronteira/. Acesso em: 1 set. 2023.

(OHCHR), explorando as interseções entre direitos humanos e padrões técnicos de tecnologias emergentes;

- Fomos responsáveis pelo Secretariado da Força Tarefa de Transformação Digital Inclusiva do T20[14], grupo de *think tanks* responsáveis por produzir subsídios aos países que integram o G20, durante a presidência brasileira de 2024;
- Nossa participação ativa em conferências internacionais como a Computers, Privacy and Data Protection Conference (CPDP)[15] e a RightsCon[16] destaca nosso compromisso com a construção de pontes entre a academia, tomadores de decisão e profissionais interessados nas convergências entre direito, dados e tecnologias;
- E em eventos locais, em espaços como a CPDP LatAm[17], o Fórum da Internet no Brasil[18] e o Seminário de Privacidade e Proteção de Dados do CGI.br[19], nos posicionando como atores-chave no debate sobre privacidade e proteção de dados pessoais na América Latina.

[14] Leia sobre a Força-Tarefa de Transformação Digital Inclusiva, coordenada pela Data Privacy Brasil no âmbito do T20, visite: https://www.dataprivacybr.org/projeto/data-privacy-brasil-no-t20-transformacao-digital-inclusiva/.

[15] DATA PRIVACY BRASIL. **Data Privacy Brasil envia contribuição ao Comitê de Direitos Humanos da ONU**. 28 jul. 2023. Disponível em: https://www.dataprivacybr.org/data-privacy-brasil-envia-contribuicao-ao-comite-de-direitos-humanos-da-onu/. Acesso em: 1 set. 2023.

[16] DATA PRIVACY BRASIL. **Data Privacy organiza painel sobre tecnoautoritarismo no Fórum de Governança da Internet**. 9 jun. 2021. Disponível em: https://www.dataprivacybr.org/data-privacy-organiza-painel-sobre-tecnoautoritarismo-no-forum-de-governanca-da-internet/. Acesso em: 1 set. 2023.

[17] DATA PRIVACY BRASIL. **Mesa no CPDP-LATAM: "Multissetorialismo na forma e no conteúdo da LGPD: qual é o papel dessa abordagem para a formação de uma cultura de proteção de dados no Brasil?"**. Disponível em: https://www.dataprivacybr.org/documentos/mesa-no-cpdp-latam-multissetorialismo-na-forma-e-no-conteudo-da-lgpd-qual-e-o-papel-dessa-abordagem-para-a-formacao-de-uma-cultura-de-protecao-de-dados-no-brasil/. Acesso em: 1 set. 2023.

[18] DATA PRIVACY BRASIL. **Associação Data Privacy Brasil de Pesquisa participa do painel "Proteção de criança online na pandemia: ferramentas e boas práticas para um ambiente seguro"**. Disponível em: https://www.dataprivacybr.org/associacao-data-privacy-brasil-de-pesquisa-participa-do-painel-protecao-de-crianca-online-na-pandemia-ferramentas-e-boas-praticas-para-um-ambiente-seguro/. Acesso em: 1 set. 2023.

[19] DATA PRIVACY BRASIL. **13º Seminário de Proteção à Privacidade e aos Dados Pessoais**. [online] São Paulo: 22 ago. 2022. Disponível em: https://www.dataprivacybr.org/13o-seminario-de-protecao-a-privacidade-e-aos-dados-pessoais/. Acesso em: 01 set. 2023.

A capacidade do Data Privacy Brasil para enriquecer o debate sobre a proteção de dados é reconhecida pela imprensa nacional, como Folha de S. Paulo[20], O Estado de S. Paulo[21], Exame[22], entre outros, que veiculam tanto projetos da Associação, quanto entrevistam seus membros para esclarecimentos técnicos.

Dentre os temas sobre os quais o Data Privacy Brasil se debruça, destaca-se a **proteção de dados pessoais de crianças e adolescentes, inclusive no contexto educacional**. Nesse sentido, a organização colaborou em 2020 com a **elaboração do Comentário Geral 25 sobre os direitos da criança em relação ao ambiente digital**[23], da Organização das Nações Unidas (ONU), o qual traça parâmetros bastante relevantes sobre a proteção de dados pessoais de crianças e adolescentes no contexto atual. A publicação do Comentário Geral 25 motivou a organização a se juntar com o Instituto Alana e a *Asociación por los Derechos Civiles* (ADC) - organização da Argentina - em um grupo de estudos que pensava a privacidade e proteção de dados de crianças e adolescentes no contexto sul-americano. **O grupo culminou em um policy paper**[24]**, cujo objetivo primordial foi democratizar o debate, especialmente a partir da perspectiva do sul global**, acerca do cenário do tema da região.

Desde janeiro de 2023, o Data Privacy Brasil o projeto **"IA na sala de aula: modelos de participação para a comunidade escolar"**[25], situado justamente na intersecção entre proteção de dados, infância e educação. Em 2024, foi publicada um dos seus principais resultados, a **Cartilha**

---

[20] MENA, Fernanda; SOPRANA, Paula. **Apps e sites usados em aulas online no Brasil coletaram dados privados de crianças**. Folha de S.Paulo, São Paulo, 24 maio 2022. Disponível em: https://www1.folha.uol.com.br/educacao/2022/05/apps-e-sites-usados-em-aulas-online-no-brasil-coletaram-dados-privados-de-criancas.shtml. Acesso em: 1 set. 2023.

[21] ROMANI, Bruno. **ChatGPT vive à sombra de um grande escândalo de dados; entenda**. O Estado de S. Paulo, 2023. Disponível em: https://www.estadao.com.br/amp/link/cultura-digital/chatgpt-vive-a-sombra-de-um-grande-escandalo-de-dados-entenda/. Acesso em 01 set. 2023.

[22] MALAR, João Pedro. **"Worldcoin, dono do ChatGPT, gera preocupação sobre segurança de dados e privacidade"**. Exame, 27 jul. 2023. Disponível em: https://exame.com/future-of-money/worldcoin-preocupacao-seguranca-dados-privacidade/. Acesso em: 1 set. 2023.

[23] DATA PRIVACY BRASIL. **Contribuição para ONU (Comentário Geral 25)**. [online]. Disponível em: https://www.dataprivacybr.org/documentos/contribuicao-para-onu-comentario-geral-25/. Acesso em: 1 set. 2023.

[24] DATA PRIVACY BRASIL. **Proteção infantil na América Latina: debates sob o olhar do Brasil e da Argentina**. [online]. Disponível em: https://www.dataprivacybr.org/documentos/protecao-infantil-na-america-latina-debates-sob-o-olhar-do-brasil-e-da-argentina/. Acesso em: 1 set. 2023.

[25] DATA PRIVACY BRASIL. **IA na sala de aula: construindo modelos participativos para a comunidade escolar**. [online]. Disponível em: https://www.dataprivacybr.org/documentos/ia-na-sala-de-aula-construindo-modelos-participativos-para-a-comunidade-escolar/. Acesso em: 2 jan. 2025.

Digital "IA na sala de aula: Construindo modelos participativos para a comunidade escolar"[26], a qual é pautada por dois objetivos centrais: envolver crianças e adolescentes desde as reflexões sobre quando e por que introduzir determinada tecnologia no ambiente escolar; e, caso positivo, permitir que participem ativamente na escolha do produto ou serviço, considerando as realidades específicas de cada ambiente escolar. No âmbito do mesmo projeto, a organização também **contribuiu com o Comitê de Direitos Humanos da ONU**[27] e ofereceu recomendações relacionadas à utilização de tecnologias e coleta em larga escala de dados pessoais de crianças e adolescentes nas escolas públicas brasileiras - inclusive mencionando a pesquisa publicada pela Human Rights Watch.

Em 2024, a Data Privacy Brasil **integrou o Grupo de Trabalho do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda)** que visa a construção de uma Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Nesse contexto, além das trocas realizadas em reuniões temáticas, **a organização também submeteu uma contribuição**[28], através da qual sugeriu diretrizes para a formulação de estratégias de capacitação da comunidade escolar (estudantes, professores, famílias e gestores escolares) em proteção de dados pessoais e direitos digitais, a formulação de parâmetros legais claros para contratações públicas na área de educação, entre outros pontos primordiais para a proteção de crianças e adolescentes no ambiente digital . Toda a discussão foi publicizada e detalhada na **Aula Aberta "Por que precisamos de uma política nacional para proteção dos direitos das crianças no ambiente digital?"**, realizada em 29 de novembro, pelos professores Júlia Mendonça e Rafael Zanatta[29].

Em resumo, a Data Privacy Brasil tem qualificado o debate sobre proteção de dados no país e se mostrado um dos principais atores com contribuições que o interseccionam com infância, adolescência e educação. Do processo de formulação da LGPD até os contornos constitucionais da

---

[26] DATA PRIVACY BRASIL. **IA na sala de aula: construindo modelos participativos para a comunidade escolar**. São Paulo: Data Privacy Brasil, 2024. Disponível em: https://conteudos.dataprivacy.com.br/cartilha-ia-na-sala-de-aula. Acesso em: 2 jan. 2025.

[27] MENDONÇA, Eduardo; MENDONÇA, Júlia; MEIRA, Marina. **Data Privacy Brasil envia contribuição ao Comitê de Direitos Humanos da ONU**. Data Privacy Brasil Research, 28 jul. 2023. Disponível em: https://www.dataprivacybr.org/data-privacy-brasil-envia-contribuicao-ao-comite-de-direitos-humanos-da-onu/. Acesso em: 1 set. 2023.

[28] DATA PRIVACY BRASIL. **Data Privacy Brasil submete contribuição para o Grupo de Trabalho do Conanda**. 25 out. 2024. Disponível em: https://www.dataprivacybr.org/data-submete-contribuicao-para-o-grupo-de-trabalho-do-conanda/. Acesso em: 1 set. 2023.

[29] DATA PRIVACY BRASIL. **Aula Aberta: Política nacional para proteção dos direitos das crianças no ambiente digital**. Disponível em: https://www.youtube.com/watch?v=hJdjO8AHq3k&ab_channel=DataPrivacyBrasil. Acesso em: 2 jan. 2025.

matéria no Poder Legislativo (PEC 17/2019) a associação e seus membros têm contribuído de forma coerente, contínua e pertinente, o que a credencia para a posição de terceiro interessado.

3. ESTUDO TÉCNICO-JURÍDICO

Em 2024, diante da construção de argumentos técnicos para contribuição com o processo em curso (ANPD 00261.001328/2023-77), a Data Privacy Brasil firmou parceria com **KU Leuven Centre for IT and IP Law** (CiTiP – Bélgica[30]), na figura da pesquisadora e pós-doutoranda Elora Fernandes[31], para elaborar o Estudo Técnico-Jurídico com base na LGPD sobre o relatório "*How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*", anexado à presente petição.

Em síntese, o Estudo Técnico se debruça sobre os seguintes tópicos:

1. **Violação ao Princípio do Melhor Interesse da Criança e Impacto nos seus Direitos fundamentais:**
   1.1. As Secretarias de Educação e as empresas de EdTech atuam como controladoras conjuntas e aparentam estar em patente desacordo com o art. 6, I e o art. 14, caput, da LGPD.
   1.2. O tratamento de dados pessoais para fins de perfilamento comercial e publicidade direcionada **não atende ao melhor interesse de crianças e adolescentes**, tornando a finalidade ilegítima estando e, portanto, em desacordo com a LGPD.
   1.3. Tais práticas, além de abusivas, violam direitos fundamentais, como privacidade e proteção de dados de crianças e adolescentes. Além disso, **extrapolam a finalidade**

[30] O Centre for IT & IP Law (CiTiP) é um centro de pesquisa da Faculdade de Direito e Criminologia da Universidade de Leuven (KU Leuven), especializado em aspectos jurídicos e éticos da inovação em TI e propriedade intelectual. Com uma equipe de mais de 85 pesquisadores, o CiTiP é internacionalmente reconhecido por sua expertise em áreas como inteligência artificial, proteção de dados, eHealth, ética e direito, propriedade intelectual, mídia e telecomunicações e (ciber)segurança. Para mais informações, visite: https://www.law.kuleuven.be/citip/en.

[31] Elora Fernandes é Pesquisadora de Pós-doutorado no KU Leuven Centre for IT and IP Law (CiTiP – Bélgica), onde foca sua pesquisa nos direitos de crianças no ambiente digital. Anteriormente, trabalhou em ONGs de direitos digitais em diferentes países e atuou como Trainee e Legal Officer (Interina) no European Data Protection Supervisor (EDPS). Elora defendeu seu Doutorado em Direito na Universidade do Estado do Rio de Janeiro (UERJ) em cotutela com a KU Leuven, com tese acerca da proteção de dados de crianças em tecnologias educacionais (edtech). Obteve Mestrado em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF, Brasil) e concluiu a Graduação em Direito na mesma instituição, incluindo um período de mobilidade acadêmica na Universidade de Salamanca (Espanha). Além disso, coordenou a equipe de assistentes da Revista de Estudos Empíricos em Direito (REED) e é *alumna* do Deutscher Akademischer Austauschdienst (DAAD).

educacional, não trazem benefícios aos estudantes e afetam negativamente seu desenvolvimento progressivo, violando o princípio da proteção integral com prioridade absoluta garantido pela Constituição Federal.

2. **Desrespeito ao Princípio da Minimização de Dados:**

2.1. A HRW não conseguiu identificar como os dados tratados estão alinhados com as atividades educacionais das EdTechs, **o que configura uma clara violação ao art. 14, §4º, da LGPD**.

Entre as infrações observadas estão:

- Rastreamento de localização e contatos telefônicos de estudantes;
- Coleta e compartilhamento de dados com empresas de publicidade;
- Criação de perfis comportamentais para segmentação comercial, sem que os estudantes ou seus responsáveis pudessem recusar esse tratamento.

2.2. O referido artigo enfatiza rigorosamente a minimização do tratamento de dados de crianças desde a coleta, exigindo que os controladores não condicionem a participação das crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais que não sejam estritamente necessárias para a atividade em questão.

3. **Importância Ética e Social e Soberania Digital:**

3.1. A implementação das EdTechs ocorreu sem um debate público aprofundado e desconsiderou políticas que respeitem a soberania digital brasileira. A investigação evidenciou que as decisões foram tomadas sem critérios claros de proteção de dados pessoais e sem avaliação de impacto, colocando crianças e adolescentes em situação de vulnerabilidade extrema.

3.2. Garantir a conformidade legal com a LGPD é mais do que um requisito técnico; é uma questão de ética e responsabilidade social, especialmente no ambiente educacional. A ausência de governança adequada na implementação dessas tecnologias compromete a segurança, a autonomia e os direitos fundamentais à

privacidade e proteção de dados de crianças e adolescentes. Diante desse cenário, é necessário promover um desenvolvimento equitativo e seguro das crianças.

4. ARGUMENTO DEFENDIDO PERANTE A ANPD

O cenário fático analisado nesta investigação preliminar é **grave**, pois envolve um conjunto de empresas do setor educacional que, valendo-se de ausências de cláusulas contratuais sobre proteção de dados pessoais nos contratos de doação com o setor público, exploraram comercialmente dados obtidos por rastreadores (*cookies*), em violação ao princípio de finalidade ("realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[32]) e de adequação ("compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento"[33]) da Lei Geral de Proteção de Dados Pessoais, bem como uma ostensiva violação à norma jurídica de proibição de tratamento de dados pessoais de crianças e adolescentes além das atividades estritamente necessárias do art. 14, § 4º da LGPD[34].

Nos termos do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021, **recomenda-se que a ANPD adote atividades preventivas**, nos termos do Art. 15, § 3º, utilizando-se de "métodos e ferramentas que almejam a promover a orientação, a conscientização e a educação dos agentes de tratamento e dos titulares de dados pessoais".

Entre as atividades preventivas de grande urgência, estão (i) a conscientização das Secretarias de Educação sobre a necessidade de cláusulas em contratos de doações de tecnologias[35], proibindo qualquer tipo de prática de análise agregada de dados oriundos de rastreadores (*cookies*) fora das atividades estritamente necessárias (em respeito ao art. 14, §4º da LGPD) e (ii) o reconhecimento de que as tecnologias intrusivas de rastreamento em aplicações de internet

[32] Lei 13.709/2018, art. 6º, I.

[33] Lei 13.709/2018, art. 6º, II.

[34] Lei 13.709/2018, Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. (...) § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

[35] AMIEL, Tel; ZANATTA, Rafael A. F.; PEZZO, Thiago. **The hidden costs of free services: how donations support the corporate platformization of education**. Learning, Media and Technology, v. 49, n. 1, p. 1-14, 2024. Disponível em: https://doi.org/10.1080/17439884.2024.2396916. Acesso em: 8 mar. 2025.

utilizadas por crianças e adolescentes no ambiente educacional produzem um cenário de "exploração comercial", que é vedado tanto pela Lei Geral de Proteção de Dados Pessoais, quanto pelas novas Diretrizes Gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital (Resolução nº 257, de 12 de dezembro de 2024),[36] em especial o princípio de prevenção contra exploração comercial no ambiente digital (art. 3º, V) quanto o eixo temático da política nacional de enfrentamento da exploração comercial no ambiente digital (art. 4º, I).

Lembramos que compete à ANPD estimular a adoção de padrões para serviços que facilitem o exercício de controle dos titulares sobre os dados e fortaleçam a autodeterminação informativa (art. 55-J, VIII, LGPD), sendo possível, no âmbito das atividades preventivas, a aprovação de uma resolução específica sobre proteção de dados pessoais em *edtechs*, com normas proibitivas sobre a exploração comercial de cookies, a partir dos aprendizados dos eventos ocorridos em 2020 em São Paulo e em Minas Gerais.

5. DOS PEDIDOS

Ante o exposto, os *amici curiae* da Data Privacy Brasil, devidamente admitidos por esta Autoridade Nacional de Proteção de Dados para auxiliar nos procedimentos do feito, requerem que esta ANPD declare a ilegalidade das práticas de tratamento de dados pessoais de crianças e adolescentes por plataformas educacionais que extrapolam a finalidade educacional, violando o princípio do melhor interesse da criança e os direitos fundamentais de privacidade e proteção de dados, conforme apurado no relatório da Human Rights Watch e detalhado no Estudo Técnico-Jurídico elaborado em parceria com o KU Leuven Centre for IT and IP Law.

Subsidiariamente, requer seja determinada a imediata adoção de medidas preventivas pela ANPD, nos termos do Art. 15, § 3º da Resolução CD/ANPD nº 1/2021, para: (i) Promover a conscientização das Secretarias de Educação sobre a necessidade de incluir cláusulas em contratos de doações de tecnologias que proíbam qualquer tipo de prática de análise agregada de dados oriundos de rastreadores (*cookies*) fora das atividades estritamente necessárias, em respeito ao art. 14, §4º da LGPD; (ii) Reconhecer que as tecnologias intrusivas de rastreamento em aplicações de internet utilizadas por crianças e adolescentes no ambiente educacional produzem um cenário de "exploração

[36] Para mais detalhes sobre as diretrizes gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, consulte a Resolução nº 257, de 12 de dezembro de 2024, disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/61597.

comercial" vedado pela LGPD e pelas Diretrizes Gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital (Resolução nº 257/2024); (iii) Aprovar uma resolução específica sobre proteção de dados pessoais em *edtechs*, com normas proibitivas sobre a exploração comercial de cookies e demais tecnologias de rastreamento, baseando-se nos eventos ocorridos em 2020 em São Paulo e Minas Gerais.

Nestes termos, pede deferimento.

São Paulo, 10 de março de 2025

RAFAEL AUGUSTO FERREIRA ZANATTA

Assinado de forma digital por RAFAEL AUGUSTO FERREIRA ZANATTA
Dados: 2025.03.13 16:24:53 -03'00'

Bruno Ricardo Bioni
Diretor
OAB/SP 316.083

Mariana Marques Rielli
Diretora
OAB/SP 408.049

Rafael A. F. Zanatta
Diretor
OAB/SP 311.418

Carla Rodrigues
Coordenadora da Área de Plataformas e Mercados

Júlia Mendonça
Pesquisadora
OAB/BA 71.485

Eduardo Mendonça
Pesquisador

Estudo Técnico-Jurídico com base na LGPD sobre o relatório "'*How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*"

Subsídios para a Participação da Associação Data Privacy Brasil de Pesquisa como *amicus curiae* no processo de investigação ANPD nº4281521

Elora Fernandes[1]

SUMÁRIO

1.Introdução..... 2
1.1 As parcerias entre empresas de EdTech e escolas brasileira..... 3
2. Implicações do Relatório "'*How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*" para a realidade brasileira..... 6
2.1 As tecnologias de rastreamento nas EdTech analisadas pela HRW 6
2.1.1 Identificação de quem são as crianças 7
2.1.2 Vigilância inescapável 8
2.1.3 Rastreamento de localização 8
2.1.4 Rastreamento de quem as crianças conhecem..... 9
2.1.5 Rastreamento do que crianças fazem em sala de aula 9
2.1.6 Rastreamento do que crianças fazem fora da sala de aula 10
2.2 O envolvimento da Meta e do Google 18
3. Riscos para a proteção de dados de crianças e adolescentes na utilização de edtech..... 19
3.1 A proteção de dados de crianças e adolescentes na educação..... 19
3.2 A importância da confiança para a aprendizagem e o desenvolvimento da autonomia 23
4. A LGPD e o regime especial para a proteção de dados de crianças e adolescentes..... 24
4.1 O melhor interesse da criança e do adolescente como filtro para a identificação de finalidades legítimas para o tratamento de dados de crianças e adolescentes..... 26
4.2 Uma interpretação mais restritiva ao princípio da necessidade no tratamento de dados de crianças e adolescentes 30
5.Conclusão..... 31
6.Referências..... 32

---

[1] Elora Fernandes é Pesquisadora de Pós-doutorado no KU Leuven Centre for IT and IP Law (CiTiP – Bélgica), onde foca sua pesquisa nos direitos de crianças no ambiente digital. Anteriormente, trabalhou em ONGs de direitos digitais em diferentes países e atuou como Trainee e Legal Officer (Interina) no European Data Protection Supervisor (EDPS). Elora defendeu seu Doutorado em Direito na Universidade do Estado do Rio de Janeiro (UERJ) em cotutela com a KU Leuven, com tese acerca da proteção de dados de crianças em tecnologias educacionais (edtech). Obteve Mestrado em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF, Brasil) e concluiu a Graduação em Direito na mesma instituição, incluindo um período de mobilidade acadêmica na Universidade de Salamanca (Espanha). Além disso, coordenou a equipe de assistentes da Revista de Estudos Empíricos em Direito (REED) e é *alumna* do Deutscher Akademischer Austauschdienst (DAAD).

1. Introdução

[1] Em 2020, a pandemia da COVID-19 causou uma grande disrupção na vida social ao redor do mundo e todas as interações se tornaram digitais por padrão. Na educação, isso não foi diferente. Apesar de as tecnologias digitais de informação e comunicação (TICs) já estarem presentes no ambiente escolar, a pandemia acelerou sua implementação de forma abrupta. Com isso, a indústria de EdTech está em ascensão, contribuindo com cerca de 6% do produto interno bruto (PIB) global.[2] Espera-se que o mercado global de EdTech valha 404 bilhões de dólares até o final de 2025[3] e 700 bilhões de dólares até 2028.[4] Isso representa um aumento significativo em comparação com a avaliação projetada de 76,4 bilhões de dólares para o mercado mundial em 2019.[5]

[2] Em 2021, a plataforma de aprendizado online Coursera, por exemplo, registrou 20 milhões de novas matrículas de estudantes[6] e existem pelo menos 30 corporações financiadas na ordem de milhões de dólares (*multi-million-dollar-funded corporations*) ao redor do mundo focadas no desenvolvimento de ferramentas de IA para a educação.[7] Com aumento na procura, veio também o aumento nas receitas. O financiamento de capital de risco para startups de EdTech disparou para um recorde de 16,1 bilhões de dólares em 2020, mais do que o dobro dos 7 bilhões de dólares arrecadados em 2019.[8]

[3] A pandemia criou a necessidade de uma adoção repentina de tecnologias para a manutenção das atividades de educação, não permitindo um debate público adequado sobre como esse processo deveria ocorrer. Muitos governos foram pegos desprevenidos, não estando preparados técnica e organizacionalmente para a rápida implementação de tecnologias de apoio à educação à distância. A urgência na tomada de decisões e a falta de uma visão holística dos direitos fundamentais de crianças e adolescentes levaram à implementação e, até hoje, à manutenção de EdTechs problemáticas. Isso inclui a utilização de tecnologias que tratam dados (sensíveis) de crianças de forma massiva e não alinhada com o seu melhor interesse.

[4] Em investigação conduzida em Novembro de 2022 e revisada em janeiro de 2023, a Human Rights Watch (HRW) analisou as tecnologias educacionais utilizadas pelos 68 países mais populosos do mundo, incluindo o Brasil. Essa investigação deu origem ao relatório "'*How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*". No caso do Brasil, foram selecionados os dois estados mais populosos para análise, isto é, São Paulo e Minas Gerais, que à época utilizavam oito aplicações

---

[2] PANGARKAR, Tajammul, Eye-Opening EdTech Statistics: Opportunities and Obstacles, **Market.US**, 2023.
[3] HOLONIQ EDUCATION INTELLIGENCE UNIT, **Global EdTech market to reach $404B by 2025 - 16.3% CAGR**, HolonIQ, disponível em: <https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025>. acesso em: 12 nov. 2023.
[4] WALKER, Christopher, Unlocking the impact of edtech, **impactInvestor**, 2023.
[5] GRAND VIEW RESEARCH, **Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 - 2030**, [s.l.: s.n.], 2023.
[6] COURSERA, **2021 Impact Report. Serving the world through learning**, [s.l.: s.n.], 2021.
[7] HOLMES, Wayne, **The Unintended Consequences of Artificial Intelligence**, [s.l.: s.n.], 2023, p. 64.
[8] 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**, [s.l.: s.n.], 2022.

no total: Estude em Casa, Centro de Mídias da Educação de São Paulo, Descomplica, Escola Mais, Explicaê, MangaHigh, Stoodi e Revisa Enem. O site DragonLearn também foi analisado, mas, após a investigação, foi retirado do ar.

[5] Com a exceção do site Revisa Enem, todas as outras EdTech utilizadas pelos dois estados brasileiros examinadas pela HRW coletaram grandes quantidades de dados de crianças e adolescentes e os enviaram para empresas especializadas em publicidade comportamental. Em resposta à investigação, a Secretaria Estadual de Educação de Minas Gerais removeu todo o rastreamento relacionado a publicidade direcionada de seu site. Já a Secretaria Estadual de São Paulo não respondeu a quatro pedidos de esclarecimento da HRW até abril de 2023.[9]

[6] Em abril de 2023, a HRW realizou reunião com a Autoridade Nacional de Proteção de Dados (ANPD) para discutir medidas de proteção de crianças e adolescentes no ambiente digital.[10] Durante o encontro, as informações coletadas pela HRW e detalhadas em seu relatório foram compartilhadas com a ANPD, resultando na abertura de um processo de investigação (Despacho SEI nº 4281521), que acolheu a Nota Técnica 64 (SEI nº 4274209). Este *amicus curiae* se insere no contexto dessa investigação, contribuindo para o aprofundamento das questões ali discutidas.

[7] O propósito deste *amicus curiae* é o de contribuir com a ANPD na análise deste caso, que pode servir como um precedente para outras EdTech, escolas e secretarias de educação no Brasil, demonstrando o que não pode ocorrer no tratamento de dados de crianças e adolescentes. Após essa introdução e uma breve discussão acerca das parcerias entre empresas de EdTech e escolas brasileiras (seção 1.1), a seção 2 destrinchará o relatório, apresentando seus principais achados empíricos. A seção 3 apresenta os riscos que essas atividades podem gerar para a proteção de dados de crianças e adolescentes, especialmente em relação ao seu direito à educação. Na seção 4, exploraremos os principais mecanismos presentes na Lei Geral de Proteção de Dados Pessoais (LGPD) que foram violados pelas EdTechs analisadas pela HRW no Brasil e discutiremos como ela deve ser interpretada para promover ao máximo o melhor interesse da criança. Por fim, apresentamos considerações finais e recomendações.

1.1 As parcerias entre empresas de EdTech e escolas brasileiras

[8] A fim de compreender melhor o contexto brasileiro acerca da utilização de EdTech nas escolas, especialmente após a irrupção da pandemia, a pesquisa TIC Educação, levada a cabo pelo Núcleo de Informação e Coordenação do Ponto BR (Nic.br), é um bom ponto de partida.[11]

---

[9] HUMAN RIGHTS WATCH, **Brasil: ferramentas de educação online coletam dados de crianças**, disponível em: <https://www.hrw.org/pt/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data>. acesso em: 13 ago. 2024.

[10] ANPD, **ANPD reúne-se com a Human Rights Watch para tratar da proteção de dados pessoais de crianças e adolescentes**, disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-reune-se-com-a-human-rights-watch-para-tratar-da-protecao-de-dados-pessoais-de-criancas-e-adolescentes>. acesso em: 13 ago. 2024.

[11] BRAZILIAN NETWORK INFORMATION CENTER, **2022 ICT in Education. Survey on the Use of Information and Communication Technologies in Brazilian Schools**, São Paulo: [s.n.], 2023.

[9] Os dados da 13ª edição da pesquisa foram coletados entre maio de 2022 e outubro de 2023, marcando a primeira coleta de dados presencial após a reabertura das escolas depois da pandemia da Covid-19. No que se refere a aplicativos e plataformas digitais, 77% das escolas que participaram da pesquisa empregaram diário de classe online ou sistema de controle de matrícula, notas e frequência de alunos em 2022. 33% das escolas disseram que adotaram oficialmente um ambiente ou plataforma virtual de aprendizagem, em comparação com 51% na edição de 2020, o que provavelmente foi atribuído ao retorno às salas de aula presenciais. No entanto, 47% dos professores relataram usar um ambiente ou plataforma virtual de aprendizagem, e 48% relataram usar o Google Classroom em específico, mostrando um descompasso entre a adoção de tecnologias pelas escolas e pelos professores.

[10] O processo de escolha dessas tecnologias pelos governos municipais, estaduais ou federais não é de todo transparente e os critérios adotados não são homogêneos. De acordo com a pesquisa TIC Educação, a proteção de dados pessoais foi uma preocupação entre os educadores e 27% das escolas de ensino fundamental e médio se abstiveram de adotar uma edtech por esse motivo. Todavia, o fato de a tecnologia ser gratuita apareceu como o principal fator de escolha para 69% dos educadores, superando até mesmo sua adequação ao currículo e aos objetivos de aprendizagem.

[11] A pesquisa realizada pela Derechos Digitales e Privacy International acerca da utilização de tecnologias educacionais por alguns estados brasileiros teve resultados diferentes. As secretarias de educação estaduais da amostra não incluíram considerações sobre proteção de dados pessoais de crianças e adolescentes como um fator importante no processo de escolha.[12] Outro estudo mostra que alguns estados adotaram a tecnologia com base apenas em sua adoção por outros estados do país, o que indicaria que ela passou por algum tipo de "verificação" ou "teste".[13] Cruz e Venturini também enfatizam que algumas secretarias de educação adotaram as tecnologias do Google porque elas já eram utilizadas por professores e alunos, tornando a transição para um ambiente de aprendizado remoto/híbrido mais suave.[14]

[12] Percebe-se, portanto, a existência de indícios de que a conveniência e o caráter "gratuito" das tecnologias têm tido mais peso do que o impacto destas nos direitos fundamentais de crianças e adolescentes, em especial a proteção de seus dados pessoais. Isso é ainda reforçado pelo próprio modelo de adesão dessas tecnologias, que muitas vezes ocorre através de termos de cooperação, convênios, planos de trabalho etc. Pesquisa realizada por Amiel e outros,[15] que envolveu pedidos de informação a instituições públicas de ensino, incluindo Secretarias Estaduais de

---

[12] DERECHOS DIGITALES; PRIVACY INTERNATIONAL, **Stakeholder Report. Universal Periodic Review 41st Session -Brazil**, [s.l.: s.n.], 2022.

[13] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR, **Educação em um cenário de plataformização e de economia de dados: parcerias e assimetrias**, São Paulo: [s.n.], 2022.

[14] CRUZ, Leonardo Ribeiro da; VENTURINI, Jamila Rodrigues, Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19, **Revista Brasileira de Informática na Educação**, v. 28, p. 1060–1085, 2020.

[15] AMIEL, Tel *et al*, Os modos de adesão e a abrangência do capitalismo de vigilância na educação brasileira, **Perspectiva**, v. 39, n. 3, p. 1–22, 2021.

Educação, Institutos Federais de Educação e Universidades Federais, mostrou que, muitas vezes, o objeto dos acordos é moldado para especificar um mero serviço de consultoria técnica, utilizando expressões como "incentivar a adoção de tecnologia", "fornecer soluções", "promover a melhoria das ações educacionais" e "criar um ambiente digital".[16] A facilidade de acesso a estas tecnologias, muitas vezes solicitadas diretamente online, pode levar à conclusão errônea de que não há uma contratação entre as partes.

[13] De acordo com a legislação brasileira, os termos de cooperação devem ser utilizados apenas quando ambas as partes compartilham um interesse comum (alinhado ao interesse público) e não é permitida a transferência de recursos. Esses são instrumentos previstos na Lei nº 13.019/2014 e destinados ao estabelecimento de parcerias entre a administração e as organizações da sociedade civil. Embora a lei em si não mencione explicitamente as entidades com fins lucrativos, é pacífico na doutrina brasileira que, considerando a função social da empresa e o princípio da solidariedade, ainda seria possível estabelecer parcerias que não envolvam a transferência de recursos entre o Estado e entidades com fins lucrativos, contornando, assim, as leis de licitação. A ausência de repasse monetário, porém, não implica que o produto possa ser considerado gratuito ou que não haja interesse econômico por parte da empresa no contrato. A existência de interesses comuns, especialmente alinhados ao interesse público, também é questionável.

[14] A adoção das tecnologias através desses instrumentos faz com que etapas importantes que garantem a transparência e o devido processo nos procedimentos de licitação não sejam obrigatoriamente seguidas. O art. 118, da Lei nº 14.133/2021, estabelece que as disposições da lei podem reger esse tipo de acordo, quando aplicável, na ausência de uma regulamentação específica. Assim, embora os acordos de cooperação estejam, *a priori*, isentos das regras específicas do processo licitatório, eles não estão totalmente fora do escopo de aplicação da Lei nº 14.133/2021, cujos parâmetros poderiam ser utilizados. Na ausência de legislação específica para instrumentos congêneres, há uma norma subsidiária de aplicação da legislação e, em especial, a dimensão dos princípios constitucionais do direito administrativo.[17]

[15] Embora este *amicus curiae* não se concentre especificamente nas normas de contratação pública, é importante destacar como a ausência de preocupações com privacidade e proteção de dados nas licitações públicas e no desenvolvimento de tecnologias por agentes públicos representa um desafio significativo, especialmente no contexto de crianças e adolescentes que estão em estágio especial de desenvolvimento. O relatório publicado pela HRW, cujas principais conclusões serão detalhadas na próxima seção, revela apenas uma pequena amostra da situação precária de desenvolvimento e aplicação de EdTech pelas escolas brasileiras e que exige monitoramento mais rigoroso e cuidadoso.

---

[16] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR, **Educação em um cenário de plataformização e de economia de dados: parcerias e assimetrias**.
[17] *Ibid*.

2. Implicações do Relatório "'*How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*" para a realidade brasileira

[16] No contexto emergencial da Covid-19, a HRW examinou os planos de resposta no campo educacional dos 68 dos países mais populosos do mundo, incluindo o Brasil (especificamente os dois estados mais populosos: São Paulo e Minas Gerais). A partir disso, 163 EdTech foram avaliadas através de uma análise técnica para identificar como dados de crianças e adolescentes eram tratados e, em seguida, estes resultados foram comparados com as suas políticas de privacidade. Além disso, a HRW investigou as empresas de tecnologia de publicidade (AdTech) e os corretores de dados que receberam essas informações, assim como os materiais de *marketing* e a documentação dos desenvolvedores dessas empresas, especialmente aqueles que recebiam quantidades significativas de dados.

[17] No caso de aplicativos Android, foram utilizadas duas metodologias de análise técnica: a análise estática — que examina o código do aplicativo para identificar suas capacidades, isto é, as funções que podem ser executadas — e a análise dinâmica, que envolve a execução do aplicativo em condições reais para observar quais dados são transmitidos, para quem e para onde. Para a análise de websites, a HRW utilizou a ferramenta *Blacklight*, um inspetor de privacidade de websites em tempo real. A fim de simular a experiência de uma criança acessando o website de edtech em seu próprio país, a HRW realizou todos os testes técnicos utilizando um VPN configurado para o país onde o produto era recomendado pelo governo para a educação.

[18] Além disso, a HRW colaborou com quatro crianças de diferentes países — Índia, Indonésia, África do Sul e Turquia — e entrevistou estudantes, pais e professores entre abril de 2020 e abril de 2021, abrangendo 17 países, incluindo Austrália, Chile, Dinamarca, Alemanha, Indonésia, Índia, Irã, Itália, Líbano, Coreia do Sul, Rússia, Sérvia, Espanha, África do Sul, Turquia, Reino Unido e Estados Unidos.

2.1 As tecnologias de rastreamento nas EdTech analisadas pela HRW

[19] O principal modelo de negócios das plataformas digitais atuais é focado no que O'Reilly e outros descrevem como "rendas de atenção algorítmica" (*algorithmic attention rents*, na expressão em inglês). Segundo os autores, essas "rendas", no vocabulário econômico, estão relacionadas ao controle de um fator de produção escasso, que permite ao detentor obter lucros além do que seria normalmente alcançado em um mercado competitivo. Em vez de resultarem de melhorias produtivas que impulsionam o crescimento econômico, essas rendas representam uma realocação de valor econômico de uma parte para outra devido ao poder de mercado. No caso das plataformas digitais, o fator escasso é a atenção dos usuários e esse tipo de renda está associado à capacidade de distorcer resultados que seriam organicamente criados. Assim, a alocação de atenção dentro das plataformas direciona a distribuição de valor.[18]

[18] O'REILLY, Tim; STRAUSS, Ilan; MAZZUCATO, Mariana, **Algorithmic Attention Rents: A theory of digital platform market power**, [s.l.: s.n.], 2023.

[20] Contudo, o aumento atual de rendas de maneira geral é um grande contribuinte para o crescimento da desigualdade, a criação de ecossistemas empresariais menos dinâmicos e a redução dos níveis de crescimento da produtividade e investimento nas economias modernas.[19] No caso das plataformas digitais, dados pessoais são utilizados não apenas para conhecer melhor os indivíduos e direcionar anúncios potencialmente relevantes, mas também para alocar de forma mais "eficaz" a atenção dos usuários, prolongando seu tempo de permanência na plataforma e aumentando a frequência com que são expostos a anúncios. Isso é fundamentado na crença de que anúncios personalizados são mais persuasivos e lucrativos. Com o objetivo de personalizar anúncios, perfis são criados a partir de dados pessoais e não pessoais tratados dentro de um ecossistema complexo que inclui empresas de AdTech, corretores de dados, entre outros.

[21] O relatório desenvolvido pela HRW analisou o perfilamento de crianças e adolescentes em tecnologias educacionais a partir de seis eixos principais: identificação de quem são as crianças; vigilância inescapável; rastreamento de localização; rastreamento de quem as crianças conhecem; rastreamento do que crianças fazem em sala de aula; e rastreamento do que crianças fazem fora da sala de aula. Cada um desses eixos será brevemente resumido abaixo e serão destacados os principais achados relativos às EdTech utilizadas pelos estados de São Paulo e Minas Gerais.

2.1.1 Identificação de quem são as crianças

[22] Para desenvolver o perfil dos usuários, empresas de AdTech atribuem a cada um uma sequência de números e letras que funciona como um identificador persistente e único: ele se refere a uma única criança ou dispositivo e costuma se manter o mesmo ao longo do tempo. Essas ferramentas podem ser utilizadas por outras empresas em diferentes setores para a mesma finalidade de criação de perfis, incluindo diretamente as empresas de edtech. Cada vez que um estudante se conecta à internet e interage com tecnologias de rastreamento, qualquer informação coletada sobre ele — como onde mora, quem são seus amigos, que tipo de dispositivo sua família pode comprar, como ela interage com determinado conteúdo educacional etc. — é associada ao identificador atribuído a ele, resultando em um perfil detalhado ao longo do tempo.

[23] Os *insights* coletados através dessa criação de perfil são então utilizados para vender serviços de direcionamento para anunciantes através de plataformas de leilão em tempo real. Esses *insights* também podem ser vendidos ou compartilhados com corretores de dados, autoridades policiais, governos ou outros que desejam direcionar conteúdo a um grupo definido de pessoas com características semelhantes. Além disso, podem ser utilizados para aprimorar algoritmos ou produtos das próprias empresas de adtech ou edtech.

[24] Dentre os 73 aplicativos analisados pela HRW, 56% tinha a capacidade de coletar o identificador único que tem como única finalidade a propaganda direcionada, o que incluiu os aplicativos "Descomplica" e "Stoodi", utilizados pelo

[19] *Ibid.*

estado de São Paulo por mais de 1 milhão de usuários. Nenhum desses aplicativos possibilitou que crianças recusassem o tratamento para essa finalidade. Coletivamente, os aplicativos com essa capacidade compartilharam os dados com 33 empresas de AdTech através de *software development kits* (SDKs). SDKs são blocos ou bibliotecas de código escritos por uma empresa terceirizada que executam funções definidas (como uma página de login ou pop-ups de notificação). Assim, desenvolvedores de aplicativos podem usar SDKs ao criar seus aplicativos para não precisar criar funcionalidades do zero e para utilizar serviços de terceiros.

2.1.2 Vigilância inescapável

[25] Em sua pesquisa, a HRW descobriu que alguns dos identificadores instalados nos dispositivos de crianças e adolescentes são tão persistentes que são praticamente impossíveis de evitar ou eliminar, a menos que o dispositivo físico seja descartado. Assim, há uma vigilância inescapável e da qual, muitas vezes os estudantes ou os seus pais não estão a par. 14 aplicativos analisados pela HRW foram identificados como tendo a possibilidade de coletar dois desses identificadores: o endereço de *Wi-Fi Media Access Control* (MAC) e o *International Mobile Equipment Identity* (IMEI).

[26] O aplicativo Stoodi foi identificado como um dos que poderiam não apenas coletar os chamados números IMEI — identificador este que também não pode ser modificado, a não ser pela mudança de dispositivo — mas também de juntá-lo com o identificadores para publicidade direcionada descritos acima. Essa prática (chamada em inglês de *bridgind)* não foi informada aos usuários na sua política de privacidade.

[27] Já no que se refere aos websites, uma das técnicas mais problemáticas identificadas em oito dos 124 websites analisados (nenhum deles utilizado pelas escolas brasileiras da amostra) foi a chamada *canvas fingerprinting*. A partir dessa técnica, formas e textos ocultos são desenhados na página da web de um usuário, fazendo com que ele seja unicamente rastreável. Configurações padrão de privacidade ou técnicas de bloqueio de anúncios não são capazes de bloquear esta atividade. Os websites utilizados pelos governos de São Paulo e Minas Gerais não foram identificados como tendo essa capacidade técnica.

2.1.3 Rastreamento de localização

[28] Dados relativos à localização de uma criança ou adolescente são extremamente críticos, podendo ser utilizados para fins de sequestro, abuso físico e mental, abuso sexual e tráfico de crianças. Ademais, saber onde estão e quando pode ser utilizado para gerar diversas inferências acerca de sua vida e rotina. Isso inclui, por exemplo, determinar onde o estudante passa seu tempo livre, quem costuma visitar, assim como qual o seu padrão socioeconômico ou *status* de saúde a depender de onde frequenta.

[29] Dos 73 aplicativos analisados pela HRW, 21 deles tinham a capacidade de coletar dados de localização com precisão de 4,9m, assim como o tempo exato dessa localização, o que permite a criação de um rastro perfeito da movimentação diária dos estudantes (inclusive fora do horário escolar). Os aplicativos específicos

utilizados pelos estados de São Paulo e Minas Gerais que fizeram parte da análise da HRW não estão incluídos. Todavia, a lista apresenta aplicações extremamente utilizadas por diversas escolas brasileiras ou adotadas pontualmente por professores, como identificado nas pesquisas descritas na seção 1. Exemplos são Microsoft Teams, Zoom, Moodle, Padlet, YouTube, WhatsApp, Telegram etc. Juntos, os 21 aplicativos permitiam que outras 15 empresas tivessem acesso a esses dados de localização. A HRW não conseguiu identificar evidências de que a localização da criança pudesse trazer qualquer benefício às funcionalidades de 20 dos 21 aplicativos. Ademais, 18 aplicativos podiam coletar também informação sobre as redes wi-fi utilizadas pela criança, o que permite rastrear a sua localização e outras informações sobre o local em que ela se encontra conectada.

[30] No que se refere aos websites analisados pela pesquisa, uma forma corrente de inferir a localização de usuários se dá pelo seu endereço IP. Apesar de tecnicamente não ser possível identificar se uma empresa utiliza o endereço de IP para determinar a localização dos usuários, a maior parte das empresas de AdTech que recebiam dados dos websites da amostra ofereciam esse serviço. A pesquisa cita o caso da Criteo, que foi identificada como recebendo dados dos websites Descomplica e Escola Mais, mas que confirmou prestar serviços apenas para o primeiro.

2.1.4 Rastreamento de quem as crianças conhecem

[31] Identificar com quem uma pessoa se relaciona ou tem contato pode ser extremamente valioso para empresas de AdTech, uma vez que uma das formas mais eficazes de propaganda é a recomendação de pessoas conhecidas. A HRW identificou 18 aplicativos em sua amostra que eram capazes de coletar informações sobre os contatos dos usuários, incluindo não apenas números de telefone, mas também dados como e-mails, endereços e o grau de parentesco. Embora essas atividades não tenham sido detectadas nos aplicativos analisados especificamente na amostra brasileira, elas são comuns em outros amplamente utilizados no país, como Microsoft Teams, Zoom, Padlet, Dropbox, YouTube, WhatsApp, Telegram, Google Meet e Facebook.

2.1.5 Rastreamento do que crianças fazem em sala de aula

[32] Outra questão identificada pela HRW na amostra selecionada foi a vigilância desnecessária e desproporcional de estudantes em relação às suas atividades em sala de aula. Um exemplo seria a implementação de JavaScript *scripts* ou *web beacons* nos websites que rastreiam as atividades das crianças. Do total de 124 websites analisados, 112 instalaram rastreadores de terceiros nos dispositivos e navegadores utilizados pelas crianças e adolescentes, o que é proporcionalmente maior do que a porcentagem de websites populares focados em adultos. Estes 112 websites, que incluíam os websites brasileiros, enviaram dados para 161 empresas diferentes.

[33] Outras atividades identificadas pela HRW em determinados websites foram as chamadas *session recording* e *key logging* que possibilitam o registro de basicamente toda a atividade da criança online, incluindo movimento de mouse, clicks, movimento ao redor da página e digitação, mesmo quando a informação não

é submetida pela criança em determinado formulário. Dos websites analisados, 23 utilizavam *session recording*, incluindo os websites Descomplica, DragonLearn, Manga High e Stoodi utilizados pelo Estado de São Paulo, e 16 utilizavam *key logging*, includingo Descomplica, Manga High e Stoodi. No caso do website Stoodi, a HRW destaca que essa prática não era declarada na sua Política de Privacidade, assim como a informação de que esses dados seriam repassados a terceiros.

[34] No caso de aplicativos, uma tecnologia importante de rastreamento de atividades em sala de aula são os SDKs, como já explicado na sessão 2.1.1. Alguns SDKs são necessários para funcionalidades básicas dos aplicativos. Todavia, outros são desenvolvidos apenas com a finalidade de coletar dados para publicidade direcionada. É importante destacar que a empresa que desenvolve os SDKs incluídos em determinado aplicativo recebe o mesmo tipo de permissão que o aplicativo em si.

[35] Apesar de não ser possível determinar exatamente como SDKs são utilizados em um determinado aplicativo, muitos deles possibilitam diversas capacidades para além da coleta de dados para publicidade, que podem ser, inclusive, boas e importantes para o funcionamento do aplicativo. Todavia, algumas funções, mesmo que utilizadas com a finalidade de promover algum direito continuam sendo perigosas e invasivas caso salvaguardas não sejam implementadas. O aplicativo do Centro de Mídias da Educação de São Paulo, por exemplo, possuía instalado um SDK da Google, que dava acesso à câmera e ao microfone do celular. Outros aplicativos como Descomplica, Explicaê e Stoodi foram identificados como possibilitando acessos parecidos (ver detalhes na Tabela 1, abaixo). Nenhum dos 66 aplicativos analisados permitia que usuários recusassem desse tratamento de dados.

2.1.6 Rastreamento do que crianças fazem fora da sala de aula

[36] Mesmo quando as crianças não estão mais em suas salas de aula virtuais, elas podem ser rastreadas durante atividades não relacionadas à escola. Isso pode acontecer, por exemplo, por meio da instalação de *cookies*. Dos 124 sites investigados pela HRW, 66 continham 470 *cookies* de terceiros. Um estudante que acessa uma dessas 66 plataformas pode ser rastreado, em média, por sete *cookies* ou encontrar uma mediana (o valor central do conjunto) de três *cookies*. O número de empresas de AdTech ou outras empresas terceiras que recebem dados das crianças é ainda maior do que o número de sites de EdTech que compartilham esses dados (66 sites transmitem dados de crianças para 85 empresas terceiras).

****

[37] A **Tabela 1**, abaixo, sistematiza a coleta de dados descrita acima de cada uma das EdTech criadas ou endossadas pelos estados de Minas Gerais e São Paulo. Uma ficha completa da análise técnica de cada EdTech analisada pela HRW pode ser encontrada no site da campanha "*Students not Products*"[20] (também linkadas individualmente na tabela abaixo). A HRW contatou, à época da elaboração do

[20]HUMAN RIGHTS WATCH, **Students Not Products**, disponível em: <https://www.hrw.org/StudentsNotProducts>. acesso em: 13 ago. 2024.

relatório, as Secretarias de Educação e empresas de EdTech respectivas, que deram as respostas abaixo.[21]

[38] No caso de **Minas Gerais**:

"Quando contatada para comentar em abril de 2022, a Secretaria de Educação afirmou que 'o Estude em Casa não coleta dados para fins publicitários ou qualquer fim comercial'", e que 'não utiliza nem coleta dados dos estudantes, pois não requer qualquer tipo de login para acessar a plataforma", mas reconheceu utilizar o Google Analytics 'para acompanhamento e fins de monitoramento'.

Em novembro de 2022 e novamente em janeiro de 2023, a Human Rights Watch descobriu que o Estude em Casa continuou a enviar dados de usuários para a mesma empresa terceirizada e sua divisão de publicidade, por meio de três rastreadores de anúncios, três cookies de terceiros e a ferramenta de "públicos de remarketing" do Google Analytics.

Após a comunicação da Human Rights Watch, a Secretaria de Educação prontamente removeu todo o rastreamento de anúncios do Estude em Casa em 24 de março de 2023."

[39] No caso de **São Paulo**:

"**Centro de Mídias de São Paulo** é um site e aplicativo desenvolvido e utilizado pela Secretaria Estadual de Educação de São Paulo para oferecer aulas gratuitas durante o fechamento das escolas devido à Covid-19, e continua sendo atualizado regularmente com videoaulas e materiais.

Em maio e novembro de 2022 e novamente em janeiro de 2023, a HRW descobriu que o site enviava dados dos usuários para duas empresas terceirizadas por meio de quatro rastreadores de anúncios, incluindo um script de rastreamento que poderia permitir a publicidade.

A Secretaria Estadual de Educação de São Paulo não respondeu a quatro pedidos de esclarecimento, os últimos enviados à nova administração em janeiro e março [de 2023], tampouco respondeu à oferta da Human Rights Watch, em março de 2023, de discutir essas descobertas antes da publicação."

"**Descomplica** é um site e aplicativo desenvolvido pela empresa brasileira Descomplica Cursos Livres Via Web, destinado a estudantes do ENEM e vestibulares de universidades brasileiras. A Descomplica afirma ser a maior plataforma de ensino online do país e autorizada pelo Ministério da Educação.

Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou seu uso para estudantes do ensino médio que se preparavam para o ENEM durante o fechamento das escolas devido à Covid-19. O uso foi gratuito até dezembro de 2020.

[21] HUMAN RIGHTS WATCH, **Brasil: ferramentas de educação online coletam dados de crianças**.

[...] A Descomplica não respondeu a quatro pedidos de esclarecimento pela Human Rights Watch."

"**DragonLearn** era um site construído por uma empresa brasileira de mesmo nome. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou seu uso para estudantes do ensino fundamental durante o fechamento das escolas devido à Covid-19, e o uso do site foi gratuito até dezembro de 2020.

[...] O site DragonLearn foi retirado da internet após a investigação de maio da Human Rights Watch e subsequentes reportagens da imprensa. A DragonLearn não respondeu a três pedidos de esclarecimentos da Human Rights Watch."

"**Escola Mais** é um site desenvolvido por uma empresa brasileira de mesmo nome, que oferta aulas presenciais para estudantes do ensino fundamental e médio. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou o uso dos guias de estudo e vídeos da Escola Mais para estudantes do ensino fundamental durante o fechamento das escolas devido à Covid-19, e o site foi gratuito até janeiro de 2021.

[...] A Escola Mais não respondeu a quatro pedidos de esclarecimento da Human Rights Watch."

"Após a publicação, em 3 de abril de 2023, a Escola Mais tomou medidas para proteger seus estudantes da vigilância de dados dirigida a adultos".[22]

"**Explicaê** é um site construído pela empresa brasileira Explicaê Conteúdo e Educação Digital. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou seu uso para estudantes do ensino médio que se preparavam para o ENEM e vestibulares no Brasil durante o fechamento das escolas devido à Covid-19, e seu uso foi gratuito até janeiro de 2021.

[...] A Explicaê não respondeu a quatro pedidos de esclarecimento da Human Rights Watch."

"**MangaHigh** é um site criado pela empresa britânica Blue Duck Education Limited e oferece jogos educativos de matemática para estudantes do ensino fundamental e médio. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou seu uso para estudantes do ensino fundamental durante o fechamento das escolas devido à Covid-19, e seu uso foi gratuito até dezembro de 2021.

[...] Quando contatada em dezembro de 2022, a Blue Duck Education Limited solicitou detalhes da nova análise técnica. A Human Rights Watch forneceu uma cópia completa das evidências e resultados. A Blue Duck Education Limited não respondeu."

"**Revisa Enem** é um site desenvolvido por uma empresa brasileira de mesmo nome. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo

[22] HAN, Hye Jung, **Empresa brasileira toma providências para proteger estudantes de vigilância de dados**, Human Rights Wtach, disponível em: <https://www.hrw.org/pt/news/2023/04/04/brazilian-company-moves-shield-students-data-surveillance>. acesso em: 15 ago. 2024.

endossou seu uso durante o fechamento das escolas devido à Covid-19 para estudantes do ensino médio que se preparavam para o ENEM e vestibulares no Brasil, e seu uso foi gratuito até dezembro de 2021.

[...] A Revisa Enem não respondeu a vários pedidos de esclarecimento da Human Rights Watch."

"**Stoodi** é um site desenvolvido por uma empresa brasileira de mesmo nome. Em 26 de março de 2020, a Secretaria Estadual de Educação de São Paulo endossou seu uso durante o fechamento das escolas devido à Covid-19 para estudantes do ensino médio que se preparam para o ENEM e vestibulares no Brasil, e seu uso foi gratuito até fevereiro de 2021.

[...] Quando contatada em dezembro de 2022, a Stoodi reconheceu as conclusões da Human Rights Watch e disse que suas práticas de dados eram para melhorar a experiência do usuário e para "a Stoodi anunciar aos clientes em potencial e permitir ações comerciais de CRM [gerenciamento de relacionamento com o cliente]". A Stoodi disse que seus usuários tinham 16 anos ou mais, que não vendia dados pessoais a terceiros e que não mantinha contrato ativo com instituição pública de ensino desde 2021.

A pedido da Stoodi, a Human Rights Watch forneceu uma cópia completa de suas evidências técnicas e resultados. A Stoodi não respondeu."

TABELA 1 – COLETA DE DADOS PESSOAIS NAS EDTECH ANALISADAS PELA HRW									
WEBSITE	**Estado**	**Feito p/ crianças**	**Pol. de Priv.**	**Dados coletados no Website para:**					
				Rastrear o usuário para fins de publicidade	**Assistir e gravar o usuário**	**Capturar o que o usuário digita**	**Identificar o usuário - *Canvas fingerprinting***	**Rastrear o usuário através da internet**	**Compartilhar dados com**
Estude em Casa	Minas Gerais	Sim	Não	4 rastreadores enviaram dados para o Google	Não	Não	Não	3 cookies p/ Google	Google Analytics' 'remarketing audiences'
Centro de Mídias da Educação de São Paulo	São Paulo	Sim	Sim	2 rastreadores enviaram dados p/ Google; 2 p/ Microsoft	Não	Não	Não	Não	Não
Descomplica	São Paulo	Sim	Sim	6 rastreadores enviaram dados p/ Google; 3 p/ Microsoft; 2 de cada p/ Facebook, Criteo, Hubspot, Mixpanel, Twitter; 1 de cada p/ WarnerMedia, Hotjar, OneSignal, Pinterest, Wingify, TikTok, Awin	Sim + enviado para Hojar	Não	Não	10 cookies p/Microsoft; 3 cookies para Google; 2 cookies para WarnerMedia; 1 cookie cada para Twitter, getblue, Meu Dim Dim e Enviou.	Facebook Pixel; Google Analytics' 'remarketing audiences'
Dragon Learn	São Paulo	Sim	Sim	3 rastreadores enviaram dados p/ Google; 1 de cada p/ Facebook, Intercom, Yandex, Mail.Ru Group OOO, ZenDesk	Sim + enviado para Yandex	Não	Não	3 cookies p/ Google	Facebook Pixel; Google Analytics' 'remarketing audiences'

Escola Mais	São Paulo	Sim	Não	3 rastreadores enviaram dados p/ Google; 2 de cada p/ Facebook, Criteo, UOL; 1 de cada p/ Taboola, Instapage	Não	Não	Não	3 cookies p/ Google; 2 cookies p/ Taboola; 1 cookie p/ Instapage	Facebook Pixel; Google Analytics' 'remarketing audiences'
Explicaê	São Paulo	Sim	Sim	3 rastreadores enviaram dados p/ Google; 2 p/ Facebook; 1 de cada p/ Amazon, RD Gestão e Sistemas Ltda. EPP	Não	Não	Não	1 cookie p/ huggy.io	Facebook Pixel; Google Analytics' 'remarketing audiences'
Manga High	São Paulo	Sim	Sim	3 rastreadores enviaram dados p/ Google; 2 de cada p/ Facebook, Hotjar; 1 p/ Functional Software	Sim + enviado p/ Hotjar	Sim + enviado p/ Manga High	Não	Não	Facebook Pixel; Google Analytics' 'remarketing audiences'
Revisa Enem	São Paulo	Sim	Não	1 rastreador enviou dados p/ Google	Não	Não	Não	Não	Não
Stoodi	São Paulo	Sim	Sim	3 rastreadores enviaram dados p/ Google; 2 de cada p/ Facebook, Mixpanel, Datadog; 1 de cada p/ Microsoft, Crazy Egg,, Cloudflare, Hotjar, The Nielsen Company, Optomaton UG (haftungsbeschränkt), RudderLabs, Sales Analytics, omguk.com, rtb123.com, Awim, Kenshoo TLD, Ve Global	Sim + enviado p/ Hotjar	Sim + enviado para Ve Global e Stoodi	Não	15 cookies p/ Pipefy; 3 cookies p/ Google; 2 cookies p/ Microsoft; 1 cookie p/ Ve Global	Facebook Pixel; Google Analytics' 'remarketing audiences'

APP	Estado	Feito p/ crianças	Pol. de Priv.	Dados coletados no APP para:					
				Identificar o usuário (id. persistente)	Localizar o usuário	Coletar dados de contatos	Rastrear atividades do usuário	Acessar dados sensíveis (classificação Android)	Compartilhar dados com terceiros
Centro de Mídias da Educação de São Paulo	São Paulo	Sim	Sim	Não	Não	Não	Câmera e Microfone	- READ_EXTERNAL_STORAGE - WRITE_EXTERNAL_STORAGE - READ_PHONE_STATE - CAMERA - SYSTEM_ALERT_WINDOW - RECORD_AUDIO	Google Firebase Analytics; Google Crashlytics
Descomplica	São Paulo	Sim	Sim	Sim (Android Advertising ID)	Não	Não	Câmera	- READ_EXTERNAL_STORAGE - WRITE_EXTERNAL_STORAGE - CAMERA	Google Crashlytics; Google Firebase Analytics; Google AdMob; Facebook Analytics; Facebook Login; Facebook Places; Facebook

									Share; MixPanel
Explicaê	São Paulo	Sim	Sim	Não	Não	Não	Câmera	- READ_EXTERNAL_STORAGE - WRITE_EXTERNAL_STORAGE - CAMERA	Google Firebase Analytics; Google Crashlytics; Facebook Analytics; Facebook Login
Stoodi	São Paulo	Sim	Sim	Sim (Android Advertising ID; IMEI)	Não	Não	Não	- READ_EXTERNAL_STORAGE - WRITE_EXTERNAL_STORAGE - READ_PHONE_STATE	Google Crashlytics; Google Firebase Analytics; Google Tag Manager; Google Analytics Facebook Analytics; Facebook Login;

									Facebook Share; Segment

2.2 O envolvimento da Meta e do Google

[40] A tabela acima deixa explícito a participação massiva de duas empresas *big tech* no tratamento de dados de crianças e adolescentes para a publicidade direcionada: a Meta (à época ainda Facebook) e o Google.

[41] Como uma das maiores redes sociais do mundo, a **Meta** contava com mais de 3,5 bilhões de usuários mensais em seus diversos produtos em 2021. Os dados coletados pela empresa são utilizados para treinar algoritmos que determinam o que cada usuário verá em suas plataformas. Dessa forma, a empresa desempenha um papel crucial na influência das opiniões e crenças das pessoas, bem como no controle sobre o que elas podem ou não acessar online. Além disso, esses *insights* são usados para direcionar anúncios.

[42] Em setembro de 2021, um conjunto de documentos internos vazados pela *whistleblower* Frances Haugen e publicado inicialmente pelo Wall Street Journal revelou que, ao longo de três anos, pesquisadores da empresa documentaram que o Instagram estava prejudicando a saúde mental e emocional de um número significativo de seus usuários jovens.[23] Embora a empresa tenha negado a caracterização do problema feita por Haugen, nove dias depois o Facebook suspendeu o desenvolvimento de um serviço chamado Instagram Kids, voltado para crianças de até 13 anos.

[43] A HRW descobriu que 30 sites de EdTech estavam enviando dados de seus usuários para o Facebook por meio de uma tecnologia específica de rastreamento conhecida como Facebook Pixel. Essa tecnologia coleta informações sobre as atividades de estudantes e professores nesses sites e envia os dados para o Facebook. Posteriormente, o site de EdTech pode usar essas informações para direcionar anúncios no Facebook e Instagram. Além disso, o Facebook pode reter e usar esses dados para seus próprios fins publicitários. O Facebook Pixel também pode permitir que a empresa colete dados pessoais e crie chamados *shadow profiles*, isto é, perfis de pessoas que nunca usaram seus serviços ou criaram uma conta (e que muitas vezes não sabem que seus dados estão sendo tratados), gerando várias questões acerca da conformidade com a LGPD.

[44] A HRW procurou o Facebook para comentar os achados, mas além de não reconhecer que recebe dados dos produtos listados pela HRW, a empresa afirmou que cabe aos seus clientes cumprir suas políticas e as leis aplicáveis.

[45] O **Google**, por sua vez, se destaca por seu domínio incomparável sobre o mercado global de publicidade digital, sendo líder nesse segmento há mais de uma década e o inventor do modelo de negócios online baseado na coleta de dados para publicidade.[24] O enorme controle do Google sobre a publicidade online é reforçado pela predominância de seus outros serviços, que se tornaram indispensáveis para a vida digital da maioria das pessoas. Nove produtos da empresa — Android, Chrome, Gmail, Google Drive, Google Maps, Google Play Store, Google Photos, Google Search e YouTube — contam com mais de um bilhão de usuários cada.

---

[23] MAC, Ryan; KANG, Cecilia, Whistle-Blower Says Facebook 'Chooses Profits Over Safety', **Wall Street Journal**, 2021.
[24] ZUBOFF, Shoshana, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, New York: PublicAffairs, 2019.

[46] A empresa coleta dados não apenas de pessoas que usam diretamente seus serviços, mas de qualquer pessoa que encontre suas tecnologias de rastreamento incorporadas pela internet. Dos 163 produtos de EdTech examinados pela HRW, 131 produtos (80 por cento) foram encontrados com tecnologias de rastreamento embutidas desenvolvidas pelo Google.

[47] Apesar de as políticas de publicidade do Google proibirem a segmentação de crianças menores de 13 anos com publicidade comportamental ou a coleta de suas informações pessoais para esse fim, a empresa coloca a responsabilidade no desenvolvedor para seguir essas políticas. A Google também tem sua própria EdTech — O Google Workspace for Education — que já foi alvo de decisões no âmbito de dez autoridades de proteção de dados na Europa e que também está em desconformidade com a LGPD.[25]

[48] Muito recentemente, o Financial Times revelou que essas duas empresas fizeram um acordo secreto para direcionar anúncios para crianças e adolescentes no YouTube.[26] Considerando que essa prática vai além do que é detalhado pelas próprias empresas em seus Termos de Uso e Políticas de Privacidade, essa revelação demonstra não apenas a necessidade de análises técnicas e auditorias por terceiros, mas também da regulamentação dos incentivos financeiros que advêm deste modelo de negócios através da proibição do uso comercial de dados de crianças e adolescentes não alinhados ao seu melhor interesse.

3 Riscos para a proteção de dados de crianças e adolescentes na utilização de edtech

3.1 A proteção de dados de crianças e adolescentes na educação

[49] Como uma preocupação coletiva, a dataficação da infância e da adolescência apresenta desafios significativos devido às incertezas que rodeiam as suas implicações futuras. Embora alguns dos impactos a direitos humanos, especialmente em relação a discriminação e ao acesso equitativo das crianças à educação, ao emprego, ao crédito e aos serviços públicos, já sejam perceptíveis, os efeitos cumulativos a longo prazo da dataficação permanecem invisíveis. A vulnerabilidade deste grupo nos obriga a pensar nos impactos a longo prazo das tecnologias e na sociedade que estamos construindo ao datificar cidadãos desde a infância.

[50] Mais do que uma forma de promover direitos fundamentais, as tecnologias digitais são cada vez mais a porta única de entrada para a sua concretização, de forma que crianças e adolescentes, muitas vezes, não têm o direito de escolher se querem ou não utilizá-las. Pais, educadores, governos e empresas tomam decisões em seu nome e tecnologias são utilizadas em ambientes de passagem obrigatória, como na escola. Neste sentido, as oportunidades trazidas pelas tecnologias digitais precisam de ser

[25] Para um estudo de caso acerca das decisões europeias e uma descrição da (des)conformidade com a LGPD, cf. FERNANDES, Elora, **Navigating the Digital Classroom: Analyzing Risks To Children's Data Protection in Educational Technology**, Doctoral Thesis, State University of Rio de Janeiro; KU Leuven, 2024.

[26] MORRIS, Stephen; MURPHY, Hannah, Google and Meta struck secret ads deal to target teenagers, **Financial Times**, 2024.

cuidadosamente equilibradas com os riscos que representam para os direitos de crianças e adolescentes, uma vez que este grupo possui agência reduzida no seu exercício. A natureza dinâmica e em constante mudança do ambiente digital também significa que os riscos estão em evolução. Como consequência, crianças e adolescentes muitas vezes enfrentam riscos emergentes muito antes de os adultos serem capazes de analisá-los adequadamente.[27]

[51] É importante também ressaltar que os direitos fundamentais são indivisíveis e interligados. Isto significa que a realização ou violação de um afeta automaticamente outros direitos. Por exemplo, se forem tomadas medidas para proteger as crianças de potenciais danos online sem considerar simultaneamente o seu direito à liberdade de expressão, as medidas de proteção podem limitar excessivamente essa liberdade.[28] Nesse sentido, uma matriz interessante para a classificação de risco das atividades online de crianças e adolescentes é a chamada 4Cs. Com base na classificação apresentada pela EU Kids Online em 2009 e numa extensa revisão da literatura de iniciativas semelhantes, o projeto CO:RE introduz os 4Cs para a compreensão dos riscos online que as crianças enfrentam levando em consideração seus diferentes tipos e dimensões. Os 4Cs são riscos de conteúdo, contato, conduta e contrato:[29]

[52] **Riscos de Conteúdo:** A criança se envolve ou é exposta a conteúdo potencialmente prejudicial. Isso pode incluir conteúdo violento, sangrento, de ódio ou extremista, bem como conteúdo pornográfico ou sexualizado que pode ser ilegal ou prejudicial, inclusive por ser inadequado para a idade. O conteúdo online pode ser produzido em massa ou gerado por usuários (incluindo pela própria criança) e pode ser amplamente compartilhado ou não.

[53] **Riscos de Contato:** A criança experimenta ou é alvo de contato em uma interação potencialmente prejudicial **iniciada por um adulto**, que pode ser conhecido ou não pela criança. Isso pode estar relacionado a assédio (incluindo sexual), perseguição, comportamento odioso, aliciamento sexual, *sextorsão* ou à geração e compartilhamento de material de abuso sexual infantil.

[54] **Riscos de Conduta:** A criança testemunha, participa ou é vítima de conduta potencialmente prejudicial, como *bullying*, atividade odiosa **entre pares**, *trolling*, mensagens sexuais, pressões ou assédio, ou é exposta a comunidades de usuários potencialmente prejudiciais (por exemplo, relacionadas a automutilação ou distúrbios alimentares). Os riscos de conduta geralmente surgem de interações entre pares, embora não necessariamente de igual *status*.

[55] **Riscos de Contrato:** A criança participa e/ou é explorada por interesses comerciais ou contratuais potencialmente prejudiciais (jogos de azar, publicidade ou inadequado para a idade, etc.). Isso pode ser mediado pelo processamento automatizado (algorítmico) de dados. Inclui riscos ligados a serviços digitais mal desenhados ou inseguros que deixam a criança vulnerável a roubo de identidade, fraude ou golpes. Também inclui contratos

---

[27] SIIBAK, Andra; MASCHERONI, Giovanna, **Children's data and privacy in the digital age**, Hamburg: [s.n.], 2021.
[28] LIVINGSTONE, Sonia; LIEVENS, Eva; CARR, John, **Handbook for policy makers on the rights of the child in the digital environment**, [s.l.: s.n.], 2020.
[29] LIVINGSTONE, Sonia; STOILOVA, Mariya, **The 4Cs: Classifying Online Risk to Children**, Hamburg: [s.n.], 2021, p. 11.

feitos entre outras partes envolvendo uma criança (tráfico, transmissão de abuso sexual infantil).

[56] Cada tipo de risco é dividido em três dimensões relativas à sua natureza: agressivo, sexual ou relacionado a valores. Além dessas dimensões, a classificação reconhece que alguns riscos se relacionam à maioria ou a todas as quatro categorias e podem ter múltiplas manifestações nas diferentes dimensões. Estes foram considerados **riscos transversais** (que incluem riscos online relacionados com **privacidade**, saúde física ou mental, desigualdades ou discriminação), conforme ilustrado na tabela abaixo, em inglês:

CO RE	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Figura 1: Matriz de Risco 4Cs - CO:RE[30]

[57] Nestes três contextos, crianças e adolescentes enfrentam riscos de privacidade (entendida amplamente pelo estudo de forma a incorporar a proteção de dados) que, além de serem um problema em si, podem afetar outras dimensões, e por isso é considerada um risco transversal. A lista de riscos gerados a partir de questões relacionadas à privacidade/proteção de dados é extensa e inclui publicidade direcionada, danos à reputação, chantagem, perseguição, roubo de identidade, contato indesejado com estranhos, rastreamento de localização, manipulação, discriminação e decisões enviesadas, e a potencial limitação de oportunidades futuras.[31]

[58] Além dos riscos já mencionados associados ao tratamento massivo de dados pessoais de crianças e adolescentes,[32] a investigação conduzida pela HRW destaca especialmente os **riscos advindos do perfilamento desse grupo**. Quando os dados de crianças e adolescentes são utilizados para fins de perfilamento, a sua experiência online é diretamente influenciada, determinando as informações que recebem. Nos aplicativos e

[30] *Ibid.*, p. 12.

[31] LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita, **Children's data and privacy online. Growing up in a digital age: An evidence review**, [s.l.: s.n.], 2018.

[32] Para um mapeamento completo dos riscos que EdTech podem apresentar para a proteção de dados de crianças e adolescentes, cf. FERNANDES, **Navigating the Digital Classroom: Analyzing Risks To Children's Data Protection in Educational Technology**.

websites analisados pela HRW, observou-se que o perfilamento e o direcionamento de informações para crianças e adolescentes não estavam relacionados a atividades educacionais e não proporcionaram benefícios para esse público. Esses riscos são pertinentes à aplicação do art. 14, §4º, da LGPD, como será discutido na Seção 4, a seguir.

[59] O perfilamento em si, independentemente da finalidade de tratamento, pode afetar diretamente diversos direitos fundamentais de crianças. Riscos dessa automaticidade vão desde o vazamento de dados e roubo de identidade, até a limitação de oportunidades devido a erros e vieses.[33] De maneira específica, um dos principais focos do perfilamento identificado pela pesquisa foi a publicidade direcionada.[34] Durante o estágio particular de desenvolvimento de crianças e adolescentes, no qual suas habilidades cognitivas, mecanismos de inibição de impulsos e discernimento ainda estão em formação, eles são especialmente vulneráveis à publicidade e muitas vezes não conseguem identificar estratégias persuasivas.[35] Dessa forma, o risco de manipulação de crianças e adolescentes no ambiente online por meio de publicidade direcionada é extremamente elevado. Esse problema torna-se ainda mais grave em contextos onde esses indivíduos não têm a possibilidade de recusar o tratamento de seus dados pessoais, como no caso da educação.

[60] O direcionamento de conteúdo de forma geral pode ainda moldar as opiniões e crenças de crianças e adolescentes, explorando sua falta de compreensão e capacidade de tomar decisões autônomas, tanto a curto quanto a longo prazo. Isso afeta diretamente os seus direitos à liberdade de pensamento, expressão e ao acesso à informação, que são essenciais no desenvolvimento de cidadãos críticos através da educação. Uma das funções da educação é justamente assegurar que crianças e adolescentes tenham acesso às mais diversas informações e áreas do conhecimento, podendo experimentar e se desenvolver de forma aberta e não discriminatória.[36] Nesse sentido, o Comentário Geral nº 25 do Comitê sobre os Direitos da Criança[37] destaca a necessidade de as crianças poderem encontrar informações de qualidade online e independente de interesses comerciais ou políticos. Ademais, ressalta que governos devem assegurar que buscas automatizadas e filtragem de informações, incluindo através de sistemas de recomendação, não priorizem conteúdos pagos com motivação comercial ou política em relação às escolhas de crianças e adolescentes ou ao seu direito à informação.

3.2 A importância da confiança para a aprendizagem e o desenvolvimento da autonomia

[61] Uma dimensão crítica que deve ser considerada ao se avaliar os impactos da EdTech nos direitos fundamentais de crianças e adolescentes é sua influência nas oportunidades que estes atores têm de confiar e serem confiáveis. A ubiquidade das TICs digitais na

---

[33] VAN DER HOF, Simone *et al*, The Child's Right to Protection against Economic Exploitation in the Digital World, **International Journal of Children's Rights**, v. 28, n. 4, p. 833–859, 2020.

[34] Apesar de este não ter sido o foco da pesquisa, é bastante comum que outros objetivos comerciais sejam utilizados para justificar o perfilamento, como o treinamento de inteligência artificial ou o melhoramento de produtos.

[35] HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro, A proibição do direcionamento de publicidade microssegmentada para crianças e adolescente e a abusividade do uso de dados pessoais para fins de exploração comercial infanto-juvenil, *in*: LATERÇA, Priscilla *et al* (Orgs.), **Privacidade e Proteção de Dados de Crianças e Adolescentes**, Rio de Janeiro: Obliq; ITS Rio, 2021, p. 427–453.

[36] BARASSI, Veronica, **CHILD | DATA | CITIZEN**, [s.l.]: MIT Press, 2020, p. 80.

[37] 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**, [s.l.: s.n.], 2021, parag. 53.

educação, juntamente com um modelo de negócios prevalente que incentiva a coleta e mercantilização massiva de dados pessoais faz com que crianças e adolescentes sejam mergulhados em um estado constante de vigilância. Isso não se aplica apenas às tecnologias especificamente desenvolvidas para monitorar crianças em ambientes educacionais, como sistemas de monitoramento de comportamento ou *e-proctoring*. Isso também estende a tecnologias aparentemente inofensivas ou de baixo risco que fazem parte de uma rede mais ampla de partes interessadas e práticas de compartilhamento de dados, como demonstrado pelo relatório da HRW.

[62] A presença ubíqua dessas tecnologias na educação pode incentivar uma abordagem da infância e da adolescência que visa deixar pouco ao acaso e alcançar um ambiente livre de riscos. Essa abordagem ignora a importância de equilibrar confiança e risco, assim como as oportunidades para que as crianças negociem sua "liberdade" e desenvolvam certas habilidades e competências.[38]

[63] Ao criar desconforto e medo, tecnologias de vigilância têm o potencial de mudar a experiência de confiança de uma criança e até mesmo substituir relacionamentos anteriormente baseados na confiança, como aquele entre educador e educando. Como demonstrado pelas entrevistas realizadas pela HRW para o relatório e por diversos outros estudos na área,[39] crianças percebem a vigilância como um meio de controle que restringe suas opções e dificulta sua capacidade de agir de forma independente. Obter informações através da vigilância pressupõe que as crianças e adolescentes não podem ser confiáveis. A utilização de mecanismos de punição e recompensa na educação pode influenciar diretamente o comportamento da criança, que passa a ser motivada a agir de forma correta devido ao medo e não ao desenvolvimento de princípios morais e éticos. Esse tipo de orientação priva crianças e adolescentes da chance de experimentar a tomada de decisões críticas e éticas, levando, em última análise, à redução da autorregulação e autonomia.[40]

[64] Quando as crianças são monitoradas sem seu conhecimento, como demonstrado pelo relatório da HRW, isso pode ser ainda mais prejudicial. A decepção envolvida no monitoramento em segredo pode danificar a própria base da confiança que elas têm em relação a adultos. O uso de tecnologias de vigilância pode, portanto, aumentar a suspeita em vez de promover uma sensação de segurança na aprendizagem. De modo geral, crianças têm menos escolha quando se trata da necessidade de confiar nos outros. Elas estão em uma fase crucial do seu desenvolvimento para a compreensão da alteridade e da sociedade de forma mais ampla, de forma que a falta de oportunidades de exercer a confiança tem o potencial de minar o desenvolvimento de sua identidade e autoconfiança.[41]

[65] Isso também está diretamente ligado ao desenvolvimento da autonomia e da forma como crianças e adolescentes conceptualizam a privacidade e a proteção de dados pessoais. A autonomia é essencial para que indivíduos exerçam seus direitos à privacidade

---

[38] ROONEY, Tanya, Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility, **Surveillance & Society**, v. 7, n. 3/4, p. 344–355, 2010.
[39] Cf. LIVINGSTONE; STOILOVA; NANDAGIRI, **Children's data and privacy online. Growing up in a digital age: An evidence review**.
[40] NOLAN, Jason; RAYNES-GOLDIE, Kate; MCBRIDE, Melanie, The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media, **Journal of Childhood Studies**, v. 36, n. 2, p. 24–32, 2011.
[41] ROONEY, Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility.

e à proteção de dados, permitindo que tomem decisões livres de influências externas. Por outro lado, a privacidade e a proteção de dados também são cruciais para o desenvolvimento da autonomia, pois as pessoas precisam de seu próprio espaço para refletir sobre seus valores, crenças e preferências sem manipulação ou outras interferências externas. Isso é especialmente importante durante o desenvolvimento desses valores na infância e adolescência e no ambiente educacional. Se crianças e adolescentes não têm a oportunidade de experimentar espaços com privacidade e proteção de dados pessoais garantidos, a sua habilidade de estabelecer e defender seus próprios direitos (ou reconhecer os direitos de outras pessoas) encontra-se prejudicada.

[66] Na primeira infância, as crianças demonstram um desejo por privacidade e autonomia ao se engajarem em pequenos atos de independência e resistência à autoridade, como fazer bagunça, barulho ou fugir quando chamadas. A experimentação e a criatividade também dependem diretamente de privacidade e autonomia e, em última análise, é o que permite a própria evolução social. No entanto, isso nos leva a questionar se é possível cultivar a autonomia genuína em espaços onde as crianças estão sob constante vigilância e sua única forma de resistir à heteronomia é através de segredo ou subversão.[42] Se crianças e adolescentes não confiam no ambiente e nos adultos que as acompanham durante sua educação, isso as leva a participar menos por medo de errar e sofrer consequências. No entanto, cometer erros é uma parte essencial e natural do processo de aprendizado, especialmente no contexto escolar. Sem um espaço seguro para errar, corremos o risco de formar uma geração que não apenas enfrenta dificuldades na aprendizagem, mas também na construção de uma cidadania crítica e criativa, capaz de enfrentar os desafios do mundo moderno.

4. A LGPD e o regime especial para a proteção de dados de crianças e adolescentes

[67] A LGPD adota um regime especial para a proteção de dados de crianças e adolescentes em sua Seção III e pode-se dizer que esse tratamento especial é fundamentado em dois principais argumentos. Em primeiro lugar, crianças e adolescentes são um grupo mais vulnerável da população, que demanda proteção específica.

[68] No ambiente digital, todo ser humano pode ser considerado vulnerável devido à grande assimetria de poder ali existente. A vulnerabilidade sempre resulta de situações sociais em que indivíduos ou grupos são dependentes de outra pessoa ou grupo, independentemente de sua vontade. No caso do ambiente digital, agentes de tratamento frequentemente possuem mais informações sobre a pessoa a quem os dados se referem e sobre as consequências desse tratamento do que os próprios titulares dos dados.

[69] Todavia, a relação entre alguns indivíduos ou grupos e seu ambiente faz com que outras camadas de vulnerabilidade possam ser identificadas, como idade, condições de saúde, raça, gênero, nacionalidade, etc. Assim, **Luna** propõe que o conceito de vulnerabilidade seja entendido de forma dinâmica e relacional.[43] A camada extra de

---

[42] NOLAN; RAYNES-GOLDIE; MCBRIDE, The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media.

[43] LUNA, Florencia, Elucidating the Concept of Vulnerability: Layers Not Labels, **International Journal of Feminist Approaches to Bioethics**, v. 2, n. 1, p. 121–139, 2009.

vulnerabilidade relacionada à idade, no caso de crianças e adolescentes, está relacionada ao fato de que elas ainda estão se desenvolvendo fisicamente, mentalmente, emocionalmente e espiritualmente. Isso significa que elas ainda dependem, em diferentes graus, de outras pessoas para proteção, provisão e tomada de decisões.[44]

[70] O Comitê sobre os Direitos da Criança também reconhece essa vulnerabilidade e especifica que, a nível universal, todas as crianças de 0 a 18 anos são consideradas vulneráveis até a conclusão de seu crescimento e desenvolvimento neural, psicológico, social e físico. Bebês e crianças pequenas estão em ainda maior risco devido à imaturidade de seu cérebro em desenvolvimento e sua completa dependência de adultos.[45]

[71] Mais especificamente no âmbito da proteção de dados, as implicações do tratamento de dados pessoais já são complexas para o entendimento de os adultos, sendo ainda mais difíceis para crianças e adolescentes. Estes são menos experientes, especialmente em relação a possíveis riscos e danos, e podem ser facilmente manipulados. Por essa razão, sua capacidade de agir é limitada e outras pessoas frequentemente tomam decisões em seu nome. Há também uma gravidade particular nas violações dos direitos deste grupo, pois frequentemente têm impacto severo e duradouro no desenvolvimento infantil.[46] Por fim, é preciso destacar que eles têm menos meios para contestar as inferências feitas sobre eles e decisões (especialmente as automatizadas) tomadas em seu nome.

[72] Isso se relaciona à distinção entre os riscos de vulnerabilidade relacionados ao *tratamento de dados em si* e aqueles relacionados aos *resultados desse tratamento*.[47] No que se refere ao primeiro, os riscos estão relacionados à compreensão das informações sobre o tratamento de dados, o que pode dificultar, por exemplo, o consentimento livre quando necessário, bem como o exercício efetivo dos direitos de proteção de dados. Do segundo ponto de vista, a vulnerabilidade se manifesta por meio de danos específicos a que as crianças e adolescentes podem estar expostos como resultado do tratamento de seus dados, como, por exemplo, a restrição de oportunidades educacionais e de trabalho.

[73] A segunda razão pela qual um regime especial para crianças e adolescentes é necessário está ligada à pegada digital proporcionalmente maior destes sujeitos. A infância e adolescência atual começa a ser datificada antes mesmo do nascimento. Pesquisas na internet, uso de aplicativos de gravidez, postagens de imagens de ultrassom nas redes sociais e consultas médicas que geram dados sobre a saúde do nascituro são apenas alguns exemplos de como empresas e governos têm acesso cada vez mais precoce aos dados pessoais desse grupo. Após o nascimento, essa coleta de dados se intensifica com o uso de brinquedos conectados, *wearables* e outras tecnologias digitais em casa e na escola, por eles, por pais ou por terceiros. A cada ano, uma criança terá mais dados tratados sobre ela do que qualquer outra nascida em anos anteriores.[48]

---

[44] SANDBERG, Kirsten, The convention on the rights of the child and the vulnerability of children, **Nordic Journal of International Law**, v. 84, n. 2, p. 221–247, 2015.
[45] COMMITTEE ON THE RIGHTS OF THE CHILD, **General comment No. 13 (2011).The right of the child to freedom from all forms of violence. CRC/C/GC/13**, [s.l.: s.n.], 2011, parag. 72.
[46] COMMITTEE ON THE RIGHTS OF THE CHILD, **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16**, [s.l.: s.n.], 2013, parag. 24.
[47] MALGIERI, Gianclaudio; NIKLAS, Jędrzej, Vulnerable data subjects, **Computer Law and Security Review**, v. 37, 2020.
[48] YOUNG, Andrew; VERHULST, Stephan G., Why we need responsible data for children, **The Conversation**, 2020.

[74] Nas seções abaixo destrinchamos como os pilares essenciais dessa proteção especial da LGPD devem se refletir na análise do caso em questão.

4.1 O melhor interesse da criança e do adolescente como filtro para a identificação de finalidades legítimas para o tratamento de dados de crianças e adolescentes

[75] O *caput* do artigo 14, da LGPD, determina que o tratamento de dados de crianças e adolescentes deverá ser realizado em seu melhor interesse. Sendo este um conceito amplo, o Comentário Geral nº 14, de 2013, do Comitê sobre os Direitos da Criança,[49] elaborou as três funções que o princípio do melhor interesse pode desempenhar. Em primeiro lugar, é um direito fundamental autoexecutável de crianças e adolescentes a terem seu melhor interesse considerado, de forma primordial, quando uma decisão que os implique, direta ou indiretamente, seja tomada. Em segundo lugar, é um princípio jurídico interpretativo, exigindo que, diante de disposições legais sujeitas a mais de uma interpretação, seja escolhida aquela que melhor atende aos interesses de crianças e adolescentes. Por fim, é também uma regra procedimental, determinando que processos decisórios que possam afetar crianças ou adolescentes devem sempre ser precedidos de avaliação de seu impacto positivo ou negativo neste grupo. Essas funções do melhor interesse são importantes para a funcionalidade do art. 14. Isto é, para além de um direito em si, ele deve servir, dentro da LGPD, como uma lente para interpretar todos os dispositivos da lei e justificar a necessidade de realização de Relatórios de Impacto à Proteção de Dados devido ao entendimento do melhor interesse como regra de procedimento.

[76] A indeterminação e dinamicidade do princípio do melhor interesse é proposital, a fim de que seja utilizado de forma flexível nas mais diversas situações que dizem respeito a uma criança ou grupo de crianças (no conceito amplo utilizado pela Convenção, como pessoas de 0 a 18 anos). Assim, a identificação do conteúdo do melhor interesse sempre ocorre no caso concreto, a partir do balanceamento de diversos direitos da criança.

[77] É importante destacar que a análise do que significa o melhor interesse da criança em cada caso, ou seja, de seu conteúdo, não pode ser um exercício subjetivo. Tomadores de decisão não devem escolher a dedo alguns direitos que serão analisados, mas compreender os direitos na Convenção e no ordenamento brasileiro como um todo (assim como determinado pelo *caput* do art. 14, da LGPD). Isso não inclui apenas direitos de proteção (inclusive a proteção à privacidade e aos dados pessoais), mas também direitos de provisão, como o direito à liberdade de expressão, educação ou participação no ambiente digital. Esse balanceamento para a identificação do melhor interesse deve ser feito através da realização dos chamados *Children Rights Impact Assessments - CRIAs*[50] que pode ser holisticamente integrado na elaboração de RIPD.

---

[49] COMMITTEE ON THE RIGHTS OF THE CHILD, **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14**, [s.l.: s.n.], 2013.

[50] UNICEF; DANISH INSTITUTE FOR HUMAN RIGHTS, **Children's Rights in Impact Assessments. A guide for integrating children's rights into impact assessments and taking action for children**, [s.l.: s.n.], 2013; MUKHERJEE, Sudeshna; POTHONG, Kruakae; LIVINGSTONE, Sonia, **Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment**, [s.l.: s.n.], 2021; COMMITTEE ON THE RIGHTS OF THE CHILD, **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16**; HOF, Simone van der; LIEVENS, Eva, The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR,

[78] Apesar de o Comitê não prescrever o que é do melhor interesse da criança em determinada situação, pois isso varia caso a caso, ele fornece parâmetros que devem ser utilizados por aqueles que tomam estas decisões. São eles: a) A natureza universal, indivisível, interdependente e inter-relacionada dos direitos das crianças; b) O reconhecimento das crianças como titulares de direitos; c) A natureza global e o alcance da Convenção; d) A obrigação dos Estados Partes de respeitar, proteger e cumprir todos os direitos na Convenção; e) Os efeitos de curto, médio e longo prazo das ações relacionadas ao desenvolvimento da criança ao longo do tempo.

[79] Destaquemos alguns destes critérios no caso a que se refere esta contribuição. Em primeiro lugar, a análise dos impactos relativos a um tratamento de dados pessoais deve sempre levar em consideração a natureza universal, indivisível, interdependente e inter-relacionada dos direitos das crianças. Isso quer dizer que oportunidades devem ser balanceadas com riscos do tratamento em relação a todos os direitos presentes na Convenção e no ordenamento jurídico brasileiro.

[80] Em segundo lugar, deve-se analisar não apenas os efeitos de curto prazo, mas, em especial, aqueles de médio e longo prazo que possam afetar o desenvolvimento, oportunidades e interesses da criança ou adolescente ao longo de sua vida. Aqui destaca-se como o melhor interesse deve ser visto como um princípio de precaução, que requer a avaliação da possibilidade de risco e dano futuros e outras consequências da decisão para os direitos da criança.[51] Essa compreensão obriga controladores a agir com cautela, mesmo quando o potencial perigo de uma determinada tecnologia não está totalmente estabelecido, mas há indicações de que não agir neste momento poderia causar danos. Isso é especialmente importante no caso de tecnologias cujos benefícios não são confirmados por evidências científicas.[52] Assim, o princípio de precaução inverte a lógica e acrescenta importância à verificação de que a tecnologia traz, de fato, benefícios, ao invés de apenas provar que ela realmente causa ou pode causar danos no futuro.

[81] Aplicando-se esses dois primeiros critérios ao caso em questão, o tratamento de dados para fins comerciais e, mais especificamente, para o perfilamento comercial de crianças e adolescentes identificados pela HRW, não traz qualquer benefício aos direitos de crianças e adolescentes. Os riscos, como sumarizados na seção anterior, são graves e extensos, podendo gerar efeitos imediatos e futuros como discriminação e restrição de oportunidades para crianças e adolescentes.

[82] Em terceiro lugar, Estados estão vinculados diretamente pela Convenção e devem realizar todos os esforços necessários para realizar os direitos fundamentais de crianças e adolescentes. Isso é extremamente importante quando se trata de serviços públicos essenciais e de atendimento obrigatório como a educação. Neste sentido, crianças e adolescentes possuem quase nenhum poder de barganha em relação às tecnologias utilizadas na sua educação e no tratamento de seus dados pessoais. Assim, o Estado deve ter responsabilidade redobrada não apenas em relação às tecnologias por eles

---

Communications Law: The Journal of Computer, Media and Telecommunications Law, v. 23, n. 1, p. 33–43, 2018.

[51] COMMITTEE ON THE RIGHTS OF THE CHILD, **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14**, parag. 74.

[52] LIEVENS, Eva, Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights, **Nordic Journal of Human Rights**, v. 39, n. 2, p. 128–145, 2021.

desenvolvidas, mas também aquelas de organizações terceiras licitadas ou amplamente utilizadas. Nesse sentido, é essencial que a investigação leve em consideração a responsabilidade das respectivas secretarias de educação que deveriam agir como controladoras e se responsabilizar pelas finalidades e meios de tratamento de dados dos estudantes.

[83] A partir do reconhecimento da eficácia horizontal dos direitos humanos e da necessidade de empresas respeitarem esses direitos conforme os Princípios Orientadores de Empresas e Direitos Humanos da ONU,[53] bem como dos requisitos específicos apresentada pelo *caput* do art. 14 da LGPD e pelo artigo 227 da CRFB, o setor privado também tem a obrigação de respeitar e ativamente promover o melhor interesse da criança. A pesquisa da HRW demonstrou que, ao contrário, as empresas envolvidas não apenas não promoveram os direitos dos estudantes em questão, mas nem sequer os respeitaram.

[84] Após a realização do exercício de identificação do que é de melhor interesse da criança, a partir dos critérios desenvolvidos acima, este deve ser considerado com absoluta prioridade (art. 227, CRFB). Abstratamente, isso não quer dizer que outros direitos (especialmente quando relacionados ao interesse público), não possam eventualmente prevalecer sobre os direitos da criança e do adolescente. Contudo, o melhor interesse deve ser uma consideração primária ao tomar uma decisão e não apenas um dos critérios a serem ponderados. Isso significa que outro interesse precisa sobrepujar significativamente o interesse da criança ou adolescente para prevalecer em um exercício de balanceamento. Isso reforça a necessidade de realização do CRIA junto do RIPD não apenas para levar a cabo esse exercício, mas também fornecer provas deste com base no princípio da responsabilização e prestação de contas.

[85] Isso está diretamente ligado ao impacto do melhor interesse na caracterização do que é considerada uma finalidade legítima, como disposto no art. 6º, I, da LGPD. Esse critério vai além da mera existência de base legal na LGPD e deve considerar a legalidade mais ampla do tratamento de dados pessoais. Isso inclui, além do *caput* do artigo 14, todo o arcabouço jurídico de proteção de crianças e adolescentes. Assim, só deve ser considerada legítima a finalidade de tratamento caso ela leve em consideração o melhor interesse da criança e do adolescente.

[86] Um exemplo claro de situação em que o melhor interesse da criança deve sempre prevalecer é o caso de tratamento de dados para fins comerciais, que muito frequentemente não coincidem com os interesses e direitos de crianças, como pode ser destacado no caso em questão. Em seu Comentário Geral 25,[54] o Comitê destacou como os interesses comerciais podem impactar negativamente os direitos das crianças à informação independente (para. 53), a liberdade de expressão (para. 61) e o direito das crianças de brincar (para. 110). Outros exemplos de direitos afetados pelo uso de dados para fins comerciais incluem o direito à proteção contra a exploração econômica, o direito à não discriminação, ao desenvolvimento, à saúde e à educação.

---

[53] UNITED NATIONS HUMAN RIGHTS. OFFICE OF THE HIGH COMMISSIONER, **Guiding Principles on Business and Human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. HR/PUB/11/04**, [s.l.: s.n.], 2011.

[54] 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**.

[87] No caso em questão, a HRW identificou que grande parte dos aplicativos e websites em questão estavam perfilando crianças para fins comerciais e, mais especificamente, para o direcionamento de publicidade direcionado. De maneira geral, entende-se que a publicidade para crianças em qualquer mídia já é prática abusiva no Brasil.[55] De forma específica a publicidade direcionada, que ocorre através do perfilamento de crianças e adolescentes, não está alinhada com o seu melhor interesse e, portanto, também pode ser considerada abusiva. Nesse sentido, em seu Comentário Geral Nº 25[56], o Comitê sobre os Direitos da Criança defende que Estados Membros proíbam o uso de perfilamento de crianças e adolescentes para finalidades comerciais, incluindo dados coletivos ou de grupos. Assim, a finalidade de perfilamento para fins comerciais no âmbito dos aplicativos e sites analisados pela HRW não pode ser considerada legítima de acordo com o art. 6º, I, em consonância com o art. 14, *caput*, da LGPD.

[88] De fato, o perfilamento pode ocorrer para diversas finalidades no ambiente digital que não necessariamente para fins comerciais ou de publicidade de forma específica, como no caso de tecnologias de educação que buscam aplicar metodologias de ensino personalizado. Neste caso, é essencial que o agente de tratamento demonstre que este perfilamento de crianças é indispensável para alcançar uma finalidade consistente com os seus melhores interesses. Ademais, essa indispensabilidade deve ser baseada em evidências científicas claras e no princípio da precaução (o que, como defendido em outra instância, não é o caso de tecnologias de ensino personalizado[57]). Isso, pois o perfilamento em si, independentemente da finalidade de tratamento, pode afetar diretamente diversos direitos de crianças, como descrito anteriormente. Riscos dessa automaticidade vão desde o vazamento de dados e roubo de identidade, até a limitação de oportunidades devido a erros e vieses.[58]

[89] Destaca-se, ainda, que os aplicativos e websites analisados pela HRW, para além de perfilarem crianças e adolescentes para finalidades de publicidade direcionada, compartilharam esses dados com empresas terceiras de AdTech sem que isso estivesse alinhado diretamente ao melhor interesse dos estudantes, o que também não pode ser considerado uma finalidade legítima.

4.2 Uma interpretação mais restritiva ao princípio da necessidade no tratamento de dados de crianças e adolescentes

[90] O art. 6º, III, da LGPD, determina que o tratamento de dados pessoais deve ser restringido ao mínimo necessário, relevante, proporcional e não excessivo para alcançar os fins especificados pelos controladores. No entanto, além de reforçar esse princípio, o art. 14, §4º, vai além ao utilizar a expressão "estritamente necessário para a atividade".

[91] De maneira geral, o princípio da necessidade disposto no art. 6º está intrinsecamente relacionado ao princípio da finalidade e não existe por si só. Isto é, o que é considerado

---

[55] HENRIQUES; MEIRA; HARTUNG, A proibição do direcionamento de publicidade microssegmentada para crianças e adolescente e a abusividade do uso de dados pessoais para fins de exploração comercial infanto-juvenil.
[56] 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**, parag. 42.
[57] FERNANDES, Elora, Ensino personalizado: desafios à proteção de dados de crianças e adolescentes, *in*: FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sergio (Orgs.), **Privacidade e Proteção de Dados de Crianças e Adolescentes**, 2. ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS-Rio), 2024.
[58] VAN DER HOF *et al*, **The Child's Right to Protection against Economic Exploitation in the Digital World.**

necessário sempre dependerá da finalidade para o tratamento de dados pessoais (que, como demonstrado acima, deve estar alinhada ao melhor interesse da criança e do adolescente). Assim, caso a finalidade seja legítima e o controlador tenha uma base legal para tratar os dados necessários para essa finalidade, basta que ele a anuncie em sua política de privacidade e esteja em conformidade com o restante da LGPD.

[92] Todavia, o art. 14, §4º, apresenta regra mais restritiva para o tratamento de dados de crianças (titulares de que se trata o §1º do art. 14). Este dispositivo dispõe que os controladores não deverão condicionar a sua participação em jogos, aplicações de internet ou outras atividades ao fornecimento de informações para além das estritamente necessárias à atividade. O legislador cita jogos e aplicações de internet como exemplos de atividades (tendo em vista os ter inserido logo antes da expressão "ou outras atividades"). Assim, entende-se que não se trata de dados necessário a determinada *finalidade* de tratamento de dados, mas sim de tratamento necessário para a aplicação prática ou funcional específica, para o serviço ou produto mais amplo que requer o tratamento de dado pessoal. Embora essa atividade possa envolver diversas finalidades de tratamento, os dados coletados, observados ou inferidos devem ter uma relação direta com a atividade em questão.

[93] Tomemos como exemplo hipotético um aplicativo educacional que tem como objetivo (ou como atividade principal) o fornecimento de exercícios de revisão do conteúdo testado na prova do ENEM. Uma situação clara de tratamento em desconformidade com o art. 14, §4º, seria o aplicativo querer coletar a localização do usuário. Este dado não é necessário para fornecer exercícios de revisão, pois não tem relação direta com a funcionalidade principal do aplicativo. Em outro exemplo, o aplicativo gostaria de tratar dados para personalizar a experiência do usuário e sugerir websites relacionados. Dependendo do caso concreto, isso pode até ser uma finalidade legítima e alinhada ao melhor interesse da criança. Todavia, esses dados podem não ser indispensáveis para a função básica do aplicativo de oferecer exercícios de revisão e, portanto, não estariam alinhados ao art. 14, §4º.

[94] O art. 14, §4º privilegia de forma estrita e ao máximo a minimização do tratamento de dados de crianças, a fim de que a coleta e o uso de informações sejam limitados ao que é essencial para a atividade principal. Portanto, os dados pessoais coletados devem aderir estritamente ao que é indispensável e justificável,[59] o que também está alinhado ao princípio da boa-fé. Isso diminui os riscos que advêm da própria coleta de dados pessoais de forma excessiva, reduzindo chances de tratamento ilegal de dado pessoal e de danos aos direitos fundamentais.

[95] Destaca-se que essa interpretação mais restritiva em relação aos princípios da finalidade e necessidade é uma tendência mundial. Já em seu comentário sobre o princípio da finalidade em 2013, o Article 29 Data Protection Working Party (WP29), antecessor do European Data Protection Board, já afirmava que quanto mais sensível o dado (e, no documento, isso é estendido para dados de crianças e adolescentes), mais

[59] ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Julia, Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD, *in*: LATERÇA, Priscilla *et al* (Orgs.), **Privacidade e Proteção de Dados de Crianças e Adolescentes**, Rio de Janeiro: Obliq; ITS Rio, 2021.

restrita deve ser a interpretação destes princípios, inclusive para a análise de finalidades compatíveis quando do uso secundário de dados.[60]

[96] No âmbito dos EUA, a Federal Trade Commission (FTC), responsável pela aplicação do COPPA, publicou uma *Notice of Proposed Rulemaking* (NPRM) a fim de propor mudanças à legislação. De acordo com a FTC Chair, Lina M. Khan, crianças devem poder brincar e aprender no ambiente digital sem serem rastreadas por empresas que procuram rentabilizar os seus dados pessoais. A proposta impõe obrigações diretas aos prestadores de serviços, incluindo a proibição do uso comercial de dados de crianças — inclusive para o desenvolvimento de serviços; a proibição de condicionar a participação de uma criança em um serviço digital à coleta de informações pessoais (o que está diretamente alinhado ao art. 14, §4º, da LGPD), e limites para incentivar crianças a permanecerem online.[61]

[97] Os aplicativos e websites analisados pela HRW não coletaram apenas os dados necessários para a atividade em questão, isto é, para a provisão das atividades educacionais. Foram coletados dados de forma excessiva e para finalidades ilegítimas, como perfilamento de estudantes e o compartilhamento de dados com terceiros. Assim, para além de não tratar dados para finalidades legítimas, esses dados também não eram necessários para as atividades educacionais propostas pelas aplicações, o que vai de encontro com o art. 14, §4º, da LGPD.

5. Conclusão

[98] As Tecnologias da Informação e Comunicação (TICs) digitais têm sido parte integrante da educação há décadas, mas a pandemia de Covid-19 precipitou uma adoção acelerada de EdTechs para garantir a continuidade das atividades educacionais em todo o mundo. No Brasil, os governos estaduais enfrentaram essa transição repentina sem o devido preparo e o debate público sobre a escolha dessas tecnologias foi praticamente inexistente. Com frequência, as razões por trás da adoção das EdTechs pelas secretarias de educação não consideraram a proteção dos dados pessoais de crianças e adolescentes, sendo muitas vezes guiadas por argumentos financeiros, conforme apontado pela última pesquisa TIC Educação.

[99] A investigação levada a cabo pela HRW revela as graves consequências de políticas públicas que desconsideram uma análise aprofundada sobre o tratamento de dados por essas tecnologias e os impactos sobre os direitos fundamentais das crianças e adolescentes. Isso é particularmente preocupante na educação básica, um espaço crucial para o desenvolvimento de cidadãos críticos e autônomos, cuja frequência é obrigatória no Brasil, e onde o uso de EdTechs é muitas vezes compulsório.

[100] Embora os riscos associados à coleta massiva de dados pelas EdTechs sejam variados e complexos, a HRW destacou especificamente os perigos do perfilamento de crianças e adolescentes para fins comerciais, especialmente para publicidade direcionada. Essa prática foi identificada em todas as tecnologias desenvolvidas ou recomendadas pelas

---

[60] WP29, **Opinion 03/2013 on purpose limitation**, [s.l.: s.n.], 2013, p. 25.

[61] FEDERAL TRADE COMMISSION (FTC), **FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data**, disponível em: <https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>. acesso em: 25 dez. 2023.

secretarias de educação de Minas Gerais e São Paulo, e não estava relacionada às atividades educacionais, tampouco gerava qualquer benefício aos direitos fundamentais de estudantes.

[101] O perfilamento, por si só, independentemente da finalidade, pode afetar diretamente vários direitos fundamentais das crianças, como discutido na seção 3 deste estudo. No entanto, quando é realizado para fins de publicidade direcionada, torna-se ainda mais abusivo, considerando o estágio de desenvolvimento cognitivo de crianças e adolescentes, que muitas vezes são incapazes de distinguir entre estratégias de *marketing* e conteúdos autênticos e orgânicos.

[102] Ao se analisar o caso à luz da LGPD, duas questões se destacam. Primeiro, as Secretarias de Educação e as empresas de EdTech, atuando como controladoras conjuntas, parecem estar em desacordo com o art. 6, I e o art. 14, caput da LGPD, pois o tratamento de dados para fins de perfilamento comercial e compartilhamento com empresas de AdTech não está alinhado com o melhor interesse das crianças e adolescentes, tornando a finalidade ilegítima.

[103] Em segundo lugar, a HRW não conseguiu identificar como os dados tratados estão alinhados com as atividades educacionais das EdTechs, o que configura uma clara violação ao art. 14, §4º, da LGPD. Este artigo enfatiza rigorosamente a minimização do tratamento de dados de crianças desde a coleta, exigindo que os controladores não condicionem a participação das crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais que não sejam estritamente necessárias para a atividade em questão.

[104] A educação é a pedra angular de qualquer sociedade contemporânea. Mais do que um elemento isolado utilizado como ferramenta para adquirir conhecimento e habilidades, a educação desempenha um papel multiplicador no progresso da humanidade e é a base sobre a qual todas as outras esferas da sociedade são construídas. A forma como as crianças são educadas molda o potencial de desenvolvimento de qualquer população, o que torna cada decisão tomada nesse ambiente altamente política por consequências graves em curto, médio e longo prazo.

[105] Assim, a análise da HRW evidencia não apenas uma falta de alinhamento com a LGPD e com a soberania digital brasileira, mas também a necessidade urgente de um debate mais amplo e informado sobre a escolha e implementação de EdTechs nas escolas brasileiras. Garantir que o tratamento de dados respeite os direitos fundamentais dos estudantes não é apenas uma questão de conformidade legal, mas de ética e responsabilidade social, essencial para a construção de um ambiente educacional seguro, equitativo e que favoreça o desenvolvimento pleno e o florescimento da geração atual.

Referências

AMIEL, Tel; PEZZO, Thiago; DA CRUZ, Leonardo Ribeiro; *et al*. Os modos de adesão e a abrangência do capitalismo de vigilância na educação brasileira. **Perspectiva**, v. 39, n. 3, p. 1–22, 2021.

ANPD. **ANPD reúne-se com a Human Rights Watch para tratar da proteção de dados pessoais de crianças e adolescentes**. Disponível em: <https://www.gov.br/anpd/pt-

br/assuntos/noticias/anpd-reune-se-com-a-human-rights-watch-para-tratar-da-protecao-de-dados-pessoais-de-criancas-e-adolescentes>. Acesso em: 13 ago. 2024.

BARASSI, Veronica. **CHILD | DATA | CITIZEN**. [s.l.]: MIT Press, 2020.

BRAZILIAN NETWORK INFORMATION CENTER. **2022 ICT in Education. Survey on the Use of Information and Communication Technologies in Brazilian Schools**. São Paulo: [s.n.], 2023. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20231122132216/tic_educacao_2022_livro_completo.pdf>. Acesso em: 11 dez. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 13 (2011).The right of the child to freedom from all forms of violence. CRC/C/GC/13**. [s.l.: s.n.], 2011. Disponível em: <https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.13_en.pdf>. Acesso em: 23 jun. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14**. [s.l.: s.n.], 2013.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16**. [s.l.: s.n.], 2013. Disponível em: <https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.16.pdf>. Acesso em: 8 jul. 2023.

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**. [s.l.: s.n.], 2021. Disponível em: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>. Acesso em: 26 jun. 2023.

COURSERA. **2021 Impact Report. Serving the world through learning**. [s.l.: s.n.], 2021. Disponível em: <https://about.coursera.org/press/wp-content/uploads/2021/11/2021-Coursera-Impact-Report.pdf>. Acesso em: 12 nov. 2023.

CRUZ, Leonardo Ribeiro da; VENTURINI, Jamila Rodrigues. Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. **Revista Brasileira de Informática na Educação**, v. 28, p. 1060–1085, 2020.

DERECHOS DIGITALES; PRIVACY INTERNATIONAL. **Stakeholder Report. Universal Periodic Review 41st Session -Brazil**. [s.l.: s.n.], 2022. Disponível em: <https://privacyinternational.org/sites/default/files/2022-11/Final%20Brazil%20UPR.pdf>. Acesso em: 1 nov. 2023.

FEDERAL TRADE COMMISSION (FTC). **FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data**. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>. Acesso em: 25 dez. 2023.

FERNANDES, Elora. Ensino personalizado: desafios à proteção de dados de crianças e adolescentes. *In*: FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sergio (Orgs.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. 2. ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS-Rio), 2024.

FERNANDES, Elora. **Navigating the Digital Classroom: Analyzing Risks To Children's Data Protection in Educational Technology**. Doctoral Thesis, State University of Rio de Janeiro; KU Leuven, 2024.

GRAND VIEW RESEARCH. **Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 - 2030**. [s.l.: s.n.], 2023. Disponível em: <https://www.grandviewresearch.com/industry-analysis/education-technology-market>. Acesso em: 12 nov. 2023.

HAN, Hye Jung. **Empresa brasileira toma providências para proteger estudantes de vigilância de dados**. Human Rights Wtach. Disponível em: <https://www.hrw.org/pt/news/2023/04/04/brazilian-company-moves-shield-students-data-surveillance>. Acesso em: 15 ago. 2024.

HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro. A proibição do direcionamento de publicidade microssegmentada para crianças e adolescente e a abusividade do uso de dados pessoais para fins de exploração comercial infanto-juvenil. *In*: LATERÇA, Priscilla; FERNANDES, Elora; TEFFÉ, Chiara de; *et al* (Orgs.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Obliq; ITS Rio, 2021, p. 427–453. Disponível em: <https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>. Acesso em: 3 nov. 2023.

HOF, Simone van der; LIEVENS, Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children´s personal data under the GDPR. **Communications Law: The Journal of Computer, Media and Telecommunications Law**, v. 23, n. 1, p. 33–43, 2018. Disponível em: <https://infolawcentre.blogs.sas.ac.uk/files/2018/03/Comms_Law_23.1.pdf>. Acesso em: 16 jul. 2023.

HOLMES, Wayne. **The Unintended Consequences of Artificial Intelligence**. [s.l.: s.n.], 2023. Disponível em: <https://www.ei-ie.org/en/item/28115:the-unintended-consequences-of-artificial-intelligence-and-education>. Acesso em: 21 out. 2023.

HOLONIQ EDUCATION INTELLIGENCE UNIT. **Global EdTech market to reach $404B by 2025 - 16.3% CAGR**. HolonIQ. Disponível em: <https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025>. Acesso em: 12 nov. 2023.

HUMAN RIGHTS WATCH. **Brasil: ferramentas de educação online coletam dados de crianças**. Disponível em: <https://www.hrw.org/pt/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data>. Acesso em: 13 ago. 2024.

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**. [s.l.: s.n.], 2022.

HUMAN RIGHTS WATCH. **Students Not Products**. Disponível em: <https://www.hrw.org/StudentsNotProducts>. Acesso em: 13 ago. 2024.

LIEVENS, Eva. Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children´s Rights. **Nordic Journal of Human Rights**, v. 39, n. 2, p. 128–145, 2021.

LIVINGSTONE, Sonia; LIEVENS, Eva; CARR, John. **Handbook for policy makers on the rights of the child in the digital environment**. [s.l.: s.n.], 2020. Disponível em:

<https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>. Acesso em: 26 jun. 2023.

LIVINGSTONE, Sonia; STOILOVA, Mariya. **The 4Cs: Classifying Online Risk to Children**. Hamburg: [s.n.], 2021. Disponível em: <www.ssoar.infoEvidence.https://doi.org/10.21241/ssoar.71817>.

LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. **Children's data and privacy online. Growing up in a digital age: An evidence review**. [s.l.: s.n.], 2018. Disponível em: <https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf>. Acesso em: 25 jul. 2023.

LUNA, Florencia. Elucidating the Concept of Vulnerability: Layers Not Labels. **International Journal of Feminist Approaches to Bioethics**, v. 2, n. 1, p. 121–139, 2009. Disponível em: <https://www.jstor.org/stable/40339200>.

MAC, Ryan; KANG, Cecilia. Whistle-Blower Says Facebook 'Chooses Profits Over Safety'. **Wall Street Journal**, 2021. Disponível em: <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>. Acesso em: 15 ago. 2024.

MALGIERI, Gianclaudio; NIKLAS, Jędrzej. Vulnerable data subjects. **Computer Law and Security Review**, v. 37, 2020.

MORRIS, Stephen; MURPHY, Hannah. Google and Meta struck secret ads deal to target teenagers. **Financial Times**, 2024. Disponível em: <https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8?countryCode=BEL>. Acesso em: 11 ago. 2024.

MUKHERJEE, Sudeshna; POTHONG, Kruakae; LIVINGSTONE, Sonia. **Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment**. [s.l.: s.n.], 2021. Disponível em: <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf>. Acesso em: 10 abr. 2024.

NOLAN, Jason; RAYNES-GOLDIE, Kate; MCBRIDE, Melanie. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. **Journal of Childhood Studies**, v. 36, n. 2, p. 24–32, 2011.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Educação em um cenário de plataformização e de economia de dados: parcerias e assimetrias**. São Paulo: [s.n.], 2022. Disponível em: <https://cgi.br/media/docs/publicacoes/1/20221129114057/educacao_em_um_cenario_de_plataformiza%C3%A7ao_e_de_economia_de_dados_parcerias_e_assimetrias.pdf>. Acesso em: 31 out. 2023.

O'REILLY, Tim; STRAUSS, Ilan; MAZZUCATO, Mariana. **Algorithmic Attention Rents: A theory of digital platform market power**. [s.l.: s.n.], 2023. Disponível em: <https://www.ucl.ac.uk/bartlett/public-purpose/wp2023-10>.

PANGARKAR, Tajammul. Eye-Opening EdTech Statistics: Opportunities and Obstacles. **Market.US**, 2023. Disponível em: <https://scoop.market.us/edtech-statistics/>. Acesso em: 12 nov. 2023.

ROONEY, Tanya. Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility. **Surveillance & Society**, v. 7, n. 3/4, p. 344–355, 2010.

SANDBERG, Kirsten. The convention on the rights of the child and the vulnerability of children. **Nordic Journal of International Law**, v. 84, n. 2, p. 221–247, 2015.

SIIBAK, Andra; MASCHERONI, Giovanna. **Children's data and privacy in the digital age**. Hamburg: [s.n.], 2021. Disponível em: <https://www.ssoar.info/ssoar/bitstream/handle/document/76251/ssoar-2021-siibak_et_al-Childrens_data_and_privacy_in.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-siibak_et_al-Childrens_data_and_privacy_in.pdf>. Acesso em: 30 dez. 2023.

UNICEF; DANISH INSTITUTE FOR HUMAN RIGHTS. **Children's Rights in Impact Assessments. A guide for integrating children's rights into impact assessments and taking action for children**. [s.l.: s.n.], 2013. Disponível em: <https://sites.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf>. Acesso em: 9 jul. 2023.

UNITED NATIONS HUMAN RIGHTS. OFFICE OF THE HIGH COMMISSIONER. **Guiding Principles on Business and Human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework. HR/PUB/11/04**. [s.l.: s.n.], 2011. Disponível em: <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>. Acesso em: 9 jul. 2023.

VAN DER HOF, Simone; LIEVENS, E.; MILKAITE, I.; *et al*. The Child's Right to Protection against Economic Exploitation in the Digital World. **International Journal of Children's Rights**, v. 28, n. 4, p. 833–859, 2020.

WALKER, Christopher. Unlocking the impact of edtech. **impactInvestor**, 2023. Disponível em: <https://impact-investor.com/unlocking-the-impact-of-edtech/>. Acesso em: 23 dez. 2023.

WP29. **Opinion 03/2013 on purpose limitation**. [s.l.: s.n.], 2013. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 18 jul. 2023.

YOUNG, Andrew; VERHULST, Stephan G. Why we need responsible data for children. **The Conversation**, 2020. Disponível em: <https://theconversation.com/why-we-need-responsible-data-for-children-134052>. Acesso em: 24 jun. 2023.

ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Julia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. *In*: LATERÇA, Priscilla; FERNANDES, Elora; TEFFÉ, Chiara de; *et al* (Orgs.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Obliq; ITS Rio, 2021. Disponível em: <https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes/>. Acesso em: 5 out. 2023.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.