Contribuições da Data Privacy Brasil para a Tomada de Subsídios de Tratamento de Dados Pessoais de Crianças e Adolescentes da Autoridade Nacional de Proteção de Dados Pessoais

2024

DataPrivacyBR
Research

Ficha técnica

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo.

Fundada em 2018, a Data Privacy Brasil Ensino surge como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para um linguagem mais prática, com exercícios e estudos de caso, esta é uma escola para todos aqueles que se interessam e querem se aprofundar na rica temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva da justiça social e assimetrias de poder.

A partir de 2023, as duas instituições se unem para formar uma única organização, mantendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos uma sociedade democrática onde as tecnologias estejam à serviço da autonomia e dignidade das pessoas.

www.dataprivacy.com.br
www.dataprivacybr.org

Direção
Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação
Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe
Alicia Lobato, Eduarda Costa, Eduardo Mendonça, Gabriela Vergili, Horrara Moreira, Isabela Gomes, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Júlia Mendonça, Louise Karczeski, Matheus Arcanjo, Mekebib Assefa, Nathan Paschoalini, Otávio Almeida, Pedro Henrique, Rafael Guimarães, Rafael Regatieri, Rennan Willian, Roberto Junior, Rodolfo Rodrigues e Vinicius Silva

Imprensa
Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacybr.org

Como citar esse documento
RODRIGUES, Carla; MENDONÇA, Eduardo; MENDONÇA, Julia; ZANATTA, Rafael. Contribuições da Data Privacy Brasil para a Tomada de Subsídios de Tratamento de Dados Pessoais de Crianças e Adolescentes da Autoridade Nacional de Proteção de Dados Pessoais. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024.

Introdução

Em junho de 2024, a Autoridade Nacional de Proteção de Dados (ANPD) abriu a Tomada de Subsídios para o Projeto Regulatório sobre o Tratamento de Dados de Crianças e Adolescentes. O objetivo é embasar a análise e a proposição de projeto regulatório a respeito desse grupo de titulares.

A ANPD já analisou o tema em outras oportunidades. Em setembro de 2022, foi disponibilizada uma Consulta Pública que resultou no "Enunciado CD/ANPD nº 01/2023", que uniformizou a interpretação sobre as hipóteses legais aplicáveis ao tratamento de dados dos mais jovens. Posteriormente, a ANPD publicou guia orientativo sobre a hipótese legal do legítimo interesse, que buscou esclarecer alguns pontos da sua utilização no caso de crianças e adolescentes.

Este documento apresenta as contribuições da Data Privacy Brasil à Autoridade Nacional de Proteção de Dados Pessoais na Tomada de Subsídios de 2024. Valendo-se de um trabalho de mais de quatro anos no tema de proteção de dados pessoais e direitos das crianças[1], a Data Privacy Brasil reafirma a centralidade deste tema para a agenda de proteção de dados pessoais no Brasil.

Importante destacar que a Data Privacy Brasil tem atuado consistentemente no tema de proteção de crianças e adolescentes, em diálogo com a ANPD. Em dezembro de 2022, enviamos contribuição à Tomada de Subsídios sobre Tratamento de Dados de Crianças e Adolescentes, em conjunto com a Comissão de Defesa dos Direitos das Crianças e dos Adolescentes da Ordem dos Advogados do Brasil, Seccional de São Paulo[2]. Este trabalho apoiou-se nos resultados de uma longa pesquisa realizada em conjunto com o Instituto Alana e a *Asociación por los Derechos Civiles* de Buenos Aires, lançada na conferência *Computers, Data Protection and Privacy* (CPDP), edição América Latina, em junho de 2022[3].

---

1 Ver https://www.dataprivacybr.org/projeto/protecao-de-dados-pessoais-e-infancia.

2 DATA PRIVACY BRASIL & OAB-SP. **Contribuição à Tomada de Subsídios sobre Tratamento de Dados de Crianças e Adolescentes**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/12/tomada-subsidios-infancia.pdf. Acesso em: 12 ago. 2024..

3 ADC; DATA PRIVACY BRASIL; INSTITUTO ALANA. **Dados e direitos da infância e adolescência no ambiente digital: caminhos para proteção jurídica no Brasil e Argentina**. São Paulo: Instituto Alana, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/07/Dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital_VF-ACES.pdf. Acesso em: 12 ago. 2024.

Em 2023, elaboramos a contribuição na participação na consulta aberta aberta pela ANPD acerca do Estudo Preliminar sobre Legítimo Interesse. Na ocasião, pedimos uma atuação mais ampla e concreta por parte da ANPD no tema[4]. Argumentamos que, além de determinar o dever de demonstrar o cumprimento do melhor interesse, a Autoridade deveria indicar formas de como isso pode ser realizado de forma documentada através de diferentes metodologias, como o "Children's Rights Impact Assessment (CRIA)". Em outras palavras, pedimos uma *procedimentalização mais robusta da demonstração de melhor interesse*, que não pode ser algo meramente retórico. Tal procedimentalização exige processos, documentação e análise substancial de interesses em casos concretos.

Nesta contribuição de 2023 também nos manifestamos no sentido de que, diante da condição peculiar de desenvolvimento dos titulares em questão, que tem garantida pela Constituição sua proteção integral, com prioridade absoluta, fosse adotada uma postura mais prescritiva no estudo preliminar da ANPD, sendo fornecidas orientações diretas e claras a serem cumpridas, no lugar de se limitar a "indicar tendências"[5].

Entendemos que a colocação do tema de proteção de crianças e adolescentes na Agenda Regulatória da Autoridade Nacional de Proteção de Dados Pessoais é uma escolha acertada e necessária. Além dos regramentos constitucionais e do Estatuto da Criança e Adolescente, o Brasil possui normas específicas no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais que tratam de direitos fundamentais das crianças e adolescentes com relação ao uso de tecnologias.

Em abril de 2024, o Conselho Nacional dos Direitos das Crianças e dos Adolescentes (Conanda) editou a Resolução n. 245/2024, uma norma crucial para direitos das crianças e adolescentes em ambiente digital. Esta norma dialoga com o Marco Legal da Primeira Infância (Lei 13.257/2016), com o Código de Defesa do

---

4 MENDONÇA, Julia; LOBO MARTINS, Pedro; MARTINS DOS SANTOS, Pedro Henrique. **Contribuição da Data Privacy Brasil sobre Legítimo Interesse**. São Paulo: Data Privacy Brasil, 2023. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2023/11/contribuicao-legitimo-interesse-_dataprivacybrasil.pdf. Acesso em: 12 ago. 2024.

5 Conforme argumentamos, uma forma de materializar isso seria por meio de uma redação mais assertiva colocando a (i) relação prévia e direta com o controlador", (ii) "objetivo de assegurar a proteção de seus direitos e interesses" e (iii) "viabilizar a prestação de serviços que o beneficiem", não apenas como meras tendências, mas como critérios condicionantes a serem observados antes da realização da atividade de tratamento. Ver MENDONÇA, Julia; LOBO MARTINS, Pedro; MARTINS DOS SANTOS, Pedro Henrique. **Contribuição da Data Privacy Brasil sobre Legítimo Interesse**. São Paulo: Data Privacy Brasil, 2023. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2023/11/contribuicao-legitimo-interesse-_dataprivacybrasil.pdf. Acesso em: 12 ago. 2024.

Consumidor, com as Resoluções do Conanda sobre abusividade no direcionamento de publicidade e com o Comentário Geral n. 25 de 2021 do Comitê de Direitos das Crianças da ONU sobre direitos das crianças no ambiente digital, que vincula a interpretação dos direitos previstos na Convenção sobre Direitos da Criança e o Comentário Geral n. 14 sobre o direito da criança de ter seu interesse superior considerado primordialmente.

Nossas contribuições promovem uma leitura dos principais dispositivos legais da Lei Geral de Proteção de Dados Pessoais, em especial o art. 14 da LGPD, à luz das normas e teorias jurídicas do campo da proteção das crianças e adolescentes no Brasil.

Entendemos que a Autoridade Nacional de Proteção de Dados Pessoais possui uma chance única de avançar, por meio de normas regulatórias técnicas e um trabalho de supervisão do cumprimento das normas de proteção de dados pessoais pelos controladores, na garantia dos direitos de não discriminação, livre desenvolvimento da personalidade, primazia do melhor interesse das crianças, autodeterminação informativa e a garantia dos direitos das crianças e adolescentes por design dos produtos e serviços em ambientes digitais. A ANPD possui, assim, uma função crucial no auxílio no desenvolvimento de uma política nacional de proteção dos direitos da criança e do adolescente no ambiente digital.

Esperamos, também, que as contribuições da Data Privacy Brasil possam inspirar e auxiliar outras organizações civis na elaboração de seus comentários e recomendações à ANPD. Para tanto, reforçamos que todas as publicações da organização são feitas em formatos licenciados abertos e podem ser livremente utilizados, desde que citada a fonte.

Contribuições da Data Privacy Brasil na Tomada de Subsídios

A seguir, apresentamos as contribuições da Data Privacy Brasil na Tomada de Subsídios formulada pela Autoridade Nacional de Proteção de Dados Pessoais. Colocamos as perguntas da ANPD dentro de quadros e com itálico. Nossas respostas, tal como submetidas na plataforma "Participa+Brasil"[6], foram escritas abaixo dos quadros de perguntas. Também incluímos referências acadêmicas para as respostas quando necessário, com o objetivo de auxiliar a comunidade de direitos digitais e de proteção de crianças e adolescentes a conhecer mais fundo os materiais que lemos para preparação desta contribuição.

I – Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança,[1] no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU[2] e no Comentário Geral n° 25, de 2021, do Comitê dos Direitos da Criança.[3] Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz. Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

6 Ver https://www.gov.br/participamaisbrasil/tscriancaeadolescente.

Este tópico é bastante sensível para a Data Privacy Brasil e se conecta com nosso trabalho sobre Legítimo Interesse de 2021[7] e com nosso estudo, feito com Alana e ADC, sobre o significado do "melhor interesse"[8].

Nossas sugestões enviadas para a ANPD em 2023 não foram integralmente acatadas na produção do Guia do Legítimo Interesse da ANPD[9]. De início, reiteramos que o melhor interesse não é um elemento adicional a ser considerado em um teste de balanceamento, mas sim o núcleo de qualquer relação entre um controlador de dados e um titular que seja criança ou adolescente[10]. Para aferir o "melhor interesse", nós defendemos uma abordagem procedimental centrada em um teste, inspirado nos mecanismos e metodologias adotados em legislações do Reino Unido e da Califórnia, denominado "Children's Rights Impact Assessment (CRIA)". O CRIA é uma metodologia de documentação também criada pelo Comitê dos Direitos das Crianças da ONU, que tem como objetivo traduzir o artigo 3 da Convenção dos Direitos das Crianças[11], com relação à dar prioridade ao melhor interesse da criança e colocá-lo em prática de maneira estruturada e concreta[12].

Conforme destacamos na nossa contribuição para o Estudo Preliminar do Guia de Legítimo Interesse da ANPD, organizações como a Digital Futures Commission, vêm estudando e propondo a utilização desse tipo de relatório para as demandas no ambiente digital. Em 2021, a referida organização, em conjunto com a 5Rights Foundation, lançou o relatório "Child Rights Impact Assessment

---

7 BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf. Acesso em: 12 ago. 2024.

8 ADC; DATA PRIVACY BRASIL; INSTITUTO ALANA. **Dados e direitos da infância e adolescência no ambiente digital: caminhos para proteção jurídica no Brasil e Argentina**. São Paulo: Instituto Alana, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/07/Dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital_VF-ACES.pdf. Acesso em: 12 ago. 2024.

9 MENDONÇA, Julia; LOBO MARTINS, Pedro; MARTINS DOS SANTOS, Pedro Henrique. **Contribuição da Data Privacy Brasil sobre Legítimo Interesse**. São Paulo: Data Privacy Brasil, 2023. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2023/11/contribuicao-legitimo-interesse-_dataprivacybrasil.pdf. Acesso em: 12 ago. 2024.

10 MENDONÇA, Julia; LOBO MARTINS, Pedro; MARTINS DOS SANTOS, Pedro Henrique. **Contribuição da Data Privacy Brasil sobre Legítimo Interesse**. São Paulo: Data Privacy Brasil, 2023. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2023/11/contribuicao-legitimo-interesse-_dataprivacybrasil.pdf. Acesso em: 12 ago. 2024.

11 BRASIL. Decreto nº 99.710, de 21 de novembro de 1990. **Promulga a Convenção sobre os Direitos da Criança**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 12 ago. 2024.

12 DIGITAL FUTURES COMMISSION. **A Digital Future for Children: The Case for a Digital Environment that Works for Children**. 2021. Disponível em: https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf. Acesso em: 12 ago. 2024.

(CRIA): A tool to realise child rights in the digital environment"[13], que faz uma retrospectiva do uso desse tipo de documentação, além de fornecer uma listagem dos principais modelos de CRIA's produzidos e utilizados em diferentes países. Interessante mencionar também que o setor governamental também vêm se movimentando nesse sentido. O governo do Canadá, por exemplo, também disponibiliza em seu site um modelo de CRIA[14] voltado para a "orientação das autoridades federais sobre como considerar os direitos das crianças em suas iniciativas".

Importante dizer também que o Guia Orientativo[15] foi pensado para aspectos gerais do legítimo interesse, incluindo a discussão de crianças e adolescentes como um capítulo, o que, ao nosso sentir, não seria a forma mais adequada de tratar a discussão. Essa tendência de pensar o tópico de crianças e adolescentes como um "anexo", acabou produzindo uma lógica mais frouxa e flexível, por exemplo, para produção de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) quando há uma situação concreta de risco aos direitos fundamentais.

Isso porque, se por um lado a versão final do guia exige unicamente a elaboração de um RIPD "caso seja identificada, na situação concreta, a existência de alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais dos titulares", por outro lado, a dúvida que apresentamos anteriormente permanece: **como demonstrar isso de forma segura e consistente, sem a elaboração de um RIPD?** Essa lógica pressupõe que os riscos já são conhecidos e dá início a um procedimento de avaliação dos mesmos para, eventualmente, mitigá-los.

Nós defendemos que, no caso de crianças e adolescentes, essa regra flexível do Guia Orientativo é incompatível com a gramática constitucional de proteção de crianças e adolescentes, que possui uma base normativa forte na Constituição Federal, considerando que a proteção de crianças e adolescentes é dever de todos (responsabilidade compartilhada na sociedade[16]) e é prioridade absoluta.

---

13 DIGITAL FUTURES COMMISSION. **A Digital Future for Children: The Case for a Digital Environment that Works for Children**. 2021. Disponível em: https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf. Acesso em: 12 ago. 2024.

14 CANADÁ. Department of Justice. **Child Rights Impact Assessment (CRIA)**. Disponível em: https://www.justice.gc.ca/eng/csj-sjc/cria-erde/tool-outil.html. Acesso em: 12 ago. 2024.

15 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de Legitimo Interesse**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 12 ago. 2024.

16 Lei 8.069/1990, Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profis-

Considerando que o regime jurídico de proteção de crianças e adolescentes é específico e possui um conjunto maior de obrigações de mitigação e prevenção de riscos a direitos e liberdades fundamentais, **recomendamos que a orientação de elaboração de RIPD seja para toda e atividade de tratamento de dados de crianças e adolescentes, especialmente no caso de aplicação do legítimo interesse**. Só assim os riscos poderão ser efetivamente mapeados e reconhecidos para, posteriormente, serem mitigados, ou mesmo para ser identificada a impossibilidade de realização daquela operação de tratamento.

O exemplo **do caso recente da decisão cautelar contra a Meta[17] é bastante ilustrativo para essa discussão**. Na oportunidade, a ANPD verificou que que dados pessoais de crianças e adolescentes, como fotos, vídeos e postagens, poderiam estar sendo coletados e utilizados para treinar os sistemas de Inteligência Artificial (IA) da Meta.

A problemática se complexificou quando foi identificado que a política de privacidade da empresa é totalmente silente sobre o tratamento de dados de crianças e adolescentes, bem como nada menciona sobre medidas adotadas para que seja assegurado o seu melhor interesse, resultando em incertezas e potenciais danos a tais titulares. Sendo assim, tal conjuntura estaria totalmente incompatível não apenas com a Constituição Federal, mas com toda arquitetura jurídica de proteção dos mais jovens.

Aliado a isso, no tocante à avaliação de riscos envolvidos, a Autoridade reforçou que o controlador - nesse caso, a Meta- deveria adotar uma série de "salvaguardas e medidas de mitigação de risco capazes de demonstrar que, no caso concreto, o eventual tratamento de dados pessoais de crianças e adolescentes será realizado em seu melhor interesse", o que não foi verificado no caso concreto. Ressalte-se, ainda que o voto da Diretora Miriam Wimmer reforçou, ainda, que que os **riscos associados ao uso de dados pessoais de crianças e adolescente são tema de crescente preocupação na sociedade brasileira, o que demanda "uma atuação incisiva da ANPD** no cumprimento de seu mandato legal de zelar pela

---

sionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

17 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Voto nº 11/2023 – Suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf. Acesso em: 12 ago. 2024.

proteção de dados pessoais desses titulares"[18].

Ou seja, considerando que a necessidade de uma atuação mais incisiva na mitigação de riscos a crianças e adolescentes foi reconhecido pela própria Autoridade como uma prioridade, isso apenas reforça que a postura flexível na elaboração de RIPD anteriormente adotada não é a mais adequada. Em nossa visão, **para que tratamentos ilegais de dados pessoais de crianças e adolescentes que geram riscos a direitos fundamentais, como no caso da Meta, sejam evitados, é necessária a obrigatoriedade para elaboração de RIPD para toda operação de tratamento que envolvam dados de tais sujeitos**, especialmente no caso de utilização da base legal de legítimo interesse.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Na Data Privacy Brasil entendemos que existem algumas questões sobre melhor interesse que merecem maior detalhamento. De início, reforçamos o quanto apontado na pergunta anterior: a necessidade de adoção de uma abordagem procedimental e documentada, como a realização de um CRIA, é essencial para que seja efetivamente possível entender que o controlador está, de fato, pautando o tratamento de dados pessoais pelo melhor interesse da criança.

De igual maneira, entendemos que é de extrema relevância abordarmos algumas questões concretas, à luz do arcabouço jurídico protetivo de crianças e adolescentes, principalmente do Estatuto da Criança e do Adolescente (ECA). Tais questões podem servir de **balizas concretas para avaliação do melhor interesse em situações reais**, especialmente dentro da perspectiva procedimental acima mencionada. Dessa forma, é necessário avaliar no caso concreto, considerando as diretrizes normativas do ECA:

18 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Voto nº 11/2023 – Suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf. Acesso em: 12 ago. 2024.

1. A situação de "melhor interesse" aprofunda e concretiza um direito fundamental já previsto, como direito à vida, direito à educação, direito à vida comunitária, direito ao desenvolvimento da personalidade?[19]
2. A situação de "melhor interesse", em razão da mediação tecnológica e dos usos de dados, produz algum risco novo e específico que pode afetar a dignidade e liberdade da pessoa humana em situação futura?
3. Há possibilidade de que a utilização de dados pessoais se volte contra os interesses das crianças, produzindo novas violações de direitos e liberdades?

Com base nas perguntas acima, entendemos como relevante e ilustrativo a menção ao caso das escolas do Paraná[20]. A implementação das câmeras de reconhecimento facial para automação das chamadas é um exemplo de "contexto específico de tratamento de dados pessoais" no qual a produção de riscos aos direitos fundamentais é detrimental às crianças, falhando em atingir o teste do melhor interesse no ambiente digital, nos termos da Resolução n. 245/2024 do Conanda. É preciso que a interpretação da **noção de risco seja feita à luz do conceito de "proteção integral"**, o que exige uma concepção rigorosa preventiva, que precisa de uma devida cognição e avaliação dos mesmos.

No início de 2023, iniciaram os relatos de que estavam sendo implementados aparelhos denominados pela Secretaria de Educação do Estado de "Educatron", que deveriam ficar ao lado do professor, dentro da sala de aula. Em tese, o aparelho deveria ser utilizado com o objetivo de transmitir conteúdos multimídia e fazer videochamadas com outros professores e palestrantes. Na prática, ele também era utilizado para "fazer o reconhecimento facial dos alunos, substituindo a tradicional chamada dos nomes dos alunos por ordem alfabética[21]".

---

19 Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

20 VOGT, Amanda. **Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas**. Agência Pública, 03 out. 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/. Acesso em: 12 ago. 2024.

21 VOGT, Amanda. **Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas**. Agência Pública, 03 out. 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/. Acesso em: 12 ago. 2024.

A questão central é que a referida prática implica na coleta e tratamento massivo de dados pessoais e biométricos de crianças e adolescentes no ambiente escolar, por uma tecnologia permeada por inúmeras falhas e desenvolvida por empresas que atuam com pouquíssima transparência[22].

O argumento principal para a aplicação desse tipo de tecnologia, costuma estar atrelado à diferentes justificativas, como a ideia de "otimização da gestão do ambiente escolar", de forma que o reconhecimento facial seja vendido como uma ferramenta de ganho de eficiência e economia de tempo de aula dos(as) docentes, além de possibilitar, por exemplo, a administração de faltas escolares[23]. É comum também serem levantadas hipóteses de essa tecnologia permitiria que os professores possam "focar mais no aprendizado do aluno"[24], por conta do suposto tempo economizado na realização das chamadas.

Em análise pouco aprofundada, poderia ser argumentado que tais fins estariam concretizando ou aprofundando o direito fundamental à educação, o que supostamente harmonizaria com o princípio do melhor interesse. No entanto, basta uma simples análise mais aprofundada para compreender que tal argumento não se sustenta.

Ao analisarmos se a mediação tecnológica e uso de dados produz algum risco novo e específico que pode afetar a dignidade e liberdade da pessoa humana em situação futura (umas das perguntas sugeridas anteriormente), já encontramos barreiras para as referidas operações de tratamento. Isso porque, **a coleta de dados biométricos - que são dados sensíveis- de maneira massiva por tais tecnologias podem gerar sérios riscos de discriminação e desvios de finalidade**.

Segundo o relatório "Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras[25]" do Inter-

---

22 CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA (CESeC). **O Panóptico: Monitor do Reconhecimento Facial no Brasil**. Rio de Janeiro: CESeC, 2023. Disponível em: https://cesecseguranca.com.br/projeto/o-panoptico-monitor-do-reconhecimento-facial-no-brasil/. Acesso em: 12 ago. 2024.

23 INTERNETLAB. **Educação na mira: o uso de dados e tecnologias digitais em escolas públicas no Brasil**. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 12 ago. 2024.

24 MONTEIRO, Luiz Augusto Ferreira; SILVA, Bárbara Elis Nascimento; LEITE, Danilo Rangel Arruda. Inteligência artificial: a importância do reconhecimento facial na educação. Revista Presença Geográfica, Fundação Universidade Federal de Rondônia, vol. 07, n. 01, 2020. Disponível em: http://portal.amelica.org/ameli/jatsRepo/274/2741159009/index.html. Acesso em: 12 ago. 2024.

25 INTERNETLAB. **Educação na mira: o uso de dados e tecnologias digitais em escolas públicas no Brasil**. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf.

netlab, de imediato, dois riscos podem ser identificados de prontidão: (i) a possibilidade de discriminação de grupos historicamente minorizados, tais como mulheres, pessoas negras e LGBTQIA+, uma vez que tais tecnologias tem reprodução de vieses discriminatórios que podem levar a erros persistentes na operação da tecnologia; (ii) a possibilidade de inferências discriminatórias, considerando quando o reconhecimento facial busca não apenas verificar ou identificar determinada pessoa, mas também atribuir características físicas ou comportamentais. O documento aponta, ainda, que a **possibilidade do compartilhamento de dados entre órgãos públicos (coletados normalmente por empresas da iniciativa privada, ressalte-se), como o que ocorre entre o município de Morrinhos e o Conselho Tutelar para registro de evasão escolar, gera vários riscos de acessos indevidos a tais bases de dados, inclusive por parte de autoridades de investigação criminal**[26], aumentando também o potencial de ocorrerem desvios de finalidade.

Relevante salientar que através da mesma tecnologia, o mencionado Educatron, também foram realizados capturas das emoções dos estudantes, para "medir o desempenho dos alunos, com o objetivo de gerar gráficos e índices sobre o rendimento da turma"[27], bem como "medir comportamentos que possam representar riscos à integridade" dos mesmos[28].

Mais uma vez, realizando um exercício hipotético, poderia ser argumentado, em rasa análise, que o melhor interesse estaria sendo cumprido por estar, por exemplo, "aprofundando o direito à segurança". No entanto, essa conclusão não é adequada ou coerente com o melhor interesse da criança, conforme iremos detalhar a seguir.

Primeiramente, **existe a possibilidade de que a utilização dos dados pessoais -inclusive biométricos- coletados se voltem contra os interesses das mesmas, produzindo novas violações de direitos e liberdades**. Segundo o relatório "Reco-

---

Acesso em: 12 ago. 2024.

26 TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. **"Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras"**. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 12 ago. 2024.

27 Reconhecimento facial nas escolas públicas do Paraná / Carolina Batista Israel, Rodrigo Firmino, coordenadores; [autores] Carolina Batista Israel ... [et al.]; capa, Manoela M. Jazar – Curitiba : UFPR, 2023. Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/12/RF_PR_2023.pdf. Acesso em: 12 ago. 2024.

28 AUDI, Amanda. **Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas**. 27 out. 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/#_. Acesso em: 12 ago. 2024.

nhecimento Facial nas escolas públicas do Paraná"[29], pautando-se nas pesquisas de Lisa Barrett, eles apontam que não há como identificar padrões universais de análise de expressões faciais, uma vez que precisam de uma apreciação holística e contextual para serem efetivamente compreendidas, bem como possuem diferentes variações geográficas e culturais. Dessa forma, **no momento em que uma tecnologia capta a reação de um estudante e classificá-la como "violento" ou "hostil", além de ter grandes possibilidades de estar incorreta, podem gerar inferências que prejudiquem a criança não apenas no ambiente escolar e no mercado de trabalho[30], mas também em diferentes âmbitos da sua vida**.

A utilização de técnicas computacionais para inclusão de categorias e rótulos em crianças e adolescentes em softwares e sistemas computacionais, a partir do seu comportamento em sala de aula e análise de suas informações biométricas, representa uma violação ao livre desenvolvimento da personalidade em razão do conjunto de decisões que podem ser tomadas a partir da análise dessa categoria ou mesmo em razão das automações em sistemas computacionais. Em sociedades democráticas, as crianças e adolescentes são livres para terem comportamentos erráticos e amadurecerem no ambiente escolar, sem o risco de cristalização permanente de traços de suas personalidades em sistemas automatizados, o que produz situações de prejuízo à fruição plena de direitos fundamentais[31].

O relatório destaca, ainda, **a criação de outros riscos novos e específicos, que podem concretamente afetar a dignidade e liberdade da pessoa humana em situação futura**, quais sejam: (i) O progressivo uso da classificação de emoções para a tomada de decisões administrativas que afetarão o futuro das pessoas, seja no ambiente de trabalho ou escolar; (ii)O Impacto psicológico e emocional decorrente da vigilância contínua de comportamentos emocionais pouco ou não controláveis; (iii) Ausência de regulamentação e conscientização social que restrinja o uso abusivo de tais tecnologias; (iv)E, a perda do direito à liberdade de expressão, dados os condicionantes sociotécnicos de modulação comportamental, derivado desse

---

29 Reconhecimento facial nas escolas públicas do Paraná / Carolina Batista Israel, Rodrigo Firmino, coordenadores; [autores] Carolina Batista Israel ... [et al.]; capa, Manoela M. Jazar – Curitiba : UFPR, 2023. Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/12/RF_PR_2023.pdf. Acesso em: 12 ago. 2024.

30 AUDI, Amanda. **Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas**. 27 out. 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/#_. Acesso em: 12 ago. 2024.

31 MILLER, Arthur. **The Assault on Privacy**. Ann Arbor: University of Michigan Press, 1970.

conjunto de elementos[32].

Resta nítido, portanto, que a análise do melhor interesse da criança precisa de procedimentalização e documentação, pautando-se por critérios concretos. Nesse sentido, reiteramos a recomendação de realização de um CRIA e o estabelecimento de parâmetros específicos, como os que foram acima sugeridos.

II – Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

A crescente utilização das Tecnologias da Informação e Comunicação (TICs) e a participação cada vez maior de crianças e adolescentes em ambientes digitais trazem novos desafios quanto à proteção dos mesmos. A Pesquisa TIC Kids Online de 2022 mostra que 92% das pessoas entre 9 e 17 anos tinham acesso à internet,

32 **Reconhecimento facial nas escolas públicas do Paraná** / Carolina Batista Israel, Rodrigo Firmino, coordenadores; [autores] Carolina Batista Israel ... [et al.]; capa, Manoela M. Jazar – Curitiba : UFPR, 2023. Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/12/RF_PR_2023.pdf. Acesso em: 12 ago. 2024.

com 70% baixando aplicativos e 98% jogando online[33]. Esses dados evidenciam a necessidade de uma proteção rigorosa dos dados pessoais de crianças e adolescentes, garantindo que sua interação no ambiente digital seja pautada em segurança e responsabilidade.

Nesse contexto, entendemos que o melhor interesse da criança e do adolescente, conforme estabelecido no caput do art. 14 da LGPD, deve ser uma prioridade nas atividades que envolvam o tratamento de seus dados pessoais. O proveito gerado para quem segue esses passos é duplo, já que, por um lado, garante legitimidade às suas atividades, por outro, oferece uma interação segura e responsável com quem utiliza seus produtos ou serviços.

À vista disso, a Data Privacy Brasil considera essencial que o consentimento para o tratamento de dados pessoais seja claro, específico e destinado a uma finalidade previamente informada, evitando termos genéricos ou abrangentes que possam gerar ambiguidades. Esse consentimento deve ser destacado de outros termos e condições contratuais, garantindo que os pais ou responsáveis compreendam plenamente o que estão consentindo. Esse entendimento está alinhado com as disposições dos arts. 7º e 8º da LGPD, que exigem que o tratamento posterior de dados pessoais seja precedido por consentimento fornecido por escrito e destacado das demais cláusulas contratuais.

A resolução do Conanda (Resolução n. 245/2024) aponta que "sempre que o tratamento de dados pessoais de crianças e adolescentes for realizado com base no consentimento **deverá ser obtido de forma livre e prévia junto aos responsáveis, solicitado de forma específica e destacada**, para finalidades específicas e, sempre que possível, junto à criança ou adolescente, observado seu grau de maturidade e compreensão sobre os efeitos do consentimento" (art. 14).

Isso implica dizer que o termo de consentimento deve detalhar de maneira clara e compreensível quem são os agentes de tratamento e o controlador, quais dados serão coletados, a finalidade da coleta, como serão utilizados, e, se aplicável, com quem serão compartilhados, por quanto tempo serão retidos, além de informações sobre como agir em caso de incidentes e responsabilidades pelo tratamento inadequado dos dados. Essas informações devem evitar ao máximo jargões jurídicos complexos que dificultem a compreensão pelos pais ou responsáveis.

---

33 Comitê Gestor da Internet no Brasil – CGI.br. (2022). **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil** – TIC Kids Online Brasil 2022. Disponível em: https://cetic.br/media/docs/publicacoes/1/20230825142135/tic_kids_online_2022_livro_eletronico.pdf. Acesso em: 12 ago. 2024.

Considerando o contexto de desigualdades sociais e a diversidade linguística presente no Brasil, acreditamos ser crucial considerar formas alternativas de obtenção do consentimento. Em situações onde a formalização escrita possa ser um obstáculo, alternativas como consentimento oral ou por vídeo podem ser consideradas, desde que devidamente documentadas. Em comunidades onde o português não é a língua principal, o consentimento deve ser disponibilizado em outros idiomas e também considerar os dialetos locais para assegurar compreensão total do termo pelos pais ou responsáveis.

Nós acreditamos que a acessibilidade dos termos de consentimento é indispensável para assegurar que as pessoas deficientes sejam reconhecidas e respeitadas como titulares de direitos. Tanto em meios digitais quanto físicos, é imprescindível que o conteúdo do consentimento esteja disponível em formatos acessíveis, como texto em braille e recursos auditivos ou visuais adaptados. Isso garante que todas as pessoas, independentemente de suas limitações físicas ou sensoriais, possam compreender plenamente os termos aos quais estão consentindo.

Por fim, além dos pontos específicos já mencionados, entendemos que seja essencial que os controladores mantenham uma cultura de transparência. Devem manter publicamente acessíveis aos titulares informações sobre os tipos de dados coletados, finalidades do uso, e os direitos dos titulares, como confirmação da existência de tratamento, acesso aos dados, correção, anonimização, bloqueio ou a possibilidade de eliminação de dados desnecessários, a portabilidade dos dados e outras informações precisas para o exercício de direitos do titular. Devem fornecer mecanismos de forma clara e acessível, facilitando a interação e o exercício de direitos pelos pais ou responsáveis das crianças e adolescentes.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

A LGPD atribui a responsabilidade de identificação e autenticação ao exigir do controlador, no § 5º, art. 14, esforços para verificar se o consentimento é legítimo, para atender ao melhor interesse da criança e do adolescente. Conforme reconhe-

cido no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU, a ANPD reitera que este conceito trata-se de um direito, um princípio e uma regra processual, exigindo que o tratamento de dados priorize a proteção e promoção dos direitos das crianças, incluindo privacidade e a dignidade[34].

Para garantir a proteção dos direitos de crianças e adolescentes, consideramos fundamental que os controladores adotem processos claros, transparentes e inequívocos para a obtenção do consentimento, conforme estabelece o § 1º do art. 9 da LGPD. Esses processos devem ir além da simples criação de termos de consentimento separados e destacados; é necessário considerar as desigualdades sociais, a diversidade linguística e as limitações físicas e sensoriais dos titulares de dados. Dessa forma, assegura-se que pais ou responsáveis compreendam plenamente os termos apresentados.

Cabe destacar que crianças e adolescentes, como titulares de dados, em nossa percepção, têm direito a uma transparência qualificada[35], conforme previsto no § 2º do artigo 14 da LGPD[36]. Esse direito exige uma abordagem diferenciada, que vá além das obrigações de transparência geral aplicáveis a todos os titulares de dados. O artigo 14, especialmente nos parágrafos 2º e 6º, estipula que as informações sobre os dados coletados, sua utilização e os procedimentos para o exercício dos direitos devem ser disponibilizados de forma proativa e detalhada, mesmo na ausência de uma solicitação direta dos titulares.

Essa exigência impõe aos controladores a obrigação de garantir que a transparência no tratamento de dados seja específica e destacada para esse público vulnerável, diferenciando-se das regras aplicáveis a adultos. A ANPD já ressaltou a importância dessa transparência qualificada na Nota Técnica 6/2023[37], criti-

---

34 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Estudo preliminar: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/aberta-tomada-de-subsidios-sobre-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/2022.09.06_EstudoTcnicoCrianaseAdolescentes.pdf. Acesso em: 12 ago. 2024.

35 COSTA, Eduarda; MENDONÇA, Eduardo; MONAGREDA, Johanna; MENDONÇA, Julia; GUEDES, Paula; MARTINS, Pedro; SANTOS, Pedro Henrique. **Contribuição Data Privacy Brasil – Tomada de Subsídios Direitos dos Titulares**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024. Disponível em: https://drive.google.com/file/d/1p1HWSTu_oID7SYOMXlqivfomEhTU-Sahk/view. Acesso em: 13 ago. 2024.

36 De acordo com o artigo 14 da LGPD (Lei nº 13.709/2018), "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse" e os controladores "deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos" (BRASIL, 2018, Art. 14, § 2º).

37 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 6/2023/CGF/ANPD**. Nota Técnica 6 (3961973) SEI 00261.000297/2021-75. Coordenação-Geral de Fiscalização. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf. Acesso em: 13 ago. 2024.

cando a generalidade das finalidades de tratamento apresentadas pela plataforma TikTok e sublinhando a necessidade de informações precisas e adaptadas às particularidades das crianças e adolescentes. Portanto, entendemos que a transparência qualificada deve ser implementada desde o design, com diretrizes robustas que assegurem o pleno cumprimento dos direitos desses titulares.

No ambiente digital, onde a autenticação pode ser mais desafiadora, entendemos que os controladores devem adotar mecanismos robustos para verificar a idade da pessoa que está consentindo. Métodos existentes, como verificações adicionais via smartphone, onde um código de verificação é enviado para o número de telefone dos pais ou responsáveis, podem ser eficazes. Outra prática é a solicitação de informações adicionais, como uma assinatura digital, que certifiquem a identificação da pessoa consente.

Ferramentas de autenticação multifatorial, que requerem duas ou mais provas de identidade (por exemplo, uma combinação de senha e biometria), também podem ser adotadas.

Nós consideramos que os controladores devem também adotar boas práticas para a criação de ambientes digitais seguros e adequados. O relatório "But how do they know it is a child?' Age Assurance in the Digital World" da 5Rights Foundation[38] sugere a implementação de interfaces de usuário que facilitem a compreensão e interação com os termos de consentimento. Isso inclui o uso de ícones visuais, vídeos explicativos e fluxos de consentimento passo a passo, que guiem os pais ou responsáveis de maneira intuitiva e informativa, diferente do padrão adotado hoje no Brasil com extensas cláusulas escritas para dificultar o entendimento.

A Agência Espanhola de Proteção de Dados (AEPD) oferece diretrizes para verificação de idade e proteção de crianças e adolescentes contra conteúdos impróprios. O "Decálogo de princípios"[39] e a "Nota técnica"[40] descreve provas de conceito para sistemas de verificação etária eficazes, baseados na confirmação de dife-

---

38 5RIGHTS FOUNDATION. But how do they know it is a child? Age assurance in the digital world. Outubro 2021. Disponível em: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf. Acesso em: 12 ago. 2024.

39 AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Decálogo de principios: verificación de edad y protección de personas menores de edad ante contenidos inadecuados**. Diciembre 2023. Disponível em: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf. Acesso em: 12 ago. 2024.

40 AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Nota técnica: descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados**. Diciembre 2023. Disponível em: https://www.aepd.es/guias/nota-pruebas-concepto-verificacion-edad.pdf. Acesso em: 12 ago. 2024.

rentes fatores para confirmação de identidade. A publicação "*Menores, Salud Digital y Privacidad: Estrategia y Líneas de Acción*"[41] traça estratégias para a proteção de crianças e adolescentes, enfatizando a importância da educação digital e a cooperação com outras entidades para criar ambientes seguros.

Nos Estados Unidos, a Lei de Proteção à Privacidade Online das Crianças (COPPA) exige que sites e serviços online que coletam dados de crianças com idade abaixo de 13 anos sigam práticas rigorosas. As empresas passaram a incluir ferramentas mais precisas para obter o consentimento dos pais para a coleta, uso e divulgação de informações, além de passarem a informar os pais sobre o uso dos serviços e obter o consentimento por meio de e-mail, telefone, carta ou formulário assinado. De igual maneira, os controladores foram obrigados a implementar mecanismos para notificar os pais quando seus filhos utilizarem um serviço online.

Portanto, consideramos que os controladores devem adotar uma abordagem multifacetada, que inclua termos de consentimento claros, verificação robusta de identidade, consideração das desigualdades sociais e linguísticas, e transparência em todos os processos. Essas medidas garantirão uma interação segura e responsável com os dados pessoais de crianças e adolescentes, alinhando-se à LGPD e às melhores práticas internacionais.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

De antemão, ressaltamos que a LGPD não existe no vácuo, mas está inserida em um contexto jurídico mais amplo, que inclui a Constituição Federal, o Estatuto da Criança e do Adolescente (ECA), o Código Civil e demais regulamentações infraconstitucionais e infralegais que visam o melhor interesse da criança e do adolescentes.

---

41 AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Menores, salud digital y privacidad: estrategia y líneas de acción**. Janeiro 2024. Disponível em: https://www.aepd.es/guias/estrategia-menores-aepd-lineas-accion.pdf. Acesso em: 12 ago. 2024.

Sendo assim, a Data Privacy Brasil defende que a obtenção de consentimento para o tratamento de dados pessoais de crianças e adolescentes no ambiente digital deve seguir as disposições do direito civil em relação às capacidades civis. Para jovens considerados absolutamente incapazes, ou seja, aqueles com menos de 16 anos, a regra geral é a necessidade de representação para que seja fornecido o consentimento por seus pais ou responsáveis. Já para adolescentes relativamente incapazes, que são aqueles na faixa etária entre 16 e 18 anos, o consentimento deve ser dado com a assistência dos pais ou responsáveis legais, interpretação conforme disposto no Código Civil.

É importante mencionar que existem narrativas em construção de que, com base na autonomia progressiva de crianças e adolescentes, seria possível que o consentimento parental fosse "suprido" pelos próprios jovens, independentemente de assistência ou representação, posição que tendemos a discordar.

Em nosso sentir, ainda é necessário um maior aprofundamento das discussões sobre a conexão entre esses dois temas (consentimento para tratamento de dados pessoais e autonomia progressiva) no caso concreto, especialmente em se tratando do ambiente digital, que possui diversos riscos sistêmicos para os mais jovens, podendo agravar a sua condição de vulnerabilidade. Merece destaque o fato de que encontramos apenas três teses de doutorado, na Biblioteca de Teses da CAPES, sobre o tema "autonomia progressiva", que tratam sobre o tema de forma aprofundada.

Sendo assim, reforçamos a necessidade de aprofundamento do debate no contexto nacional sem a adoção de interpretações irrefletidas que possam colocar em risco o melhor interesse e a proteção integral dos mais jovens . A argumentação sobre "autonomia progressiva" para suprir eventual consentimento parental não deve servir como escudo ou proteção para flexibilização de regras que envolvem tratamento de dados pessoais de crianças e adolescentes. Tal cautela é importante ao se considerar as evidências científicas sobre danos em usos de redes sociais e aplicações de Internet, tal como feito por Jonathan Haidt no seu livro "A Geração Ansiosa"[42]. Essa também é uma discussão que está sendo amplamente debatida no cenário internacional, com a realização de investigações sobre o potencial dano à saúde causado pelas plataformas digitais, como a recente denúncia do Departa-

42 TEIXEIRA, Jerônimo. **Infância hiperconectada cria "geração ansiosa", diz o livro mais discutido do ano**. Brazil Journal, 1 jun. 2024. Disponível em: https://braziljournal.com/infancia-hiperconectada-cria-geracao-ansiosa-diz-o-livro-mais-discutido-do-ano/. Acesso em: 12 ago. 2024

mento de Justiça dos Estados Unidos, junto com a Federal Trade Comission (FTC) contra a plataforma Tik Tok[43].

III – Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações "estritamente necessárias à atividade".

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos

43 UNITED STATES. Department of Justice. **Justice Department Sues TikTok and Parent Company ByteDance for Widespread Violations of Children's Privacy**. 11 ago. 2024. Disponível em: https://www.justice.gov/opa/pr/justice-department-sues-tiktok-and-parent-company-bytedance-widespread-violations-childrens. Acesso em: 12 ago. 2024.

audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Para assegurar o respeito ao melhor interesse de crianças e adolescentes, bem como promover níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso de plataformas digitais, consideramos que é fundamental observar diversos princípios, parâmetros e salvaguardas, incluindo medidas de design[44]. Primeiramente, deve-se considerar os princípios fundamentais da Lei Geral de Proteção de Dados (LGPD) brasileira, que incluem a finalidade, a necessidade e a adequação. Esses princípios determinam que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para realizar finalidades específicas, legítimas e informadas aos titulares, sem permitir o uso posterior de forma incompatível com essas finalidades. Além disso, a transparência é essencial, exigindo que os controladores forneçam informações explícitas, precisas e de fácil acesso sobre o tratamento dos dados e os respectivos agentes de tratamento.

44 HARTUNG, Pedro. **The children's rights-by-design standard for data use by tech companies**. Unicef Good Governance of Children's Data Project, 2020. Disponível em: https://tinyurl.com/2s42h5k4. Acesso em: 12 ago. 2024.

Conforme o parágrafo 6º do art. 14 da LGPD, essas informações devem considerar as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais das crianças[45], utilizando recursos audiovisuais quando apropriado.

No contexto internacional, destacam-se parâmetros estabelecidos por regulamentações como o Age Appropriate Design Code (ICO) do Reino Unido, o código da Irlanda e a legislação da Califórnia. O Age Appropriate Design Code (ICO) impõe 15 normas que as plataformas digitais devem seguir para garantir a proteção dos dados de crianças. Entre essas normas, estão a configuração de privacidade padrão para o nível mais alto e a limitação do uso de técnicas de engajamento que incentivem o uso prolongado das plataformas. Essas medidas visam proteger a privacidade das crianças desde o design inicial do produto, colocando seu melhor interesse como prioridade.

O código da Irlanda foca na transparência e no consentimento informado, assegurando que as crianças e seus pais compreendam claramente como os dados são coletados e utilizados. Este código promove a implementação de medidas que restringem a coleta de dados desnecessários, garantindo que apenas informações essenciais sejam coletadas e tratadas de maneira adequada. A proposta da Califórnia sugere a implementação de padrões rigorosos de proteção de dados, como a **minimização da coleta de dados e a segmentação comportamental não poderia nem com o consentimento parental, ao menos em se tratando de publicidade**. Este enfoque reforça a necessidade de salvaguardas adicionais para proteger a privacidade e a segurança das crianças no ambiente digital.

Adicionalmente, acreditamos que é fundamental que o design e desenvolvimento dos serviços considerem o melhor interesse da criança como prioridade. Isso inclui a implementação de boas práticas e padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão. Importante destacar que essas exigências não se aplicam apenas aos jogos, mas a qualquer serviço ou plataforma online que possa ser acessada por crianças, conforme os critérios do Age Appropriate Design Code. Portanto, ao alinhar-se com esses princípios e parâmetros internacionais, é possível criar um ambiente digital mais seguro e responsável para crianças e adolescentes, garantindo a proteção de seus dados pessoais e promovendo seu bem-estar no uso de plataformas digitais.

---

45 BUITELAAR, J. C. **Child's best interest and informational self-determination: what the GDPR can learn from children's rights**. International Data Privacy Law, v. 8, n. 4, p. 293–308, 2018.

A partir das normas aprovadas na Califórnia, que possuem alto parâmetro protetivo com relação ao processo de design de códigos, plataformas e softwares, podemos pensar em um check-list operacional para design a partir das seguintes perguntas:

- Qual é o propósito deste produto, serviço ou funcionalidade? *Estou ciente de como este propósito pode impactar o bem-estar das crianças?*
- Como este produto, serviço ou funcionalidade utiliza as informações pessoais de crianças? *Existe uma justificativa clara e necessária para a coleta e uso dessas informações?*
- Este design pode expor crianças a conteúdos prejudiciais ou potencialmente prejudiciais? *Estou adotando medidas para prevenir essa exposição?*
- Este design pode levar crianças a serem alvo de contatos prejudiciais ou potencialmente prejudiciais na plataforma? *Existem proteções adequadas para evitar que crianças sejam abordadas de forma inapropriada?*
- Este design permite que as crianças testemunhem, participem ou sejam sujeitas a condutas prejudiciais ou potencialmente prejudiciais na plataforma? *O design promove ou impede tais comportamentos?*
- Este design pode permitir que as crianças sejam exploradas por contatos prejudiciais ou potencialmente prejudiciais na plataforma? *Quais barreiras estou implementando para proteger as crianças?*
- Os algoritmos usados neste produto, serviço ou funcionalidade podem prejudicar as crianças? *Estou testando os algoritmos para identificar e mitigar possíveis danos?*
- Os sistemas de publicidade direcionada usados neste produto, serviço ou funcionalidade podem prejudicar as crianças? *Estou garantindo que a publicidade seja adequada à faixa etária e não explore as vulnerabilidades das crianças?*
- Este design pode prolongar, aumentar ou sustentar o uso do produto, serviço ou funcionalidade por crianças de maneira não saudável (e.g., recompensas, notificações, autoplay de mídia)? *Estou avaliando o impacto psicológico e o tempo de tela excessivo?*

- Este design inclui a coleta ou processamento de informações pessoais sensíveis de crianças? *Se sim, para que finalidade essas informações são coletadas e processadas, e como estou garantindo sua proteção?*
- Estou realizando uma Avaliação de Impacto de Proteção de Dados (DPIA) completa e documentada para este design? *Estou revisando e atualizando essa avaliação regularmente para garantir conformidade contínua?*

Essas perguntas são típicas de um processo de due diligence e avaliação de risco feito por grandes organizações e seus times de privacidade e proteção de dados pessoais na Califórnia[46]. Apesar de o Brasil não possuir uma legislação federal específica sobre design, a garantia e efetivação dos direitos da criança e do adolescente em ambiente digital é pautada pelo princípio da "garantia dos direitos das crianças e adolescentes por design dos produtos e serviços em ambientes digitais", de acordo com o art. 3, X, da Resolução n. 245/2024.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

Fixamos que é necessário que alcancemos um equilíbrio entre a liberdade empresarial e a proteção dos dados pessoais, garantindo que a Autoridade Nacional de Proteção de Dados (ANPD) não estabeleça restrições excessivas. Um exemplo comum de verificação de idade é a solicitação de documentos de identidade. Esse método, embora eficaz, pode ser considerado intrusivo e levantar preocupações sobre privacidade e sobre a proteção dos dados pessoais. Os gargalos desse método, como a coleta excessiva de informações pessoais e o risco de vazamentos de dados, são desafios que precisam ser refletidos e abordados.

Os métodos menos intrusivos para verificação de idade incluem o uso de algoritmos de inteligência artificial que estimam a idade com base em padrões de comportamento online ou características faciais. Essas técnicas, embora inovadoras, ainda requerem aprimoramento para garantir precisão e minimizar riscos

46 ORATZ, Lisa; ASARE-KONADU, Akua. **Four Key Considerations for Implementing the California Age-Appropriate Design Code**, PerkinsCoie, 2023. https://www.perkinscoie.com/en/news-insights/four-key-considerations-for-implementing--the-california-age-appropriate-design-code.html

à privacidade e a proteção de dados pessoais.

Há também técnicas contextuais de verificação de idade que utilizam de saberes históricos, os quais uma criança raramente saberia e que podem ser alternativas menos intrusivas. Por exemplo, em determinadas aplicações de Internet é possível utilizar um jogo de verificação de idade no qual o usuário precisa identificar uma fita VHS dentre várias imagens. Há também soluções de verificação de idade que mostram imagens de objetos já obsoletos, como disquetes, câmeras filmadoras e outros dispositivos que adultos teriam alta probabilidade de compreensão. Tais métodos, uma vez demonstrados que possuem eficácia e validade estatística em um grupo de teste, podem ser utilizados de modo a atingir o mesmo fim (determinar se o consentimento está mesmo sendo dado por um adulto), sem necessariamente utilizar-se de métodos intrusivos, como a coleta de informação biométrica.

A discussão sobre elementos não intrusivos na França ganhou relevância com o Decreto de 2021, que proibiu a prática de raspagem de histórico de navegação para verificar a idade dos usuários online. O objetivo era encontrar um equilíbrio entre a proteção de crianças e adolescentes e a privacidade dos indivíduos, uma vez que técnicas como raspagem de dados podem expor informações sensíveis e comprometer a privacidade dos usuários. O Decreto refletiu a preocupação com a intrusividade de certos métodos de verificação de idade, promovendo abordagens que minimizem o impacto sobre a privacidade, como o uso de terceiros confiáveis e a não coleta direta de dados identificáveis pelos sites.

Essa abordagem foi em linha com as recomendações da Comissão Nacional de Informática e Liberdades (CNIL), que enfatizou a necessidade de preservar a privacidade dos usuários enquanto se assegura que menores não acessem conteúdo impróprio. A CNIL enfatizou que técnicas intrusivas, como a análise de metadados e histórico de navegação, devem ser abordadas com extrema cautela para evitar violações da privacidade dos usuários. A autoridade francesa de proteção de dados recomendou que a verificação de idade online fosse feita de maneira que não exigisse a coleta de documentos de identidade diretamente pelos sites, evitando também o uso de dados biométricos ou inferências baseadas em histórico de navegação. O foco nas soluções menos intrusivas reflete o esforço contínuo da França em proteger tanto os direitos das crianças e adolescentes quanto a privacidade dos usuários na era digital.

A CNIL também estabeleceu princípios essenciais para a implementação

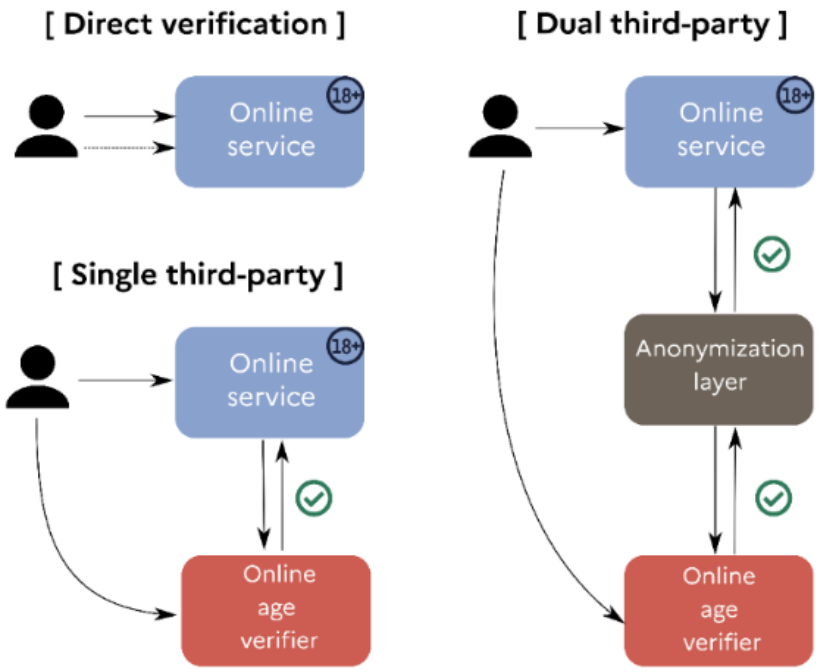
de sistemas de verificação de idade, com foco em minimizar a coleta de dados e garantir a proporcionalidade das medidas. Entre esses princípios estão a simplicidade, robustez, padronização e a intervenção de terceiros confiáveis para gerenciar a verificação sem comprometer a identidade dos usuários. A ideia é que o controle sobre esses processos permaneça, sempre que possível, nas mãos dos próprios usuários, evitando centralizações que possam exacerbar riscos à privacidade. A abordagem francesa, que exige a verificação de idade como uma medida essencial para proteger os jovens online, deve, no entanto, ser conduzida de maneira que minimize o impacto sobre a privacidade dos usuários e evite a coleta excessiva de dados pessoais.

Para promover um ambiente digital seguro e apropriado para crianças, é fundamental que os profissionais de design adotem boas práticas que vão além da conformidade com regulamentações:

1. Os engenheiros de sistema e designers devem garantir que a privacidade das crianças seja protegida desde o início, incorporando padrões elevados de segurança e minimizando a coleta de dados ao que é estritamente necessário para o funcionamento básico do serviço. Isso inclui adotar configurações de privacidade como padrão e fornecer informações claras e compreensíveis para crianças e seus responsáveis, reforçando o compromisso com a transparência e a proteção de dados;
2. A criação de interfaces deve ser orientada pela usabilidade infantil, com designs que sejam intuitivos, acessíveis e adaptados ao nível de compreensão das crianças. É crucial que os profissionais testem regularmente seus produtos com usuários reais na faixa etária pretendida, para garantir que as funcionalidades sejam facilmente navegáveis e que a experiência do usuário seja positiva e educativa. A simplicidade no design, a clareza na comunicação visual e o ajuste contínuo com base em feedback são componentes essenciais para um design adequado; e
3. Para assegurar que as crianças estão protegidas contra riscos online, os designers devem implementar mecanismos robustos de controle de conteúdo e sistemas de moderação eficazes. Isso inclui o uso de filtros que bloqueiem material inadequado, a facilidade de denúncia para os usuários e a garantia de que o consentimento parental seja sempre obtido em situações que envolvem implicações maiores, como transações financeiras ou compartilhamento de informações pessoais. Esses procedi-

mentos não apenas cumprem os requisitos legais, mas também refletem o compromisso ético de criar um ambiente digital que respeite e proteja o bem-estar de crianças e adolescentes.

A CNIL também recomenda a utilização de sistemas de autenticação providos por terceiros (*third parties*). Nesse sentido, um estudo técnico realizado em 2022 afirmou categoricamente que: "é essencial que a verificação da idade não seja realizada diretamente pela plataforma ou serviço online para reduzir o risco de referência cruzada ou reutilização de dados coletados durante a verificação. Um mecanismo de terceiros, ou mesmo um mecanismo de terceiros duplo, pode ser colocado em prática para a transmissão do resultado da verificação precisamente para minimizar esse risco" (CNIL, 2022). Esquematicamente, a CNIL construiu um fluxograma que detalha a viabilidade de aplicação de camadas de anonimização no processo de autenticação realizado por terceiros (o que eles chamam de *dual third-party*).



Fonte: CNIL (2022)

Consideramos que incentivar o desenvolvimento e a adoção de métodos de verificação de idade que respeitem a privacidade dos usuários e sejam proporcionais à finalidade do tratamento de dados é essencial. Isso inclui promover a criação de soluções que equilibrem a necessidade de proteção dos dados pessoais com a liberdade empresarial, sem a necessidade de imposições rigorosas por parte da ANPD.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

Na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, pontuamos que é crucial observar uma série de limitações específicas, conforme estabelecido pelo art. 14, § 4º, da Lei Geral de Proteção de Dados (LGPD). Este artigo prevê que o tratamento de dados deve ser restrito às informações "estritamente necessárias à atividade", especialmente em contextos como jogos e aplicações de internet. Essa diretriz está alinhada com os princípios da LGPD, que enfatizam a necessidade e a proporcionalidade no tratamento de dados.

Primeiramente, o princípio da necessidade, previsto no art. 6º da LGPD, exige que a coleta de dados seja limitada ao mínimo necessário para atingir a finalidade pretendida. Isso implica que plataformas digitais não devem coletar dados adicionais além do estritamente necessário para a operação do serviço, como em jogos e aplicativos. Esta limitação busca evitar a coleta excessiva e proteger a privacidade dos usuários, especialmente de crianças e adolescentes que estão em uma fase de desenvolvimento e podem não compreender completamente as implicações da coleta de seus dados.

A Resolução do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) proíbe especificamente a formação de perfis comportamentais de crianças e adolescentes para fins comerciais. Esse tipo de prática é considerado abusivo, pois utiliza dados pessoais para criar perfis detalhados que podem ser explorados de maneiras que não beneficiam diretamente o bem-estar de crianças e adolescentes. A proibição reflete a preocupação com a proteção da privacidade e com a prevenção de práticas discriminatórias e exploratórias.

No contexto das Edtechs, essas plataformas devem garantir que a coleta de dados pessoais de estudantes seja estritamente necessária para fins educacionais e que não haja uso de dados para formar perfis comportamentais ou para qualquer finalidade além da educação. As Edtechs precisam adotar medidas que assegurem a proteção de dados e a conformidade com os princípios da LGPD, evitando práticas que possam infringir os direitos dos alunos.

Ao considerar o regime jurídico de proteção de crianças e adolescentes, especialmente conforme o art. 14 da LGPD, é essencial reconhecer que a coleta de dados pessoais deve ser estritamente limitada ao necessário, mesmo quando são aplicados processos de anonimização ou remoção de identificadores pessoais. Do ponto de vista da privacidade individual, a anonimização dos dados não elimina totalmente os riscos associados à exploração comercial e ao uso indevido dessas informações.

O art. 14 da LGPD, em conjunto com a Resolução Conanda, impõe restrições rigorosas para proteger crianças e adolescentes de práticas abusivas, como a criação de perfis comportamentais. Mesmo quando os dados são agregados ou transformados em metadados, a possibilidade de reidentificação e de exploração comercial continua a ser uma preocupação significativa. Essas práticas, que exploram a vulnerabilidade dos jovens, violam os princípios de necessidade e proporcionalidade que regem o tratamento de dados pessoais.

Portanto, a coleta de dados de crianças e adolescentes não é possível ultrapassar o estritamente necessário, pois, mesmo com a anonimização, os riscos de exploração abusiva e violação dos direitos fundamentais persistem. A proteção integral desses direitos exige um controle rigoroso e justificação clara para qualquer coleta de dados, assegurando que esteja sempre em conformidade com os princípios da LGPD e que priorize a proteção da privacidade e o bem-estar das crianças e adolescentes.

O conceito de coleta abusiva versus coleta excessiva deve ser visivelmente compreendido[47]. A coleta abusiva refere-se a práticas que exploram a vulnerabilidade das crianças e adolescentes, enquanto a coleta excessiva diz respeito à obtenção de mais dados do que o necessário para a finalidade declarada. A LGPD estabelece novos contornos jurídicos que buscam equilibrar a necessidade de dados para a operação de serviços com a proteção dos direitos das crianças e adolescentes, impondo limites que evitam tanto a coleta abusiva quanto a excessiva.

47 ZANATTA, Rafael; JONAS, Valente; JÚLIA, Mendonça. **Entre o abusivo eo excessivo: Novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD**. Privacidade e Proteção de Dados de Crianças e Adolescentes. in: Priscilla Laterça, Elora Fernandes, Chiara Teffé and Sérgio Branco. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, p. 396–426, 2021.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

Para assegurar que os pais e responsáveis por crianças e adolescentes desempenhem um papel mais ativo na proteção dos dados pessoais, acreditamos que as plataformas digitais podem adotar boas práticas que descrevemos a seguir. Uma abordagem possível é oferecer ferramentas que possibilitem aos pais e responsáveis o gerenciamento e o uso das tecnologias pelas crianças e adolescentes. Essas ferramentas poderiam incluir funcionalidades vinculadas ao acesso a conteúdos adultos, notificações de tempo de uso e definição de limites na coleta de dados pessoais. Além disso, as plataformas podem garantir que as configurações de privacidade sejam intuitivas e acessíveis, facilitando ajustes adequados por parte dos pais e responsáveis.

Um aspecto importante é a implementação de sistemas que tenham o consentimento explícito dos pais e responsáveis para a coleta e o tratamento de dados pessoais. Este processo deve ser evidente e direto, assegurando que os pais e responsáveis compreendam o que estão autorizando. A transparência é igualmente essencial, as plataformas devem fornecer informações claras sobre como os dados são coletados, utilizados e compartilhados, permitindo que os pais e responsáveis compreendam os riscos e as práticas associadas.

É essencial encontrar um equilíbrio entre proteger a privacidade das crianças e adolescentes e permitir que desenvolvam autonomia e habilidades digitais. O controle excessivo pode limitar a capacidade das crianças e adolescentes de aprender a gerenciar sua própria privacidade e segurança. Além disso, a privacidade dos pais também deve ser considerada, garantindo que as ferramentas de controle não sejam invasivas.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Para garantir a transparência e o fornecimento de informações de maneira simples, clara e acessível, consideramos que as plataformas digitais devem adotar

boas práticas que considerem as necessidades específicas de crianças e adolescentes e estejam alinhadas com diretrizes de design e regulamentações como a Resolução do Conanda. Essas práticas devem assegurar que as crianças e adolescentes possam compreender como seus dados pessoais são coletados, utilizados e protegidos, e que possam exercer seus direitos de forma eficaz.

A Resolução do Conanda estabelece que informações devem ser oferecidas de forma acessível e compreensível para crianças e adolescentes, **considerando suas características cognitivas** e de desenvolvimento. Isso inclui a criação de seções dedicadas à privacidade e à proteção de dados, que devem ser facilmente localizáveis dentro das plataformas. O uso de recursos audiovisuais, como animações e jogos educativos, pode ser uma estratégia eficaz para envolver as crianças e adolescentes e facilitar a compreensão dos conceitos relacionados à privacidade.

As plataformas digitais devem projetar suas interfaces de forma a serem adequadas à faixa etária dos usuários. Isso significa usar uma linguagem simples e direta, evitando jargões técnicos e complexidade desnecessária. Informações sobre o tratamento de dados pessoais devem ser apresentadas de maneira que as crianças possam entender, usando recursos visuais, como ícones, cores e gráficos que ajudem a explicar conceitos de forma intuitiva. Por exemplo, plataformas podem utilizar elementos visuais e interativos, como infográficos e vídeos curtos, para explicar como os dados são coletados e usados.

Faz-se necessário que as plataformas proporcionem mecanismos que permitam que crianças e adolescentes exerçam seus direitos de acesso aos seus dados pessoais de forma prática. Isso pode incluir funcionalidades que permitam a visualização e a gestão das informações coletadas, bem como a opção de fazer solicitações de correção ou exclusão de dados de forma fácil e direta. Por exemplo, em um jogo digital, um painel de controle acessível pode permitir que o usuário visualize e ajuste as configurações de privacidade, além de oferecer opções claras para solicitar alterações ou exclusões de dados.

Em termos de design, as plataformas devem evitar textos longos e complexos, substituindo-os por resumos ou explicações breves que capturem os pontos principais de maneira clara. Informações essenciais sobre privacidade e proteção de dados devem ser destacadas e de fácil acesso, sem exigir que os usuários naveguem por múltiplas páginas para encontrar as informações necessárias.

Exemplos concretos de boas práticas incluem a criação de interfaces amigá-

veis, como as utilizadas por algumas plataformas educacionais que empregam mascotes ou personagens animados para explicar conceitos de proteção de dados de forma lúdica e envolvente. Além disso, plataformas de jogos podem utilizar tutoriais interativos que ensinem sobre privacidade e segurança enquanto os jogadores progridem no jogo, integrando a educação sobre dados pessoais de forma natural e atraente. Em jogos como LEGO, a interface é projetada com elementos visuais e interativos que atraem e são apropriados para a faixa etária dos jogadores. Por exemplo, os jogos podem utilizar gráficos coloridos e personagens amigáveis que ajudam a explicar conceitos de forma intuitiva.

A comunicação sobre privacidade e dados pessoais dos jogos LEGO é abordada de forma visual e interativa. Em vez de textos extensos e complexos, o LEGO utiliza elementos gráficos e interativos que permitem às crianças entender seus direitos e como gerenciá-los de forma prática e engajante. Por exemplo, ao acessar as configurações de conta, os jogadores podem ver ícones e botões claramente rotulados que permitem a edição de suas informações ou a desativação de newsletters e e-mails publicitários. Essas opções são apresentadas em um formato simplificado, como painéis de controle com animações e explicações curtas, tornando a navegação mais intuitiva. A política de privacidade e os direitos dos usuários são traduzidos em pequenos tutoriais ou seções dentro do jogo que utilizam personagens e histórias para explicar conceitos como o direito de acesso, retificação e eliminação de dados. Por exemplo, um personagem do jogo pode guiar os jogadores através de um processo interativo onde eles podem solicitar uma cópia das informações coletadas, corrigir dados incorretos ou até mesmo excluir dados, tudo isso de maneira visual e divertida.

O conceito de linguagem clara e acessível também envolve a compreensão do contexto linguístico do titular de dados, especialmente em situações de diversidade linguística. Por exemplo, comunidades indígenas não possuem condições, em alguns casos, de compreensão plena da língua portuguesa. Nesse sentido, controladores podem ser estimulados a utilizarem sistemas de IA e processamento de linguagem natural para adaptação de seus textos para línguas locais, incluindo línguas de povos originários, como o guarani.

Nesse sentido, a acessibilidade deve guiar a escrita e apresentação dos termos de consentimento. Essa é uma abordagem essencial para garantir que pessoas com deficiência e/ou audição e visibilidade reduzida sejam devidamente reconhecidas e respeitadas como titulares de direitos. O conteúdo do consentimento tem que

ser oferecido em formatos acessíveis, como texto em braille, recursos auditivos ou visuais adaptados. Isso garante que todas as pessoas, independentemente de suas limitações físicas ou sensoriais, possam compreender plenamente os termos aos quais estão consentindo.

Entendemos que essas abordagens não apenas facilitam a compreensão das políticas de privacidade, mas também permitem que as crianças exerçam seus direitos de forma prática e acessível, alinhando-se às boas práticas de transparência e proteção de dados. O uso de elementos visuais e interativos ajuda a transformar informações complexas em experiências compreensíveis e envolventes, adequadas à faixa etária dos usuários.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Sim, há questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem um esclarecimento mais detalhado ou uma regulamentação adicional.

Um aspecto fundamental a ser considerado é a exceção prevista no parágrafo 3º do art. 14 da LGPD, que permite o tratamento de dados pessoais de crianças sem o consentimento dos pais ou responsáveis legais, desde que a coleta seja necessária para contatá-los ou para a sua proteção. Isso porque, ainda não firmadas interpretações concretas sobre o que significa a exceção da exigência do consentimento para garantir a proteção da criança.

Desse modo, é relevante que a ANPD se posicione para que tal interpretação seja azeitada com o arcabouço de proteção dos mais jovens. Um caminho que entendemos como adequado, em síntese, seria que a interpretação "de proteção" estivesse pautada pelo cumprimento expresso, devidamente justificado, de algum dos direitos estabelecidos no Estatuto da Criança e do Adolescente.

Outra agenda urgente de ser incluída no **Projeto Regulatório da ANPD sobre o tema é o desenvolvimento e a adoção de um Código de Design Apropriado à Idade**, que deve incluir diretrizes específicas que ajudem a garantir que as práticas de coleta e tratamento de dados respeitem o melhor interesse em todos os serviços e produtos que **sejam destinados ou que possam ser acessados por crianças ou adolescentes**.

O caso do LEGO serve como um bom exemplo de boas práticas nesse contexto. A política de privacidade do LEGO[48] exemplifica como a empresa coleta e utiliza dados pessoais de forma transparente e adequada. O LEGO informa aos usuários sobre a coleta de dados de maneira clara e acessível, destacando a necessidade de autorização para a coleta, o uso restrito dos dados para as finalidades acordadas e a conformidade com a legislação local. O LEGO também oferece informações sobre como os dados são usados, armazenados e protegidos, e garante que dados pessoais não sejam compartilhados sem autorização ou, no caso de pessoas abaixo de 16 anos, sem a permissão dos pais.

O LEGO emprega práticas que facilitam a compreensão dos usuários sobre seus direitos. Por exemplo, oferece instruções evidentes sobre como acessar, corrigir, ou excluir informações pessoais e como lidar com cookies e outros aspectos relacionados à privacidade. O design das interfaces e a comunicação visual são projetados para serem amigáveis e apropriados para a faixa etária dos usuários, o que contribui para uma melhor compreensão e gestão dos dados pessoais. Essas práticas exemplificam como a criação de interfaces e políticas de privacidade adaptadas à idade pode ajudar a proteger a privacidade de crianças e adolescentes, assegurar a transparência no tratamento de dados e garantir que as informações sejam acessíveis e compreensíveis para crianças e adolescentes e seus responsáveis legais.

48 LEGO. Política de Privacidade. Disponível em: https://kids.lego.com/pt-br/legal/privacy-policy. Acesso em: 12 ago. 2024.

Referências

5RIGHTS FOUNDATION. **But how do they know it is a child? Age assurance in the digital world**. Outubro 2021. Disponível em: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf. Acesso em: 12 ago. 2024.

ADC; DATA PRIVACY BRASIL; INSTITUTO ALANA. **Dados e direitos da infância e adolescência no ambiente digital: caminhos para proteção jurídica no Brasil e Argentina**. São Paulo: Instituto Alana, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/07/Dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital_VF-ACES.pdf. Acesso em: 12 ago. 2024.

AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Decálogo de principios: verificación de edad y protección de personas menores de edad ante contenidos inadecuados**. Diciembre 2023. Disponível em: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf. Acesso em: 12 ago. 2024.

AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Menores, salud digital y privacidad: estrategia y líneas de acción**. Janeiro 2024. Disponível em: https://www.aepd.es/guias/estrategia-menores-aepd-lineas-accion.pdf. Acesso em: 12 ago. 2024.

AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS. **Nota técnica: descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados**. Diciembre 2023. Disponível em: https://www.aepd.es/guias/nota-pruebas-concepto-verificacion-edad.pdf. Acesso em: 12 ago. 2024.

AUDI, Amanda. **Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas**. 27 out. 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/#_. Acesso em: 12 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Estudo preliminar: hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/aberta-tomada-de-subsidios-sobre-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/2022.09.06_EstudoTcnico-CrianaseAdolescentes.pdf. Acesso em: 12 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia de Legítimo Interesse**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 12 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Nota Técnica nº 6/2023/CGF/ANPD**. Nota Técnica 6 (3961973) SEI 00261.000297/2021-75. Coordenação-Geral de Fiscalização. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf. Acesso em: 13 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Voto nº 11/2023 - Suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf. Acesso em: 12 ago. 2024.

BRASIL. Decreto nº 99.710, de 21 de novembro de 1990. **Promulga a Convenção sobre os Direitos da Criança**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 12 ago. 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Diário Oficial da União: Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 13 ago. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e dá outras providências**. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 ago. 2024.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Diário Oficial da União: Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 13 ago. 2024.

BRASIL. **Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes**. Participa + Brasil. Disponível em: https://www.gov.br/participamaisbrasil/tscriancaeadolescente. Acesso em: 13 ago. 2024.

BUITELAAR, J. C. **Child's best interest and informational self-determination: what the GDPR can learn from children's rights**. International Data Privacy Law, v. 8, n. 4, p. 293-308, 2018.

CANADÁ. Department of Justice. **Child Rights Impact Assessment (CRIA)**. Disponível em: https://www.justice.gc.ca/eng/csj-sjc/cria-erde/tool-outil.html. Acesso em: 12 ago. 2024.

CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA (CESeC). **O Panóptico: Monitor do Reconhecimento Facial no Brasil**. Rio de Janeiro: CESeC, 2023. Disponível em: https://cesecseguranca.com.br/projeto/o-panoptico-monitor-do-reconhecimento-facial-no-brasil/. Acesso em: 12 ago. 2024.

COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil** - TIC Kids Online Brasil 2022. Disponível em: https://cetic.br/media/docs/publicacoes/1/20230825142135/tic_kids_online_2022_livro_eletronico.pdf. Acesso em: 12 ago. 2024.

COSTA, Eduarda; MENDONÇA, Eduardo; MONAGREDA, Johanna; MENDONÇA, Julia; GUEDES, Paula; MARTINS, Pedro; SANTOS, Pedro Henrique. **Contribuição Data Privacy Brasil - Tomada de Subsídios Direitos dos Titulares**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024. Disponível em: https://drive.google.com/file/d/1p1HWSTu_oID7SY0MXlqiv-

fomEhTUSahk/view. Acesso em: 13 ago. 2024.

DATA PRIVACY BRASIL & OAB-SP. **Contribuição à Tomada de Subsídios sobre Tratamento de Dados de Crianças e Adolescentes**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/12/tomada-subsidios-infancia.pdf. Acesso em: 12 ago. 2024.

DIGITAL FUTURES COMMISSION. **A Digital Future for Children: The Case for a Digital Environment that Works for Children**. 2021. Disponível em: https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf. Acesso em: 12 ago. 2024.

HARTUNG, Pedro. **The children's rights-by-design standard for data use by tech companies**. Unicef Good Governance of Children's Data Project, 2020. Disponível em: https://tinyurl.com/2s42h5k4. Acesso em: 12 ago. 2024.

INTERNETLAB. **Educação na mira: o uso de dados e tecnologias digitais em escolas públicas no Brasil**. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 12 ago. 2024.

LEGO. **Política de Privacidade**. Disponível em: https://kids.lego.com/pt-br/legal/privacy-policy. Acesso em: 12 ago. 2024.

MENDONÇA, Julia; LOBO MARTINS, Pedro; MARTINS DOS SANTOS, Pedro Henrique. **Contribuição da Data Privacy Brasil sobre Legítimo Interesse**. São Paulo: Data Privacy Brasil, 2023. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2023/11/contribuicao-legitimo-interesse-_dataprivacybrasil.pdf. Acesso em: 12 ago. 2024.

MILLER, Arthur. **The Assault on Privacy**. Ann Arbor: University of Michigan Press, 1970.

MONTEIRO, Luiz Augusto Ferreira; SILVA, Bárbara de Oliveira. **O Impacto da LGPD na Privacidade Infantil: Uma Análise das Medidas de Proteção**. Revista Brasileira de Política e Direito, v. 16, n. 2, p. 127-146, 2022.

REIS, Pedro. **A Proteção dos Dados Pessoais e a Criança: Uma Análise Crítica do Regulamento Geral sobre a Proteção de Dados da União Europeia**. Porto: Porto Editora, 2020.

UNICEF. **Digital Privacy and Protection: The Rights of Children and Adolescents in a Digital Age**. Disponível em: https://www.unicef.org/reports/digital-privacy-and-protection-rights-children-and-adolescents-digital-age. Acesso em: 12 ago. 2024.

UNICEF. **Principles for Digital Child Rights: Recommendations for Policy Makers**. Disponível em: https://www.unicef.org/documents/principles-digital-child-rights-recommendations-policy-makers. Acesso em: 12 ago. 2024.

YOUNG, Kirstie. **Age Assurance Technologies and Child Online Safety: A Review of Current Practices**. 2022. Disponível em: https://www.ictworks.org/age-assurance-technologies-child-safety-review/. Acesso em: 12 ago. 2024.

ZANATTA, Rafael; JONAS, Valente; JÚLIA, Mendonça. **Entre o abusivo e o excessivo: Novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD**. Privacidade e Proteção de Dados de Crianças e Adolescentes. in: Priscilla Laterça, Elora Fernandes, Chiara Teffé and Sérgio Branco. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, p. 396-426, 2021.