



São Paulo, 31 de agosto de 2022

À
Autoridade Nacional de Proteção de Dados

Ref.: Sugestão à tomada de subsídios aberta pela Autoridade Nacional de Proteção de Dados (ANPD) para construção da Agenda Regulatória do biênio 2023-2024.

Prezado Diretor-Presidente Waldemar Gonçalves Ortunho Júnior,

O **Instituto Alana**¹, vem, respeitosamente, por meio de seu programa **Criança e Consumo**², **tecer considerações** quanto à tomada de subsídios³ que visa subsidiar a elaboração de minuta da Agenda Regulatória do biênio 2023-2024 da Autoridade Nacional de Proteção de Dados.

I. O Instituto Alana e o Programa Criança e Consumo

1. O Instituto Alana é uma organização da sociedade civil, sem fins lucrativos, que aposta em iniciativas que buscam a garantia de condições para a vivência plena das

¹ <https://alana.org.br/>

² <https://criancaeconsumo.org.br/>

³ Disponível em: <https://www.gov.br/participamaisbrasil/tomada-de-subsidios-agenda-regulatoria>. Acesso em: 09.08.2022.

crianças e adolescentes. Criado em 1994, conta hoje com programas, plataformas, projetos próprios e parcerias e tem como missão “honrar a criança⁴”.

2. Em 2006, para divulgar e debater ideias sobre as questões relacionadas aos direitos das crianças e dos adolescentes no âmbito das relações de consumo, perante o consumismo ao qual são expostos, assim como para apontar meios de minimizar e prevenir os prejuízos decorrentes da comunicação mercadológica e da exploração comercial voltadas ao público infantojuvenil, cria-se o programa **Criança e Consumo**.

3. Com a compreensão de que crianças e adolescentes são grandes usuárias, mas também consumidoras de mídias digitais e de novas tecnologias de comunicação e informação, o programa estabeleceu enquanto eixo de trabalho a defesa dos direitos digitais das crianças e dos adolescentes por meio do combate à exploração comercial infantil, especialmente em um contexto de avanço de práticas vigilantistas que transformam os dados coletados das crianças em importantes ativos comerciais, em detrimento de seu pleno desenvolvimento e autonomia formacional e informacional. Nessa toada, entende-se como essencial a proteção da imagem, privacidade, intimidade e desenvolvimento saudável e livre de interferências externas das crianças e adolescentes no ambiente digital.

II. Crianças e adolescentes são prioridade da nação

4. O artigo 227 da Constituição Federal inaugurou a Doutrina da Proteção Integral da criança e do adolescente no Brasil, sendo responsável pelo reconhecimento de crianças e adolescentes como sujeitos de direitos em etapa peculiar de desenvolvimento, a demandar especial e prioritária atenção na salvaguarda de seus direitos fundamentais.

5. A referida disposição legal expressamente prevê o dever compartilhado pelo Estado, família e toda a sociedade em zelar pela garantia do devido cumprimento dos direitos reservados às crianças e adolescentes.

6. De forma complementar, o Estatuto da Criança e do Adolescente assegura que crianças e adolescentes, além dos direitos fundamentais reservados a todos os cidadãos, também são titulares de proteção integral e especial, reservando-lhes uma série de direitos específicos, dado o fato de serem pessoas em desenvolvimento biopsicossocial⁵.

7. O mesmo diploma legal define em seu artigo 4º que a absoluta prioridade na efetivação dos direitos de crianças e adolescentes se dá também para a formulação e execução

⁴ A definição de “criança” adotada pelo **Instituto Alana** é a mesma estabelecida pela Convenção sobre os Direitos da Criança de 1989, que a define, em seu artigo 1º, como “todo ser humano com menos de 18 anos de idade, salvo quando, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes”. Disponível em: <<https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>> Acesso em 11.08.2022.

⁵ Art. 3º da Lei 8.069/90: A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

de políticas públicas⁶. Por isso, esses direitos também devem integrar, com prioridade, as discussões a serem travadas no âmbito de atuação desta importante Autoridade.

8. Tanto é assim que a Lei Geral de Proteção de Dados Pessoais, em seu artigo 14, já define regra específica e mais protetiva para o tratamento dos dados pessoais de crianças e adolescentes, prova da irradiação a outras normas da disposição constitucional da prioridade absoluta e a disposição estatutária da proteção integral:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

9. O melhor interesse da criança é um conceito amplo que atua para garantir que em qualquer situação em que potencialmente crianças e adolescentes sejam afetadas, busque-se a alternativa que melhor satisfaça e se adeque aos direitos desses grupos de pessoas. No contexto específico da LGPD, a primazia do melhor interesse é posta, pela lei, como régua guia para o tratamento de dados pessoais de crianças e adolescentes. É ilegal, portanto, o tratamento de dados pessoais de crianças e adolescentes pautado em interesses incompatíveis com o melhor interesse desse grupo de indivíduos.

10. Inclusive, em potencial colisão de direitos ou de interesses, ainda que de grande relevância social, a regra da prioridade absoluta nos assegura que prevaleçam os interesses da criança e do adolescente, individualmente ou coletivamente afetados.

11. Apesar disso, ainda existem disputas de narrativas ao redor da norma, o que coloca, na prática, os interesses e direitos desse grupo de titulares em risco. As crianças e adolescentes estão rotineiramente em contato, tanto no ambiente presencial como no ambiente virtual, com plataformas digitais, sites, jogos e outros serviços que usam dados pessoais como substrato de seus negócios, muito embora o tratamento de seus dados pessoais seja realizado, em muitos destes casos, à revelia do quanto disposto na legislação.

12. É absolutamente imperioso, portanto, que, dada a prioridade absoluta e a proteção integral dos direitos de crianças e adolescentes, bem como de seu melhor interesse, esse grupo de indivíduos seja uma das prioridades da Autoridade Nacional de Proteção de Dados, inclusive enquanto aspecto transversal dos eixos temáticos a serem trabalhados pela Autoridade.

13. A ANPD possui competência e protagonismo para fomentar a necessária segurança ao tratamento dos dados pessoais de crianças e adolescentes sempre com base em seu melhor interesse, evitando-se assim a sua exploração comercial, de modo que os dados

⁶Art. 4º da Lei 8.069/90: 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. Parágrafo único. A garantia de prioridade compreende: a) primazia de receber proteção e socorro em quaisquer circunstâncias; b) precedência de atendimento nos serviços públicos ou de relevância pública; c) preferência na formulação e na execução das políticas sociais públicas; d) destinação privilegiada de recursos públicos nas áreas relacionadas com a proteção à infância e à juventude.

personais e a privacidade das crianças sejam protegidos. Para isso, os materiais a serem eventualmente elaborados pela Autoridade devem contemplar diretrizes para usuários, agentes empresariais, operadores e toda a cadeia de agentes de tratamento dos dados pessoais.

14. Nesse sentido, o **Instituto Alana** requer à Autoridade Nacional de Proteção de Dados que empregue prioritária atenção para o tratamento de dados de crianças e adolescentes, dado todo o arcabouço jurídico de proteção a esses indivíduos e o fato de que as práticas de tratamento realizadas, em especial no ambiente digital, possuem potencial de afetar enormemente a privacidade e outros direitos de seus titulares, pessoas em etapa peculiar de desenvolvimento.

15. Ainda, destaca que, se as práticas predatórias de coleta e exploração comercial dos dados pessoais de crianças e adolescentes são absolutamente contrárias a suas liberdades e seus direitos, espera-se, portanto, que em nível de regulamentação seja sua ilegalidade e proibição reafirmadas.

III. A regulação do setor econômico da educação na perspectiva da proteção de dados também é urgente e deve ser uma das prioridades da ANPD

16. Instituições públicas e privadas educacionais constantemente tratam dados pessoais de estudantes. Nome, endereço, data de nascimento, alergias, frequência, notas e muitas outras informações são armazenadas e transmitidas nos espaços físicos e digitais dos ambientes educacionais⁷.

17. Segundo dados da TIC Educação de 2020, divulgados recentemente na publicação “PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: Perspectivas de indivíduos, empresas e organizações públicas no Brasil”⁸, 85% das escolas públicas de educação básica consultam ou armazenam dados cadastrais dos alunos e alunas em formatos eletrônicos⁹.

18. A manipulação de dados pessoais de alunos e alunas, especialmente crianças e adolescentes, gera preocupações quanto à segurança do armazenamento, transparência na coleta e compartilhamento, dentre outros questionamentos. Apesar do grande volume de dados tratados pelas instituições educacionais, a TIC Educação de 2020 também apontou que 60% das escolas particulares e apenas 37% das escolas públicas municipais, estaduais e

⁷ O Instituto Alana, EducaDigital e Intervenções, sob apoio do NIC.BR, elaboraram, em 2021, um guia intitulado “A escola no mundo digital: dados e direitos de estudantes”. A publicação define dados pessoais estudantis como: “Toda informação que identifica cada estudante e cuja coleta e uso estejam relacionados à sua vida escolar”. Disponível em: <https://dadosstudentis.org.br/glossario-2/>. O documento integral está disponível em: <https://dadosstudentis.org.br/wp-content/uploads/2021/03/AEMDV3-1.pdf>. Acesso em: 30.8.2022.

⁸ Disponível em:

https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 29.8.2022.

⁹ Privacidade e proteção de dados pessoais 2021 [livro eletrônico] : perspectivas de indivíduos, empresas e organizações públicas no Brasil. Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo : Comitê Gestor da Internet no Brasil, 2022, 109.

federais de educação básica possuem documento que define a política de proteção de dados e de segurança da informação¹⁰. A ausência de documentos como estes coloca não só os titulares dos dados em posição vulnerável, mas a própria instituição que realiza o tratamento, que deixa de apontar, por exemplo, as bases legais que amparam as práticas de tratamento de dados realizadas.

19. Para além dos dados pessoais informados pelos estudantes, a ampliação do uso de plataformas virtuais e ambientes digitais aumenta a quantidade e os tipos de dados sob posse das instituições educacionais. Nesse contexto, dados rastreados, obtidos em razão de atividades realizadas pelos usuários de plataformas e tecnologias educacionais online, como buscas, interação, dentre outros, além de dados inferidos, obtidos por meio de técnicas que mesclam os dados obtidos do usuário, prevendo comportamentos e interesses, passam a compor o quadro de dados pessoais tratados pelas instituições, elevando assim os riscos aos titulares.

20. A divulgação recente da pesquisa “TIC Educação 2021” trouxe outros indicadores importantes para confirmar a percepção já existente quanto a disponibilização e uso de ferramentas tecnológicas para a educação. Isso porque 54% dos professores utilizam ambiente ou plataforma virtual de aprendizagem em atividades com os seus alunos e alunas¹¹. A despeito da plataformização da educação ser ou não positiva para o aprendizado, é fato que essa inserção para além de ser uma realidade também potencializa os tipos de análises disponíveis aos professores e gestores.

21. Especificamente sobre essa última afirmação, a TIC Educação 2021 questionou os professores quanto aos recursos de análise de aprendizagem disponíveis no ambiente ou na plataforma virtual de aprendizagem por eles utilizada. Dentre as respostas, 37% indicou que conseguia “medir a interação dos alunos e o seu nível de participação” e 39% tinha à sua disposição “relatórios e estatísticas sobre o desempenho de cada aluno e o seu nível de aprendizagem”¹².

22. Além de dados pessoais estudantis relacionados à aprendizagem, outros dados pessoais, inclusive sensíveis, podem sofrer tratamentos por instituições e estabelecimentos educacionais. De acordo com a edição 2020 da pesquisa TIC Educação, uma porcentagem pequena de escolas públicas contava com sistemas de identificação dos estudantes pela digital ou palma da mão (2%), contudo, há uma crescente procura por soluções tecnológicas que

¹⁰ Privacidade e proteção de dados pessoais 2021 [livro eletrônico] : perspectivas de indivíduos, empresas e organizações públicas no Brasil. Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo : Comitê Gestor da Internet no Brasil, 2022, p. 108.

¹¹ CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras - TIC Educação 2021 (Edição COVID-19 - Metodologia adaptada). Disponível em: <https://www.cetic.br/pt/tics/educacao/2021/professores/11/>. Acesso em: 29.8.2022.

¹² CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras - TIC Educação 2021 (Edição COVID-19 - Metodologia adaptada). Disponível em: <https://www.cetic.br/pt/tics/educacao/2021/professores/12/>. Acesso em: 29.8.2022.

associem identificação, controle de frequência e automatização da gestão de informações dos estudantes¹³.

23. Além do quadro já apontado, em recente estudo “*Como eles ousam espiar minha privacidade?*”¹⁴, organizado pela organização internacional Human Rights Watch, comprovou-se que, em razão da abrupta necessidade de adoção de plataformas para o ensino remoto, diversos governos ao redor do globo recomendaram aplicações e sites de amparo à educação básica que violaram a proteção de dados e a privacidade dos estudantes — crianças e adolescentes, portanto.

24. No que tange ao Brasil, o estudo analisou dois aplicativos desenvolvidos por governos estaduais (Minas Gerais e São Paulo) e seis aplicativos desenvolvidos por empresas privadas, mas recomendados por governos estaduais brasileiros. Em todos eles, em diferentes níveis, encontraram-se configurações que colocavam os dados dos alunos usuários em risco. Em alguns casos, nome completo, idade, localidade e outras informações foram indevidamente coletadas e tratadas para finalidades diversas, inclusive para o direcionamento de publicidade.

25. Essa constatação é grave. Para a garantia da continuidade do ensino, dados pessoais e a privacidade das crianças e adolescentes foram violados, em desrespeito à Constituição Federal, Estatuto da Criança e do Adolescente e à própria legislação de proteção de dados pessoais brasileira (LGPD).

26. Diante de todo o exposto, é urgente que a Autoridade Nacional de Proteção de Dados tenha a regulação do setor econômico da educação como tema prioritário de sua agenda, na perspectiva da proteção de dados, a fim de que possa garantir que também nos espaços educacionais, essenciais para a vivência de direitos sociais, em especial as crianças e adolescentes, tenham seus dados pessoais respeitados e tratados sempre de acordo com a legislação e em seu melhor interesse.

IV. Conclusão e Pedidos

27. Atendendo ao mandamento constitucional disposto no artigo 227, o Estatuto da Criança e do Adolescente define que crianças e adolescentes possuem garantia à proteção integral ainda quanto à formulação de políticas públicas. Por isso, seus direitos também devem integrar, com prioridade, as discussões a serem travadas no âmbito de atuação desta importante Autoridade.

¹³ Segundo informações divulgadas pelo grupo Globo de comunicação, na Bahia, mais de 7 mil estudantes já são monitorados em tempo real. Disponível em:

<https://g1.globo.com/jornal-nacional/noticia/2022/02/09/escolas-publicas-de-municipio-baiano-usam-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml>. Acesso em: 29.8.2022.

¹⁴ O relatório completo, em inglês, está disponível no seguinte link: https://www.hrw.org/sites/default/files/media_2022/07/HRW_20220711_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf. O sumário, com os principais resultados e recomendações, em português, pode ser acessado pelo link: https://www.hrw.org/sites/default/files/media_2022/07/Portuguese_EdTech%20Report_Sum%26Recs.pdf.

28. A consideração primordial a crianças e adolescentes é refletida, igualmente, na necessidade de regulamentação do setor econômico da educação. Uma vez que dados pessoais estudantis diversos são objeto de tratamento por instituições e estabelecimentos público e privados de educação, em especial aqueles de nível básico, é essencial que a Autoridade Nacional de Proteção de Dados tenha especial atenção quanto a este tema.

29. Destaca-se que a plataformização da educação, de modo a inserir no ambiente escolar plataformas digitais, sites e outros recursos tecnológicos, ampliam a coleta e as fontes de dados pessoais que podem ser objeto de tratamento, todavia, as pesquisas e dados disponíveis apontam que ainda há um importante caminho a ser percorrido para a garantia da cultura de proteção de dados pelo setor econômico da educação.

30. Todo o exposto, portanto, indica a inegável importância da regulação do setor econômico da educação, na perspectiva da proteção de dados, de forma prioritária pela Autoridade.

Diante disso, o **Instituto Alana** solicita que a Autoridade Nacional de Proteção de Dados garanta:

- a) Máxima prioridade para o tema do tratamento de dados de crianças e adolescentes (art. 14 da LGPD) e;
- b) Máxima prioridade para a regulação do setor econômico da educação, na perspectiva da proteção de dados.

31. Sem mais, o **Instituto Alana** aproveita para renovar os protestos de elevada estima e consideração por V. Sa., permanecendo, desde logo, à inteira disposição para eventuais esclarecimentos que se fizerem necessários, bem como para seguir contribuindo com os debates, estudos e demais materiais, inclusive regulatórios, a serem elaborados por essa ilustre Autoridade.

Atenciosamente,

Instituto Alana
Programa Criança e Consumo

Renato Godoy
Diretor de Relações
Governamentais do Instituto
Alana

Maria Mello
Coordenadora do programa
Criança e Consumo

João Francisco de Aguiar
Advogado do programa
Criança e Consumo

Moara Oliveira
Analista de Relações
Governamentais do Instituto
Alana

Thaís Rugolo
Advogada do programa
Criança e Consumo



HUMAN
RIGHTS
WATCH

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments
That Endorsed Online Learning During
the Covid-19 Pandemic

HUMAN
RIGHTS
WATCH

STUDENTS —
NOT PRODUCTS

Copyright © 2022 Human Rights Watch

All rights reserved.

Printed in the United States of America

ISBN: 978-1-62313-983-4

Cover illustration by: © Andrea Devia Nuño, Hero Studios

Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amsterdam, Beirut, Berlin, Brussels, Chicago, Geneva, Goma, Johannesburg, London, Los Angeles, Moscow, Nairobi, New York, Paris, San Francisco, Sydney, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: [HRW.org](https://www.hrw.org)

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

Summary	1
Recommendations	5
To Governments	5
To Ministries and Departments of Education	6
To Education Technology Companies	7
To Advertising Technology Companies and other Third-Party Companies that May Receive Data from EdTech Productss	8
Methodology	9
Selection Criteria	9
Product Types	10
Access and Archival	11
Technical Analysis: Apps	12
Dynamic Analysis and Children’s Participation	12
Technical Analysis: Websites	13
Technical Limitations	14
Interviews with Children, Parents, and Teachers	15
Requests for Comment	15
I. Covid-19, Education, and Technology	16
Covid-19 and Children’s Education	16
How the Internet-Based Economy Works	18
II. Hidden Surveillance: Children’s Data Harvested	21
Children’s Data and their Right to Privacy	21
Finding Out Who Children Are	23
Apps: Persistent Identifiers	24
Inescapable Surveillance	27
Websites: Canvas Fingerprinting	31
Tracking Where Children Are	31
Apps: Precise Location Data	32
Websites: Coarse Location Data	37
Tracking Who Children Know	38
Tracking What Children Do in the Classroom	40
Websites: Ad Trackers	41
Websites: Session Recording, Key Logging	48
Apps: Software Development Kits (SDKs)	52
Tracking Children Outside of the Classroom	64
Website Cookies	65

III. Hidden Manipulation: How Children’s Data Are Used	67
Profiled and Targeted	67
Behavioral Advertising	68
Influencing Information, Shaping Beliefs	78
Facebook (Meta)	80
Google	85
IV. Failure to Protect	88
Companies’ and Governments’ Child Rights Responsibilities	88
Child Data Protection Laws	89
Education	90
Students, Parents, and Teachers	91
Operating in Blind Faith	
Companies Failed to Protect	92
Governments Failed to Protect	93
Governments Directly Engage in Rights Violations	95
No Choice	98
Acknowledgments	100

Summary



On school days, 9-year-old Rodin wakes up every morning at 8 a.m. in Istanbul, Turkey. He eats a bowl of chocolate cereal for breakfast; his mother reminds him, as she always does, to brush his teeth afterwards. By 9 a.m., he logs into class and waves hello to his teacher and to his classmates. He hopes that no one can tell that he's a little sleepy, or that he's behind on his homework.

During breaks between classes, Rodin reads chat messages from his classmates and idly doodles on the virtual whiteboard that his teacher leaves open. He watches his best friend draw a cat; he thinks his friend is much better at drawing than he is. Later in the afternoon, Rodin opens up a website to watch the nationally televised math class for that day. At the end of each day, he posts a picture of his homework to his teacher's social media page.

Unbeknownst to him, an invisible swarm of tracking technologies surveil Rodin's online interactions throughout his day. Within milliseconds of Rodin logging into class in the morning, his school's online learning platform begins tracking Rodin's physical location—at home in his family's living room, where he has spent most of his days during the pandemic lockdown. The virtual whiteboard passes along information about his doodling habits to advertising technology (AdTech) and other companies; when Rodin's math class is over, trackers follow him outside of his virtual classroom and to the different apps and sites he visits across the internet. The social media platform Rodin uses to post his homework silently accesses his phone's contact list and downloads personal details about his family and friends. Sophisticated algorithms review this trove of data, enough to piece together an intimate portrait of Rodin in order to figure out how he might be easily influenced.

Neither Rodin nor his mother were aware that this was going on. They were only told by his teacher that he had to use these platforms every day to be marked as attending school during the Covid-19 pandemic.¹

This report is a global investigation of the education technology (EdTech) endorsed by 49 governments for children's education during the pandemic. Based on technical and policy analysis of 163 EdTech products, Human Rights Watch finds that governments' endorsements of the majority of these online learning platforms put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education.

¹ Human Rights Watch interview with Rodin R. and his mother, Istanbul, Turkey, June 11, 2021. The names of all children quoted in this report have been changed to protect their privacy.



Human Rights Watch observed 146 EdTech products directly sending or granting access to children's personal data to 199 AdTech companies.

The coronavirus pandemic upended the lives and learning of children around the world. Most countries pivoted to some form of online learning, replacing physical classrooms with EdTech websites and apps; this helped fill urgent gaps in delivering some form of education to many children.

But in their rush to connect children to virtual classrooms, few governments checked whether the EdTech they were rapidly endorsing or procuring for schools were safe for children. As a result, children whose families were able to afford access to the internet and connected devices, or who made hard sacrifices in order to do so, were exposed to the privacy practices of the EdTech products they were told or required to use during Covid-19 school closures.

Human Rights Watch conducted its technical analysis of the products between March and August 2021, and subsequently verified its findings as detailed in the methodology section. Each analysis essentially took a snapshot of the prevalence and frequency of tracking technologies embedded in each product on a given date in that window. That prevalence and frequency may fluctuate over time based on multiple factors, meaning that an analysis conducted on later dates might observe variations in the behavior of the products.

Of the 163 EdTech products reviewed, 145 (89 percent) appeared to engage in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights. These products monitored or had the capacity to monitor children, in most cases secretly and without the consent of children or their parents, in many cases harvesting data on who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use.

Most online learning platforms installed tracking technologies that trailed children outside of their virtual classrooms and across the internet, over time. Some invisibly tagged and fingerprinted children in ways that were impossible to avoid or get rid of—even if children, their parents, and teachers had been aware and had the desire and digital literacy to do so—without throwing the device away in the trash.

Most online learning platforms sent or granted access to children's data to third-party companies, usually advertising technology (AdTech) companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyze these data to guess at a child's personal characteristics and interests, and to predict what a child might do next and how they might be influenced. Access to these insights could then be sold to anyone—advertisers, data brokers, and others—who sought to target a defined group of people with similar characteristics online.

Children are surveilled at dizzying scale in their online classrooms. Human Rights Watch observed 145 EdTech products directly sending or granting access to children's personal data to 196 third-party companies, overwhelmingly AdTech. Put another way, the number of AdTech companies receiving children's data was discovered to be far greater than the EdTech companies sending this data to them, illustrating the financial incentives that place economic value on children's data and fuel extraordinarily intrusive surveillance and deep erosions of their privacy.

Some EdTech products targeted children with behavioral advertising. By using children's data—extracted from educational settings—to target them with personalized content and advertisements that follow them across the internet, these companies not only distorted children's online experiences, but also risked influencing their opinions and beliefs at a time in their lives when they are at high risk of manipulative interference. Many more EdTech products sent children's data to AdTech companies that specialize in behavioral advertising or whose algorithms determine what children see online.

It is not possible for Human Rights Watch to reach definitive conclusions as to the companies' motivations in engaging in these actions, beyond reporting on what we observed in the data and the companies' and governments' own statements. In response to requests for comment, several EdTech companies denied collecting children's data. Some companies denied that their products were intended for children's use, or stressed that their virtual classroom pages for children's use had adequate privacy protections, even if Human Rights Watch's analysis found that pages adjacent to the virtual classroom pages (such as the login page, home page or adjacent page with children's content) did not. AdTech companies denied knowledge that the data was being sent to them, indicating that in any case it was their clients' responsibility not to send them children's data.

Governments bear the ultimate responsibility for failing to protect children's right to education. With the exception of a single government—Morocco—all governments reviewed in this report endorsed at least one EdTech product that risked or undermined children's rights. Most EdTech products were offered to governments at no direct financial cost to them; in the process of endorsing and ensuring their wide adoption during Covid-19 school closures, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy, access to information, and potentially freedom of thought.

Many governments put at risk or violated children's rights directly. Of the 42 governments that provided online education to children by building and offering their own EdTech products for use during the pandemic, 39 governments produced products that handled children's personal data in ways that risked or infringed on their rights. Some of these governments made it compulsory for students and teachers to use their EdTech product, not only subjecting them to the risks of misuse or exploitation of their data, but also making it impossible for children to protect themselves by opting for alternatives to access their education.

Children, parents, and teachers were denied the knowledge or opportunity to challenge these data surveillance practices. Most EdTech companies did not disclose their surveillance of children through their data; similarly, most governments did not provide notice to students, parents, and teachers when announcing their EdTech endorsements.

In all cases, this data surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most EdTech companies did not allow their students to decline to be tracked; most of this monitoring happened secretly, without the child's knowledge or consent. In most instances, it was impossible for children to opt out of such surveillance and data collection without opting out of compulsory education and giving up on formal learning altogether during the pandemic.

Remedy is urgently needed for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. Governments should conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.

In line with child data protection principles and corporations' human rights responsibilities as outlined in the United Nations Guiding Principles on Business and Human Rights, EdTech and AdTech companies should not collect and process children's data for advertising. Companies should inventory and identify all children's data ingested during the pandemic, and ensure that they do not process, share, or use children's data for purposes unrelated to the provision of children's education. AdTech companies should immediately delete any children's data they received; EdTech companies should work with governments to define clear retention and deletion rules for children's data collected during the pandemic.

As more children spend increasing amounts of their childhood online, their reliance on the connected world and digital services that enable their education will continue long after the end of the pandemic. Governments should develop, refine, and enforce modern child data protection laws and standards, and ensure that children who want to learn are not compelled to give up their other rights in order to do so.

Children should be actively consulted throughout these processes, helping to build safeguards that protect meaningful, safe access to online learning environments that provide the space for children to develop their personalities and their mental and physical abilities to their fullest potential.

Recommendations

To Governments

Facilitate urgent remedy for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. To do so:

- Conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.
- Require EdTech companies with failed data privacy audits to identify and immediately delete any children's data collected during the pandemic.
- Require AdTech companies to identify and immediately delete any children's data they received from EdTech companies during the pandemic.
- Prevent the further collection and processing of children's data by technology companies for the purposes of profiling, behavioral advertising, and other uses unrelated to the purpose of providing education.

Adopt child-specific data protection laws that address the significant child rights impacts of the collection, processing, and use of children's personal data. Where child data protection laws already exist, update and strengthen implementation measures to deliver a modern child data protection framework that protects the best interests of the child in complex online environments.

Enact and enforce laws ensuring that companies respect children's rights and are held accountable if they fail to do so. In line with the United Nations Guiding Principles on Business and Human Rights, such laws should require companies to:

- Conduct and publish child rights due diligence processes.
- Provide full transparency in data supply chains, and publicly report on how children's data are collected and processed, where they are sent, to whom, and for what purpose.
- Provide child-friendly, age-appropriate processes for remedy and redress for children who have experienced infringements on their rights; such mechanisms should be transparent, independently accountable, and enforceable.

Require child rights impact assessments in any public procurement processes that provide essential services to children through technology.

Ban behavioral advertising to children. Commercial interests and behavioral advertising should not be considered legitimate grounds of data processing that override a child's best interests or their fundamental rights.

Ban the profiling of children. In exceptional circumstances, governments may lift this restriction when it is in the best interests of the child, and only if appropriate safeguards are provided for by law.

To Ministries and Departments of Education

Where online learning is adopted as a preferred or hybrid mechanism for delivering education, allocate funding to pay for services that safely enable online education, rather than allowing the sale and trading of children's data to finance the services.

Ensure that any services that are endorsed or procured to deliver online education are safe for children. In coordination with data protection authorities and other relevant institutions:

- Require all companies providing educational services to children to identify, prevent, and mitigate negative impacts on children's rights, including across their business relationships and global operations.
- Require child data protection impact assessments of any educational technology provider seeking public investment, procurement, or endorsement.
- Ensure that public and private educational institutions enter into written contracts with EdTech providers that include protections for children's data. Children should not be expected to enter into a contract, and children and guardians cannot give valid consent when it cannot be freely refused without jeopardizing a child's right to education.
- Define and provide special protections for categories of sensitive personal data that should never be collected from children in educational settings, such as precise geolocation data.

Provide child-friendly, age-appropriate, and confidential reporting mechanisms, access to expert help, and provisions for collective action in local languages for children seeking justice and remedy. Such measures should avoid placing undue burden or exclusive responsibility on children or their caregivers to seek remedy from companies by acting individually or exposing themselves in the process.

Develop and promote digital literacy and children's data privacy in curricula. Provide training programs for ministry staff, teachers, and other school staff in digital literacy skills and protection of children's data privacy, to support teachers to conduct online learning for children safely.

Seek out children's views in developing policies that protect the best interests of the child in online educational settings, and meaningfully engage children in enhancing the positive benefits that access to the internet and educational technologies can provide for their education, skills, and opportunities.

To Education Technology Companies

Provide urgent remedy and redress where children's rights have been put at risk or infringed through companies' data practices during the pandemic. To do so:

- Immediately stop collecting and processing children's data for user profiling, behavioral advertising, or any purpose other than what is strictly necessary and relevant for the provision of education.
- Stop sharing children's data for purposes that are unnecessary and disproportionate to the provision of their education. In instances where children's data are disclosed to a third party for a legitimate purpose, in line with child rights principles and data protection laws, enter into explicit contracts with third-party data processors, and apply strict limits to their processing, use, and retention of the data they receive.
- Apply child flags to any data shared with third parties, to ensure that adequate notice is provided to all companies in the technology stack that they are receiving children's personal data, and thus obliged to apply enhanced protections in their processing of this data.
- Inventory and identify children's personal data ingested during the pandemic, and take measures to ensure that these data are no longer processed, shared, retained, or used for commercial or other purposes that are not strictly related to the provision of children's education.
- Companies with EdTech products designed for use by children should stop collecting specific categories of children's data that heighten risks to children's rights, including their precise location data and advertising identifiers.

Undertake child rights due diligence to identify, prevent, and mitigate companies' negative impact on children's rights, including across their business relationships and global operations, and publish the outcomes of this due diligence process.

Respect and promote children's rights in the development, operation, distribution, and marketing of EdTech products and services. Ensure that children's data are collected, processed, used, protected, and deleted in line with child data protection principles and applicable laws.

Provide privacy policies that are written in clear, child-friendly, and age-appropriate language. These should be separate from legal and contractual terms for guardians and educators.

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for rights abuses when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged abuses, and should effectively end ongoing infringements on rights.

To Advertising Technology Companies and other Third-Party Companies that May Receive Data from EdTech Products

Inventory and identify all children's data received through tracking technologies the technology companies own and take measures to promptly delete these data and ensure that these data are not processed, shared, or used. To do so:

- Identify all apps and websites that have installed tracking technologies owned by technology companies and transmitted user data to them.
- Of these, classify and create a list of services primarily directed at children, which should be monitored and updated periodically. Notify the parent companies of these services that they need to provide explicit evidence that their service is not made for children to remove their product from this list.
- Using this list, companies should review and promptly delete any children's data received from services made for children.

Prevent the use of technology companies' tracking technologies to surveil children, or any user of these services designed for use by children.

- Regularly audit incoming data and the companies sending them. Delete or otherwise disable the use of any received children's data or user data received from services designed for use by children, when detected.
- Notify and require companies and clients that use tracking technologies to declare any children's data collected through these tools with a child flag or through other means, so that tagged data can be automatically flagged and deleted before transmission to third-party companies.

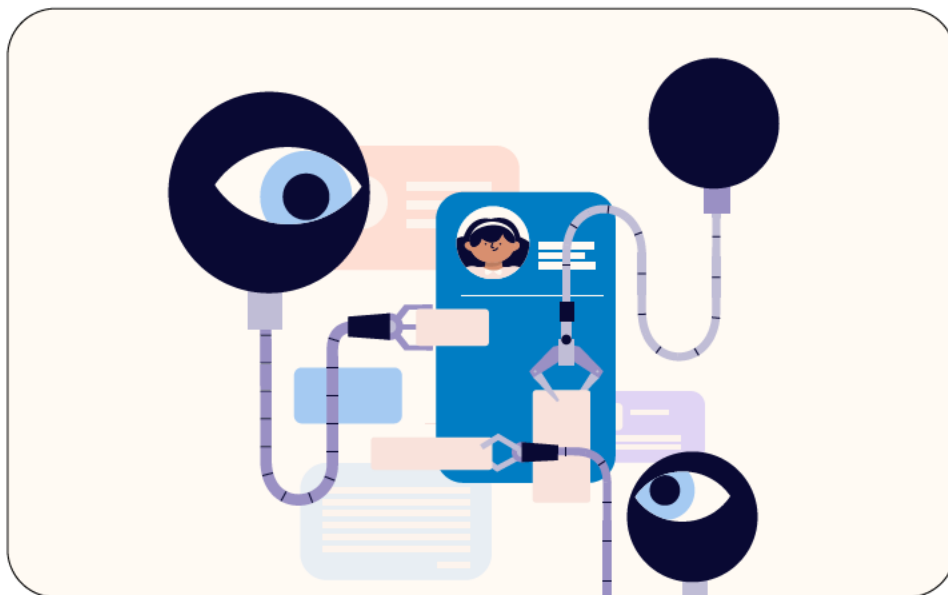
Develop and implement effective processes to detect and prevent the commercial use of children's data collected by technology companies' tracking technologies.

Undertake child rights due diligence to identify, prevent, and mitigate technology companies' impact on children's rights, including across their business relationships and across global operations, and publish the outcomes of this due diligence process..

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for infringements on rights when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged infringements, and should end ongoing violations.

Methodology

This report covers 49 countries that recommended 163 educational technology (EdTech) products for children to use for online learning during Covid-19 school closures.



Human Rights Watch conducted technical analysis on each product to assess how it handled children's data, then compared the results to the product's privacy policy to determine whether the EdTech company disclosed its data practices to children and their caregivers. Human Rights Watch also examined the advertising technology (AdTech) companies and data brokers found to receive children's data, and analyzed the marketing materials and developer documentation of those found to be receiving significant amounts of children's data.

The methods used in this report were free and available for use by governments prior to endorsing or procuring any of the EdTech products analyzed here. While a tool that was used to analyze websites, Blacklight, was published in September 2020, the tests it runs to identify privacy-infringing technologies were individually available and free to use in the form of various privacy census tools built over the past decade. As of November 2021, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.

Human Rights Watch invites experts, journalists, policymakers, and readers to recreate, test, and engage with our findings and research methods. Our datasets, preserved evidence, and a detailed technical methodology can be found online.

Selection Criteria

Human Rights Watch examined the Covid-19 education emergency response plans, documents, and announcements of 68 of the world's most populous countries. Of these, 49 countries adopted online learning as a component of their national plans for continued learning throughout school closures. The EdTech products endorsed or procured by these ministries or departments of education were included for analysis in this report.

In countries where the education ministry recommended a large number of EdTech products—in some cases, numbering in the hundreds—a Mersenne Twister pseudorandom number generator was used to randomly select a maximum of ten products that would serve as an illustrative sample of that education ministry's decisions.²

² Widely used in statistics, computer science, and cryptography, a Mersenne Twister is a pseudorandom number generator, or an algorithm that generates a sequence of numbers that are fairly random. See: Wikipedia, "Mersenne Twister," https://en.wikipedia.org/wiki/Mersenne_Twister (accessed November 8, 2021).

Seven countries—Australia, Brazil, Canada, Germany, India, Spain, and the United States—delegate significant decision-making authority to state—or regional—level education authorities. During the pandemic, this included decisions about what EdTech to endorse or procure for school use. Human Rights Watch identified the two most populous states or provinces in these countries and included their EdTech endorsements for analysis. Similarly for the United Kingdom, the two most populous constituent countries—England and Scotland—were identified for analysis.

As a result, 163 products were analyzed from the following 49 countries: Argentina, Australia (New South Wales, Victoria), Brazil (Minas Gerais, São Paulo), Burkina Faso, Cameroon, Canada (Quebec)³, Chile, China, Colombia, Côte d'Ivoire, Ecuador, Egypt, France, Germany (Baden-Württemberg, Bavaria), Ghana, Guatemala, India (Maharashtra, national, Uttar Pradesh), Indonesia, Iran, Iraq, Italy, Japan, Kazakhstan, Kenya, Malawi, Malaysia, Mexico, Morocco, Nepal, Nigeria, Pakistan, Peru, Poland, Republic of Korea, Romania, Russian Federation, Saudi Arabia, South Africa, Spain (Andalucía, Catalonia), Sri Lanka, Taiwan, Thailand, Turkey, United Kingdom (England, Scotland), United States (California, Texas), Uzbekistan, Venezuela, Vietnam, and Zambia.

Product Types

Of the 163 EdTech products investigated by Human Rights Watch, 39 were mobile applications (“apps”), 90 were websites, and 34 were available in both formats. Of the products available in both app and website formats, Human Rights Watch analyzed both, except for four products where the app versions were no longer available online, or offered only in iOS, Apple’s operating system.

Apps running on Google’s Android operating system are the focus of this report. Android is the dominant mobile operating system worldwide, in large part due to the ubiquity of lower-cost mobile phones that run Android.⁴ Children living in the countries covered by this report are more likely to have access to an Android device, if they have access to a device at all. This was reflected in the choices that governments made: almost all EdTech products endorsed by the governments covered in this report offer their apps for the Android platform.

In addition, Android’s open architecture makes it possible to easily access and observe the interactions between an app and the operating system, as well as to identify the data transmissions from the device running the app to online servers.

While this report focuses on apps built for Android, apps built for Apple’s iOS can also employ data tracking technologies and target behavioral advertising to users.⁵

3 Canada’s Ontario, and the single EdTech product that it recommended, was originally included in our analysis. After additional rounds of data verification and analysis of the EdTech product, which yielded an inconclusive assessment, Human Rights Watch removed Ontario from its list.

4 By one estimate, Android has 72.83 percent market share worldwide, with iOS taking up 26.35 percent. See: StatCounter, “Mobile Operating System Market Share Worldwide, June 2020-June 2021,” <https://web.archive.org/web/20210728054452/https://gs.statcounter.com/os-market-share/mobile/worldwide> (accessed July 27, 2021).

5 Thorin Klosowski, “We Checked 250 iPhone Apps—This is How They’re Tracking You,” *New York Times*, May 6, 2021, <https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/> (accessed April 14, 2022); Thorin Klosowski, “Looking Back on a Year of Apple’s Privacy Labels and Tracking,” *New York Times*, March 31, 2022, <https://www.nytimes.com/wirecutter/blog/apple-privacy-labels-tracking/> (accessed April 14, 2022).

Access and Archival

To investigate how EdTech products handled children's data and their rights, Human Rights Watch downloaded a copy of the latest version of the product and its privacy policy between February 19 and March 15, 2021. Human Rights Watch conducted the primary phase of its investigation between March and August 2021, and conducted further checks in November 2021 to verify findings.

To preserve documentation and to invite readers to recreate, test, and engage with our findings, the privacy policy, and EdTech website or app were archived, whenever available, on the Internet Archive's Wayback Machine. The versions of the EdTech apps examined by Human Rights Watch are listed in the appendices.

EdTech products were sorted into the following categories:

- | | |
|--|---|
| <p>1.
Products that do not require a user account to access learning content;</p> | <p>3.
Products that require a user account to access learning content; and</p> |
| <p>2.
Products that offer the choice to sign up for an optional user account;</p> | <p>4.
Products that require verification of the child's identity as a student, either by their school or their ministry of education, to set up a mandatory account to access the service.</p> |

To avoid misleading EdTech companies as to our affiliation and the nature of our research, no user accounts were created for products identified in categories 1, 2, and 4.

Human Rights Watch created user accounts for a limited number of EdTech products in category 3. As it is possible to disassemble and analyze apps' code without having to sign into a user account, accounts were created only for 27 websites in this category to test for privacy violations in the same environment used by children to attend classes. In these instances, Human Rights Watch explicitly identified the nature of our engagement, populating mandatory input fields with the following values to signal our affiliation and intent. Optional fields were left blank.

Email: [REDACTED]
 User name: hrwresearcher
 Organization / School name: Human Rights Watch
 First Name: HRW
 Last Name: Researcher
 Phone number: [a real number]

Throughout its investigation, Human Rights Watch did not interact with other users or enter into virtual classrooms.

Human Rights Watch did not create user accounts for products in category 4, as that would have entailed falsely assuming the identity of a real student. For these websites, technical analysis was restricted to webpages that children likely had to interact with in order to access their virtual classroom, prior to logging in, such as the product's home page or login page.

Some of the companies that offered EdTech products in category 4 told Human Rights Watch that the virtual classrooms and related spaces accessible to children after the login were adequately protective of privacy. These companies asserted that the pages before their product's login (e.g., the login page, home page, or adjacent page designed for children) were designed for use by teachers, parents and other adults, and not properly described as designed for children's use.

Technical Analysis: Apps

There are two methods of disassembling and analyzing a mobile app. The first is through static analysis, which analyzes an app's code and identifies its capabilities, or the functions and instructions that may be executed when the app is run. The second is through dynamic analysis, which runs the app under realistic conditions and observes what data is transmitted where, and to whom.

Human Rights Watch conducted manual static analysis tests on 73 apps, using Android Developer Studio to decompile the app and to analyze its code. All results were verified by scanning each app using Pithus, an open source mobile threat intelligence platform that conducts automated static analysis tests on mobile apps, and Exodus by Exodus Privacy, an open source privacy auditing platform that scans for trackers embedded in Android apps, and corroborating the results against Human Rights Watch's analyses.⁶

Additionally, Human Rights Watch commissioned Esther Onfroy, founder of Defensive Lab Agency, and the creator of both Pithus and Exodus Privacy, to conduct in-depth static and dynamic analysis on eight apps, which were used as a final check to ensure the accuracy of our results.

Dynamic Analysis and Children's Participation

Human Rights Watch collaborated with four children from India, Indonesia, South Africa, and Turkey who participated in an in-depth investigation to uncover how an EdTech app recommended by their government handled their privacy.

These children and their guardians were informed of the nature and purpose of our research, that they would receive no personal service or benefit for speaking to us, and our intention to publish a report with the information gathered. Human Rights Watch requested and received consent from the children and their guardians, and informed each that they were under no obligation to speak with us or to participate in the project.

Human Rights Watch asked each child to download a virtual private network (VPN) and the EdTech app on their mobile device. They were then asked to open, run, and close the VPN and the EdTech app several times within a single day, interacting with the app as if they were using it for school or for learning. After 24 hours, children deleted both from their phones.

Esther Onfroy of the Defensive Lab Agency received the data files and analyzed them to identify data flows and transmissions. These findings were corroborated against dynamic analysis conducted on each app, using a VPN to simulate app usage in the child's country. This methodology design maximally protected children's privacy by encrypting the child's data and ensuring that only the data flows could be analyzed, without revealing the substance of children's personal data.

All children's data were securely stored, then deleted, at the end of the investigation. The data files for one child's experiment were provided to the child, at their request.

⁶ Pithus, "Mobile threat intelligence for the masses," <https://beta.pithus.org/> (accessed September 21, 2021); Exodus Privacy, "Exodus Privacy," <https://exodus-privacy.eu.org/en/> (accessed September 21, 2021).

Technical Analysis: Websites

To understand how websites handle children's data, Human Rights Watch used Blacklight, a real-time website privacy inspector built by Surya Mattu, senior data engineer and investigative data journalist at The Markup.⁷

Released in September 2020, Blacklight emulates how a user might be surveilled while browsing the web.⁸ The tool scans any website, runs tests for seven known types of surveillance, and returns an instant privacy analysis of the inspected site. Built on the foundation of robust privacy census tools built over the past decade, Blacklight monitors scripts and network requests to observe when and how user data is being collected, and records when this data is being sent to known third-party AdTech companies.⁹

Blacklight exists in two formats: as a user-friendly interface on The Markup's website, and as an open source command-line tool.¹⁰ Human Rights Watch chose to work with the latter, as it provides the flexibility to adapt the tool to provide customized analysis, as well as a higher observational power that yields fine-grained evidence of the surveillance it detects on websites. Surya Mattu of The Markup generously assisted Human Rights Watch in customizing Blacklight for this investigation.

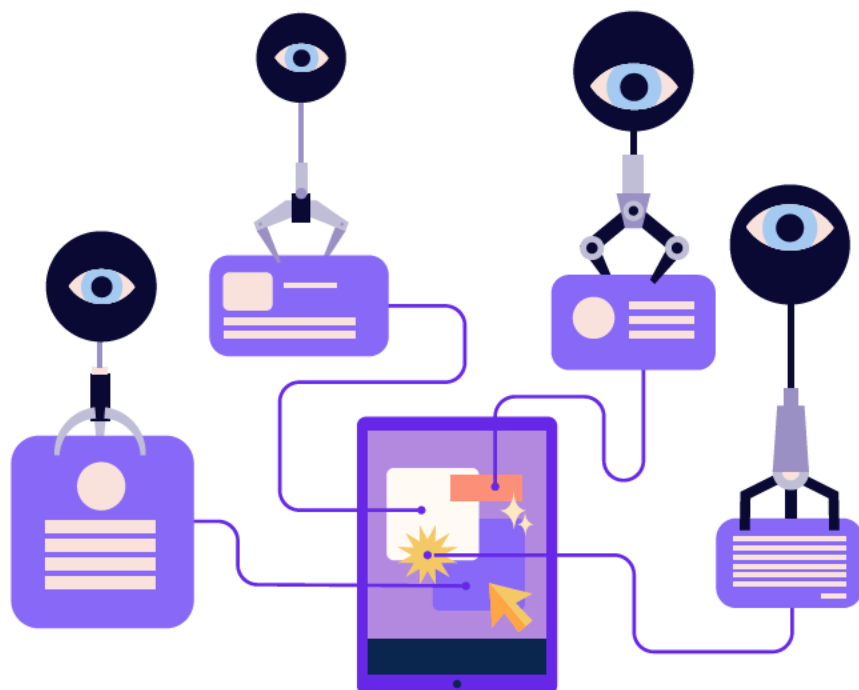
In order to recreate the experience of a child using an EdTech website in their country, and how their data might be collected, handled, and sent to third parties, Human Rights Watch conducted all technical tests while running a VPN set to the country where the product was endorsed by the government for children's education. This proved essential: early tests conducted by Human Rights Watch found that the prevalence of surveillance technologies embedded in a website changed depending on the country the website believed that its user was located. Many of the observed differences appeared to be related to that country's data protection laws, where they exist.

7 The Markup, "Blacklight," <https://themarkup.org/blacklight> (accessed September 21, 2021).

8 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 7, 2021).

9 Ibid. AdTech companies and their domains were identified by using DuckDuckGo Tracker Radar. See: DuckDuckGo, "DuckDuckGo Tracker Radar Exposes Hidden Tracking," March 5, 2020, <https://spreadprivacy.com/duckduckgo-tracker-radar/> (accessed March 1, 2021).

10 The Markup, "Blacklight Collector," GitHub, <https://github.com/the-markup/blacklight-collector> (accessed March 1, 2021); The Markup, "Blacklight Reporter," GitHub, <https://github.com/the-markup/blacklight-reporter> (accessed March 1, 2021).



Human Rights Watch selected for examination websites that were explicitly recommended by governments for use for children's online education. In response to Human Rights Watch's findings, some companies noted that their government-recommended products were designed for use by teachers, parents and other adults, and not for use by children. Accepting those claims as fact, this still raises the question of why the governments recommended pages for use by children that were not adequately vetted to protect their privacy, as well as the question of whether the companies should have changed their privacy practices on those pages once the government made its recommendation.

Technical Limitations

Analyzing apps using static analysis may yield false positives, as not all of the app's source code might be implemented in practice when a user runs the app. Put another way, an app may not use all of the programmed functionalities of which it is capable. Human Rights Watch notes this limitation by distinguishing between analysis of the code's capabilities (static analysis) and detections of actual transmission of children's data (dynamic analysis) throughout the report.

A technical analysis does not definitively determine the intent of any particular tracking technology, or how the collected data is used. For example, an EdTech product can include third party computer code that collects information that may be useful to monitor the product's performance and stability. The same data collected by the same third-party code may also be used in tandem with other third-party code to enable data collection for advertising or other marketing purposes. In a static analysis, it is not possible to conclude whether user data were collected, or the scope or purpose of the data collection. Neither is it possible solely with a technical analysis to determine how the collected data is used by the third party.

As another example, third-party computer code embedded in a product to perform an administrative function can be designed also to enable access to a device's camera, microphone, or another feature. In a static analysis, it is possible to detect the capability, but not whether the capability is utilized. In addition, the EdTech company implementing such third-party code for an administrative function may not have plans to enable those features, and may not be aware of the possibility. Note also that access by any code to an Android device's camera or microphone is possible only if the user settings on the device enable such sharing.

Where possible, Human Rights Watch worked to reduce ambiguity by examining the parent companies that own the tracking technologies found in an EdTech product, as well as the companies found to receive transmissions of children's data. Human Rights Watch conducted further analysis on companies that receive, analyze, trade, or sell people's personal data for commercial and other purposes, and reviewed their publicly available marketing materials and developer documentation.

Blacklight's analysis is limited by three other factors: the simulation may trigger different surveillance responses from the website under examination, because it is a simulation of user behavior, not actual user behavior; the possibility of producing false positives while scanning for canvas fingerprinting; the possibility of producing false negatives through a stack tracing technique. Further investigation by The Markup determined that the probability of these false errors occurring is very low, and that Human Rights Watch's methodology design may have further reduced this risk.¹¹ A detailed discussion of these technical limitations can be found on Blacklight's methodology, available online.¹²

11 According to The Markup, false positives with canvas fingerprinting occur "very occasionally" when Blacklight is run in the cloud, because it is difficult to distinguish the tool from any other bot. As Human Rights Watch conducted its technical tests by running Blacklight on a local machine with a VPN, this, in theory, would have further reduced the risk of false positives. Furthermore, The Markup notes that the stack tracing technique did not produce false negatives in their tests or in their survey of the 100,000 most popular websites on the internet. See: Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," The Markup, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 7, 2021).

12 Ibid.

For readers seeking to replicate Human Rights Watch’s findings, it is important to note that the observed behavior of these apps and websites, and the detected prevalence and frequency of tracking technologies embedded in them, may fluctuate. This is influenced by multiple factors, including the geographical location of the user, date and time of testing, and the device or browser type, among other variables. In addition, apps and websites that use AdTech services to offer advertisers and other third-party companies the opportunity to target their students with ads through an electronic high-frequency trading process known as real-time bidding, further described in Chapter 1, may yield different results as to the recipient of the children’s data, as different third parties may have won the bid each time.

Human Rights Watch conducted manual analysis on four websites—Distance Learning (Cameroon), Eduyun (China), Smart Revision (Zambia), and e-learning portal (Zambia)—on which Blacklight tests failed for a variety of technical failures. One site was incompatible with the browser used by Blacklight, and another refused to load upon detecting the VPN service used by Human Rights Watch. The manual analysis conducted on these four sites followed the same methodology used by the Blacklight tool.

Interviews with Children, Parents, and Teachers

Human Rights Watch interviewed students, parents, and teachers between April 2020 and April 2021 about their experiences with online learning. Interviewees were based in the following 17 countries: Australia, Chile, Denmark, Germany, Indonesia, India, Iran, Italy, Lebanon, Republic of Korea, Russia, Serbia, Spain, South Africa, Turkey, United Kingdom, and the United States.

Interviewees lived in capital cities, other cities, Indigenous communities, rural and remote locations, suburbs, towns, and villages.

Interviews were conducted directly, or with interpretation, in Arabic, Bahasa Indonesian, Danish, English, Ewe, Farsi, German, Hindi, Italian, Korean, Russian, Serbian, Spanish, and Turkish.

Interviewees were not paid to participate. Interviewees were informed of the purpose of the interview, its voluntary nature, and the ways in which the information would be used. They provided oral and written consent to be interviewed.

Many parents and teachers requested that their names not be used in this report to protect their privacy or the privacy of their children or students, or to feel free to speak about their school, or for cultural reasons. Children’s identities are protected with pseudonyms of their own choosing. Pseudonyms are reflected in the text with a first name followed by an initial and are noted in the footnotes.

Requests for Comment

Human Rights Watch shared the findings presented in this report with 95 EdTech companies, 199 AdTech companies, and the 49 governments covered in this report, and gave them the opportunity to respond and provide comments and clarifications. Of these, 48 EdTech companies, 78 AdTech companies, and 10 governments responded as of May 24, 2022 at 12:00pm EDT.

I. Covid-19, Education, and Technology

13 Human Rights Watch interview with mother, Izhevsk, Russia, June 12, 2020.

14 Human Rights Watch, “*Years Don’t Wait for Them*”: Increased Inequalities In Children’s Right to Education Due to the Covid-19 Pandemic (New York: Human Rights Watch, 2021), <https://www.hrw.org/report/2021/05/17/years-dont-wait-them/increased-inequalities-childrens-right-education-due-covid>.

15 United Nations Educational, Scientific and Cultural Organization (UNESCO) Institute for Statistics, “Education: From disruption to recovery,” 2021, <https://en.unesco.org/covid19/educationresponse/> (accessed June 21, 2021).

16 UNESCO, “One Year into Covid-19 Education Disruption: Where Do We Stand?” March 19, 2021, <https://en.unesco.org/news/one-year-covid-19-education-disruption-where-do-we-stand> (accessed June 21, 2021).

17 Online learning was the most used remote learning method by governments worldwide. According to a survey of 129 countries, 90 percent offered learning through online platforms. UNESCO, UNICEF, World Bank, “What Have We Learnt? Overview of Findings from a Survey of Ministries of Education on National Responses to Covid-19,” October 2020, <https://data.unicef.org/resources/national-education-responses-to-covid19/> (accessed June 22, 2021), p. 21.



There were no doubts that the online platforms and tools used could be unsafe. It was never questioned.

— A single mother of two school-aged boys, Izhevsk, Udmurt Republic, Russia¹³

Covid-19 and Children’s Education

The novel coronavirus has devastated children’s education around the world.¹⁴ On March 11, 2020, the World Health Organization (WHO) declared that an outbreak of Covid-19 had reached global pandemic levels. Within weeks, almost every country in the world closed down their schools in an attempt to stop the spread of Covid-19, upending the lives and learning of 1.6 billion children and young adults, or 90 percent of the world’s students.¹⁵ By March 2021, a full year into the pandemic, half of the global student population remained shut out of school.¹⁶

Most countries pivoted to some form of online learning, replacing physical classrooms with phones, tablets, and computers.¹⁷ This deepened existing inequities in children’s access to education, in the form of digital divides between children with access to technologies critical for online learning, and those without. It also created a dependence and need for affordable, reliable connectivity and devices so overwhelming that it triggered global shortages for both. Supply chains for computers buckled under staggering demand, as shortages of essential parts created two-year shipment delays

18 Kellen Browning, "The Digital Divide Starts With a Laptop Shortage," *New York Times*, October 12, 2020, <https://www.nytimes.com/2020/10/12/technology/laptops-schools-digital-divide.html> (accessed June 22, 2021); Paresh Dave, "Laptops, desktop sales see 'renaissance'; shortages won't ease until 2022," *Reuters*, December 24, 2020, <https://www.reuters.com/article/us-tech-hardware-yearend/laptops-desktop-sales-see-renaissance-shortages-wont-ease-until-2022-idUSKBN28Y12M> (accessed June 22, 2021).

19 Hadas Gold, "Netflix and YouTube are slowing down in Europe to keep the internet from breaking," *CNN Business*, March 20, 2020, <https://www.cnn.com/2020/03/19/tech/netflix-internet-overload-eu/index.html> (accessed June 21, 2021); Klint Finley, "YouTube Slashes Video Quality to Save Bandwidth," *WIRED*, March 24, 2020, <https://www.wired.com/story/youtube-slashes-video-quality-save-bandwidth/> (accessed June 21, 2021); Cecilia Kang, Davey Alba, and Adam Satariano, "Surging Traffic is Slowing Down Our Internet," *New York Times*, March 26, 2020, <https://www.nytimes.com/2020/03/26/business/coronavirus-internet-traffic-speed.html> (accessed June 21, 2021).

20 See, for example, Microsoft Stories Asia, "Enabling A Digital Future for Vietnam," Microsoft, July 8, 2020, <https://web.archive.org/web/20210819180052/https://news.microsoft.com/apac/2020/07/08/enabling-a-digital-future-for-vietnam/> (accessed July 28, 2021); Microsoft News Center, "Egypt's Ministry of Education Makes Office 365 Available For All Students And Teachers Through New Online Self-Services Portal," Microsoft, December 21, 2020, <https://web.archive.org/web/20210819180141/https://news.microsoft.com/en-xm/2020/12/21/the-ministry-of-education-signs-an-agreement-with-microsoft-to-provide-a-unified-platform-for-students-and-teachers/> (accessed July 28, 2021); Mitch Tarica, "Zoom Selected by Los Angeles Unified School District," post to "Zoom Blog" (blog), Zoom, July 2, 2020, <https://web.archive.org/web/20210819175013/https://blog.zoom.us/zoom-selected-by-los-angeles-unified-school-district/> (accessed August 19, 2021); Board of Education of the City of Los Angeles, "Regular Meeting Order of Business," June 8, 2021, <https://web.archive.org/web/20210819175920/http://laschoolboard.org/sites/default/files/06-08-21RegBdOBMaterialsWithLinksPublic.pdf> (accessed August 19, 2021), p. 29.

worldwide and pitted desperate schools and education ministries against one another.¹⁸ As more people became heavily reliant on the internet to work, communicate, play, and study during Covid-19 lockdowns, the resulting explosion of traffic clogged the internet and dumped unprecedented stress on its infrastructure. Nine days after the WHO's pandemic declaration, the European Commission took the extraordinary step of asking internet companies, video streaming services, and gaming platforms to reduce their services in Europe to reserve bandwidth for work and education.¹⁹

Teachers and schools faced a bewildering array of digital platforms to choose from as they scrambled to set up virtual classrooms. In response, governments issued endorsements of educational technologies (EdTech) for use. Some governments rapidly signed contracts with EdTech companies to purchase millions of licenses for teachers and students.²⁰

As a result, EdTech companies experienced explosive, unprecedented demand for their products. In the days and weeks after the WHO's pandemic declaration, education app downloads worldwide surged 90 percent compared to the weekly average at the end of 2019.²¹ Children spent significantly more time online in virtual classrooms; by September 2020, the number of hours spent in education apps globally each week had increased to an estimated 100 million hours, up 90 percent compared to the same period in 2019.²²

Google Classroom, Google's teacher-student communication platform, reported that the pandemic had almost quadrupled its users to more than 150 million, up from 40 million in 2019; similarly, G Suite for Education, Google's classroom software, reported doubling its users to more than 170 million students and educators.²³ "We have seen incredible growth," Javier Soltero, a vice president at the company, said in an interview with *Bloomberg*. "It actually mirrors, unfortunately, the ramp up and spread of the disease."²⁴

The explosive demand also generated record revenues and profits. As the global economy plummeted, venture capital financing for EdTech startups surged to a record-setting US\$16.1 billion in 2020, more than doubling the \$7 billion raised in 2019.²⁵ Two companies, Byju's and Yuanfudao, became the first EdTech companies to achieve "decacorn" status—an exclusive group of the world's most valuable privately-held

21 Lexi Sydow, "Mobile Minute: Global Classrooms Rely on Education Apps As Remote Learning Accelerates," post to "App Annie" (blog), App Annie, April 8, 2020, <http://web.archive.org/web/20200416093942/https://www.appannie.com/en/insights/mobile-minute/education-apps-grow-remote-learning-coronavirus/> (accessed June 22, 2021).

22 Lexi Sydow, "Mobile Minute: Remote Return to School Sees 90% Boost Across Top Education Apps," post to "App Annie" (blog), App Annie, September 23, 2020, <http://web.archive.org/web/20200926051917/https://www.appannie.com/en/insights/mobile-minute/top-education-apps-growth-2020/> (accessed June 22, 2021).

23 In February 2021, Google rebranded G Suite for Education to Google Workspace for Education Fundamentals. See: Melanie Lazare, "A Peek At What's Next for Google Classroom," post to Google: The Keyword (blog), February 17, 2021, <https://web.archive.org/web/20210819180239/https://blog.google/outreach-initiatives/education/classroom-roadmap/> (accessed June 21, 2021); Shantanu Sinha, "More Options for Learning With Google Workspace for Education," post to Google: The Keyword (blog), February 17, 2021, <https://web.archive.org/web/20210819180354/https://www.blog.google/outreach-initiatives/education/google-workspace-for-education/> (accessed June 21, 2021).

24 Gerrit De Vynck and Mark Bergen, "Google Classroom Users Doubled as Quarantines Spread," *Bloomberg Quint*, April 9, 2020, <https://www.bloomberg.com/news/articles/2020-04-09/google-widens-lead-in-education-market-as-students-rush-online> (accessed June 21, 2021).

25 HolonIQ, "Global EdTech Venture Capital Update – Q1 2021," March 31, 2021, <http://web.archive.org/web/20220104184935/https://www.holoniq.com/notes/global-edtech-venture-capital-update-q1-2021/> (accessed June 22, 2021).

companies, valued at more than \$10 billion—after attracting millions of new students and closing successful financing rounds during the pandemic.²⁶

Technology companies that provided free services to schools also benefited, gaining significant market share as millions of students became familiar with their product. Zoom Video Communications, which provided free services to more than 125,000 schools in 25 countries, as well as limited free services for the general public, reported its sales skyrocketing 326 percent to \$2.7 billion and its profits propelled from \$21.7 million in 2019 to \$671.5 million in 2020.²⁷

The use of EdTech helped governments to fill urgent gaps and deliver some measure of learning during the pandemic. However, governments' endorsements and procurements of EdTech also turbocharged the mass collection of children's data, exposing their personal information to the risk of misuse and exploitation by the advertising-driven internet economy and resulting in the mass surveillance of children's lives, both inside and outside of the classroom.

How the Internet-Based Economy Works

We don't monetize the things we create.

We monetize users.

—Andy Rubin, creator of Android, the world's most widely used mobile operating system²⁸

Today's internet is powered by the advertising technology (AdTech) industry. Motivated by the belief that personalized ads are more persuasive and therefore more lucrative, AdTech companies collect massive troves of data about people to target them with ads tailored to their presumed interests and desires. The revenue generated by digital advertising pays for most of the services available on the internet today.



26 Anu Raghunathan, "Indian EdTech Billionaire's Byju's Becomes Decacorn After Funding Round from Mary Meeker," *Forbes*, June 29, 2020, <https://www.forbes.com/sites/anuraghunathan/2020/06/29/indian-edtech-billionaires-byjus-becomes-decacorn-after-funding-round-from-mary-meeker/> (accessed June 22, 2021); Priyamvada Mathur, "China's Yuanfudao Claims Global EdTech Valuation Crown," *Pitchbook*, October 22, 2020, <https://pitchbook.com/news/articles/yuanfudao-edtech-valuation-china> (accessed June 22, 2021).

27 Zoom, "Teaching, Learning & Connecting in 2020: Education in an Extraordinary Year," post to "Zoom Blog" (blog), Zoom, December 21, 2020, <https://web.archive.org/web/20210819180503/https://blog.zoom.us/connecting-in-2020-education-in-an-extraordinary-year/> (accessed July 28, 2021); Zoom, "Annual Report, Fiscal 2021," <https://web.archive.org/web/20210819180624/https://investors.zoom.us/static-files/a17fd391-13ae-429b-8cb3-bfd95b61b007> (accessed July 28, 2021); Zoom, "Zoom Video Communications Reports Fourth Quarter and Fiscal Year 2021 Financial Results," March 1, 2021, <https://web.archive.org/web/20210819180506/https://investors.zoom.us/news-releases/news-release-details/zoom-video-communications-reports-fourth-quarter-and-fiscal-o> (accessed July 28, 2021).

28 Steven Levy, "The Inside Story of the Moto X: The Reason Google Bought Motorola," *WIRED*, August 1, 2013, <https://www.wired.com/2013/08/inside-story-of-moto-x/> (accessed June 21, 2021).

Most internet companies offer their website, app, or content for free, or charge a negligible fee that does not reflect the full cost of offering these services. Instead of asking people to pay for these services with money, companies require people to give up their data and attention, often without their knowledge or meaningful consent.²⁹ Companies then traffic their users' data into a complex ecosystem of AdTech companies, data brokers, and others in a set of highly profitable transactions that make up a \$378.16 billion industry.³⁰

Here's how a child using an EdTech app to attend her school online might interact with the AdTech industry. This illustration similarly describes a child's experience using an EdTech website to attend her school online.

1. EdTech companies that make educational apps for children decide to send a child's personal data to third-party companies and possibly to sell ads in their apps, in order to generate revenue.
2. AdTech companies help put ads in apps. They make packages of code, such as software development kits (SDKs) and other tracking technologies, for app makers to insert into their apps to personalize and display ads to their users. When this code is installed in the app, this code collects data that may be used by the AdTech company to target advertising, whether on the EdTech product or on another site or app.
3. A child opens the EdTech app that their school uses for online learning and logs in for class.
4. Instantly, the app begins to collect personal data about the child. This can include who the child is, where she is, what she does, who she interacts with in her virtual classroom, and what kind of device her parents can afford for her to use.
5. This data can be sent to AdTech companies, either by the EdTech app, or directly by the AdTech SDKs embedded in the app. In the process, AdTech companies assign an ID number to the child, so that they can piece together the data they receive to build a profile on her.
6. Some AdTech companies will also follow the child across the internet and over time. Some may search for even more information about her from public and private sources, adding definition and detail to an intimate profile of the child.
7. AdTech companies' sophisticated algorithms analyze the trove of data received from the app. They guess at the child's personal characteristics and interests (for example, that she's likely to be female), and predict her future behavior (this child is likely to buy a toy).
8. AdTech companies use these insights to sell to advertisers the ability to target ads to people. This happens through real-time bidding platforms, where algorithms engage in a high-frequency auction amongst advertisers to sell off the chance to show an ad to a user—in this case, a child—to the highest bidder. From start to finish, the automated process of buying and selling between advertisers takes less than a hundred milliseconds and takes place tens of billions of times each day.³¹

29 Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (New York: Knopf, 2016).

30 Several data protection authorities have recognized the economic value of users' data and companies' economic incentives to collect them, in addition to the rights associated with the collection and use of personal data. In addition, some digital platforms have explicitly acknowledged the link between the 'free' nature of their services and their use of advertising. See: Australian Competition and Consumer Commission, "Digital Platforms Inquiry, Preliminary Report," December 10, 2018, <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry.pdf> (accessed July 9, 2021) pp. 166-167; Ethan Cramer-Flood, "Worldwide Digital Ad Spending 2021," *Insider Intelligence / eMarketer*, April 29, 2021, <https://www.emarketer.com/content/worldwide-digital-ad-spending-2021> (accessed June 23, 2021).

31 See: Mike Downey, "Real-Time Bidding Is The Next Mobile Ad Breakthrough – Here's How You Can Profit," *VentureBeat*, July 23, 2012, <https://venturebeat.com/2012/07/23/real-time-bidding-is-the-next-mobile-ad-breakthrough-heres-how-you-can-profit/> (accessed June 23, 2021); Jun Wang, Weinan Zhang, and Shuai Yuan, "Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting," June 18, 2017, <https://arxiv.org/pdf/1610.03013.pdf> (accessed June 23, 2021); Amazon Web Services, "Real-Time Bidding for Advertising & Marketing," <http://web.archive.org/web/20210623132624/https://aws.amazon.com/advertising-marketing/adtech-real-time-bidding/> (accessed June 23, 2021); Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (New York: Farrar, Straus and Giroux, 2020), p. 20.

9. These insights can also be sold or shared with data brokers, law enforcement and governments, or others who wish to target a defined group of people with similar characteristics online.

A handful of the world's most valuable internet companies own entire AdTech supply chains. Alibaba, Amazon, Facebook (Meta),³² Google, Microsoft, Tencent, and Yandex offer digital services that serve as the primary channels that most of the world relies on to engage with the internet.³³ In turn, they collect extensive data about the billions of people who use or interact with these platforms. They analyze this data to infer and create new information about people, then commercialize those insights for advertising—often on their own real-time bidding platforms.

These AdTech companies may also draw upon their vast troves of data to build and offer finely-tuned tracking technologies, prediction models, and microtargeting tools to help advertisers reach their audiences. As further described in Chapter 3, these tools are embedded in most websites and apps that people use every day, enabling these AdTech companies to collect and receive data not just from people directly using their services, but from anyone who encounters their data tracking embedded across the internet. The unparalleled power of these dominant tech companies to collect, track, and combine data across much of the internet results in a powerful and pervasive surveillance of people's lives that is extremely difficult to avoid.³⁴

³² Facebook rebranded itself to Meta in October 2021. This report refers to Facebook as both the platform and the parent company, for consistency across the timeline of this investigation.

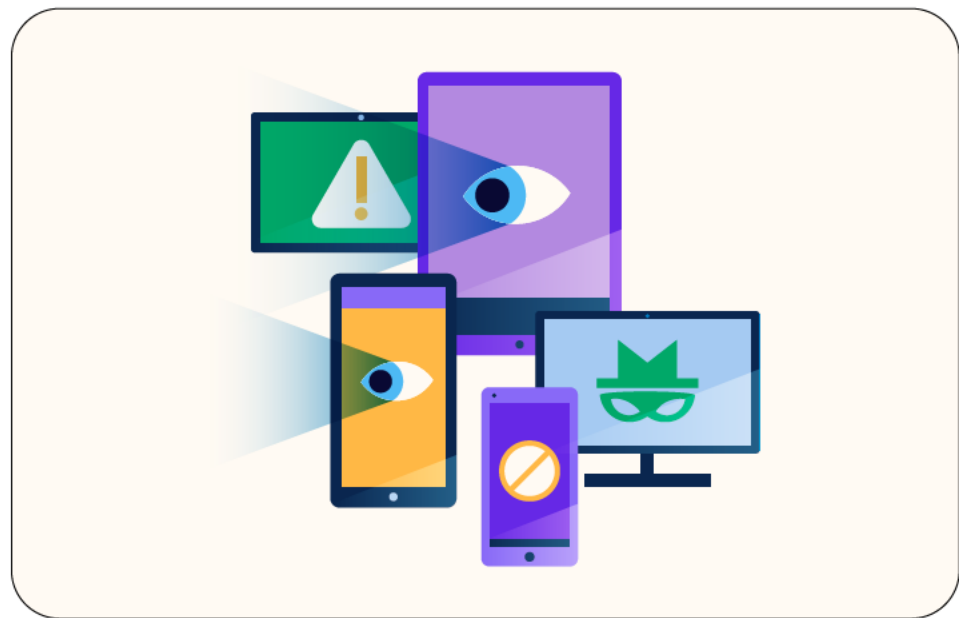
³³ See: Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/> (accessed May 5, 2021); Ethan Cramer-Flood, "Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl," *eMarketer*, May 10, 2021, <https://www.emarketer.com/content/duopoly-still-rules-global-digital-ad-market-alibaba-amazon-on-prowl> (accessed May 12, 2021); Fortune, "Global 500," 2021, <https://fortune.com/global500/> (accessed December 10, 2021).

³⁴ United States Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, "Investigation of Competition in Digital Markets," 2020, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf (accessed September 1, 2021), pp. 51-57; "Bundeskartellamt prohibits Facebook from combining user data from different sources," Bundeskartellamt press release, February 7, 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3591568 (accessed September 1, 2021); "Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector," European Commission press release, June 22, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143 (accessed September 1, 2021); Kashmir Hill, "I Tried to Live Without the Tech Giants. It Was Impossible." *New York Times*, July 31, 2020, <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html> (accessed July 29, 2021).

II. Hidden Surveillance: Children's Data Harvested

³⁵ Human Rights Watch interview with Rodin R., 9, Istanbul, Turkey, June 25, 2021. The names of all children quoted in this report have been changed to protect their privacy.

³⁶ International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, art. 17; Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, art. 16; Convention on the Rights of Persons with Disabilities, adopted December 13, 2006, G.A. Res. 61/106, Annex I, UN GAOR, 61st Sess., Supp. (No. 49) at 65, UN Doc. A/61/49 (2006), entered into force May 3, 2008, art. 22; African Charter on the Rights and Welfare of the Child, OAU Doc. CAB/LEG/24.9/49 (1990), entered into force November 29, 1999, art. 10; American Convention on Human Rights ("Pact of San José, Costa Rica"), adopted November 22, 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123, entered into force July 18, 1978, , reprinted in Basic Documents Pertaining to Human Rights in the Inter-American System, OEA/Ser.L.V/II.82 doc.6 rev.1 at 25 (1992), art. 11; Council of Europe, European Convention on Human Rights, adopted November 4, 1950, entered into force September 3, 1953, art. 8; Universal Declaration of Human Rights (UDHR), adopted December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), art. 12.



How dare they? How dare [these companies] peep into my private life?

—Rodin R., 9-year-old student, Istanbul, Turkey³⁵

Children's Data and their Right to Privacy

Privacy is a human right.³⁶ Recognized under international and regional human rights treaties, this right encompasses three connected components: the freedom from intrusion into our private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities.³⁷

Privacy is about autonomy and control over one's life. It is the ability to define for ourselves who we are to the world, on our own terms. This is especially important for children, who are entitled to special protections that guard their privacy and the space for them to grow, play, and learn.³⁸

³⁷ Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/> (accessed May 5, 2021), p. 19, UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 5; UN Human Rights Committee, *Coeriel and Aurik v. the Netherlands*, December 9, 1994, Communication No. 453/1991, para. 10.02.

³⁸ In his 2021 report to the UN Human Rights Council, the Special Rapporteur on the right to privacy stated that children's right to privacy "enables their access to their other rights critical to developing personality and personhood, such as the rights to freedom of expression and of association and the right to health, among others." See: UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, paras. 67-76.

39 Ibid.; Committee on the Rights of the Child, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 67; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 11.

40 CRC, General Comment No. 1, (2001), Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001). For more on children's privacy rights in schools, see: Human Rights Watch, *Leave No Girl Behind in Africa: Discrimination in Education against Pregnant Girls and Adolescent Mothers* (New York: Human Rights Watch, June 2018), <https://www.hrw.org/report/2018/06/14/leave-no-girl-behind-africa/discrimination-education-against-pregnant-girls-and#6484>; "I Had a Dream to Finish School": Barriers to Secondary Education in Tanzania (New York: Human Rights Watch, February 2017), <https://www.hrw.org/report/2017/02/14/i-had-dream-finish-school/barriers-secondary-education-tanzania#7406>; "Like Walking Through a Hailstorm": Discrimination against LGBT Youth in US Schools (New York: Human Rights Watch, December 2016), <https://www.hrw.org/report/2016/12/08/walking-through-hailstorm/discrimination-against-lgbt-youth-us-schools>; "Submission by Human Rights Watch to the UN Special Rapporteur on the Right to Privacy," October 19, 2020, <https://www.hrw.org/news/2020/10/19/submission-human-rights-watch-un-special-rapporteur-right-privacy>; Hye Jung Han, "Singapore Spying on Students' Laptops," commentary, Human Rights Dispatch, February 5, 2021, <https://www.hrw.org/news/2021/02/05/singapore-spying-students-laptops>; "Facial Recognition Technology in US Schools Threatens Rights," commentary, Human Rights Dispatch, June 21, 2019, <https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights>.

41 Human Rights Watch, "My Life is Not Your Porn": Digital Sex Crimes in South Korea (New York: Human Rights Watch, June 16, 2021), <https://www.hrw.org/report/2021/06/16/my-life-not-your-porn/digital-sex-crimes-south-korea>.

42 Human Rights Watch, *No Support: Russia's "Gay Propaganda" Law Imperils LGBT Youth* (New York: Human Rights Watch, December 11, 2018), <https://www.hrw.org/report/2018/12/11/no-support/russias-gay-propaganda-law-imperils-lgbt-youth>.

Children's privacy is vital to ensuring their safety, agency, and dignity.³⁹ At school, privacy enables the very purpose of education by providing the space for children to develop their personalities and abilities to their fullest potential.⁴⁰ For children who are survivors of abuse, privacy might mean the freedom to live safely, without exposing where they live, play, and go to school.⁴¹ For lesbian, gay, bisexual and transgender (LGBT) children, privacy could mean the difference between seeking life-saving information and being sent to jail, or worse.⁴²

As children spend increasing amounts of their lives online, international human rights bodies have recognized that even the mere generation, collection, and processing of a child's personal data can threaten their privacy, because in the process they lose control over information that could put their privacy at risk.⁴³ Data about children's identities, activities, communications, emotions, health, and relationships merit special consideration, as the handling of such data may result in arbitrary or unlawful abuses of children's privacy and in harms that may continue to affect them later in life.⁴⁴

The United Nations Committee on the Rights of the Child has emphasized that any digital surveillance of children, together with any associated automated processing of their data, should not be conducted routinely, indiscriminately, or without the child's knowledge or, in the case of very young children, that of their parent or caregiver.⁴⁵ Moreover, it should not take place "without the right to object to such surveillance, in commercial settings and educational and care settings," and "consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose."⁴⁶ Any restriction upon a child's privacy is only permissible if it meets the standards of legality, necessity, and proportionality.⁴⁷

The unprecedented, mass use of education technologies (EdTech) by schools during the pandemic without adequate privacy protections drastically compromised children's right to privacy. Recognizing this, the UN special rapporteur on the right to privacy warned that, "Schools and educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs."⁴⁸

43 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 67-68; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 7; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, June 30, 2014, para. 20; UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, para. 71.

44 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 68.

45 Ibid., para. 75.

46 Ibid.

47 UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, June 30, 2014, para. 23; UN Human Rights Council, "Resolution adopted by the Human Rights Council on 23 March 2017," Resolution 34/7, A/HRC/RES/34/7, para. 2; CRC, General Comment No. 1, (2001), Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001).

48 UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, <https://undocs.org/A/HRC/46/37> (accessed August 3, 2021), para. 110.

49 Ibid.

50 Bennett Cyphers and Gennie Gebhart, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance," Electronic Frontier Foundation, 2019, <https://www.eff.org/wp/behind-the-one-way-mirror> (accessed July 12, 2021).

51 Computer scientists have proven that personal information cannot be protected by current methods of 'anonymizing' data. Advertisers, data brokers, and others have long shared and sold people's personal information without violating privacy laws, under the claim that they anonymize this data by stripping people's real names out. However, computer algorithms can correctly re-identify, for example, 99.98 percent of people from almost any anonymized data set with just 15 data points, such as gender, ZIP code, or marital status. Similarly, knowing just four random pieces of information from an anonymized dataset is enough to re-identify shoppers as unique individuals and uncover the rest of their credit card records, or to uniquely identify people from four locations they were previously at. See: Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications*, vol. 10 (2019), accessed June 30, 2021, doi: 10.1038/s41467-019-10933-3; Yves-Alexandre de Montjoye et al., "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221 (2015), accessed June 30, 2021, doi:10.1126/science.1256297, pp. 536-539; Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," *Nature Scientific Reports* vol. 3 (2013), accessed June 30, 2021, doi:10.1038/srep01376.

52 See, for example, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016/679, Official Journal of the European Union, April 27, 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (accessed July 29, 2021), para. 30; Ibid., art. 4 (1), L 119/33; US Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," July 2020, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-o> (accessed July 29, 2021), art. A (3).

As described below, many EdTech products endorsed by governments and used by children to continue learning during Covid-19 school closures were found to harvest children's data unnecessarily and disproportionately, for purposes unrelated to their education. Worse still, this data collection took place in virtual classrooms and educational settings online, without giving children the ability to object to such surveillance.⁴⁹ In most instances, it was impossible for children to opt out of such data collection without opting out of compulsory schooling and giving up on learning altogether during the pandemic.

Finding Out Who Children Are

To figure out who people are on the internet, advertising technology (AdTech) companies tag each person with a string of numbers and letters that acts as an identifier number that is persistent and unique: it points to a single child or their device, and it does not change.⁵⁰

While the tools described in this discussion are ascribed to AdTech companies, the same tools can be used by other companies, including EdTech companies, to collect data about how their users (including children) use the product. Information about how a user or customer interacts with the product is useful, for example, for the company to improve its product and user experience. In our discussion in this section, we focus our discussion to AdTech companies to simplify the discussion, but the same concepts apply to technology companies that are not in AdTech.

Persistent identifiers enable AdTech companies to infer the interests and characteristics of individual children. Every time a child connects to the internet and comes into contact with tracking technology, any information collected about that child—where they live, who their friends are, what kind of device their family can afford for them—is tied back to the identifier associated with them by that AdTech company, resulting in a comprehensive profile over time. Data tied together in this way do not need a real name to be able to target a real child or person.

In addition, computers can correctly re-identify virtually any person from an anonymized dataset, using just a few random pieces of anonymous information.⁵¹ Given the risks of re-identification, many existing data protection laws recognize persistent identifiers as personal information, granting them the same considerations and legal protections.⁵²

Some persistent identifiers are built solely to be used for advertising. Other identifiers identify and track people across multiple devices, across the internet, or trail them from the online world into the physical world. And some identifiers are so inescapably tenacious that they are impossible to avoid or get rid of, without throwing one's device away in the trash.

Apps: Persistent Identifiers

Advertising Identifiers

Of the 73 EdTech apps examined by Human Rights Watch, 41 apps (56 percent) were found with the ability to collect their users' advertising IDs. This allowed these apps to tag children and identify their devices for the sole purpose of advertising to them.

An advertising ID is a persistent identifier that exists for a single use: to enable advertisers to track a person, over time and across different apps installed on their device, for advertising purposes. For those using an Android device, this is called the Android Advertising ID (AAID). An AAID is neither necessary nor relevant for an app to function; Google's developer guidelines stipulate that app developers must "only use an Advertising ID for user profiling or ads use cases."⁵³

The 41 apps that were found to have the capability to collect AAID were endorsed by 29 governments for children's learning during Covid-19. Altogether, these apps may identify, tag, and track an estimated 6.24 billion users, including children.

Of these, 33 apps appear to have the ability to collect AAID from an estimated 86.9 million children, because their own materials describe and appear to market them for children's education, with children apparently intended as their primary users.

App	Country	Apparently designed for use by children?	Developer	Estimated Users ⁵⁴
Minecraft: Education Edition	Australia: Victoria	Yes	Private	500,000
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, United States: California	No	Private	1,000,000
Descomplica	Brazil: São Paulo	Yes	Private	1,000,000
Stoodi	Brazil: São Paulo	Yes	Private	1,000,000
Storyline Online	Canada: Quebec	Yes	Private	50,000
Remind	Colombia	Yes	Private	10,000,000
Dropbox	Colombia	No	Private	1,000,000,000
Edmodo	Colombia, Egypt, Ghana, Nigeria, Romania, Thailand	Yes	Private	10,000,000
Padlet	Colombia, Germany: Bavaria, Romania	No	Private	5,000,000
SchoolFox	Germany: Bavaria	Yes	Private	100,000
itslearning	Germany: Bavaria	Yes	Private	1,000,000
Ghana Library App	Ghana	No	Government	10,000

⁵³ Android for Developers, "Best Practices for Unique Identifiers," July 1, 2021, <https://web.archive.org/web/20210706170748/https://developer.android.com/training/articles/user-data-ids> (accessed July 6, 2021).

⁵⁴ As verified by Google Play Store user installs globally, as of October 2021.

Diksha	India: Maharashtra, National, Uttar Pradesh)	Yes	Government	10,000,000
e-Pathshala	India: Maharashtra, National, Uttar Pradesh)	Yes	Government	1,000,000
Rumah Belajar	Indonesia	Yes	Government	1,000,000
Quipper	Indonesia	Yes	Private	1,000,000
Ruangguru	Indonesia	Yes	Private	10,000,000
Kelas Pintar	Indonesia	Yes	Private	1,000,000
Shad	Iran	Yes	Government	18,000,000 ⁵⁵
Newton	Iraq	Yes	Government	50,000
WeSchool	Italy	Yes	Private	1,000,000
schoolTakt	Japan	Yes	Private	1,000
Study Sapuri	Japan	Yes	Private	500,000
Bilimland	Kazakhstan	Yes	Private	500,000
Daryn Online	Kazakhstan	Yes	Private	1,000,000
Kundelik	Kazakhstan	Yes	Private	1,000,000
Muse	Pakistan	Yes	Private	10,000
Taleemabad	Pakistan	Yes	Private	1,000,000
Naver Band	Republic of Korea	No	Private	50,000,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Miro	Romania	No	Private	1,000,000
Kinderpedia	Romania	Yes	Private	10,000
My Achievements	Russian Federation	Yes	Government	100
iEN	Saudi Arabia	Yes	Government	500,000
Extramarks	South Africa	Yes	Private	100,000
Nenasa	Sri Lanka	Yes	Government	50,000
PaGamO	Taiwan	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000
Eğitim Bilişim Ağı	Turkey	Yes	Government	10,000,000
Özelim Eğitimdeyim	Turkey	Yes	Government	500,000
Schoology	US: Texas	Yes	Private	5,000,000

⁵⁵ Shad is a learning app that is built and offered by the Iranian Ministry of Education for children's learning during Covid-19 school closures. It is not offered through the Google Play Store; no externally verified source for user downloads exist for this app, though the government has self-reported 18 million installs of Shad as of October 28, 2021. See: Government of Iran, Ministry of Education, "Shad," <https://web.archive.org/web/20211028212342/http://www.shad.ir/> (accessed October 28, 2021).

56 Android offers users the ability to manually reset the AAID, which would, in theory, make it more difficult for advertisers to associate a child's activities with the digital dossier compiled on their past behaviors. In reality, most users, particularly children, are unlikely to be aware of this, or go to the trouble to find and manually reset their AAID. Furthermore, the ability to reset the AAID is only effective if it is the only persistent identifier collected and transmitted; if the AAID is collected alongside other identifiers, the tracker can not only continue to track the same child, but they can also determine that the AAID had been reset.

57 Kementerian Pendidikan dan Kebudayaan, "Kemendikbud Gandeng Swasta Siapkan Sistem Belajar Daring," March 15, 2020, <https://www.kemdikbud.go.id/main/blog/2020/03/kemendikbud-gandeng-swasta-siapkan-sistem-belajar-daring> (accessed July 6, 2021).

58 Rumah Belajar, "Privacy Policy," February 4, 2020, <http://apps.belajar.kemdikbud.go.id/privacypolicy.html> (accessed July 6, 2021).

59 For further discussion on these findings, please refer to the SDK section later in this chapter.

60 While children's data are categorized as "personal data of a specific nature," the draft data protection bill makes no mention of the significance of this definition. Nor does it provide any specific protections to data of this nature. See: Dewan Perwakilan Rakyat Republik Indonesia, "DPR Officially Extends Discussion on PDP Bill and Disaster Management" ("DPR Resmi Perpanjang Pembahasan RUU PDP dan Penanggulangan Bencana"), June 22, 2021, <https://www.dpr.go.id/berita/detail/id/33528> (accessed July 29, 2021); Personal Data Protection Bill ("RUU tentang Perlindungan Data Pribadi"), <https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf> (accessed July 29, 2021), art. 3(3)(g).

61 The Google Play Store requires app developers to post a link to the app's privacy policy. Instead of pointing to a privacy policy, EĞitim Bilişim Ağı's privacy policy link points back to the home page of its website, <https://www.eba.gov.tr/>, which also does not have a privacy policy. See: "EBA," Google Play Store, <https://web.archive.org/web/20210526213628/https://play.google.com/store/apps/details?id=tr.gov.eba.hesap> (accessed July 6, 2021).

None of these apps allowed their users to decline to be tracked. In fact, this data collection is invisible to the child, who simply sees the app's interface on their device. This activity is even more covert in 27 apps that fail to inform their students—either through their privacy policy, or elsewhere on their product—that the app and its embedded third-party AdTech trackers may collect their device's AAIDs in order to track, profile, and target students with advertising. In doing so, these apps deny children, parents, and teachers knowledge of this practice and the ability to consent, and impede their right to effective remedy (as discussed in Chapter 4).⁵⁶

Collectively, these EdTech apps may have provided 33 AdTech companies with access to their students' AAIDs. This was done through software development kits (SDKs), or packages of code embedded in an EdTech app that can be used to facilitate the transmission of users' personal data to advertisers.

When reached for comment, Cisco stated that Webex does not collect users' AAIDs, and that it does not share user data with third-party companies that own the SDKs embedded in Webex.

Notably, nine governments—Ghana, India, Indonesia, Iran, Iraq, Russia, Saudi Arabia, Sri Lanka, and Turkey—directly built and offered eleven learning apps that may collect AAID from children. In doing so, these governments granted themselves the ability to track an estimated 41.1 million students and teachers purely for advertising and monetization.

Some governments disclosed in their app's privacy policy that the app collects students' AAID for commercial purposes. Rumah Belajar, for example, is an EdTech website and app developed and operated by Indonesia's Ministry of Education and Culture to provide online education to preschool, primary, and secondary school students during the pandemic.⁵⁷ Through Rumah Belajar's privacy policy, the Indonesian government discloses that it automatically collects children's "unique device identifiers" and "mobile device unique ID," which may be used to "show advertisements to you," "to advertise on third party websites to you after you visited our service," and shared with third party "business partners" so that they can "offer you certain products, services or promotions."⁵⁸

Through dynamic analysis commissioned by Human Rights Watch and conducted by the Defensive Lab Agency, Human Rights Watch detected students' AAID sent from Rumah Belajar to Google and to Facebook. Specifically, children's AAID were sent to the Google-owned domain **app-measurement.com**, and to the Facebook-owned domain **graph.facebook.com**.⁵⁹

Indonesia does not have a data protection law, or specific regulations that protect children's data privacy. A draft data protection bill, introduced in January 2020 and pending further discussion in the House of Representatives as of September 2021, does not provide dedicated protections for children.⁶⁰

In contrast, EĞitim Bilişim Ağı, developed by Turkey's Ministry of National Education for preschool, primary, and secondary school students to continue learning during Covid-19 school closures, does not provide a privacy policy at all. Nor does the app provide a disclosure elsewhere on the product to notify students that their AAID is collected and sent to third-party companies for advertising purposes.⁶¹

Through dynamic analysis, Human Rights Watch detected students' AAID transmitted from EĞitim Bilişim Ağı to Google via the Google-owned domains **www.googleadservices.com** and **app-measurement.com**. **www.googleadservices.com** is operated by Google Ads, the company's online advertising platform. Google Ads uses the information it collects to

understand a person's interests and auctions off to the highest bidder the chance to show an ad to those in the advertiser's target audience.⁶²

Neither Indonesia's Ministry of Education and Culture nor Turkey's Ministry of National Education responded to Human Rights Watch's requests for comment. Cisco informed Human Rights Watch that Webex does not collect AADs.

The collection of AAD from children is neither necessary nor proportionate to the purpose of providing them with education, and risks exposing children to rights abuses as discussed in Chapter 3.

Inescapable Surveillance

Human Rights Watch found 14 EdTech apps with access to either the Wi-Fi Media Access Control (MAC) address or the International Mobile Equipment Identity (IMEI) on children's devices, two persistent identifiers that are so strong that a child or their parent cannot avoid or protect against their surveillance even if they take the extraordinary step of wiping their phones or performing a factory reset.

Eight apps granted themselves the ability to collect the Wi-Fi MAC address of a device's networking hardware. Located in any device that can connect to the internet, this identifier is extremely persistent and cannot be changed by wiping the device clean with a factory reset. Any instance of an app collecting the Wi-Fi MAC address is notable; in 2015, Google banned developers from accessing the Wi-Fi MAC address over privacy concerns that it was being used by third-party tracking companies as a persistent identifier that could not realistically be changed by users.⁶³

Recommended by 13 governments, these apps had the ability to collect the Wi-Fi MAC addresses of an estimated 15.6 billion users. Three of these apps appear to have the ability to do so from an estimated 610,000 children, as their own materials describe and appear to market them for children's education.

⁶² See, for example, Google Ads, "Display Campaigns," https://web.archive.org/web/20210825072918/https://ads.google.com/intl/en_us/home/campaigns/display-ads/ (accessed August 25, 2021); Google Ads, "Discovery Ads," https://web.archive.org/web/20210825072911/https://ads.google.com/intl/en_us/home/campaigns/discovery-ads/ (accessed August 25, 2021).

⁶³ In research commissioned by the Australian Competition and Consumer Commission, security researchers from AppCensus noted security vulnerabilities in Android that, when exploited, allow apps to collect the Wi-Fi MAC by circumventing the permission systems' protections. See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_o.pdf (accessed April 3, 2021), pp. 17, 47. See also: Android for Developers, "Android 6.0 Changes," March 11, 2021, <https://developer.android.com/about/versions/marshmallow/android-6.0-changes> (accessed July 7, 2021).

⁶⁴ As verified by Google Play Store user installs, as of October 2021.

App	Country	Apparently designed for use by children?	Developer	Estimated Users ⁶⁴
Minecraft: Education Edition	Australia: Victoria	Yes	Private	500,000
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Private	10,000,000,000
Padlet	Colombia, Germany: Bavaria, Romania	No	Private	5,000,000
LINE	Japan, Taiwan	No	Private	500,000,000
Muse	Pakistan	Yes	Private	10,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Extramarks	South Africa	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000

Eight apps were found with the ability to collect International Mobile Equipment Identity (IMEI) numbers. Used to connect to cellular networks and to trace stolen phones, every mobile device has an IMEI number baked into its hardware. An IMEI cannot be changed, and it is illegal to do so in some countries.⁶⁵ The only means of changing one's IMEI is to throw the phone away and purchase a new one.

Recommended for children's learning by 12 governments, these apps may have collected in the aggregate IMEI numbers from an estimated 5.6 billion users. Four of these apps are apparently designed exclusively for children, so they may collect IMEI numbers from an estimated 3.1 million children in Brazil, Indonesia, Pakistan, and South Africa.

App	Country	Apparently designed for use by children?	Developer	Estimated Users ⁶⁶
Stoodi	Brazil: São Paulo	Yes	Private	1,000,000
Kelas Pintar	Indonesia	Yes	Private	1,000,000
LINE	Japan, Taiwan	No	Private	500,000,000
Taleemabad	Pakistan	Yes	Private	1,000,000
Telegram	Russia	No	Private	1,000,000,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Extramarks	South Africa	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000

⁶⁵ For example, see: Mobile Phones (Re-programming) Act 2002, UK Public General Acts, 2002 c.31, Section 1, <https://www.legislation.gov.uk/ukpga/2002/31/section/1> (accessed July 7, 2021); Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017, Government of India Ministry of Telecommunications, August 25, 2017, https://dot.gov.in/sites/default/files/2017_10_23%20Prevention%20of%20Mobile%20Tampering.pdf (accessed July 7, 2021).

⁶⁶ As verified by Google Play Store user installs globally, as of October 2021.

⁶⁷ International Digital Accountability Council, "Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic," September 1, 2020, <https://digitalwatchdog.org/privacy-considerations-as-schools-and-parents-expand-utilization-of-ed-tech-apps-during-the-covid-19-pandemic/> (accessed December 10, 2020), pp. 11-12.

⁶⁸ Google Play Console, "Ads," <https://web.archive.org/web/20210707220131/https://support.google.com/googleplay/android-developer/answer/9857753> (accessed July 7, 2021).

Human Rights Watch found nine apps potentially engaging in ID bridging. When the AAID is collected and bundled alongside another persistent device identifier, the resulting "bridge" between the two is so powerful that it bypasses any privacy controls that the user may have set on their device to protect themselves. This allows companies to track users with an AAID that can never be reset, in effect creating an accurate advertising profile of a user that lasts in perpetuity.⁶⁷

Given the risks that ID bridging poses to users' privacy, Google's own policies warn developers that the "advertising identifier may not be connected to persistent device identifiers (for example: SSAID, MAC address, IMEI, etc.) for any advertising purpose."⁶⁸

App	Country	Apparently designed for use by children?	Potential ID bridging	Developer	Estimated Users ⁶⁹
-----	---------	--	-----------------------	-----------	-------------------------------

Minecraft: Education Edition	Australia: Victoria	Yes	Wi-Fi MAC	Private	500,000
Stoodi	Brazil: São Paulo	Yes	IMEI	Private	1,000,000
Padlet	Germany: Bavaria, Romania, Colombia	Yes	Wi-Fi MAC	Private	1,000,000
Kelas Pintar	Indonesia	Yes	IMEI	Private	1,000,000
Muse	Pakistan	Yes	Wi-Fi MAC	Private	10,000
Taleemabad	Pakistan	Yes	IMEI	Private	500,000
KakaoTalk	Republic of Korea	No	Wi-Fi MAC, IMEI	Private	100,000,000
Extramarks	South Africa	Yes	Wi-Fi MAC, IMEI	Private	100,000
Facebook	Taiwan	No	Wi-Fi MAC, IMEI	Private	5,000,000,000

Muse, for example, was conclusively found to be engaging in ID bridging. Through dynamic analysis, Human Rights Watch observed Muse collecting and transmitting bridged ID data to Facebook through the Facebook-owned domain **graph.facebook.com**.

Of the 14 apps discovered to grant themselves access to their users' Wi-Fi MAC or IMEI, 10 did not disclose this in their privacy policies. None of the 10 apps found to engage in ID bridging disclosed this practice to their users.

When reached for comment, Microsoft denied that its product engages in ID bridging, and Padlet responded that it did not intend to collect the data needed for ID bridging. In their responses, Facebook (Meta) and Muse did not answer whether their products engage in ID bridging. Kakao declined to respond to our request for comment; Extramarks, Kelas Pintar, Stoodi, and Taleemabad did not respond.⁷⁰

These practices are not necessary for EdTech apps to function or for the purpose of providing children's education.

Websites: Canvas Fingerprinting

Of the many tracking technologies that websites can use to identify people and their

⁶⁹ As verified by Google Play Store user installs globally, as of October 2021.

⁷⁰ Human Rights Watch email correspondence with Robyn Blum, Global Corporate Communications, Cisco, January 19, 2022; with Steve Crown, Vice President and Deputy General Counsel, Microsoft, April 15, 2022; with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; with Hassan Bin Rizwan, Founder, SABAQ / MUSE, April 2, 2022; and with Suwon Kim, Policy Team, Kakao Corp., April 21, 2022.

⁷¹ Gunes Acar et al., “The Web Never Forgets: Persistent Tracking Mechanisms In the Wild,” In Proceedings of CCS 2014, November 2014, <https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html> (accessed July 7, 2021). See also: Julia Angwin, “Meet the Online Tracking Device That is Virtually Impossible to Block,” *ProPublica*, July 21, 2014, <https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block> (accessed July 7, 2021); Surya Mattu and Aaron Sankin, “How We Built a Real-time Privacy Inspector,” *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 7, 2021).

⁷² Canadian Broadcasting Corporation (CBC), “2020-2021 Annual Report,” <https://cbc.radio-canada.ca/en/impact-and-accountability/finances/annual-reports/ar-2020-2021/highlights/financial-highlights> (accessed January 13, 2021).

⁷³ Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, “Learning Support Content For Elementary School Mathematics (as of February 8, 3rd Year of Reiwa)” (“小学校算数における学習支援コンテンツ(令和3年2月8日時点)”), https://web.archive.org/web/20210420015931/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00042.html (accessed July 10, 2021); Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, “Learning Support Content For Junior High School Language (as of February 8, 3rd Year of Reiwa)” (“中学校国語における学習支援コンテンツ(令和3年2月8日時点)”), https://web.archive.org/web/20210420000505/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00055.html (accessed July 10, 2021); Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, “Learning Support Content For High School (as of February 8, 3rd Year of Reiwa)” (“高等学校における学習支援コンテンツ(令和3年2月8日時点)”), https://web.archive.org/web/20210710231357/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00461.html (accessed July 10, 2021).

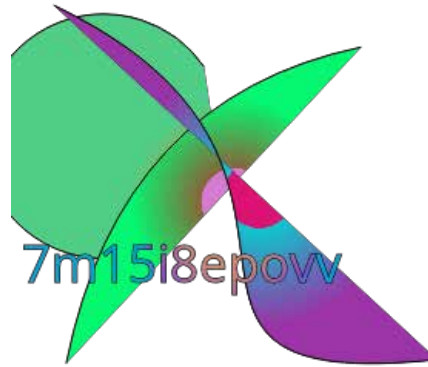
behaviors online, one of the most invasive is canvas fingerprinting. Virtually impossible for users to block, this technique works by drawing hidden shapes and text on a user’s webpage. Because each computer draws these shapes slightly differently, these images can be used by marketers and others to assign a unique number to a user’s device, which is then used as a singular identifier to track the user’s activities across the internet.⁷¹ Users cannot protect themselves by using standard web browser privacy settings or ad-blocking software.

Of the 124 EdTech websites examined by Human Rights Watch, eight websites were found “fingerprinting” their users and tracking them across the internet.

Notably, two of these websites are directly built and operated by government—Moscow Electronic School (Russia) and Digital Lessons (Russia)—for children’s educational use. Another website, CBC Kids (Canada), receives the majority of its funding from government.⁷²

Website	Country	Apparently designed for use by children?	Developer	Canvas fingerprinting script loaded from:
CBC Kids	Canada: Quebec	Yes	Government	https://gem.cbc.ca/akam/11/4c588f3 https://www.cbc.ca/akam/11/b62e49a
WorkFlowy	Colombia	No	Private	https://workflowy.com/media/js/82cab8d21714ada491b4.js https://workflowy.com/media/js/auth_embed.min.js
Top Parent	India: Uttar Pradesh	Yes	Private	https://cdnjs.cloudflare.com/ajax/libs/fingerprintjs2/2.1.0/fingerprint2.min.js
WeSchool	Italy	Yes	Private	https://m.stripe.network/out-4.5.35.js
Z-kai	Japan	Yes	Private	https://spider.af/t/k5lcn2yw?s=01&o=-gvd5xkmg7be&a=1623564108947&u=https://spider.af/t/k5lcn2yw?s=01&
iMektep	Kazakhstan	Yes	Private	https://st.vk.com/js/cmodules/mobile
Moscow Electronic School	Russia	Yes	Government	https://stats.mos.ru/ss2.min.js
Digital Lessons	Russia	Yes	Government	https://st.vk.com/js/cmodules/mobile

One EdTech website, Z-kai, was endorsed by the Japanese Education Ministry for all elementary, middle, and high school students to learn core subjects during Covid-19 school closures.⁷³ Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers:



Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers. © 2022 Hye Jung Han/Human Rights Watch

Two such canvas fingerprinting scripts were built and loaded on the Z-kai site by spider.af, a Japanese company that specializes in ensuring that advertisers' intended audiences see their ads.⁷⁴

Z-kai and spider.af did not respond to our request for comment.

It is not possible to determine the intent behind the use of canvas fingerprinting and how it is used by the product it is embedded in. However, none of these eight websites disclosed their use of canvas fingerprinting to their users. In doing so, these companies effectively kept their users in the dark that they were being invisibly identified and followed around the internet by tracking technology that is difficult to avoid or protect against.

This technique is neither proportionate nor necessary for these websites to function or deliver educational content to children. Its use on children in an educational setting infringes upon children's right to privacy.

Tracking Where Children Are

Just thinking about my whole age group, the amount of data they share is not even funny. Our everyday lives, our locations. So, their whole lives must be in danger if their data is getting sold off. It's really scary.

—Priyanka S., 16, Uttar Pradesh, India⁷⁵

To know where a child is, and when, is to possess information so sensitive that some governments provide special protections against its misuse and the risks of “abduction, physical and mental abuse, sexual abuse and trafficking.”⁷⁶

⁷⁴ Spider.af, “Spider.af,” <https://web.archive.org/web/20210708001253/https://spideraf.com/intl/en> (accessed July 10, 2021).

⁷⁵ Human Rights Watch interview with Priyanka S., Uttar Pradesh, India, August 2, 2021.

⁷⁶ See, for example, UK Information Commissioner's Office, “Age Appropriate Design: A Code of Practice for Online Services; 10. Geolocation,” September 2, 2020, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/> (accessed July 9, 2021); Government of the Republic of Korea, “Location Information Act” (“위치정보의 보호 및 이용 등에 관한 법률”), Act No. 14224, May 30, 2017, <https://law.go.kr/LSW/lsInfoP.do?lsiSeq=183644&lsId=009882&chrClsCd=010202&urlM-ode=lsInfoP&viewCls=lsInfoP&efY-d=20170530&vSct=&ancYnChk=undefined#0000>, art. 26; in 2013, the US Federal Trade Commission revised the country's Children's Online Privacy Protection Act (COPPA), or child-specific data protection law, in part motivated by concerns over the emerging misuse of children's geolocation data. See: Federal Trade Commission, “Children's Online Privacy Protection Rule; Final Rule,” 16 CFR Part 312, vol. 87 no. 12, January 17, 2013, p. 3972, https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf (accessed July 9, 2021).

Information about a child's physical location also reveals powerfully intimate details about their life far beyond their coordinates. Mobile phones have the ability to find and track a child's precise physical location over time, including when and how long they were in any given place. Once collected, these data points can reveal such sensitive information as where a child lives and where they go to school, trips between divorced parents' homes, and visits to a doctor's office specializing in childhood cancer.

Even without names or other obviously identifiable information attached to location data, it is startlingly easy to identify real children and people without their awareness or consent. A *New York Times* investigation determined that just two precise location data points is enough to identify a person; journalists were, for example, able to identify a single child and where they live by tracing their daily route from home to school, as well as a middle-school math teacher by her classroom and her doctor's office.⁷⁷

At a time when many children were remotely learning from home under Covid-19 lockdowns, the surveillance of their physical presence through location data likely revealed addresses and places most significant to them.

Apps: Precise Location Data

Of the 73 apps examined by Human Rights Watch, 21 apps (29 percent) granted themselves the ability to collect precise location data, or GPS coordinates that can identify a child's exact location to within 4.9 meters.⁷⁸ These 21 apps also had the ability to collect the time of the device's current location, as well as the last known location of the device—revealing exactly where a child is, where they were before that, and how long they stayed at each place.

Of these, 10 apps appear to have the ability to collect precise location data from an estimated 52.1 million children, as these apps' own materials describe and appear to market them for children's use in education. None of these apps apparently designed for use by children disclose to their students that they collect their precise location data.

Four apps are built and owned by the education ministries of India, Indonesia, Iran, and Turkey, giving these governments the ability to track an estimated 29.5 million children and pinpoint where they are, at any given moment, until the app is closed by the user.

⁷⁷ Stuart A. Thompson and Charlie Warzel, "One Nation, Tracked: Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> (accessed July 8, 2021); Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> (accessed July 8, 2021). See also: Charlie Warzel and Stuart A. Thompson, "Where Even the Children Are Being Tracked," *New York Times*, December 21, 2019, <https://www.nytimes.com/interactive/2019/12/21/opinion/pasadena-smartphone-spying.html> (accessed July 8, 2021).

⁷⁸ US National Coordination Office for Space-Based Positioning, Navigation, and Timing, Global Positioning System (GPS), "GPS Accuracy," <https://www.gps.gov/systems/gps/performance/accuracy/> (accessed July 8, 2021).

EdTech Product	Country	Apparently designed for use by children?	Developer	GPS	Timestamp of current location	Last known location	Disclosed in privacy policy?	Estimated Users ⁷⁹
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Private	Yes	Yes	Yes	Yes	100,000,000
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Private	Yes	Yes	Yes	No	500,000,000
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Private	Yes	Yes	Yes	No	1,000,000
Threema Work	Germany: Baden-Württemberg, Germany: Bavaria	No	Private	Yes	Yes	Yes	Yes	500,000
Moodle	Germany: Baden-Württemberg, Romania, Kazakhstan	Yes	Private	Yes	Yes	Yes	No	10,000,000
Padlet	Germany: Bavaria, Romania, Colombia	No	Private	Yes	Yes	Yes	Yes	5,000,000
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Private	Yes	Yes	Yes	Yes	10,000,000,000
Diksha	India: National	Yes	Government	Yes	Yes	Yes	No	10,000,000

⁷⁹ As verified by Google Play Store user installs globally, as of October 2021.

WhatsApp	India: Uttar Pradesh, Cameroon	No	Private	Yes	Yes	Yes	Yes	5,000,000,000
Rumah Belajar	Indonesia	Yes	Government	Yes	Yes	Yes	No	1,000,000
Ruangguru	Indonesia	Yes	Private	Yes	Yes	Yes	No	10,000,000
Sekolah.mu	Indonesia	Yes	Private	Yes	Yes	Yes	No	1,000,000
Shad	Iran	Yes	Government	Yes	Yes	Yes	No	18,000,000
LINE	Japan, Taiwan	No	Private	Yes	Yes	Yes	Yes	500,000,000
Telegram	Nigeria	No	Private	Yes	Yes	Yes	No	1,000,000,000
Taleemabad	Pakistan	Yes	Private	Yes	Yes	Yes	No	1,000,000
Naver Band	Republic of Korea	No	Private	Yes	Yes	Yes	Yes	50,000,000
KakaoTalk	Republic of Korea	No	Private	Yes	Yes	Yes	Yes	100,000,000
Extramarks	South Africa	Yes	Private	Yes	Yes	Yes	No	100,000
Facebook	Taiwan	No	Private	Yes	Yes	Yes	Yes	5,000,000,000
Özelim Eğitimdeyim	Turkey	Yes	Government	Yes	Yes	Yes	No	500,000

Altogether, these apps include code that can enable 15 third-party companies to access children's precise location data, potentially enabling these companies to analyze, trade, and monetize this information.

Of these 21 apps, 19 apps include code that can enable the collection of coarse location data, which reveals where children are with an accuracy approximately equivalent to a city block.⁸⁰ Such data can also be used to infer intimate details about a child; research scientists have concluded that just four approximate, anonymous location data points is enough to re-identify 95 percent of individuals.⁸¹

Human Rights Watch did not find evidence that precise location data was used to provide core app functionality or any educational benefit to children for 20 of the 21 apps. When reached for comment, Microsoft stated that Microsoft Teams may collect a user's precise location data for many purposes, including to comply with law for users located in the United States to collect and transmit their location data to first responders when a user makes an emergency call using Microsoft Teams.

When reached for comment, Cisco stated that Webex does not collect users' precise location, last known location or coarse location, or their call logs.

⁸⁰ Google Maps Platform, "Location Data," July 1, 2021, <https://web.archive.org/web/20210708220829/https://developers.google.com/maps/documentation/android-sdk/location> (accessed July 8, 2021).

⁸¹ Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," *Nature Scientific Reports* vol. 3 (2013), accessed June 30, 2021, doi:10.1038/srep01376.

⁸² Government of India, Department of School Education & Literacy and Ministry of Human Resource Development, "Remote Learning Initiatives Across India," June 2020, https://www.education.gov.in/sites/upload_files/mhrd/files/India_Report_Digital_Education_o.pdf (accessed May 21, 2021).

⁸³ Ishita Bhatia, "Remote learning: UP sets target, tells each govt teacher to convince 10 students to download Diksha app," *The Times of India*, November 18, 2020, <https://timesofindia.indiatimes.com/city/meerut/remote-learning-up-sets-target-tells-each-govt-teacher-to-convince-10-students-to-download-diksha-app/articleshow/79268507.cms> (accessed August 24, 2021).

⁸⁴ Government of India, Ministry of Education, National Council of Educational Research and Training, "Privacy Policy of Diksha, Version 11," April 28, 2021, <https://web.archive.org/web/20210825230434/https://static.diksha.gov.in/privacy-policy/terms-of-use.html> (accessed August 25, 2021).

⁸⁵ See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_o.pdf (accessed April 3, 2021), pp. 11, 18; Jeremy Gillula and Peter Eckersley, "Is Your Android Device Telling the World Where You've Been?" *Electronic Frontier Foundation*, July 3, 2014, <https://www.eff.org/deeplinks/2014/07/your-android-device-telling-world-where-youve-been> (accessed July 8, 2021).

⁸⁶ Wikipedia, "Wi-Fi positioning system," https://en.wikipedia.org/wiki/Wi-Fi_positioning_system (accessed July 8, 2021).

Case Study: Diksha, India

Diksha is an EdTech app owned and operated by India's Education Ministry.⁸² First launched in 2017 and later used during the pandemic as the government's primary means of delivering online education to students, Diksha offers lessons, textbooks, homework, and other educational material for grades 1 to 12. Diksha was downloaded by over 10 million students and teachers as of 2020. To drive further adoption, some state education ministries set quotas for government teachers to compel a minimum number of their students to download the app.⁸³

Human Rights Watch found that Diksha collects children's precise location data, including the date and time of their current location and their last known location. However, the Indian government does not disclose through Diksha's privacy policy or elsewhere that it collects children's location data. Instead, it misleadingly states that Diksha collects a different piece of information—a user's IP address—only once, "for the limited purpose of determining your approximate location – the State, City and District of origin... and the precise location of any User cannot be determined."⁸⁴

Diksha also granted access to its students' location data to Google, through the two SDKs—Google Firebase Analytics and Google Crashlytics—embedded in the app. Through dynamic analysis, Human Rights Watch observed Diksha collecting and transmitting children's AAID to Google. It appears that Diksha shares children's personal data with Google for advertising purposes.

India's Education Ministry, as well as the state education ministries of Maharashtra and Uttar Pradesh, which had endorsed the use of Diksha, did not respond to requests for comment.

As a result, children and their parents were denied the opportunity to make informed decisions about whether to permit the Indian government to surveil their location and share it with third-party companies.

Wi-Fi SSID

Companies can also track a child's whereabouts by collecting information about the wireless network to which their phone is connected. Because Wi-Fi routers tend to be in fixed locations, collecting the names of wireless networks to which a child has previously connected can reveal places such as their home, school, places of worship, hospitals, addresses of extended family, and other places where a child spends significant time. Such information can then be used to infer more about a child, including their habits and relationships.⁸⁵

To do this, mobile phones collect the Wi-Fi SSID, which yields the name of a Wi-Fi router that the phone is connected to or the name of one nearby. Companies can look up these routers in databases that list where public Wi-Fi locations are located in the world, then map them to precise GPS coordinates.⁸⁶

Human Rights Watch found 18 apps accessing the Wi-Fi SSID. In seven cases, the apps' own materials describe and appear to market them for children's use; two of these are owned and provided by the governments of Iran and Turkey. Seven of these apps do not disclose in their privacy policy that they collect any location data from their users, much less precise location data such as the Wi-Fi SSID.

EdTech Product	Country	Apparently designed for use by children?	Developer	Wi-Fi SSID	Disclosed in privacy policy?
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Private	Yes	Yes
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Private	Yes	No
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Private	Yes	Yes
Threema Work	Germany: Baden-Württemberg, Bavaria	No	Private	Yes	Yes
Padlet	Germany: Bavaria, Romania, Colombia	Yes	Private	Yes	Yes
LINE	Japan, Taiwan	No	Private	Yes	Yes
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, , United Kingdom: England	No	Private	Yes	Yes
WhatsApp	India: Uttar Pradesh, Cameroon	No	Private	Yes	Yes
Ruangguru	Indonesia	Yes	Private	Yes	No
Sekolah.mu	Indonesia	Yes	Private	Yes	No
Shad	Iran	Yes	Government	Yes	No
Telegram	Nigeria	No	Private	Yes	No
Taleemabad	Pakistan	Yes	Private	Yes	No
Naver Band	Republic of Korea	No	Private	Yes	Yes
KakaoTalk	Republic of Korea	No	Private	Yes	Yes
Extramarks	South Africa	Yes	Private	Yes	No
Facebook	Taiwan	No	Private	Yes	Yes
Özelim Eğitimdeyim	Turkey	Yes	Government	Yes	Yes

Websites: Coarse Location Data

Every device connected to the internet has an Internet Protocol (IP) address to send and receive data, much like a physical address is needed to send and receive physical mail.⁸⁷ Every app or website transmits its users' IP address in the standard course of communicating with an internet server. However, IP addresses can also be used to infer a user's location with coarse granularity, or to identify the country, city, and postal code of the person's location.

While it is not possible to determine from a technical assessment whether a company is using an IP address to determine a user's approximate location, most AdTech companies that Human Rights Watch observed receiving children's IP addresses from government-endorsed EdTech products offer geolocation targeting services based on IP addresses.

Criteo, for example, is an AdTech company that specializes in retargeting ads across the internet at people who have previously visited a given website. Decisions on who to target are made using what the company's CEO called its "powerful flashlight" to identify people online, which is powered by the data it holds on "2.5 billion unique users globally, of which 98 percent have persistent identifiers beyond cookies."⁸⁸ The company claims that it has "advanced AI algorithms" which "use [...] over 120 shopping signals to create a unique ad for every user designed to get the highest engagement."⁸⁹

Criteo notes that "Our partners provide us with information about your geographical location derived from your truncated IP address, points of interest that are near you (e.g. stores that are geographically close to you) ... This allows us to improve the relevance of our services by displaying advertisements for products available in your geographical area."⁹⁰

Human Rights Watch observed Criteo receiving children's data and their IP addresses from the EdTech websites Descomplica (Brazil: São Paulo), Escola Mais (Brazil: São Paulo), Study Sapuri (Japan), Z-kai (Japan), 100Ballov (Kazakhstan), Campus.pk (Pakistan), and EBS (Republic of Korea). All of these websites are designed and intended for children's use in education.

In its response, Criteo confirmed that it specializes in behavioral advertising, and that it collects truncated IP addresses to determine a person's location to within one km. While the company stated that it does not intentionally or knowingly collect personal information from children, it confirmed that three of these websites—Descomplica, Study Sapuri, and Z-kai—were current clients and said that it was not currently working with the other four websites. Criteo did not address whether it had received children's data from the EdTech websites listed above.⁹¹

⁸⁷ Electronic Frontier Foundation, "Surveillance Self-Defense, 'IP Address,'" <https://ssd.eff.org/en/glossary/ip-address> (accessed July 8, 2021).

⁸⁸ Megan Clarcken, "Edited Transcript: CRTO.OQ – Q2 2020 Criteo SA Earnings Call, July 28, 2020 / 12:00 pm GMT", Criteo, July 28, 2020, https://web.archive.org/web/20210801054221/https://filecache.investorroom.com/mr5ir_criteo/1009/download/CRTO-USQ_Transcript_2020-07-29.pdf (accessed July 31, 2021), p. 5.

⁸⁹ Criteo, "Criteo AI Engine," <https://web.archive.org/web/20210801054934/https://www.criteo.com/technology/ai-engine/> (accessed July 31, 2021).

⁹⁰ Criteo, "Privacy Policy," November 26, 2020, <https://web.archive.org/web/20210825155825/https://www.criteo.com/privacy/> (accessed August 25, 2021); Criteo, "Anatomy of an Ad Set," <https://web.archive.org/web/20210826061931/https://developers.criteo.com/marketing-solutions/docs/anatomy-of-an-ad-set> (accessed August 25, 2021).

⁹¹ Human Rights Watch email correspondence with Maribel Henriquez, Senior Communications Manager, Criteo, April 7, 2022.

92 Google Firebase, "Reward Referrals," July 8, 2021, <https://web.archive.org/web/20210709224909/https://firebase.google.com/docs/dynamic-links/use-cases/rewarded-referral> (accessed July 9, 2021).

93 "Recommendations From Friends Remain Most Credible Form of Advertising Among Consumers; Branded Websites Are The Second-Highest-Rated Form," Nielsen press release, September 28, 2015, <https://web.archive.org/web/20210709224818/https://www.nielsen.com/us/en/press-releases/2015/recommendations-from-friends-remain-most-credible-form-of-advertising/> (accessed July 9, 2021).

94 After declaring that it would no longer share such information with others in 2014, Facebook continued to give third parties access to personal data about its users and their friends. In 2014 and 2015, Facebook struck deals with companies including Netflix, Lyft, and the Royal Bank of Canada, giving them full access to its users' friends' data. In 2018, Facebook was discovered to have given advertisers and device makers access to detailed data on its users' friends—including their relationship status, religious and political leanings, and events they planned to attend—even if their users had denied Facebook permission to do so. See: Government of the United Kingdom, House of Commons, Digital, Culture, Media and Sport Committee, "Disinformation and 'fake news': Interim Report," HC 363, July 29, 2018, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf> (accessed July 9, 2021), pp. 27-30; Josh Constine, "Facebook is Shutting Down Its API For Giving Your Friends' Data To Apps," *TechCrunch*, April 28, 2015, <https://techcrunch.com/2015/04/28/facebook-api-shut-down/> (accessed July 9, 2021); Giridhari Venkatadri et al., "Investigating Sources of PII Used in Facebook's Targeted Advertising," *Proceedings On Privacy Enhancing Technologies*, vol. 2019, no. 1 (2018), accessed July 9, 2021, doi: 10.2478/popets-2019-0013, pp. 227-244; Kashmir Hill, "Facebook Is Giving Advertisers Access To Your Shadow Contact Information," *Gizmodo*, September 26, 2018, <https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051> (accessed July 9, 2021); Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York Times*, June 3, 2018, <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html> (accessed July 10, 2021).

Tracking Who Children Know

Finding out who you know has long been considered valuable by advertisers, who recognize that one of the most effective methods of attracting new customers is through referrals made by family, friends, and contacts.⁹² The Nielsen Company, a data broker and AdTech company that Human Rights Watch detected receiving children's data from three EdTech websites—Stoodi (Brazil: São Paulo), CBC Kids (Canada), and WeSchool (Italy)—notes that "the most credible form of advertising comes straight from the people we know and trust."⁹³

Contact information can also be used for shadow profiling, in which companies siphon data from their users' contacts lists in order to develop profiles on people who have never used their services. Facebook, for example, came under intense scrutiny in a series of high-profile cases for sharing the personal information of its users' friends, without their consent or awareness, between 2010 and 2018.⁹⁴ Among others, this enabled Cambridge Analytica, a political firm that claimed to influence people by creating uniquely detailed personality profiles and then tailoring political messaging to them, to collect information not only from the 270,000 users who consented to share their data through Cambridge Analytica's Facebook-linked app, but also from up to 87 million unwitting people listed as their friends on Facebook.⁹⁵

When details about the personal relationships of a child are collected without consent or awareness by the child or by the family member or friend in question, it is an arbitrary intrusion on privacy for both. For the contact, their right to privacy is affected by the "mere collection of personal data" in which they lose control over information, in addition to the risk of experiencing potential misuse of their personal data.⁹⁶

Human Rights Watch identified 18 EdTech apps (25 percent) with the ability to collect information about their users' friends, family, and other acquaintances by accessing the contacts list saved on users' phones. This may have allowed these apps to learn personal details about these contacts, including any saved names, phone numbers, emails, addresses, and relationships ("Grandma," "Dad"). In addition, all of these apps, with the exception of Telegram, had the ability to collect profile photos of the contact, if one had been saved.

Three apps developed specifically for children—Kelas Pintar (Indonesia), Shad (Iran), and Extramarks (South Africa)—do not disclose this practice in their privacy policies. Human Rights Watch found that this data was neither necessary for these apps to function, nor provided educational benefit to children.

95 Facebook, "An Update On Our Plans To Restrict Data Access On Facebook," April 4, 2018, <https://about.fb.com/news/2018/04/restricting-data-access/> (accessed July 9, 2021).

96 UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 7.

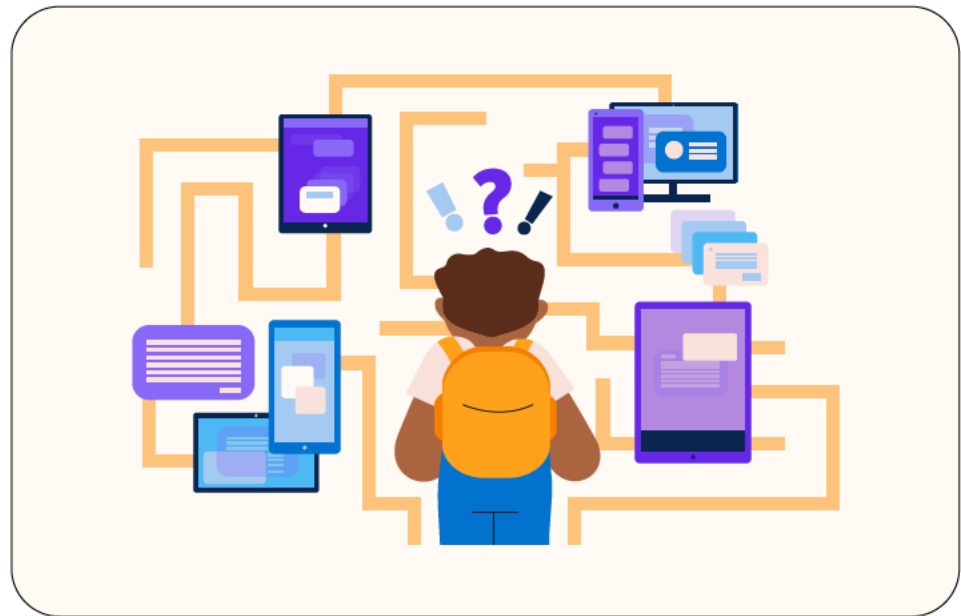
These 18 apps may have granted access to their users' contact data to 16 third-party companies.

EdTech app	Country	Apparently designed for use by children?	Contacts' details	Contacts' photos	Ed Tech app may give access to:
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Yes	Yes	Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Yes	Yes	Google Firebase Analytics, Google Crashlytics, Amplitude
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Yes	Yes	Google Firebase Analytics
Remind	Colombia	Yes	Yes	Yes	Google Firebase Analytics, Google Crashlytics, Braze, Pusher
Dropbox	Colombia	No	Yes	Yes	Google Firebase Analytics, Adjust, Bugsnag
Padlet	Germany: Bavaria, Romania, Colombia	No	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Branch, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Yes	Yes	Google Firebase Analytics, Google AdMob
WhatsApp	India: Uttar Pradesh, Cameroon	No	Yes	Yes	Google Analytics

Kelas Pintar	Indonesia	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager, Facebook Analytics, Facebook Login, Facebook Share, Adjust
Shad	Iran	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics
LINE	Japan, Taiwan	No	Yes	Yes	Google Analytics, Google AdMob, Facebook Login, Facebook Share
Telegram	Nigeria	No	Yes	No	Google Firebase Analytics
Edmodo	Nigeria, Egypt, Colombia, Ghana, Romania, Thailand	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Google AdMob, JW Player, Matomo
Naver Band	Republic of Korea	No	Yes	Yes	Google Firebase Analytics, Google AdMob, AppsFlyer, Facebook Analytics, Facebook Login, Facebook Share, InMobi, Moat
KakaoTalk	Republic of Korea	No	Yes	Yes	Google Firebase Analytics, Google Crashlytics, AdFit
Extramarks	South Africa	Yes	Yes	Yes	Google Analytics, Google Firebase Analytics, Google AdMob, Google Tag Manager, Adjust, Facebook Login, Facebook Places, Facebook Share
Google Meet	Spain, Poland, Taiwan, US: California, Texas	No	Yes	Yes	Google Firebase Analytics
Facebook	Taiwan	No	Yes	Yes	N/A

Tracking What Children Do in the Classroom

Human Rights Watch found that many governments enabled third-party companies to infringe on children's privacy by allowing them to conduct unnecessary, disproportionate surveillance on what children do in their virtual classrooms. Using tracking technologies invisible to their users, many EdTech companies examined in this report collected and sent this data to AdTech and related companies, who in turn enabled a sprawling network of advertisers and other companies to use children's data for commercial purposes, and exposed children to further risk of misuse and exploitation of their data.



Children and parents were denied the knowledge or opportunity to challenge these practices. Most EdTech companies did not disclose their surveillance of children and their data; similarly, most governments did not provide notice of these practices and their risks to students or teachers when announcing their endorsements of EdTech platforms.

But even if children were aware of being surveilled in their virtual classrooms, they could not meaningfully opt out or refuse to provide their personal data to EdTech companies. The Council of Europe noted, “[A]s the education is compulsory and refusal or withdrawal of consent could be detrimental to the development of the child, children would not be in a position to consent freely, irrespective of the assistance by parents or legal representatives.”⁹⁷ This was particularly true in countries that provided most children’s education solely through officially-endorsed EdTech platforms, as further discussed in Chapter 4.

Websites: Ad Trackers

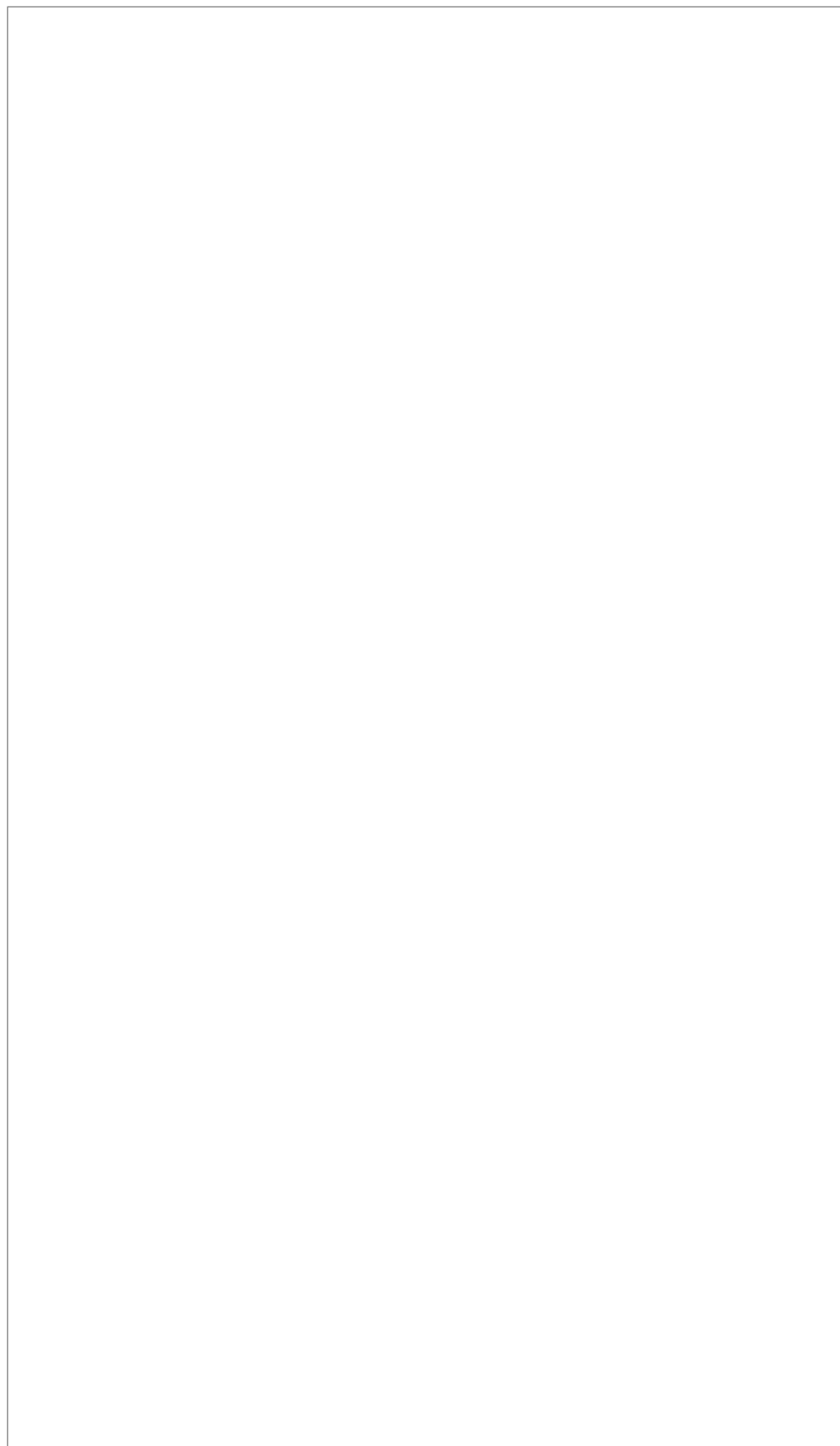
Ad trackers identify and collect information about a person visiting a website. By scrutinizing a person’s every action and behavior, ad trackers use their presumed preferences to target them with specific ads, then measure how successful the ad has been at capturing the person’s attention or enticing them to click on it.⁹⁸

Ad trackers usually take the form of JavaScript scripts or web beacons, which are near-invisible, 1x1 pixel images that are hidden on a website to silently record what users do, including when they visited the site and where they were physically located.⁹⁹

⁹⁷ “Contribution prepared by the Secretariat of the Council of Europe on the subject of the right to privacy of children, in response to the consultation carried out by the UN Special Rapporteur on the right to privacy (UNSRP),” October 5, 2020, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/privacy-child/Regional-Org-and-UN/1-CoE.docx (accessed August 3, 2021), pp. 3, 4.

⁹⁸ Surya Mattu and Aaron Sankin, “How We Built a Real-Time Privacy Inspector,” *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 10, 2021).

⁹⁹ Ibid



A 1x1 pixel image placed in the center of this page.
© 2022 Hye Jung Han/Human Rights Watch

Human Rights Watch found that children's educational websites installed as many third-party trackers on personal devices as do the world's most popular websites aimed at adults. Out of a total 124 EdTech websites, 112 websites (90 percent) placed third-party trackers on devices and browsers used by children. In comparison, an investigation conducted by The Markup in September 2020 found that of the world's over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, 84.9 percent loaded third-party trackers on their website.¹⁰⁰

Put another way, children are just as likely to be surveilled in their virtual classrooms as adults shopping in the world's largest virtual malls, if not more so.

Children are also being tracked at dizzying scale. Human Rights Watch found 717 third-party trackers embedded in these EdTech websites; a child logging into a single one of these 112 platforms at the start of the school day could expect to be tracked by an average of 6 third-party trackers. One EdTech site, Z-kai, endorsed by the Japanese Education Ministry for all elementary, middle, and high school students in Japan to learn core subjects during Covid-19 school closures, embedded 54 ad trackers that were detected transmitting students' data to 37 companies, predominantly in AdTech.

The number of advertising or other third-party companies receiving children's data was discovered to be even greater than the number of EdTech companies sending this data to them. Human Rights Watch detected these 112 websites transmitting children's data to 161 companies.

Out of the 124 websites analyzed by Human Rights Watch, just 12 websites (10 percent) did not collect and transmit data about children through third-party trackers. These were: Juana Manso (Argentina), Stile Education (Australia: Victoria), Faso e-Educ@tion (Burkina Faso), Learn (Canada: Quebec), Biblioteca Digital Escolar (Chile), Jules (France), Ma classe à la maison (France), MaSpéMaths (France), Mebis (Germany: Bavaria), Visavid (Germany: Bavaria), NHK for School (Japan), and iEN (Saudi Arabia).¹⁰¹ These sites point to an alternate vision of online education for children, one that preserves their privacy and does not surveil their students for profit.

¹⁰⁰ Surya Mattu and Aaron Sankin, "The High Privacy Cost of a 'Free' Website," *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites> (accessed July 12, 2021); Victor Le Pochat et al., "Tranco," generated on July 13, 2021, <https://tranco-list.eu/list/KLPW/1000000> (accessed July 13, 2021); see also, Victor Le Pochat et al., "TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

¹⁰¹ Human Rights Watch did not include Facebook in this list; while the website version of the product was not found with third-party ad trackers, the company relies on its own first-party tracking tools to collect and send its users' data back to itself. See: Aaron Sankin and Surya Mattu, "I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What's Going On?" *The Markup*, October 1, 2020, <https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on> (accessed July 13, 2021).

102 Human Rights Watch interview with Jae-kuk H., 14, Seoul, South Korea, June 6, 2020.

103 South Korea's education ministry invested in rapidly expanding learning content on EBS as part of the country's online learning response to Covid-19. See, for example: Korea Education and Research Information Service, "Responding to COVID-19: Online Classes in Korea," June 8, 2020, <https://www.keris.or.kr/eng/na/ntt/selectNttInfo.do?mi=1521&nttSn=36647> (accessed August 30, 2021), pp. 5, 9. See also: Republic of Korea Ministry of Education, "Elementary summer vacation, rewarding and together with educational broadcast EBS!" ("초등 여름 방학, 보람 있게 교육 방송 EBS와 함께!") Republic of Korea Ministry of Education Official Blog, July 29, 2020, <https://if-blog.tistory.com/10833> (accessed August 30, 2021); Republic of Korea Ministry of Education, "School postponed due to COVID-19, study at home like this," ("코로나19로 인한 개학연기, 가정에서 이렇게 공부하세요~") Happy Education (blog), https://happyedu.moe.go.kr/happy/bbs/selectBoardArticleInfo.do?bbsId=BBSMSTR_000000000231&nttId=10765 (accessed August 30, 2021); Danyang Primary School, "Online Learning Guide," ("온라인 학습 안내") Danyang Primary School website, https://school.cbe.go.kr/_class/board/view/danyang-e/2020/Go2020402/383390/9548791?mode=ma (accessed August 30, 2021)

104 EBS, "EBS," <https://www.ebs.co.kr/> (accessed May 22, 2022)

105 Republic of Korea Ministry of Education, "Elementary summer vacation, rewarding and together with educational broadcast EBS!" ("초등 여름 방학, 보람 있게 교육 방송 EBS와 함께!") Republic of Korea Ministry of Education Official Blog, July 29, 2020, <https://if-blog.tistory.com/10833> (accessed August 30, 2021); Republic of Korea Ministry of Education, "School postponed due to COVID-19, study at home like this," ("코로나19로 인한 개학연기, 가정에서 이렇게 공부하세요~") Happy Education (blog), https://happyedu.moe.go.kr/happy/bbs/selectBoardArticleInfo.do?bbsId=BBSMSTR_000000000231&nttId=10765 (accessed August 30, 2021). For an example of a school which adopted the education ministry's recommendations, see: Danyang Primary School, "Online Learning Guide," ("온라인 학습 안내") Danyang Primary School website, https://school.cbe.go.kr/_class/board/view/danyang-e/2020/Go2020402/383390/9548791?mode=ma (accessed August 30, 2021)

Case Study: EBS, Republic of Korea

At the beginning of the pandemic, the Republic of Korea (South Korea)'s Education Ministry suspended all in-person learning and committed to providing online classes for all primary and secondary school students in the country. Jae-kuk H., a 14-year-old boy in Seoul, told Human Rights Watch at the time: "I feel like the earth has just stopped."¹⁰² By April 20, 2020, the website of the national educational public broadcaster, Korea Educational Broadcasting System (EBS), received on average over 2.1 million users every day.¹⁰³

Human Rights Watch notes that during Covid-19 school closures, the Korean education ministry recommended watching TV broadcast lessons on EBS, and to re-watch recordings of those lessons on the EBS sites. EBS' home page is the primary gateway to access EBS' educational offerings, much of which are directed towards children.¹⁰⁴ Human Rights Watch also notes that it analyzed, among others, specific webpages that the Korean education ministry recommended for primary school students' use.¹⁰⁵

When a child opens up EBS' home page, or its main page for primary school students, to log into school for the day, a swarm of trackers get to work. Within milliseconds, 24 ad trackers begin to suck up a child's every movement and interaction within the virtual classroom and transmit this information to 15 advertising companies. A few of these recipients are large data brokers, companies that compile digital dossiers about people from information obtained from public, private, online, and offline sources.

EBS Sent Children's Data to 15 AdTech Companies

AdTech Company	AdTech Domain Receiving Children's Data	How the AdTech company uses the data it receives, based on its marketing materials
ADPIE	adpies.com	"Generate amazing ad revenue like never before." ¹⁰⁶
Appier	appier.net	"Achieve hyper-personalization and deliver 1:1 recommendations ... Engage your customers with real-time notifications triggered by their behavior." ¹⁰⁷ "[U]nifies and enriches existing customer data to help you better understand your audience and run AI models to easily predict their future actions." ¹⁰⁸

106 AdPie, "AdPie," <https://web.archive.org/web/20210804044228/https://www.adpies.com/en/> (accessed August 3, 2021).

107 Appier, "AiQua Customer Engagement Platform," <https://web.archive.org/web/20210807012038/https://www.appier.com/aiqua-customer-engagement-platform/> (accessed August 3, 2021).

108 Appier, "Aixon, Your Data Science Platform," <https://web.archive.org/web/20210807012147/https://www.appier.com/aixon-your-data-science-platform/> (accessed August 3, 2021).

¹⁰⁹ MarTech is an advertising industry term for marketing technology. See: BizSpring, "Solution," <https://web.archive.org/web/20210410200024/http://bizspring.co.kr/company/solution.php> (accessed August 3, 2021).

¹¹⁰ BizSpring, "PeopleDB: Connecting 'People' and 'Data'," <https://web.archive.org/web/20210831005229/https://drive.google.com/file/d/1Dcg4nC26lHflrtCoP7lVgumwe1EUSCSH/view> (accessed August 3, 2021), p. 4.

¹¹¹ Logger, "Marketing," <https://web.archive.org/web/20210804050116/https://logger.co.kr/product/marketing/> (accessed August 3, 2021).

¹¹² Criteo, "Criteo," <https://web.archive.org/web/20210803001340/https://www.criteo.com/> (accessed August 3, 2021).

¹¹³ Criteo, "Shopper Graph," <https://web.archive.org/web/20210826020928/https://www.criteo.com/technology/shopper-graph/> (accessed August 3, 2021).

¹¹⁴ Dable, "Dable," <https://web.archive.org/web/20210813180914/https://dable.io/en/> (accessed August 3, 2021).

¹¹⁵ Enliple, "Company Overview," <https://web.archive.org/web/20200628172500/http://enliple.com/eng/doc/corp> (accessed August 30, 2021).

BizSpring	bizspring.net	"BizSpring provides a variety of data solutions for MarTech/AdTech," "'Integrate' and 'connect' all behavioral data centered on 'people.' Predict user intentions with big data in which each individual's behavioral patterns are alive and deliver a message that can directly increase conversion performance."¹⁰⁹ "We build a single customer profile by integrating all data about the customer, including the movements and paths they take in an app or website ... and even behavioral data from 3rd parties. Customers with specific behavioral tendencies can be easily identified at the level of each 'person,' and target segments can be extracted in the form of a list according to the purpose and utilized in various marketing activities."¹¹⁰
	logger.co.kr	"Logger™ provides data that can maximize marketing performance by tracking ... every action that occurs on your website," "Track your visitor's clickstream to understand performance: ... tracks all of the activities of visitors online and provides analysis data that can determine ROI."¹¹¹
Criteo	criteo.com, criteo.net	"2.5 billion users ... active in 100+ countries: a global perspective of consumers and commerce."¹¹² "Pooled identity data within Criteo Shopper Graph ensures accurate cross-device identification from the billions of active online shoppers who use multiple devices to shop, and the tens of thousands of websites worldwide that continuously share their data with us. Stitch together device identifiers across billions of user timelines. Find patterns of behavior and listen to signals of intent."¹¹³
Dable	dable.io	"Improve traffic and advertising earnings with the best personalization platform in Asia," "consider personalization technology and native ads as effective profit models in increasing preference and user attention. Detailed targeting by interest, region, medium, time of day, etc."¹¹⁴
Enliple	mediacategory.com	"Enliple's advertising solution differentiator is to analyze customer behavior data through Big Data-based customer insight and to deliver more personalized predictive analytics and maximize user's ROI by automatically learning real-time customer behavior."¹¹⁵

116 Facebook, "Facebook Business Tools Terms," August 31, 2020, <https://web.archive.org/web/20210728002513/https://www.facebook.com/legal/terms/businessstools> (accessed July 28, 2021).

117 Google, "Google Marketing Platform," <https://marketingplatform.google.com/about/enterprise/> (accessed July 28, 2021).

118 Google, "About Discovery Campaigns," Google Ads Help, https://web.archive.org/web/20210921003622/https://support.google.com/google-ads/answer/9176876?hl=en&ref_topic=10307857 (accessed September 20, 2021).

119 Bidswitch, "Smart Infrastructure for Programmatic Platforms," <https://web.archive.org/web/20210815033808/https://www.bidswitch.com/technology/> (accessed August 15, 2021).

120 Bidswitch, "Efficient Solutions for Managing Programmatic Supply," <https://web.archive.org/web/20210810024525/https://www.bidswitch.com/solutions/dsps/> (accessed August 15, 2021).

121 Kakao, "Display Ads for Business," <https://web.archive.org/web/20200809234639/https://business.kakao.com/info/displayad/> (accessed August 15, 2021).

Facebook	facebook.com, facebook.net	"We will use Business Tool Data ... to match the Contact Information against user IDs," "to prepare reports on your behalf on the impact of your advertising campaigns and other online content ("Campaign Reports") and (b) to generate analytics and insights about people and their use of your apps, websites, products and services," "to target your ad campaigns to people who interact with your business," "use the Matched User IDs and associated Event Data to help you reach people with transactional and other commercial messages on Messenger and other Facebook Company Products," and "to improve ad delivery, personalize features and content and to improve and secure the Facebook products." ¹¹⁶
Google	google-analytics.com, doubleclick.net, googlead- services.com, googletag- manager.com, google.com	"Easily integrate and access your data to gain a deeper understanding of your customers and identify your most valuable audiences." ¹¹⁷ "Drive engagement with richer, more relevant ads. Thanks to Google's unique understanding of customer intent, you'll be able to show more relevant, meaningful ads to people when they're most interested to learn more about your products and services." ¹¹⁸
IPONWEB GmbH	bidswitch.net	"BidSwitch creates value for the Ad Tech ecosystem ... provides the underlying infrastructure that normalizes the connections between different programmatic technology platforms.... BidSwitch is continuously processing, filtering for fraud & classifying inventory opportunities, layering on data and other services, then intelligently distributing it to relevant buyers across more than 130 Demand Side Technology platforms – all in real-time." ¹¹⁹ "Features: User & ID syncing, Centralized cookie syncing and ID tables." ¹²⁰
Kakao	daum.net	"With Kakao's technology, it finds suitable users and displays advertisements by capturing the moments when advertisements are needed. Experience a variety of sophisticated targeting, such as demographics, audience behavior, interests, Kakao services, and current location." ¹²¹

122 MediaMath, “Future-Proofed Digital Advertising Platform,” <https://web.archive.org/web/20210807015327/https://www.mediamath.com/platform/> (accessed August 15, 2021).

123 Naver, “Naver Performance Display Advertising” (“네이버 성과형 디스플레이 광고”), <https://web.archive.org/web/20210920231627/https://displayad.naver.com/adplatform> (accessed September 20, 2021).

124 SK Communications, “Nate Ads Product Introduction” (“nate 광고 상품소개서”), July 2020, https://adguide.nate.com/html/download.php?filename=SK커뮤니케이션즈_매체소개서_20.07.pdf, pp. 37, 39.

125 By one estimate, BlueKai tracks over one percent of all web traffic in the world. See: Cliqz, Who Tracks Me, “BlueKai,” <https://whotracks.me/trackers/bluekai.html> (accessed July 12, 2021); Bennett Cyphers and Gennie Gebhart, “Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance,” Electronic Frontier Foundation, December 2, 2019, <https://www.eff.org/wp/behind-the-one-way-mirror> (accessed July 12, 2021).

126 Oracle, “Oracle Data Marketplace,” <https://web.archive.org/web/20210804031326/https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html> (accessed August 3, 2021); Oracle, “2019 Data Directory,” <https://web.archive.org/web/20210403010855/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf> (accessed August 3, 2021). Prominent location data brokers, including PlacelQ (p. 118), Factual (p. 59), Cuebiq (p. 43), Gravy Analytics (p. 65) make their precise geolocation data available for sale through Oracle Data Cloud’s BlueKai marketplace. See also: Privacy International, “Oracle’s PlacelQ acquisition connects physical and digital tracking,” July 13, 2016, <https://privacyinternational.org/examples/2385/oracles-placelq-acquisition-connects-physical-and-digital-tracking> (accessed August 3, 2021). In 2016 and 2017, Oracle claimed through its marketing materials that its data marketplace contained 5 billion global consumer profiles. See: Oracle, “Get to the Heart of the Matter, the Heart of Your Consumer,” 2016, <https://web.archive.org/web/20210804032442/https://www.oracle.com/assets/brochure-data-driven-marketing-odc-2894231.pdf> (accessed August 3, 2021), p. 10; Nick Whitehead, “Smart Investments in a Data Cloud Strategy,” post to “Oracle Analytics” (blog), October 3, 2017, <https://web.archive.org/web/20210804032618/https://blogs.oracle.com/analytics/post/smart-investments-in-a-cloud-data-strategy> (accessed August 3, 2021).

MediaMath	mathtag.com	“MediaMath is the demand-side platform that offers the most powerful off-the-shelf and custom capabilities for brands to reach and influence customers and prospects on any screen. [T]he digital advertising platform offers ... different targeting to drive a variety of goals/KPIs: audience, contextual, ... location.” “Identity Management: Use our flexible identity core to transact directly on a variety of common ID systems. Consumer Segmentation: Build larger and better performing audiences with our deep segmentation tool that marries data from brands/ partners with MediaMath data and third-party data.” “Easily activate native advertising [which] ... matches the form and function of the location in which it appears, providing a more seamless, higher-quality experience on the open Web for consumers.”¹²²
Naver	naver.com, naver.net	“Naver’s performance-based display advertising converts digital consumers into customers: Quickly find potential customers who can better respond to your brand message through a variety of targeting combinations, including gender, age, region, interests, and device OS.”¹²³
Oracle	bkrx.com, bluekai.com	See below.
SK Communications Co. Ltd	nate.com	“Based on users’ data, intensively focus on your key targets by: gender, age, location, and time.” “Collect data that can identify people’s tendencies, such as their internet searches, news/posts browsed, shopping, videos viewed, memberships, etc., to find your targets for selective exposure.”¹²⁴
WiderPlanet	widerplanet.com	See below.

Among these, Human Rights Watch detected EBS transmitting children’s data to Oracle’s BlueKai Data Management Platform, a data broker that has amassed one of the world’s largest troves of data on people online.¹²⁵ The company helps advertisers build even more extensive profiles on their users with the “actionable audience data” it has on billions of people, including billions of daily location signals acquired from other data brokers.¹²⁶

In June 2020, TechCrunch reported that BlueKai had left one of its servers unprotected, spilling data on billions of records on people—names, home addresses, other personally identifiable data—out onto the open web for anyone to find.¹²⁷ It was considered one of the most significant data security incidents of 2020, due to the immense size of the exposed database.¹²⁸ Human Rights Watch detected EBS sending children’s data to Oracle’s BlueKai through its ad trackers **bluekai.com** and **bkrx.com**, both before and after the reported data breach.

127 Zack Whittaker, “Oracle’s BlueKai Tracks You Across the Web. That Data Spilled Online,” *TechCrunch*, June 19, 2020, <https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/> (accessed July 12, 2021).

128 Ibid.

When reached for comment, Oracle confirmed the data leak, and said that an investigation it conducted in 2020 did not uncover evidence that data relating to children were involved. Oracle stated that any receipt of data related to children would be a violation of Oracle's agreements and policy, and did not address whether it had nonetheless received child users' data from six EdTech websites, including EBS. The company did not address whether data received from EBS were exposed as part of the 2020 security breach, and whether it had informed EBS or the other EdTech websites about the security breach.¹²⁹

EBS also sent information about children's behavior in its virtual classrooms to WiderPlanet, a Korean AdTech company. WiderPlanet advertises its "targeted advertising service" powered by the personal data they hold on "99% of Korean internet users" and information on what they do online. The company also claims it can uniquely identify 43 million people, "their interests and demographic types."¹³⁰ Given that 96 percent of Korea's population uses the internet, this claim would mean that WiderPlanet holds the personal data of almost the entire country's population.

WiderPlanet did not respond to our request for comment.

EBS' privacy policy notes that it collects and uses its users' personal information for "marketing and advertising," including "demographic analysis, analysis of service visits and usage records, and provision of customized services based on personal information and interests."¹³¹ It does not disclose the use of ad trackers on the site. Nor are the AdTech companies detected by Human Rights Watch to receive children's data disclosed in the list of third parties officially recognized as processors of EBS users' personal data.¹³²

In their response to Human Rights Watch, EBS noted that EBS' home page, "while it offers some paid subscription services such as health sciences and cooking classes for adults, mainly functions as a gateway to various Internet education websites of EBS." EBS also stated that, of the user data it sends AdTech companies, it does not send information that would identify children. EBS pointed to a website, EBS Online Class, that it opened with support from the government and provided free education during the Covid-19 pandemic, and stated that this website, which Human Rights Watch did not analyze, as it required a student login, did not share users' data with third-party companies.¹³³

Websites: Session Recording, Key Logging

Some EdTech websites are even more intrusive, embedding a tracking technology known as session recording that allows a third party to watch and record all of a user's behavior on a web page.¹³⁴ That includes mouse movements, clicks, movements around the page, and anything a user types into the page, even if they don't click submit. The collection of such data minutiae is the digital equivalent of logging video surveillance each time a child scratches their nose or grasps their pencil in class.

Typically, these data would then be scrutinized by the third-party companies that offer session recording services on behalf of the website using their services in order to guess at a child's personality, their preferences, and what they're likely to do next.

¹²⁹ Human Rights Watch email correspondence with Dorian Daley, Executive Vice President and General Counsel of Oracle, April 15, 2022.

¹³⁰ WiderPlanet, WiderPlanet," <https://web.archive.org/web/20210713204827/https://www.widerplanet.com/?lang=en> (accessed July 13, 2021).

¹³¹ EBS, "Privacy Policy" ("개인정보처리방침"), February 8, 2021, <https://web.archive.org/web/20210804035422/https://sso.ebs.co.kr/policy/privacy?date=20210208&tab=2&ver=%2Fpolicy%2Fprivacy%3Fdate%3D-20210208&fsdc=> (accessed March 2, 2021), section 1(3), (4).

¹³² Ibid., sections 4 and 5.

¹³³ Human Rights Watch email correspondence with Suh Dong Won, Policy Planning Center Public Relations Manager of EBS, May 20, 2022.

¹³⁴ A 2017 study by Princeton researchers found that session recorders were collecting sensitive information such as passwords and credit card numbers. See: Steven Englehardt, Gunes Acar, and Arvind Narayanan, "No boundaries: Exfiltration of personal data by session-reply scripts," post to "Freedom to Tinker" (blog), November 15, 2017, <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-reply-scripts/> (accessed July 12, 2021).

Human Rights Watch found 23 EdTech websites, endorsed by eight governments, using session recorders. For all but one, their own materials describe and appear to market them for children's use in education. Most transmitted children's data to the third-party companies Hotjar or Yandex. Hotjar describes itself as a "Product Experience Insights software company". Yandex, a technology company that describes itself as a "technology company that builds intelligent products powered by machine learning," including search and information services, navigation products, and other mobile applications, claims that "clicks, scrolls, keystrokes, and mouse movements are all recorded in a single informative movie... Never miss something interesting with up to 150,000 recordings per day."¹³⁵

When reached for comment, both Hotjar and Yandex answered without responding to our questions. Amazon, who owns cloudfront.net, did not respond to a request for comment.¹³⁶

EdTech Product	Country	Apparently designed for use by children?	Session recorders
Descomplica	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
DragonLearn	Brazil: São Paulo	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Manga High	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
Stoodi	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
WorkFlowy	Colombia	Yes	script.hotjar.com, static.hotjar.com
iMektep	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Kundelik	Kazakhstan	Yes	mc.yandex.ru/metrika/tag.js, mc.yandex.ru/metrika/watch.js
Daryn Online	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/tag.js
100ballov	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
iTest	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
ExamenulTau	Romania	Yes	script.hotjar.com, static.hotjar.com
Miro	Romania	No	script.hotjar.com, static.hotjar.com
ȘcoalăIntuitext	Romania	Yes	script.hotjar.com, static.hotjar.com
My School is Online	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js
Digital Lessons	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js
SberClass	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js

¹³⁵ Yandex.Metrica, "Behavioral Analytics," <https://web.archive.org/web/20210507175616/https://metrica.yandex.com/about/info/behavior> (accessed July 12, 2021).¹³⁶ Human Rights Watch email correspondence with Louanne Grech, Privacy Lead and Data Protection Office, Hotjar, March 24, 2022; and with Yandex press office, April 7, 2022.

¹³⁶ Human Rights Watch email correspondence with Louanne Grech, Privacy Lead and Data Protection Office, Hotjar, March 24, 2022; and with Yandex press office, April 7, 2022.

Russian Electronic School	Russia	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
My Achievements	Russia	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Moscow Electronic School	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js, mc.yandex.ru/metrika/watch.js
Sirius	Russia	Yes	mc.yandex.ru/metrika/watch.js
PaGamO	Taiwan	Yes	script.hotjar.com, static.hotjar.com
Kundalik	Uzbekistan	Yes	mc.yandex.ru/metrika/watch.js

A related technique is key logging, a particularly invasive procedure that surreptitiously captures personal information that people enter on forms, like names, phone numbers, and passwords, before they hit submit. This technique has been used for a variety of purposes, including identifying anonymous web users by matching them to postal addresses and real names, before they can consent to anything.¹³⁷

Human Rights Watch detected 16 websites deploying key logging techniques to send users' names, usernames, passwords, and other information to first- and third-party companies. All of these websites, save one, are products whose own materials describe and appear to market them for children's use for education.

EdTech Product	Country	Apparently designed for use by children?	Key loggers
Education Perfect: Science	Australia: Victoria	Yes	hsforms.com
Descomplica	Brazil: São Paulo	Yes	hsforms.com
Manga High	Brazil: São Paulo	Yes	mangahigh.com
Stoodi	Brazil: São Paulo	Yes	veinteractive.com, stoodi.com.br
Aprendo en Línea	Chile	Yes	nullcurriculumnacional.cl
Educar Ecuador	Ecuador	Yes	recursos.educarecuador.gob.ec
Mineduc Digital	Guatemala	Yes	mineduc.gob.gt
Daryn Online	Kazakhstan	Yes	yandex.com
Notesmaster	Malawi	Yes	youtube.com
EBS Online Classes	Republic of Korea	Yes	nullebs.co.kr
Miro	Romania	No	realtimeboard.com

¹³⁷ Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," The Markup, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 12, 2021); Surya Mattu and Kashmir Hill, "How a Company You've Never Heard of Sends You Letters About Your Medical Condition," Gizmodo, June 19, 2017, <https://gizmodo.com/how-a-company-you-ve-never-heard-of-sends-you-letters-a-1795643539> (accessed July 12, 2021).

Moscow Electronic School	Russia	Yes	yandex.ru
My School is Online	Russia	Yes	yandex.ru
Digital Lessons	Russia	Yes	yandex.ru
ST Math	US: Texas	Yes	hsforms.com

For example, Stoodi, an educational website recommended by Brazil's São Paulo Education Ministry, was found using key logging to capture children's names and what they searched for inside of Stoodi. Even if children changed their minds and decided not to submit their personal information, the captured data was still automatically sent to a third-party advertising company, Ve Global.¹³⁸ Stoodi did not disclose in its privacy policy that children's data would be captured through key logging, or that it would be sent to a third-party company for commercial use.

Brazil_Stoodi_VPN_inspection.json

```

2144     },
2145     "key_logging": {
2146       "veinteractive.com": [
2147         {
2148           "filter": [
2149             "IdaaaaTarbell",
2150             "Tarbell",
2151             "Idaaaa",
2152             "IdaaaaTarbell"
2153           ],
2154           "match_type": [
2155             "plaintext"
2156           ],
2157           "post_data": "{\n\"captureUrl\": \"stoodi.com.br/cadastro/\", \"capturedDataContext\":
{\n\"pageIdentification\": {\n\"pageType\": 0, \"inferred\": {}, \"configuredForms\": [1], \"formMappingInfo\": {\n\"1\":
{\n\"249605\": {\n\"type\": 44, \"domEventId\": 5}}, \"saleFlags\": {\n\"inferred\": false, \"pixel\": false,
\n\"identified\": false, \"total\": \"\"}, \"isPageView\": false, \"url\": {\n\"location\": \"https://www.stoodi.com.br/
cadastro/\", \"referrer\": \"\"}, \"jump\": {\n\"pageJump\": 8, \"pageJumpIn\": 3}}, \"customerId\": 1016849,
\n\"formMappings\": {\n\"249605\": \"IdaaaaTarbell\"}, \"ifsStatus\": {\n\"audit\": {\n\"isCookieAvailable\": true,
\n\"isStorageAvailable\": true, \"message\": \"\"}, \"state\":
{\n\"veCookieId\": \"2f8ae8fe-7eec-4721-b481-464105088454\", \"veCookieStatus\": 1}},
\n\"journeyCode\": \"F5982BA4-1E96-4CCB-BAA0-F40CFBCB99EF\", \"pageId\": \"1623479368085\",
\n\"sessionId\": \"28f98471-80b0-45a0-8df1-9aee4d7b44bc\", \"translatorDetected\": false, \"type\": \"pageViewed\",
\n\"version\": \"v001\"}",
2158       "post_request_url": "https://dtrcusa.veinteractive.com/FormMappings",
2159       "post_request_ps": "veinteractive.com"
2160     },

```

Evidence of Stoodi deploying key logging to send user data to Ve Global, captured in real time. Here, "Idaaaa Tarbell" is the first and last name of a fictional student interested in signing up for Stoodi's services. Once a child types in their name into Stoodi's website, Stoodi immediately captures their name (as seen here under "filter") and sends it to the web address "https://dtrcusa.veinteractive.com/FormMappings." The domain veinteractive.com is owned by the company Ve Global. © 2022 Hye Jung Han/Human Rights Watch

¹³⁸ Ve Global, formerly known as Ve Interactive, is a "technology company ... that provides advertising and marketing solutions" which "helps sell products." See: Ve, "Privacy Policy," <https://web.archive.org/web/20210809024159/https://www.ve.com/legal/privacy-policy> (accessed August 9, 2021); PitchBook, "Ve Global," <https://pitchbook.com/profiles/company/65416-69#overview> (accessed August 9, 2021).

¹³⁹ Human Rights Watch email correspondence with Barbara Lacourt, Director, Global Head of Legal, Ve, March 24, 2022.

When contacted for comment, Ve Global acknowledged that Stoodi was a former client, and confirmed that Stoodi still had Ve Global's active tracking tags embedded on its website. Ve Global confirmed that it had subsequently disabled the content of the tag.¹³⁹ This renders the tracker unusable for Stoodi to continue sending user data to Ve Global.

Stoodi did not respond to our request for comment.

Apps: Software Development Kits (SDKs)

For children who attend online classes using their mobile phones, companies are able to track what they do by embedding software development kits (SDKs) in their apps. Much like building blocks in a toy set, SDKs are blocks or libraries of code written by a third-party company that perform defined functions—like a login page, or notification popups—that app developers can conveniently use when building their app without having to create the functionality from scratch. SDKs are the primary means for app developers to enable an app to work with third-party services.

While some SDKs provide core functionality that is needed for an app to work or to improve its technical performance, others are designed solely for advertising—to track users' actions within the app, guess at their preferences, and display the most persuasive ad at the most persuasive time. Still other SDKs provide tracking services that are designed to secretly collect data about the user that can later be compiled and sold. What an SDK does, once implemented in an app, will depend on how it was designed by the third party. SDKs do not fall into neat categories at the time of this writing; for example, an SDK for an analytics company may also facilitate the preparation of user profiles, and an SDK for an advertising company may provide reporting and analytics capabilities.

When a child installs an app for school, the SDKs that the developer embedded in the app also receive the same access as the app to the mobile phone's data and system resources; this facilitates the transmission of the child's personal data directly to the third-party company that owns that SDK.¹⁴⁰

Human Rights Watch identified 243 SDKs embedded within 66 apps, giving access to a significant array of children's personal data to 33 third-party companies, many of which appear to have primary businesses in advertising and the monetization of users' personal data. It is not possible for Human Rights Watch to reach definitive conclusions as to the companies' motivations in embedding these SDKs, beyond reporting on what it observed in the data and the companies' and governments' own statements.

In the table below, Human Rights Watch lists the third-party SDKs found embedded in each EdTech app, and the “dangerous” permissions and sensitive user data to which they were granted access.¹⁴¹

Human Rights Watch notes that it does not conclusively determine how any given SDK is used by a specific app, and that some SDKs may provide multiple capabilities in addition to advertising. Human Rights Watch also notes that the use of “dangerous” permissions to access sensitive data is not inherently unsafe, but poses risks to users' privacy if there are no safeguards that protect against the abuse of such access by the host app or its embedded third-party SDKs.¹⁴²

¹⁴⁰ In research commissioned by the Australian Competition and Consumer Commission, security researchers from AppCensus conducted dynamic analysis on 1,000 of the most popular mobile Android apps in Australia, and found that “in many cases, app developers request more permissions than their apps actually need, which puts user data at risk of being accessed by third-party SDKs unnecessarily.” See: AppCensus, “1,000 Mobile Apps in Australia: A Report for the ACCC,” September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_o.pdf (accessed April 3, 2021), pp. v, 21.

¹⁴¹ Android labels permissions as “dangerous” when granting that permission to an app can “potentially affect the user's privacy or the device's normal operation,” because the app “wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps.” See: Android Developers, “Permissions overview,” May 7, 2020, <https://web.archive.org/web/20200712090715/https://developer.android.com/guide/topics/permissions/overview> (accessed April 24, 2022).

¹⁴² See, for example, Patrick McGee, “Russian tech giant Yandex's data harvesting raises security concerns,” *Financial Times*, March 29, 2022, <https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb> (accessed April 24, 2022).

EdTech app	Country	SDKs	EdTech app may give a third-party company access to a user's:
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	Microsoft: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), call log, camera, microphone
Adobe Connect	Australia: New South Wales	Google: Google Analytics	Phone number
Minecraft: Education Edition	Australia: Victoria	AppsFlyer: AppsFlyer Braze: Braze Google: Google Firebase Analytics	Persistent identifiers (Android Advertising ID, Wi-Fi MAC)
Centro de Mídias da Educação de São Paulo	Brazil: São Paulo	Google: Google Crashlytics, Google Firebase Analytics	Camera, microphone
Descomplica	Brazil: São Paulo	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob Facebook: Facebook Analytics, Facebook Login, Facebook Places, Facebook Share MixPanel: MixPanel	Persistent identifiers (Android Advertising ID), camera
Explicae	Brazil: São Paulo	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login	Camera
Stoodi	Brazil: São Paulo	Google: Google Crashlytics, Google Firebase Analytics, Google Tag Manager, Google Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share Segment: Segment	Persistent identifiers (Android Advertising ID, IMEI)
Math Kids	Canada: Quebec	None	N/A
Prof Multi	Canada: Quebec	Microsoft: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes	Microphone
Storyline Online	Canada: Quebec	Google: Google Firebase Analytics	Persistent identifiers (Android Advertising ID)

Biblioteca Digital Escolar	Chile	Google: Google Crashlytics, Google Firebase Analytics, Google Analytics	N/A
Dropbox	Colombia	Google: Google Firebase Analytics Adjust: Adjust Bugsnap: Bugsnap	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), camera
Remind	Colombia	Google: Google Crashlytics, Google Firebase Analytics Braze: Braze Pusher: Pusher	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), call log, camera, microphone
WorkFlowy	Colombia	Google: Google Firebase Analytics	Camera, microphone
Jules	France	None	N/A
Jitsi	Germany: Baden-Württemberg	Google: Google Crashlytics, Google Firebase Analytics	Camera, microphone
Threema Work	Germany: Baden-Württemberg, Germany: Bavaria	None	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
Moodle	Germany: Baden-Württemberg, Romania, Kazakhstan	Google: Google Firebase Analytics	Precise location (GPS, time of current location, last known location), coarse location, camera, microphone
IServ	Germany: Bavaria	Google: Google Firebase Analytics	N/A
itslearning	Germany: Bavaria	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera
SchoolFox	Germany: Bavaria	Google: Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Padlet	Germany: Bavaria, Romania, Colombia	Google: Google Crashlytics, Google Firebase Analytics Microsoft: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes Branch: Branch	Persistent identifiers (Android Advertising ID, Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), contacts' information (contacts, contacts' photo), phone number, camera, microphone
Ghana Library App	Ghana	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera, microphone

YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	Google: Google Firebase Analytics, Google AdMob	Persistent identifiers (Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
e-Balbharti	India: Maharashtra	None	Phone number
Learning Outcomes Smart Q	India: Maharashtra	Google: Google Firebase Analytics	None
Diksha	India: National	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), camera, microphone
ePathshala	India: National	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Top Parent	India: Uttar Pradesh	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob Facebook: Facebook Login, Facebook Share, Facebook Places CleverTap: CleverTap	N/A
WhatsApp	India: Uttar Pradesh, Cameroon	Google: Google Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, SMS logs, camera, microphone, fingerprint
Khan Academy	India: Uttar Pradesh, Pakistan, Nigeria, South Africa	Google: Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share	N/A
Kelas Pintar	Indonesia	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob, Google Analytics, Google Tag Manager Facebook: Facebook Analytics, Facebook Login, Facebook Share Adjust: Adjust	Persistent identifiers (Android Advertising ID, IMEI), contacts' information (contacts, contacts' photo), camera

Quipper	Indonesia	Google: Google Crashlytics, Google Firebase Analytics, Google Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share Brightcove: Brightcove UXCam: UXCam Wootric: Wootric	Persistent identifiers (Android Advertising ID), camera
Ruangguru	Indonesia	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Places, Facebook Share AppsFlyer: AppsFlyer OneSignal: OneSignal	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, call logs, camera, microphone, flashlight
Rumah Belajar	Indonesia	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), coarse location, camera
Sekolah.mu	Indonesia	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login Snowplow: Snowplow	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, camera, microphone
Zenius	Indonesia	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share AppsFlyer: AppsFlyer CleverTap: CleverTap	Camera, microphone
Shad	Iran	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
Newton	Iraq	Google: Google AdMob Flurry: Flurry	Persistent identifiers (Android Advertising ID)

WeSchool	Italy	Google: Google Firebase Analytics Huawei: Huawei Mobile Services (HMS) Core OneSignal: OneSignal	Persistent identifiers (Android Advertising ID), microphone
NHK for School	Japan	None	N/A
schoolTakt	Japan	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Study Sapuri	Japan	Google: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google AdMob AppsFlyer: AppsFlyer Keen: Keen Repro: Repro	Persistent identifiers (Android Advertising ID)
LINE	Japan, Taiwan	Google: Google Analytics, Google AdMob Facebook: Facebook Login, Facebook Share	Persistent identifiers (aaaaaWi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone, flashlight, fingerprint
Bilimland	Kazakhstan	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID), camera
Daryn Online	Kazakhstan	Amplitude: Amplitude	Persistent identifiers (Android Advertising ID), camera, microphone
Kundelik	Kazakhstan	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob AppMetrica: AppMetrica Vkontakte: VKontakte SDK Yandex: Yandex Ad	Persistent identifiers (Android Advertising ID), camera
TelmideTICE	Morocco	None	N/A
Telegram	Nigeria	Google: Google Firebase Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts), phone number, call logs, camera, microphone

Edmodo	Nigeria, Egypt, Colombia, Ghana, Romania, Thailand	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob JW Player: JW Player Matomo (Piwik): Matomo	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone
Learn Smart Pakistan	Pakistan	Google: Google Firebase Analytics	N/A
Muse	Pakistan	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID, Wi-Fi MAC), microphone
Taleemabad	Pakistan	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location
KakaoTalk	Republic of Korea	Google: Google Crashlytics, Google Firebase Analytics AdFit: AdFit	Persistent identifiers (Android Advertising ID, Wi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, SMS logs, camera, microphone
Naver Band	Republic of Korea	Google: Google Firebase Analytics, Google AdMob Facebook: Facebook Analytics, Facebook Login, Facebook Share AppsFlyer: AppsFlyer InMobi: InMobi Moat: Moat	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
Edpuzzle	Romania	Google: Google Crashlytics, Google Firebase Analytics	Phone number
Kinderpedia	Romania	Google: Google Crashlytics, Google Firebase Analytics Huawei: Huawei Mobile Services (HMS) Core OneSignal: OneSignal	Persistent identifiers (Android Advertising ID), phone number, call logs, camera, microphone

Miro	Romania	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob Branch: Branch	Persistent identifiers (Android Advertising ID), camera
Moscow Electronic School	Russia	Google: Google Crashlytics, Google Firebase Analytics	N/A
My Achievements	Russia	Google: Google Crashlytics Facebook: Facebook Analytics, Facebook Login, Facebook Share Flurry: Flurry Vkontakte: VKontakte SDK	Persistent identifiers (Android Advertising ID), camera, microphone
iEN	Saudi Arabia	Google: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera
African Storybook	South Africa	None	N/A
Extramarks	South Africa	Google: Google Crashlytics, Google Firebase Analytics, Google AdMob, Google Tag Manager Facebook: Facebook Places, Facebook Login, Facebook Share Adjust: Adjust	Persistent identifiers (Android Advertising ID, Wi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), call logs, SMS logs, camera, microphone
Google Meet	Spain, Poland, Taiwan, US: California, Texas	Google: Google Firebase Analytics	Contacts' information (contacts, contacts' photo), camera, microphone
Nenasa	Sri Lanka	Google: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager Facebook: Facebook Analytics, Facebook Login, Facebook Share, Facebook Places AppsFlyer: AppsFlyer	Persistent identifiers (Android Advertising ID), camera
Facebook	Taiwan	None	N/A
PaGamO	Taiwan	Google: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login, Facebook Share Amplitude: Amplitude	Persistent identifiers (Android Advertising ID)

Eğitim Bilişim Ağı	Turkey	Google: Google Firebase Analytics	Persistent identifiers (Android Advertising ID), phone number, call logs, camera, microphone
Özelim Eğitimdeyim	Turkey	Google: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager, Google AdMob Facebook: Facebook Login Flurry: Flurry StartApp: StartApp	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location
Zoom	US: California, Cameroon	Google: Google Firebase Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi BSSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call log, camera, microphone
Cisco Webex	US: California, Poland	Google: Google Crashlytics, Google Firebase Analytics Amplitude: Amplitude	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone
Schoology	US: Texas	Google: Google Crashlytics, Google Firebase Analytics Flurry: Flurry	Persistent identifiers (Android Advertising ID), camera
Seesaw	US: Texas, Nigeria	Google: Google Crashlytics, Google Firebase Analytics	Camera, microphone

Without significant technical expertise, children cannot know whether third-party SDK integrations are present in their EdTech app. But even if they were aware, none of the 66 apps analyzed by Human Rights Watch allowed their users to decline access to their data by a third-party company.

When reached for comment, Cisco stated that Webex does not share user data with Google Crashlytics or Google Firebase Analytics, as it has disabled data collection for those SDKs.

Five apps did not embed any SDKs, demonstrating that it is possible to build an app without sending children's personal information to a third-party company, and without the ability to collect information about children that is unnecessary to provide them with education. These apps, and the governments that recommended them, are: Math Kids (Canada: Quebec), Jules (France), NHK for School (Japan), TelmidTICE (Morocco), and African Storybook (South Africa).¹⁴³

143 While the Facebook app was also found without third-party SDKs, Meta is an AdTech company that relies on its own first party tracking technologies to collect and send its users' data to itself. See: Aaron Sankin and Surya Mattu, "I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What's Going On?" *The Markup*, October 1, 2020, <https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on> (accessed July 13, 2021).

144 Government of Indonesia, Kementerian Pendidikan dan Kebudayaan (Ministry of Education and Culture), “Ministry of Education and Culture Collaborates with the Private Sector to Prepare Online Learning System” (“Kemendikbud Gandeng Swasta Siapkan Sistem Belajar Daring”), March 15, 2020, <https://web.archive.org/web/20210804220824/https://www.kemendikbud.go.id/main/blog/2020/03/kemendikbud-gandeng-swasta-siapkan-sistem-belajar-daring> (accessed August 4, 2021).

145 Crunchbase, “Ruangguru: Financials,” https://www.crunchbase.com/organization/ruangguru/company_financials (accessed August 5, 2021); Ruangguru, “Ruangguru Secures USD 55 Million New Investment Led by Tiger Global Management,” post to “Ruangguru” (blog), April 19, 2021, <https://web.archive.org/web/20210805155022/https://www.ruangguru.com/blog/ruangguru-secures-usd-55-million-new-investment-led-by-tiger-global-management> (accessed August 5, 2021).

146 Ruangguru, “Ruangguru Secures USD 55 Million New Investment Led by Tiger Global Management,” post to “Ruangguru” (blog), April 19, 2021, <https://web.archive.org/web/20210805155022/https://www.ruangguru.com/blog/ruangguru-secures-usd-55-million-new-investment-led-by-tiger-global-management> (accessed August 5, 2021).

147 Ruangguru, “Press Kit,” <https://web.archive.org/web/20210805155519/https://www.ruangguru.com/press> (accessed August 5, 2021). In November 2019, the Indonesian government appointed the CEOs of seven startups, including Ruangguru, to the newly created position of Presidential Special Staff. In April 2020, Ruangguru became the subject of public controversy over a perceived conflict of interest, when Ruangguru won a significant national contract to provide services to a government social benefits program for the unemployed. See: Eisyia A. Elok Sari, “Conflict of interest? Public questions government’s relationship with start-ups,” *The Jakarta Post*, April 16, 2020, <https://www.thejakartapost.com/news/2020/04/16/conflict-of-interest-public-questions-governments-relationship-with-start-ups.html> (accessed August 5, 2021); Ihsanuddin, “Belva Devara Resigns from Presidential Special Staff” (“Belva Devara Mundur dari Staf Khusus Presiden”), April 21, 2020, <https://nasional.kompas.com/read/2020/04/21/18470591/belva-devara-mundur-dari-staf-khusus-presiden> (accessed August 5, 2021).

Human Rights Watch further selected eight apps for in-depth technical (dynamic) analysis, which was conducted by the Defensive Lab Agency. Of these, we examine Ruangguru and Muse here to illustrate how apps can allow third-party companies to surveil what students do in the virtual classroom.

Case study: Ruangguru, Indonesia

Ruangguru is an EdTech app recommended by Indonesia’s Ministry of Education and Culture.¹⁴⁴ Built by an Indonesian EdTech company of the same name, the company successfully completed a tenth round of funding in April 2021 after the pandemic drove significant growth in user volume and revenue and led to the company’s first fiscal year of profitability since its founding in 2014.¹⁴⁵

The app is widely used by children in Indonesia. Ruangguru reported that it had 22 million users in 2020, and that a free version of its product offered during the pandemic was used by over 10 million students in Indonesia.¹⁴⁶ The company also stated that “we have also been trusted to partner with 32 (out of 34) Provincial Governments and 326 City and District Governments in Indonesia.”¹⁴⁷

Forensic analysis found that Ruangguru collects personal data from its students, including their location, Android Advertising ID, information about the device they use, and in-app navigation, and transmits this to two companies: AppsFlyer and Facebook.

When a child opens up Ruangguru on their phone, the app immediately begins to track what they do in its virtual classrooms, compiling a log of everything the child does and sees in what is known as “in-app navigation.” This log is continually updated and transmitted not just to Ruangguru, via the domain **tracker.ruangguru.com**, but also to Facebook via the domain **graph.facebook.com**.

Ruangguru may surveil its virtual classrooms to target children with behavioral advertising. Ruangguru discloses in its privacy policy that it “may collect interaction information on the page (such as scrolling, clicks, or mouse movement),” for which “we’ll use this information ... to measure and understand the effectiveness of the advertising we do to you and other parties, and to serve advertisements for products and services that are relevant to you.”¹⁴⁸ Ruangguru also notes that it may share this intimate information with “[a]dvertisers and ad networks that require data to select and offer relevant advertisements to you and other users,” and that “[w]e may use the personal data we collect to fulfill advertisers’ requests by showing their ads to that target audience,” though it does not disclose the identity of the advertisers and third-party companies that receive children’s data.

However, Ruangguru misleadingly states that it does “not disclose information about identifiable individuals, but we may provide them with aggregated information about our users.”¹⁴⁹ However, forensic testing proves otherwise. Human Rights Watch and the Defensive Lab Agency found Ruangguru transmitting its students’ Android Advertising ID to AppsFlyer and to Facebook.

Ruangguru also tags its students’ devices with an additional, proprietary identifier and

148 Ruangguru, "Privacy Policy" ("Ke-bijakan Privasi"), <https://web.archive.org/web/20210623100922/https://www.ruangguru.com/privacy-policy> (accessed August 4, 2021).

149 Ibid.

150 Ibid. "We may combine information we receive from other sources with information you provide and information we collect. We may use this information as well as the combined information for the purposes set out above."

151 Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; and with Danielle Blumenstyk Peterman, Head of Corporate Comms, AppsFlyer, April 6, 2022.

152 Government of Pakistan, Ministry of Federal Education and Professional Training, "COVID Projects," <https://web.archive.org/web/20210804231133/http://www.mofept.gov.pk/Detail/YWUyZ-TdIM2QtNjQ1ZSooMTJlLWlwYjktY-jkoN2E3NmU3YmNj> (accessed August 4, 2021); Muse, "About Us: Curiosity is Natural," <https://web.archive.org/web/2020071124907/http://muse-lessons.com/Home/About> (accessed August 4, 2021); Arshad Yousafzai, "Donated lessons help put Teleschool on air within two weeks," *The News*, April 27, 2020, <https://www.thenews.com.pk/print/650286-donated-lessons-help-put-teleschool-on-air-within-two-weeks> (accessed August 4, 2021).

153 Muse, "Product: Seriously Fun," <https://web.archive.org/web/20200715123323/http://muse-lessons.com/Home/Product> (accessed July 15, 2021); e-Taleem, one portal for digital education, "Current e-learning vertices," <https://web.archive.org/web/20210805220937/https://etaleem.gov.pk/> (accessed August 4, 2021).

154 Sumera Naqvi, "Is e-learning the inevitable future?" *The News*, April 2020, <https://web.archive.org/web/20200421043621/https://www.thenews.com.pk/magazine/you/647186-is-e-learning-the-inevitable-future> (accessed August 5, 2021).

155 Mehreen Zahra-Malik, "The coronavirus effect on Pakistan's digital divide," *BBC Worklife*, July 13, 2020, <https://www.bbc.com/worklife/article/20200713-the-coronavirus-effect-on-pakistans-digital-divide> (accessed August 4, 2021).

sends it back to itself through the domains **gw.ruangguru.com** and **tracker.ruangguru.com**. It appears that the company directly engages in user profiling itself. Its privacy policy discloses that Ruangguru collects even more information about its students from other sources and combines it with the data it holds about its students for advertising and other purposes.¹⁵⁰

Ruangguru did not respond to our request for comment. In its response, Meta did not address whether Meta was receiving user data from Ruangguru. AppsFlyer responded that the company does not sell or serve any ads, build targeting profiles, or sell data, and did not specifically address our questions about Ruangguru.¹⁵¹

Case study: MUSE, Pakistan

Recommended by Pakistan's Ministry of Federal Education and Vocational Training, MUSE is an app built by SABAQ Learning Systems, a Pakistani "award-winning EdTech company."¹⁵² MUSE is targeted at students from kindergarten to fifth grade, and offers "content made for young learners: fun video lessons with lovable animated characters that keep students engaged."¹⁵³ In April 2020, *The News* reported that almost 120,000 students were using MUSE in over 1,000 schools, and that the federal government was working on disseminating the app to the country's lower primary school students.¹⁵⁴ In June 2020, MUSE reported user growth by 200 percent after school closures began.¹⁵⁵

Forensic analysis found that MUSE collects and transmits its students' personal data to two companies—Facebook and Google—through the six SDKs embedded in the app.

When a child opens up MUSE on their phone, Facebook's embedded SDKs immediately begin to track their every movement and activity in MUSE's virtual classrooms. This log is continually updated and transmitted to Facebook's domain **graph.facebook.com**. These data are further bundled and sent together with the child's Android Advertising ID, Android ID, information about the device they use, and other personal data, allowing Facebook to tie all of this information together with the child's AAID to build detailed profiles of each child.

MUSE transmits children's data to Facebook even before the child has opened the app for the first time; the app sends this data regardless of whether the child is logged into their Facebook account, or even has a Facebook account at all. Forensic testing revealed that MUSE notifies Facebook the instant the app is installed on the child's device; the app also finds and sends the child's AAID and other information about the child's device in the same data package to **graph.facebook.com**. By tagging and sending the child's persistent identifier to Facebook, MUSE sets the stage for the future collection and transmissions of that child's personal data to be tied to the user profile that Facebook keeps on them, which in turn can be used to target that child with behavioral advertising over time.

Similarly, MUSE transmits the child's AAID and other information about the child's device to Google through the domains **app-measurement.com** and **play.googleapis.com**.

All combined, the app sends more data about children to Facebook and to Google than it sends to itself. Human Rights Watch found that MUSE's data practices are unnecessary and disproportionate to the purpose of providing its child users with learning.

MUSE's privacy policy discloses that the app "may collect ... the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile internet browser you use, unique device identifiers and other diagnostic data."¹⁵⁶ However, it does not disclose the data practices observed by Human Rights Watch.

When contacted for comment, MUSE stated that it did not believe that it has "collected children specific data from the app," and doesn't maintain "any repository of children's data." MUSE also confirmed that the app included "data sharing SDKs."¹⁵⁷ In later correspondence, MUSE also stated that "the data is collected of the user so we can better understand what content items were viewed more than others," and that "Google and Facebook SDKs collect this data without sharing any data about a specific user – rather it collects the data of each user as a data point to understand overall usage."

In its response to Human Rights Watch, Meta (Facebook) did not address whether it was receiving children's user data from MUSE.¹⁵⁸ Google did not respond to our request for comment.

Tracking Children Outside of the Classroom

My teacher makes me download Facebook, BiP, and WhatsApp for school. I don't like these apps, because they understand and see everything that I do. They read my messages. They see everything that I do on my phone. This makes me feel bad.

—Rodin R., a nine-year old student in Istanbul, Turkey¹⁵⁹

Many children are tracked and surveilled even after they leave the virtual classroom. Human Rights Watch identified companies that track children online, outside of school hours, deep into their private lives, and over time.

Websites: Cookies

A cookie is a small piece of data that companies store in a person's web browser in order to uniquely identify that person. While not all cookies are trackers, third-party cookies are generally used by advertising and tracking companies to watch what people do online, infer their characteristics and interests, and deliver customized ads that then follow them around the internet.

¹⁵⁶ SABAQ, "MUSE Privacy Policy," June 22, 2019, <https://web.archive.org/web/20210223231856/http://sabaq.edu.pk/MusePrivacyPolicy/> (accessed August 4, 2021).

¹⁵⁷ Human Rights Watch email correspondence with Hassan Bin Rizwan, Founder, SABAQ / MUSE, April 2, 2022.

¹⁵⁸ Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022.



Human Rights Watch found that children's educational websites inserted as many third-party cookies on personal devices as do the world's most popular websites aimed at adults. Out of a total 124 EdTech websites, Human Rights Watch detected 66 EdTech websites that had a total of 470 third-party cookies embedded in them. A child logging into a single one of these 66 platforms might be tracked on average by seven cookies or encounter a median of three cookies. Meanwhile, an investigation conducted by The Markup in September 2020 found that of the world's over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, a site loaded a median of three third-party cookies.¹⁶⁰

Put another way, children are surveilled in their virtual classrooms and followed long after they leave, outside of school hours and across the internet, at a similar rate as adults shopping in the world's largest virtual malls.

The number of AdTech or other third-party companies receiving children's data was discovered to be even greater than the number of EdTech sites sending this data to them.

159 Human Rights Watch interview with Rodin R., 9, Istanbul, Turkey, June 11, 2021.

160 Surya Mattu and Aaron Sankin, “How We Built a Real-time Privacy Inspector,” *The Markup*, September 22, 2020, <https://themarkup.org/black-light/2020/09/22/how-we-built-a-real-time-privacy-inspector#survey> (accessed July 12, 2021); Victor Le Pochat et al., “Tranco,” generated on July 13, 2021, <https://tranco-list.eu/list/KLPW/1000000> (accessed July 13, 2021); see also, Victor Le Pochat et al., “TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation,” *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*, accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

161 Electronic Government of the Republic of Kazakhstan, e-gov, “Spheres,” <https://web.archive.org/web/20210901181204/https://egov.kz/cms/en/covid/spheres> (accessed September 1, 2021); City of Pavlodar Education Department, “Online Testing” (“ТЕСТИРОВАНИЕ ON-LINE”), <https://web.archive.org/web/20210901213326/https://goedu.kz/content/view/30/20228?lang=ru> (accessed September 1, 2021); see also example of a school; School Gymnasium No 28, “Dear Teachers and Parents!” (“Құрметті ұстаздар мен ата-аналар!”), March 27, 2020, <https://web.archive.org/web/20210121140648/https://kst28mg.kz/2020/03/27/%D2%9A%D2%B1%D1%80%D0%B-C%D0%B5%D1%82%D1%82%D1%96-%D2%B1%D1%81%D1%82%D0%Bo%D0%B7%D0%B4%D0%Bo%D1%80-%D0%BC%D0%B5%D0%BD-%D0%Bo%D1%82%D0%Bo%D0%Bo%D0%Bo%D0%Bo%D0%B-B%D0%Bo%D1%80/> (accessed September 1, 2021).

162 Oracle, “Oracle buys AddThis,” January 5, 2016, <https://www.oracle.com/corporate/acquisitions/addthis/> (accessed September 1, 2021).

Human Rights Watch detected 66 websites transmitting children’s data to 85 AdTech or third-party companies.

Some EdTech sites installed dozens of cookies. Human Rights Watch found 76 cookies installed on Z-kai, recommended by the Japanese government and noted earlier in this chapter as having installed the highest number of ad trackers amongst the EdTech websites analyzed by Human Rights Watch. These cookies trailed students even after they left Z-kai’s website to go elsewhere on the web, sending their whereabouts and activities to 31 AdTech companies.

Case study: 100Ballov, Kazakhstan

Some EdTech sites chose to install cookies by AdTech companies that engage in particularly deceptive practices. On April 3, 2020, children in Kazakhstan began logging into their first day of online classes, in accordance with their government’s pivot to online learning. Many of these children opened up 100Ballov, endorsed by the Education Ministry and adopted by schools as the “educational portal for schoolchildren and students.”¹⁶¹

Human Rights Watch detected 100Ballov sending information about its students to AddThis, a marketing company acquired by Oracle in 2016.¹⁶² AddThis offers a set of social media share buttons that allows website users to easily share interesting content on social media.

But AddThis does much more than encourage social media traffic. Whether or not a person clicks on the “share” button, AddThis instantly loads dozens of cookies and tracking pixels on website visitors’ browsers, like nesting dolls, each collecting and sending user data to Oracle and to dozens of other AdTech companies to profile and target a person or a child with behavioral advertising that follows them across the internet.¹⁶³

AddThis’ privacy policy states:

The AddThis Tools also incorporate Cookies and Pixels from Oracle partners to enable the synchronization of unique identifiers between Oracle and our third-party partners to facilitate online behavioral advertising across the online advertising ecosystem.¹⁶⁴

Human Rights Watch found six AddThis cookies on 100Ballov, which in turn loaded four other trackers by AddThis’ advertising partners: two cookies pointing to DoubleClick, Google’s advertising division, and two to Tapad.¹⁶⁵ Tapad, an AdTech company, describes its services as “enabl[ing] marketers to identify a brand customer or related household across multiple devices, unlocking key use cases across programmatic targeting, media measurement, attribution, and personalization globally.”¹⁶⁶

100Ballov did not disclose this practice on its website; it does not have a privacy policy at all.¹⁶⁷ AddThis’ button is not visible on any of 100Ballov’s webpages, indicating that AddThis and its nested cookies were harvesting children’s data without even providing its purported social media functionality, as well as denying children knowledge of these tracking practices.

In response to our request for comment, Oracle stated that any receipt of children’s data through its AddThis tools is a violation of Oracle’s policies, which prohibit advertising partners and website publishers from sending personal information from sites directed to children under 16 years old, or from consumers these companies know to be under 16 years old.¹⁶⁸ Oracle did not address whether it had received children’s data from 100Ballov.

100Ballov did not respond to our request for comment.

¹⁶³ Aaron Sankin and Surya Mattu, “The High Privacy Cost of a “Free” Website,” The Markup, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites> (accessed July 12, 2021).

¹⁶⁴ AddThis, “Privacy Policy,” January 4, 2021, <https://web.archive.org/web/20210831042530/https://www.oracle.com/legal/privacy/addthis-privacy-policy.html> (accessed August 31, 2021).

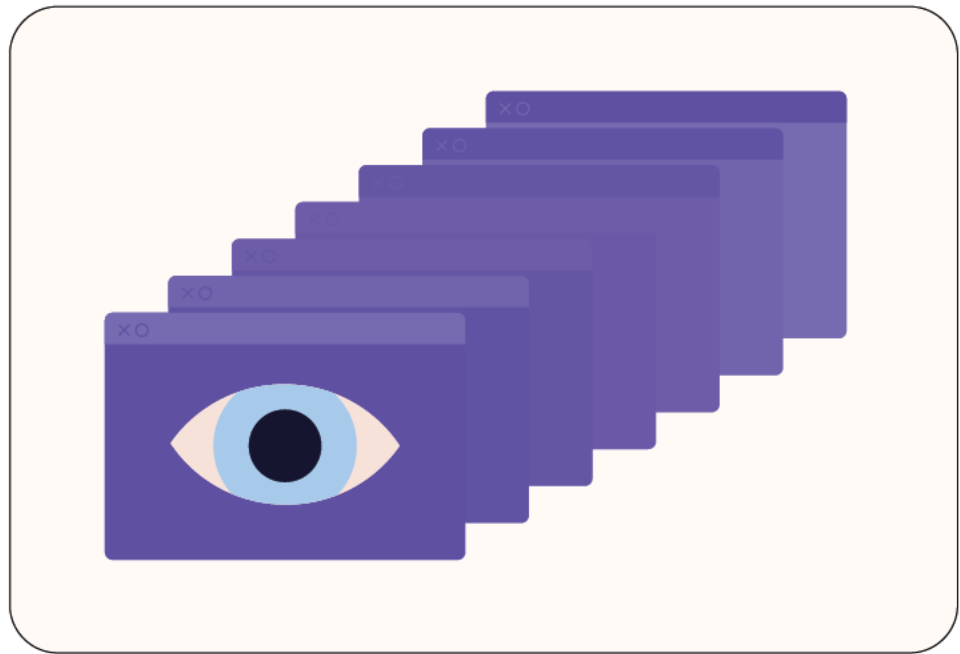
¹⁶⁵ AddThis, “Cookie & Pixel Partners,” <https://web.archive.org/web/20210901224150/https://www.addthis.com/privacy/pixel-partners/> (accessed September 1, 2021).

¹⁶⁶ Tapad, “tapad.com,” <https://web.archive.org/web/20210806200105/https://www.tapad.com/> (accessed August 6, 2021).

¹⁶⁷ 100Ballov offers a dummy “Privacy Policy” link, which points back to the site’s homepage. See: 100Ballov, “100Ballov.kz,” <https://web.archive.org/web/20210308194123/https://100ballov.kz/> (accessed March 8, 2021).

¹⁶⁸ Human Rights Watch correspondence with Dorian Daley, Executive Vice President and General Counsel, Oracle, April 15, 2022; Oracle, “Oracle Advertising Privacy Policy,” <https://www.oracle.com/legal/privacy/advertising-privacy-policy.html> (accessed April 25, 2022); Oracle, “AddThis Privacy Policy,” <https://www.oracle.com/legal/privacy/addthis-privacy-policy.html> (accessed April 25, 2022).

III. Hidden Manipulation: How Children's Data Are Used



These companies, they don't let us know. They're not transparent with us, saying that this is exactly where your data goes, and this is exactly what happens with it. We're trusting them blindly without knowing what's going on. And us kids won't doubt it at all—we won't even think that something bad is happening behind our backs. The amount that we've shared, all that we've done online, that it's all gone to some strange person ... The whole idea starts haunting you, and you get really scared.

—Priyanka S., 16, Uttar Pradesh, India¹⁶⁹

Profiled and Targeted

Most online learning platforms used during the pandemic secretly harvested vast amounts of data from children, piecing them together to deduce each child's characteristics, behaviors, and interests. Combined in this way, personal data can uniquely identify a child; algorithms can mine this data to guess at a child's identity, location, interests, emotions, health, and relationships, and use these inferences to predict what a child might do next, or how they might be influenced.

Profiling and targeting children on the basis of their actual or inferred characteristics not only infringes on their privacy, but also risks abusing or violating their other rights, particularly when this information is used to anticipate and guide them toward outcomes that are harmful or not in their best interest.

¹⁶⁹ Human Rights Watch interview with Priyanka S., 16, Uttar Pradesh, India, August 2, 2021.

170 Council of Europe, “Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications,” DGI (2017)12, March 2018, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> (accessed July 15, 2021), p. 15-16.

171 Committee on the Rights of the Child, General Comment No. 25, Children’s Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 42.

172 CRC, General Comment No. 25, Children’s Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 40; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, paras. 15, 16.

173 Council of Europe, “Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment,” Recommendation CM/Rec (2018)7 of the Committee of Ministers, September 2018, <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html> (accessed July 15, 2021), para. 37.

174 Deborah Roedder John, “Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research,” *Journal of Consumer Research*, vol. 26, no. 3 (1999): accessed July 14, 2021, doi: 10.1086/209559; Brian L. Wilcox et al., “Report of the APA Task Force on Advertising And Children,” *American Psychological Association*, February 20, 2004, <https://www.apa.org/pi/families/resources/advertising-children.pdf> (accessed July 14, 2021).

175 Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, “Children’s Data and Privacy Online: Growing Up In a Digital Age. An Evidence Review,” *London School of Economics and Political Science*, January 2019, http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (accessed July 15, 2021), p. 15; Jenny Radesky et al., “American Academy of Pediatrics Policy Statement: Digital Advertising to Children,” *Pediatrics*, vol. 146, no. 1 (2020): accessed June 8, 2021, doi: 10.1542/peds.2020-1681.

Such practices also play an enormous role in shaping children’s online experiences and determining the information they see, which can influence, shape, or modify children’s opinions and thoughts in ways that exploit their lack of understanding, affect their ability to make autonomous choices, and limit their opportunities or development. Such practices may also have adverse consequences that continue to affect children at later stages of their lives.¹⁷⁰

The United Nations Committee on the Rights of the Child has warned that such processing and use of children’s data “may result in violations or abuses of children’s rights,” and has called on states to “prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.”¹⁷¹

The Office of the High Commissioner for Human Rights has stated more broadly that the mass collection and processing of fine-grained information about people’s lives to infer their physical and mental characteristics, profile, and make decisions about them “carries risks for individuals and societies that can hardly be overestimated,”¹⁷² with implications for people’s access to health care, financial services, and due process rights, among others. In guidelines issued to its member states, the Council of Europe stated: “Profiling of children, which is any form of automated processing of personal data which consists of applying a ‘profile’ to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law.”¹⁷³

Below, we discuss the different ways in which user profiles on children can be misused. Human Rights Watch found that EdTech’s profiling and targeting of children did not yield any educational benefit to children; furthermore, the invasiveness of these data practices stands in sharp contrast to the strict limits and laws that governments place on the collection, sharing, and use of student data by schools.

Behavioral Advertising

Children are particularly susceptible to advertising, due to their still-developing cognitive abilities and impulse inhibition. Research on children’s cognitive development in relation to television commercials has demonstrated that younger children, particularly those under 7 years old, cannot identify ads or understand their persuasive intent; children at 12 years and older begin to distinguish between organic content and advertisements, though this does not translate into their ability to resist marketing.¹⁷⁴ On the internet, much like adults, many older children and teenagers struggle with understanding the opaque supply chain of commercial activity in which their personal data are valued, traded, and used.¹⁷⁵

Children are at even greater risk of manipulation by behavioral advertising online.¹⁷⁶

When children's data are collected for advertising, sophisticated algorithms extract and analyze overwhelming amounts of children's personal data for the purpose of tailoring ads accurately. These ads are embedded in personalized digital platforms that further blur the distinctions between organic and paid content. In doing so, behavioral advertising capitalizes on children's inability to identify or critically think about persuasive intent, potentially manipulating them toward outcomes that may not be in their best interest.¹⁷⁷

Behavioral advertising is even more egregious when targeted at children in settings where they cannot realistically refuse it. In the absence of alternatives, children faced a singular choice whether they were aware of it or not: attend school and use an EdTech product that infringes upon their privacy, or forgo the product altogether, be marked as absent, and be forced to drop out of school during the pandemic. Furthermore, as children spent a considerable amount of their childhood online in virtual classrooms during Covid-19 lockdowns, they were maximally exposed to the risks of collection and exploitation of their personal data.

The Committee on the Rights of the Child has stated that countries "should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling."¹⁷⁸ In a statement issued to pediatric health care providers, industry, and policy makers, the American Academy of Pediatrics raised concerns "about the practice of tracking and using children's digital behavior to inform targeted marketing campaigns, which may contribute to health disparities among vulnerable children or populations."¹⁷⁹

Human Rights Watch found that 199 third-party companies, most of them AdTech companies, received children's personal data from just 145 EdTech products. Put another way, the number of advertising companies receiving children's data vastly outnumber the number of EdTech companies collecting children's data.

Most EdTech companies concealed their data surveillance practices. Of the total 163 EdTech products reviewed by Human Rights Watch, only 35 disclosed in their privacy policies that their users' data was used for behavioral advertising. Of these, 23 products were developed with children as their primary users in mind, suggesting that behavioral advertising to children was an intended feature of the EdTech product.

176 Livingstone, Stoilova, and Nandagiri, "Children's Data and Privacy Online: Growing Up In a Digital Age, An Evidence Review," p. 15; Radesky et al., "American Academy of Pediatrics Policy Statement: Digital Advertising to Children."; Eva A. van Reijmersdal et al., "Processes and effects of targeted online advertising among children," *International Journal of Advertising*, vol. 36, no. 3 (2017):, pp. 396-414, accessed July 15, 2021, doi: 10.1080/02650487.2016.1196904.

177 One study of 231 Dutch children aged 9-13 years found that children process behavioral advertising in fundamentally different ways than adults do. Children processed behavioral ads non-critically, and did not seem to understand the targeting tactic or think that profile-targeted ads were more relevant to them. At the same time, seeing behavioral ads that were targeted at their interests and hobbies proved to be effective in creating positive associations toward the brand and increased children's intention to buy the products. See: van Reijmersdal et al., "Processes and effects of targeted online advertising among children," pp. 396-414.

178 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 42.

179 Radesky et al., "American Academy of Pediatrics Policy Statement: Digital Advertising to Children."

Case Study: ȘcoalăIntuitext, Romania

Recommended by Romania's Education Ministry, ȘcoalăIntuitext discloses in its privacy policy that it installs 23 marketing cookies in order to target its students with behavioral advertising across the internet.

Excerpt from ȘcoalăIntuitext's Privacy Policy, as seen on May 2, 2022.¹⁸⁰

Marketing cookies are used to track users from one site to another. The intent is to show relevant and engaging ads to individual users, so they are more valuable to advertising agencies and third parties dealing with advertising.

Name	Provider	Purpose	Expiry	Type
__zlcmid	Zendesk	Preserves users states across page requests.	1 year	HTTP cookie
_fbp	Meta Platforms, Inc.	Used by Facebook to deliver a series of advertising products such as real time bidding from third party advertisers.	3 months	HTTP cookie
_gcl_au	Google	Used by Google AdSense for experimenting with advertisement efficiency across websites using their services.	3 months	HTTP cookie
_hjRecording-Enabled	Hotjar	This cookie is used to identify the visitor and optimize ad-relevance by collecting visitor data from multiple websites – this exchange of visitor data is normally provided by a third-party data-center or ad-exchange.	Session	HTML Local Storage
ads/ga-audiences	Google	Used by Google AdWords to re-engage visitors that are likely to convert to customers based on the visitor's online behaviour across websites.	Session	Pixel Tracker
fr	Meta Platforms, Inc.	Used by Facebook to deliver a series of advertisement products such as real time bidding from third party advertisers.	3 months	HTTP Cookie
IDE	Google	Used by Google DoubleClick to register and report the website user's actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.	1 year	HTTP Cookie

¹⁸⁰ The first seven of the 23 marketing cookies listed in the privacy policy are excerpted here as examples. For the full list, see: ȘcoalăIntuitext, "Personal Data Processing Policy" ("Politica De Prelucrare Date Personale"), May 18, 2018, <https://web.archive.org/web/20220502221207/https://www.scoalaintuitext.ro/politica-de-confidentialitate>; <https://www.scoalaintuitext.ro/politica-de-confidentialitate> (accessed May 2, 2022).

When contacted for comment, Softwin, the Romanian EdTech company that operates ȘcoalăIntuitext, said that the product is "actually dedicated first to teachers/educators and only in a subsidiary way to children or their parents." The company acknowledged that it sends user data through marketing cookies, Facebook Pixel, and Google Analytics' 'remarketing audiences' feature, and that it does so to target adults "in the places where our main customers (teachers/educators) are active," including on Facebook and on Google. Softwin responded that, "To be clear no children's data collected by ȘcoalăIntuitext.ro is used for advertising, behavioral advertising, or any other commercial purposes."

It denied that it sends children's data to third parties or AdTech companies and said that the children's data it collects is not used for advertising, behavioral advertising, or user profiling.¹⁸¹

However, ȘcoalăIntuitext is marketed for children's use. Its home page features a marketing message directed at students that explains the benefits of the product.¹⁸² Another page on the website, titled "Children," is directed to would-be child users and states that, "ȘcoalăIntuitext is an educational platform ... intended for primary school students (Preparatory classes – IV), their parents and primary school teachers."¹⁸³

The page also asks students to advertise ȘcoalăIntuitext to their teacher: "Share with your teacher that you have discovered this useful application and enjoy the benefits of ȘcoalăIntuitext TOGETHER," and features four share buttons which, when clicked, opens a social media platform or new email message and prompts the student user to log in to share pre-populated text inviting the recipient, presumably their teacher, to use ȘcoalăIntuitext.¹⁸⁴

Human Rights Watch found that ȘcoalăIntuitext embedded tracking technologies on pages that were likely to be accessed by children, including the page titled "Children," and observed ȘcoalăIntuitext sending user data to AdTech companies through the third-party marketing cookies, Facebook Pixel and Google Analytics' 'remarketing audiences' feature that it acknowledged. The company did not acknowledge its use of ad trackers and session recording.¹⁸⁵ Human Rights Watch did not find evidence that these data practices were limited to adults.

¹⁸¹ Human Rights Watch email correspondence with Alexandru Neagu, Legal Advisor, Softwin, April 8, 2022.

¹⁸² ȘcoalăIntuitext, "Școală Intuitext," <https://web.archive.org/web/20220502210616/https://www.scoalaintuitext.ro/> (accessed May 2, 2022).

¹⁸³ ȘcoalăIntuitext, "Copii" ("Children"), <https://web.archive.org/web/20220502213856/https://www.scoalaintuitext.ro/copii> (accessed May 2, 2022).

¹⁸⁴ Ibid.

¹⁸⁵ Human Rights Watch email correspondence with Alexandru Neagu, Legal Advisor, Softwin, April 8, 2022.

Human Rights Watch also found that five governments directly built and offered EdTech products for which they disclosed, through their privacy policies, that they use children's personal data to target behavioral advertising back at them.

Country	EdTech Product	Privacy Policy
Canada	CBC Kids	"The data collected when you visit our website or click on our digital ads is used to show you future ads that match your interests. Ad targeting is used to create larger group profiles and larger audience segments made of users across Canada that share common interests." "Our advertising partners use cookies to show you ads. They'll look at the cookies you already have on your browser and decide whether and which ad they want to place on our site for you to see."¹⁸⁶
Ghana	Ghana Library Mobile Application	"We may use information collected about you via the Application to ... Deliver targeted advertising, coupons, newsletters, and other information regarding promotions and the Application to you" and "Offer new products, services, mobile applications, and/or recommendations to you." "We may share your information with third parties for marketing purposes ... Additionally, we may use third-party software to serve ads on the application, implement email marketing campaigns, and manage other interactive marketing initiatives. This third-party software may use cookies or similar tracking technology to help manage and optimize your online experience with us."¹⁸⁷
Indonesia	Rumah Belajar	"We may share Your information with Our business partners to offer You certain products, services or promotions." "We may share Your personal information with Service Providers to ... show advertisements to You to help support and maintain Our Service, to contact You, to advertise on third party websites to You after You visited our Service." "The information gathered via these Cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the Website. We may also use these Cookies to test new advertisements ... to see how our users react to them."¹⁸⁸
Republic of Korea	EBS	"«Korea Education Broadcasting Corporation» processes personal information for the following purposes: Use for marketing and advertising. Personal information is processed for the purpose of developing new services (products) and providing customized services, providing event and advertising information." "The company uses cookies for the following purpose: to provide targeted marketing and personalized services by analyzing the frequency and time of visits by members and non-members, identifying, tracing, and tracking users' preferences and interests, and identifying the degree of participation in various events and the number of visits, etc."¹⁸⁹

¹⁸⁶ Canadian Broadcasting Corporation, "CBC and your data," March 30, 2020, <https://web.archive.org/web/20210806100359/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726> (accessed August 6, 2021).

¹⁸⁷ Ghana Library Authority, "Ghana Library App Privacy Policy," June 5, 2020, https://web.archive.org/web/20210303152004/http://142.11.195.10/digital_library/privacy_policy.html (accessed August 6, 2021).

¹⁸⁸ Rumah Belajar, "Privacy Policy," February 4, 2020, <https://web.archive.org/web/20210807042148/http://apps.belajar.kemdikbud.go.id/privacypolicy.html> (accessed August 6, 2021).

¹⁸⁹ EBS, "Privacy Policy" ("개인정보처리방침"), February 8, 2021, <https://web.archive.org/web/20210804035422/https://sso.ebs.co.kr/policy/privacy?-date=20210208&tab=2&ver=%2Fpolicy%2Fprivacy%3Fdate%3D20210208&fsdc=> (accessed August 6, 2021), art. 1 (다), art. 8 (가).

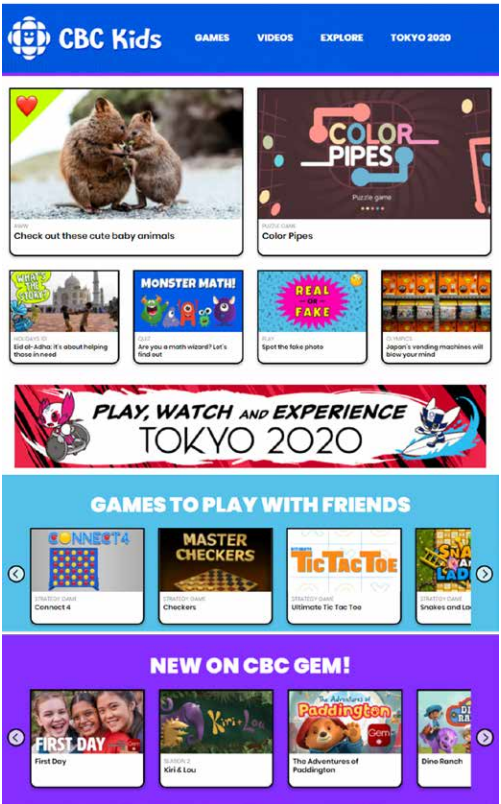
South Africa	Ministry of Education's website	“National Department of Basic Education also uses your personally identifiable information to inform you of other products or services available from National Department of Basic Education and its affiliates.” “National Department of Basic Education may, from time to time, contact you on behalf of external business partners about a particular offering that may be of interest to you.” “National Department of Basic Education keeps track of the Web sites and pages our customers visit within National Department of Basic Education ... This data is used to deliver customized content and advertising within National Department of Basic Education to customers whose behavior indicates that they are interested in a particular subject area.”¹⁹⁰
--------------	---------------------------------	--

Case Study: CBC Kids, Canada

When a child opens CBC Kids, offered by the Canadian Broadcasting Corporation and recommended by Canada’s Quebec Education Ministry for pre-primary and primary school-aged children’s learning, the first thing they see on the page are large, brightly colored tiles.¹⁹¹ In July 2021, the first tile featured a photo marked by a heart emoji and captioned, “AWW: Check out these cute baby animals.” Another tile was filled with brightly colored characters and titled “MONSTER MATH! Are you a math wizard? Let’s find out.” The front page also offered the newest episode of “The Adventures of Paddington;” the link was decorated with the smiling face of the famous fictional bear, waving his paw at the viewer.

190 Government of South Africa, National Department of Basic Education, “Privacy Statement,” <https://web.archive.org/web/20210807041929/https://www.education.gov.za/privacy.aspx> (accessed August 4, 2021).

191 CBC Kids, “CBC Kids,” <https://web.archive.org/web/20210720010630/https://www.cbc.ca/kids/> (accessed July 20, 2021). See also: Government of Quebec (“Gouvernement du Québec”), Ecole Ouverte, “CBC Kids,” June 15, 2021, https://ecoleouverte.ca/notice?id=p%3A%3Ausmarcdef_0000039521&queryId=4ddadb89-795b-45bf-a8fc-ee66084ba836&posInSet=1 (accessed July 12, 2021).



Screenshot of the CBC Kids website, as viewed by Human Rights Watch in July 2021. © CBC Kids

At the same time, when the child opens up the website, an invisible swarm of ad trackers and cookies get to work. Human Rights Watch found 29 third-party trackers collecting and sending data about children to 18 companies, mostly AdTech, and another 15 third-party cookies sending children's data to nine companies, mostly AdTech. To put this into perspective, this is more than five times the median number of three cookies and more than four times the median of seven ad trackers installed on the world's most popular internet sites—sites that include heavily trafficked e-commerce sites with explicit business interests in marketing.¹⁹²

15 third-party cookies on CBC Kids collected and sent children's data to 9 companies

AdTech company	Receiving domains
Adobe	demdex.net, dpm.demdex.net
Bombora	ml314.com
Google	doubleclick.net
LiveRamp	rlcdn.com, rlcdn.com
Lotame	crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net
Neustar	agkn.com
Piano	cxense.com
The Trade Desk	adsrvr.org
WarnerMedia	adnxs.com

29 ad trackers on CBC Kids collected and sent children's data to 18 companies

AdTech company	Receiving domains
Adobe	adobedtm.com, demdex.net, everesttech.net, omtrdc.net
Akamai Technologies	akstat.io, edgekey.net, go-mpulse.net
Amplitude	amplitude.com
Bombora	ml314.com
Chartbeat	chartbeat.com, chartbeat.net
Cheetah Digital (formerly Wayin)	wayin.com
comScore	scorecardresearch.com
Conductrics	conductrics.com
Facebook	facebook.com, facebook.net
Google	google-analytics.com, googlesyndication.com, googletagmanager.com, googletagservices.com, doubleclick.net
LiveRamp	rlcdn.com
Lotame	crwdcntrl.net
Neustar	agkn.com
Oracle	bluekai.com
Piano	cxense.com
Skimbit	skimresources.com
The Nielsen Company	exelator.com
Throttle	thrtle.com

¹⁹² Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector#survey> (accessed July 12, 2021); Victor Le Pochat et al., "Tranco," generated on July 13, 2021, <https://tranco-list.eu/list/KLPW/1000000> (accessed July 13, 2021); see also, Victor Le Pochat et al., "TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

Altogether, 20 companies involved in advertising and marketing received data about children from CBC Kids. Of these, six AdTech companies receiving data from CBC Kids—Adobe, Facebook, Google, LiveRamp, Piano, The Trade Desk—offer services to match website visitors to personally identifiable information sourced from other online and offline records, including physical addresses, location data, and credit scores,¹⁹³ building or enhancing a comprehensive profile about that person that can be used and sold to “serve targeted advertising and content to the right audience” (Adobe)¹⁹⁴ or to “understand and influence customer behavior” (Piano).¹⁹⁵

Of the 20 companies, seven companies—comScore, LiveRamp, Lotame, Neustar, Oracle, The Nielsen Company, and Throtle—have formally registered themselves with the California Data Broker Registry as data brokers, that is, companies whose primary business is the packaging and selling of people’s personal data.¹⁹⁶

Lotame, for instance, bills itself as the “World’s Largest 2nd and 3rd Party Data Marketplace” and “supplies real-time access to a firehose of raw behavioral data from billions of consumer profiles” which can be used to create user profiles.¹⁹⁷ The company assures advertisers that they “can add demographic, behavioral, geographic, and other types of data to learn more about your customers and find new ways to monetize those audiences.”¹⁹⁸ Human Rights Watch detected CBC Kids sending children’s data to Lotame through five cookies and an ad tracker.

¹⁹³ The Trade Desk shares and sells personal data from third-party data brokers such as Experian and Equifax, two credit scoring companies, and PlacIQ, Acxiom, and Foursquare, which provide location data. See: The Trade Desk, “Our Partners,” <https://web.archive.org/web/20210720042303/https://www.thetradedesk.com/us/our-platform/our-partners> (accessed July 19, 2021).

¹⁹⁴ Adobe Experience League, “Audience Manager Overview,” last updated April 13, 2021, <https://web.archive.org/web/20210807045536/https://experienceleague.adobe.com/docs/audience-manager/user-guide/overview/aam-overview.html?lang=en> (accessed July 19, 2021).

¹⁹⁵ Piano.io, “Piano,” <https://web.archive.org/web/20210807045609/https://piano.io/> (accessed July 19, 2021).

¹⁹⁶ The US State of California defines a data broker as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship,” and notes that: “A data broker collects many hundreds or thousands of data points about consumers from multiple sources ... then analyzes the data to assess content and packages the data for sale to a third party,” and that data brokers “create risks that are associated with the widespread aggregation and sale of data about consumers, including risks related to the inability of consumers to know and control information held and sold about them and risks arising from the unauthorized or harmful acquisition and use of consumer information.” See: AB-1202 Privacy: data brokers, Assembly Bill No. 1202, Chapter 753, October 11, 2019, https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201902000AB1202 (accessed July 19, 2021), section 2 (d), section 1 (d), (f), (h). To see these companies’ self-declarations, see the following submissions in the California Data Broker Registry: US State of California Department of Justice, “Data Broker Registration for Comscore, Inc.,” January 30, 2020, <https://web.archive.org/web/20210720003259/https://oag.ca.gov/data-broker/registration/186289> (accessed July 19, 2021); US State of California Department of Justice, “Data Broker Registration for LiveRamp, Inc.,” March 19, 2020, <https://web.archive.org/web/20220223115800/https://oag.ca.gov/data-broker/registration/188120> (accessed May 2, 2021); US State of California Department of Justice, “Data Broker Registration for Lotame Solutions, Inc.,” February 27, 2020, <https://web.archive.org/web/20210720003420/https://oag.ca.gov/data-broker/registration/186954> (accessed July 19, 2021); US State of California Department of Justice, “Data Broker Registration for Neustar, Inc.,” March 23, 2020, <https://web.archive.org/web/20210720003647/https://oag.ca.gov/data-broker/registration/186862> (accessed May 2, 2021); US State of California Department of Justice, “Data Broker Registration for Oracle America, Inc., Oracle Data Cloud” March 11, 2020, <https://web.archive.org/web/20210720003817/https://oag.ca.gov/data-broker/registration/185679>; (accessed July 19, 2021); US State of California Department of Justice, “Data Broker Registration for Nielsen Marketing Cloud,” August 11, 2020, <https://web.archive.org/web/20210720004748/https://oag.ca.gov/data-broker/registration/187679> (accessed July 19, 2021); US State of California Department of Justice, “Data Broker Registration for Throtle,” January 31, 2020, <https://web.archive.org/web/20210720003927/https://oag.ca.gov/data-broker/registration/185964>, (accessed July 19, 2021).

¹⁹⁷ Lotame, “Lotame Data Exchange,” <https://web.archive.org/web/20210720045203/https://www.lotame.com/products/lotame-data-exchange/> (accessed July 19, 2021); Lotame, “Data Stream,” <https://web.archive.org/web/20210807045456/https://www.lotame.com/products/lotame-connect/data-stream/> (accessed July 19, 2021).

¹⁹⁸ Lotame, “How Identity Graphs Benefit a Connected Digital Advertising Ecosystem,” December 11, 2020, <https://web.archive.org/web/20210720050850/https://www.lotame.com/how-identity-graphs-benefit-a-connected-digital-advertising-ecosystem/> (accessed July 19, 2021).

199 The Nielsen Company, “Nielsen Data As A Service,” <https://web.archive.org/web/20210712213654/https://www.nielsen.com/eu/en/solutions/capabilities/nielsenmarketingcloud-daas/> (accessed July 12, 2021); The Nielsen Company, “Nielsen Acquires eXelate,” March 4, 2015, <https://web.archive.org/web/20210807045818/https://www.nielsen.com/us/en/press-releases/2015/nielsen-acquires-exelate/> (accessed August 7, 2021).

200 Ibid.

201 Canadian Broadcasting Corporation, “CBC and your data,” March 30, 2020, <https://web.archive.org/web/20210720002724/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726> (accessed July 19, 2021).

202 Neustar, for instance, began as a division within the US defense contractor Lockheed Martin and sells access to its records on over 260 million people, linked to real names, addresses, phone numbers, email addresses, “psychological variables,” and “hundreds of demographic, behavioral, financial, property, segmentation and geographic attributes.” See: Neustar, “Engage the Right Target Audiences at Scale And Across Channels,” <https://web.archive.org/web/20210720043836/https://www.home.neustar/adadvisor> (accessed July 19, 2021); Neustar, “Customer Identity File,” 2020, <https://web.archive.org/web/20210904001854/https://www.cdn.neustar/resources/product-literature/marketing/neustar-marketing-customer-identity-file-solution-sheet.pdf> (accessed September 3, 2021); Neustar, “Neustar AdAdvisor Reference Guide,” 2020, <https://web.archive.org/web/20210720044010/https://www.cdn.neustar/resources/product-literature/marketing/neustar-adadvisor-reference-guide.pdf> (accessed July 19, 2021), p. 5.

203 LiveRamp, “Identity and Identifier Terms and Concepts: More Information About RampIDs,” last modified September 13, 2021, <https://web.archive.org/web/20220503064631/https://docs.liveramp.com/safe-haven/en/identity-and-identifier-terms-and-concepts.html> (accessed May 2, 2022).

204 Ibid.

205 LiveRamp, “Interpreting RampID, LiveRamp’s People-Based Identifier: Delivery Options and Formats,” last modified February 23, 2022, <https://web.archive.org/web/20220429143904/https://docs.liveramp.com/connect/en/interpreting-rampid-liveramp-s-people-based-identifier.html> (accessed May 2, 2022).

Human Rights Watch also found CBC Kids sending data about children to The Nielsen Company, which claims that it can “understand the personality of your customers and prospects to effectively forecast behavior with the largest personality database in the world.”¹⁹⁹ Specifically, Human Rights Watch observed CBC Kids transmitting kids’ data through the ad tracker exelator.com, which then feeds into the eXelate data pool, “Nielsen’s proprietary and highly curated mix of offline and online data,” which Nielsen can sell to other companies to “help [them] win the battle for consumer attention.”²⁰⁰

CBC Kids is covered by the privacy policy of its parent site, CBC, which reassures users that, “The vast majority of the information you create doesn’t have any indicator of who you are, personally.”²⁰¹ However, Human Rights Watch observed CBC Kids sending children’s data to companies that claim to connect real people’s offline identity records to their online activities.²⁰² One such company, LiveRamp, claims to “deterministically merg[e] offline PII (personally identifiable information, such as email address, name, postal address, and phone number) and matching to cookies, mobile device IDs, and proprietary platform IDs,” into what the company calls RampID.²⁰³ The company draws upon “a multi-billion record set” that includes public record data, publicly available data, and self-reported information.²⁰⁴

LiveRamp promises its clients “real-time people-based insights ... and build a mapping over time,” once clients place the company’s Real-Time Identity Service pixel and cookie on their website or advertisement.²⁰⁵ The pixel is programmed to send user information to LiveRamp’s domain **rlcdn.com**.²⁰⁶

Human Rights Watch found CBC Kids sending data about the children visiting its website to LiveRamp through two embedded cookies and an ad tracker pointing to the domain **rlcdn.com**, none of which were disclosed in CBC’s privacy policy or cookie policy.²⁰⁷

CBC discloses in its privacy policy that it engages in user profiling and behavioral advertising (see table above), but does not disclose the identity of these companies and data brokers that receive children’s data, or explain how they might use it. On a child-friendly webpage titled “How to Manage Your Cookies,” CBC Kids discloses that it uses “strictly necessary cookies ... needed for CBC Kids to work,” “functionality cookies ... needed for specific features of CBC Kids to work,” and “performance cookies [that] help us understand how well the CBC Kids sites are working.”²⁰⁸ However, CBC Kids does not disclose the presence of marketing cookies or ad trackers on its site, or that such tracking technologies are used to send children’s data to AdTech companies and data brokers. Moreover, children who accessed this webpage to learn how to opt out of being tracked by cookies were in turn surveilled, and their personal data transmitted, to six AdTech companies. Human Rights Watch detected cookies and ad trackers embedded in the “How to Manage Your Cookies” webpage sending children’s data to Adobe, ChartBeat, comScore, Cxense, Google, and Oracle.

206 Ibid. See also: LiveRamp, “Announcing Required Pixel Changes (7/2/2019),” last modified September 9, 2020, <https://web.archive.org/web/20211024132941/https://docs.liveramp.com/connect/en/announcing-required-pixel-changes--7-2-19-.html> (accessed May 2, 2022).

207 For CBC’s privacy policies, see: Canadian Broadcasting Corporation, “View Your Cookies,” <https://web.archive.org/web/20210720014616/https://www.cbc.ca/mycbc/viewcookies> (accessed July 19, 2021); Canadian Broadcasting Corporation, “CBC and your data,” March 30, 2020, <https://web.archive.org/web/20210720002724/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726> (accessed July 19, 2021).

208 CBC Kids, “How to Manage Your Cookies,” <https://web.archive.org/web/20210627035123/https://www.cbc.ca/kids/about/cookies> (accessed June 27, 2021).

When reached for comment, CBC said that it “explicitly prohibit[s] targeting on both our traditional and online platforms” and that “[t]he CBC.ca/kids [CBC Kids] section is ad free.”²⁰⁹ CBC confirmed the presence of 13 trackers on CBC Kids, of which 8 trackers—Adobe, Akamai, Amplitude, Chartbeat, comScore, Conductrics, Piano, Wayin—were used for site performance, functionality, and safety. The company said that another 4 trackers—Lotame, Oracle, Facebook, and Neustar—were inactive, and that trackers from Google were primarily restricted to product performance, though CBC had discovered a Google cookie that it planned to check.²¹⁰

As noted in the methodology of this report, Human Rights Watch conducted the primary phase of its investigation between May and August 2021, and conducted further checks in November 2021 to verify its findings. Human Rights Watch captured evidence, in real time, of CBC Kids transmitting data through the 29 ad trackers and 15 third-party cookies embedded on the site and listed in the tables above. These included the trackers that CBC acknowledged were present but inactive on the site.

While Human Rights Watch could not corroborate CBC’s statement that 8 trackers were used to enable core site functionality, other trackers were found sending data to domains explicitly owned by AdTech companies and used for their advertising businesses, including Google’s **doubleclick.net**.

When reached for comment, Akamai Technologies did not answer our questions regarding CBC Kids.²¹¹ Adobe, Cheetah Digital, Meta, and Oracle did not acknowledge that they receive data from CBC Kids, and said that it was their customers’ responsibility to comply with their policies and applicable laws that prohibit the collection of children’s data.²¹² LiveRamp said that it was not aware of a contractual or other relationship between LiveRamp and CBC Kids, and requested additional details.²¹³ LiveRamp had not replied to Human Rights Watch’s April 13, 2022 correspondence sharing further technical evidence at the time of this writing.²¹⁴

Bombora denied that it receives data from CBC Kids, but acknowledged that it receives data from CBC’s parent site, cbc.ca.²¹⁵ However, Human Rights Watch notes that its investigation focused on analyzing the data that was sent from eleven web pages from the CBC Kids domain (cbc.ca/kids).

In a statement, Piano said that it provided services to CBC Kids for the optimization of CBC Kids’ search engine, which did not involve the collection of children’s data from CBC Kids.²¹⁶

Amplitude did not respond to our questions on CBC Kids. comScore, Google, Lotame, Neustar, and Throttle did not respond to a request for comment.

209 Human Rights Watch email correspondence with Catherine Tait, President and CEO, CBC/Radio-Canada, April 25, 2022.

210 Ibid.

211 Human Rights Watch email correspondence with Gina Soric, Akamai Technologies, March 22, 2022.

212 Human Rights Watch email correspondence with Adobe, April 8, 2022; with Jill Knesek, Chief Security Officer and Chief Privacy Officer, Cheetah Digital (formerly Wayin), March 23, 2022; with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; and with Dorian Daley, Executive Vice President and General Counsel, Oracle, April 15, 2022.

213 Human Rights Watch email correspondence with Amy Lee Stewart, Senior Vice President, General Counsel and Chief Privacy Officer, LiveRamp, April 7, 2022; with David Reckert, Managing Privacy Counsel, LiveRamp, April 13, 2022.

214 Human Rights Watch email correspondence with David Reckert, Managing Privacy Counsel, LiveRamp, April 13, 2022.

215 Human Rights Watch email correspondence with Havona Madama, Chief Data Privacy Officer and General Counsel, Bombora, April 5, 2022.

216 Human Rights Watch email correspondence with Elissa Hill, Manager, Global Brand Marketing & Communications, Piano, April 7, 2022.

217 UN General Assembly, Interim Report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed, Freedom of thought, A/76/380, October 5, 2021, <https://www.ohchr.org/en/issues/freedomreligion/pages/annual.aspx> (accessed December 15, 2021), paras. 73-75.

218 Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, arts. 14, 17.

219 CRC, art. 14; Universal Declaration of Human Rights (UDHR), adopted December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), art. 18; see also International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, arts. 18(1), 19(1); CRC General Comment No. 1, Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001), para. 8; UN Human Rights Committee, "General Comment Adopted by the Human Rights Committee Under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights," General Comment No. 22 (48) (art. 18), CCPR/C/21/Rev.1/Add.4 (1993), paras. 1, 3; UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 22, 2015, <https://www.undocs.org/A/HRC/29/32> (accessed December 15, 2021), para. 19.

220 The UN Special Rapporteur on the right to freedom of religion or belief in a report on the Freedom of thought states that, "Some scholars define manipulation of thought as 'interference with the processes of understanding' to induce the formation of 'biased mental models [...], knowledge and ideologies', or a form of 'cognitive mind control.' See: UN General Assembly, Interim Report of the Special Rapporteur on freedom of religion or belief, A/76/380, October 5, 2021, <https://www.ohchr.org/en/issues/freedomreligion/pages/annual.aspx> (accessed December 15, 2021), paras. 35-39; 73-75.

221 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 50; CRC, art. 14; ICCPR, art. 19(2),(3); UDHR, art. 19; UN General Assembly, "Calling of an International Conference on Freedom of Information," Resolution 59 (1946), A/RES/59.

Influencing Information, Shaping Beliefs

The use of children's personal information to deliver highly targeted content and advertisements that follow them across the internet plays an enormous role in shaping children's experiences and what they see online. This can influence, modify, and manipulate their thoughts and beliefs, nudging them to particular outcomes and possibly affecting their ability to make autonomous choices.²¹⁷

Every child has the right to freedom of thought, and the right to access to information.²¹⁸

Unlike the rights to freedom of expression, association, and assembly, which can be limited, freedom of thought is an absolute right. International human rights law protects children's freedom of thought unconditionally from interference from any lawful or unlawful measure.²¹⁹ While the law on this right is underdeveloped, some experts have recently argued that targeted behavioral advertising that manipulates people's thoughts may threaten this right for all people, and particularly for children.²²⁰

The UN Committee on the Rights of the Child has noted that the digital environment "provides a unique opportunity for children to realize the right to access to information.... States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary."²²¹

The UN Committee on the Rights of the Child has noted that many automated processes shaping online experiences "may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions toward more extreme content [...] or the use of a child's personal information or location to target potentially harmful commercially driven content."²²²

As such, governments "should ensure that all children are informed about, and can easily find, diverse and good quality information online, including content independent of commercial and political interests." Governments should also "ensure that automated search and information filtering, including recommendation systems, do not prioritize paid content with a commercial or political motivation over children's choices or at the cost of children's right to information."²²³

When these automated processes affect the quality of information that children can easily find online, they risk interfering with children's right to freedom of thought.²²⁴

Because children are at high risk of manipulative interference at a time when their capacities are evolving, they may be particularly vulnerable when they come into contact with algorithms that

222 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 40.

223 Ibid, para. 53.

224 Ibid, para. 61.

225 The Council of Europe's Committee of Ministers warned that "fine grained, sub-conscious and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions." See: "Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes," Decl (13/02/2019)¹, February 13, 2019, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b (accessed July 22, 2021), para. 9. In 2018, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also noted that the "intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion," and that "[c]ommercial advertising has also sought to induce favourable opinions of and cultivate desire for particular products and services." He concludes that "[c]ompanies should, at the very least, provide meaningful information about how they develop and implement criteria for curating and personalizing content on their platforms, including policies and processes for detecting social, cultural or political biases in the design and development of relevant artificial intelligence systems." See UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/73/348, August 29, 2018, <https://www.undocs.org/A/73/348> (accessed July 22, 2021), paras. 24, 36.

226 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 61-62.

can be used to target and influence their thoughts, opinions, and beliefs through the curated display of content.²²⁵

As a result, the UN Committee on the Rights of the Child has urged governments to identify, define and prohibit practices that "manipulate or interfere with" children's freedom of thought. It has also said that governments should ensure that "automated processes of information filtering systems, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment."²²⁶

The majority of government-endorsed EdTech apps and websites examined by Human Rights Watch sent information about children to Google and Facebook, two companies that not only dominate the advertising and analytics industries, but also serve as primary channels to the internet for much of the world and whose algorithms determine what many people—and children—see online.

SDKs that Human Rights Watch observed most commonly embedded in EdTech apps

SDK	Parent company	EdTech App Count
Google Firebase Analytics	Google	56
Google Crashlytics	Google	40
Facebook Login	Facebook	20
Facebook Share	Facebook	17
Facebook Analytics	Facebook	16
Google AdMob	Google	13
Google Analytics	Google	11
AppsFlyer	AppsFlyer	6
Facebook Places	Facebook	5
Google Tag Manager	Google	5

Third-party companies that Human Rights Watch observed most commonly receiving children's data from EdTech websites through trackers

Parent company	Number of trackers found in EdTech websites
Google	315
Facebook	71
Twitter	59
Adobe	34
Microsoft	34
HubSpot	20
New Relic	18
Hotjar	16
Naver	15
Yandex	15

227 This report refers to Facebook as both the platform and the parent company, for consistency across the timeline of this investigation.

228 Facebook (Meta) owns four of the world's biggest social media platforms, listed here in descending order of users: Facebook, WhatsApp, Instagram, and Facebook Messenger. See: "Facebook Reports Second Quarter 2021 Results," Facebook press release, July 28, 2021, <https://web.archive.org/web/20210807050055/https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter-2021-Results/default.aspx> (accessed August 6, 2021); see also Statista, "Most popular social networks worldwide as of April 2021, ranked by number of monthly active users (in millions)," April 2021, [https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/](https://web.archive.org/web/20210725061434/https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/) (accessed July 22, 2021).

229 Iris Orriss, "The Internet's Language Barrier," *Innovations: Technology, Governance, Globalization* vol. 9 no. 3-4 (2014): accessed July 20, 2021, doi: 10.1162/inov_a_00223, p. 125. See also: Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar," Facebook, November 8, 2018, <https://web.archive.org/web/20210808183551/https://about.fb.com/news/2018/11/myanmar-hria/> (accessed August 8, 2021), p. 12; Saira Asher, "Myanmar coup: How Facebook became the 'digital tea shop,'" BBC, February 4, 2021, <https://www.bbc.com/news/world-asia-55929654> (accessed May 6, 2022); Leo Mirani, "Millions of Facebook users have no idea they're using the internet," *Quartz*, February 9, 2015, <https://qz.com/333313/millions-of-facebook-users-have-no-idea-theyre-using-the-internet/> (accessed May 6, 2022).

230 In 2010, Eli Pariser coined the term "filter bubble" to describe how personalized recommendation algorithms like those owned by Google and by Facebook reinforce users' beliefs by showing them more of what they prefer, based on their previous activities online. See Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2012).

231 Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," *Wall Street Journal*, May 26, 2020, <https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499> (accessed August 9, 2021).

Third-party companies that Human Rights Watch observed most commonly receiving children's data from EdTech websites through cookies

Parent company	Number of cookies found in EdTech websites
Google	98
Microsoft	46
Mail.Ru Group, OOO	25
Pipefy	16
The Trade Desk	16
WiderPlanet	16
LiveRamp	10
Oracle	10
tawk.to	10

In countries and contexts where these companies are viewed as indistinguishable from the internet, the existence of behavioral advertising aimed at children and fueled by data collected in educational contexts risks affecting children's rights to access diverse and good quality information online, including content independent of commercial interests.

Facebook (Meta)

Facebook, which rebranded itself as Meta in October 2021, is the world's dominant social media company.²²⁷ It owns four of the world's biggest social media platforms, and reported over 3.51 billion monthly users across all of its products in the second quarter of 2021.²²⁸ In 2014, Iris Orriss, Facebook's head of localization and internationalization, wrote, "Awareness of the Internet in developing countries is very limited. In fact, for many users, Facebook is the internet, as it's often the only accessible application."²²⁹

Due to Facebook's ubiquity, its News Feed algorithm, which determines what each of its 2.9 billion users see every day by providing them with a personalized, constantly updated stream of content and advertisements, plays a significant role in influencing people's opinions and beliefs by shaping the information they see online.²³⁰

Facebook uses the vast amounts of data it has on people to continually train its News Feed algorithm to choose and show content that each person is most likely to engage with. In an internal report from 2018, Facebook found that its recommendation algorithm stoked polarization. "Our algorithms exploit the human brain's attraction to divisiveness," read a slide from the 2018 presentation. "If left unchecked," it warned, Facebook would feed users "more and more divisive content in an effort to gain user attention & increase time on the platform."²³¹

232 UN Human Rights Council, "Report of the independent international fact-finding mission on Myanmar," A/HRC/39/64, September 12, 2018, https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf (accessed August 8, 2021), para. 74.

233 Ibid.; Tom Miles, "U.N. investigators cite Facebook role in Myanmar crisis," *Reuters*, March 12, 2018, <https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN> (accessed August 8, 2021). Facebook commissioned an assessment of its human rights impact in Myanmar, which found that the company had failed to prevent use of the platform to "foment division and incite offline violence." See: Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar," Facebook, November 8, 2018, <https://web.archive.org/web/20210808183551/https://about.fb.com/news/2018/11/myanmar-hria/> (accessed August 8, 2021).

234 The majority of internal studies on Instagram's effects on young users were conducted on teenagers in the United States and in the United Kingdom; one spring 2020 study surveyed 100,000 users in Australia, Brazil, France, Germany, Great Britain, India, Japan, Republic of Korea, and the US. See: Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *Wall Street Journal*, September 14, 2021, <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739> (accessed November 1, 2021). See also: Nilesh Christopher and Andrew Deck, "Instagram impacts teen mental health in the West. What about everywhere else?" *Rest of World*, November 17, 2021, <https://restofworld.org/2021/instagram-teen-mental-health/> (accessed November 18, 2021).

235 Nick Clegg, "What the Wall Street Journal Got Wrong," *Meta*, September 18, 2021, <https://about.fb.com/news/2021/09/what-the-wall-street-journal-got-wrong/> (accessed May 4, 2022).

This became reality in Myanmar, "a context where, for most users, Facebook is the Internet."²³² Given its prominence as the online population's primary source of information, Facebook's failure to prevent the spread of hate speech and disinformation that violated its policies on its platform resulted in the company playing what a UN-backed fact-finding mission later called "a determining role" in inciting real world violence in 2018.²³³

In September 2021, a trove of internal documents leaked by the whistleblower Frances Haugen and first published in the *Wall Street Journal* indicated that over three years, the company's researchers documented Instagram harming the mental and emotional health of a significant number of its child users. Instagram's recommendation algorithm and the negative social comparisons that it stoked made body image issues worse for one in three girls, according to the documents; one slide from a 2019 presentation read, "Teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups."²³⁴

In response, Facebook's Vice President of Global Affairs, Nick Clegg, said that the *Wall Street Journal*'s reporting "contained deliberate mischaracterizations of what we are trying to do, and conferred egregiously false motives to Facebook's leadership and employees," and suggested that they "need[ed] more evidence to understand social media's impact on people."²³⁵ Nine days later, Facebook paused the development of an Instagram Kids service for children ages 13 and under.²³⁶

Facebook uses its insights into its users to help advertisers target advertising to people in ways that are optimized to be persuasive to them.²³⁷ This significantly affects what people see on the platform. Over time, Facebook has increased the prevalence of advertising in its News Feed; a 2021 *Wall Street Journal* analysis of Facebook's investor calls found that the company had increased the number of ads served on its platforms by a quarterly average of nearly 30 percent year on year since the third quarter of 2015.²³⁸ Simultaneously, Facebook has also increased the visual prominence and space taken up by ads in the News Feed, continually revising its ad formats to not only make them more prominent and attractive for users, but to integrate them to further blur the lines between advertisements and organic content.²³⁹

236 Adam Satariano and Ryan Mac, "Facebook Delays Instagram App for Users 13 and Younger," *New York Times*, September 27, 2021, <https://www.nytimes.com/2021/09/27/technology/facebook-instagram-for-kids.html> (accessed May 4, 2022).

237 Facebook advertises this ability to advertisers as, "Personalize every ad for every customer, automatically: Use dynamic ads that automatically show people items they're most interested in." See: Facebook, "Facebook for Business: Retargeting," <https://web.archive.org/web/20210809232002/https://www.facebook.com/business/goals/retargeting> (accessed August 9, 2021).

238 Laura Forman, "Facebook Ads Could Be Reaching Saturation Point," *Wall Street Journal*, November 23, 2020, <https://www.wsj.com/articles/facebook-ads-could-be-reaching-saturation-point-11606132807> (accessed July 20, 2021).

239 In an earnings call with investors in January 2013, Facebook CEO Mark Zuckerberg announced a substantial redesign of the News Feed to make ads more visually prominent and attractive, explaining the change as, "Advertisers want really rich things like big pictures or videos, and we haven't provided those things historically." See: Somini Sengupta, "Face-Lift at Facebook, to Keep Its Users Engaged," *New York Times*, March 6, 2013, <https://www.nytimes.com/2013/03/07/technology/facebook-redesign-hopes-to-keep-users-engaged.html> (accessed August 9, 2021); Facebook, "A New Look for News Feed," March 7, 2013, <https://web.archive.org/web/20210809223518/https://about.fb.com/news/2013/03/a-new-look-for-news-feed/> (accessed August 9, 2021). In 2015, Andrew Bosworth, Vice President of Ads and Business Platform, described Facebook's shift to native ads—defined as ads that blend into content by matching the format or tone of the platform they appear on, making it more difficult for users to identify them as ads—as "It's about the ads not being in the right-hand column, but being a part of News Feed and having voice and actors and Likes and comments in the same way that you see this with other content in News Feed." Cade Metz, "How Zuck's Old TA Helped Facebook Master Mobile Ads," *WIRED*, September 21, 2015, <https://www.wired.com/2015/09/zucks-old-ta-helped-facebook-master-mobile-ads/> (accessed July 20, 2021).

²⁴⁰ Reset Australia, “Profiling Children for Advertising: Facebook’s Monetisation of Young People’s Personal Data,” April 2021, https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf (accessed July 13, 2021), p. 2, 13.

²⁴¹ Conor Duffy, “Facebook approves alcohol, vaping, gambling and dating ads targeting teens, lobby group finds,” ABC News, April 27, 2021, <https://www.abc.net.au/news/2021-04-28/facebook-instagram-teenager-targeted-advertising-alcohol-vaping/100097590> (accessed May 5, 2022).

²⁴² Darren Davidson, “Facebook targets ‘insecure’ young people to sell ads,” *Australian*, May 1 2017, <http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ado16eee7d7a61c3c30c909fa6> (accessed July 13, 2021), Sam Levin, “Facebook told advertisers it can identify teens feeling ‘insecure’ and ‘worthless,’” *Guardian*, May 1, 2017, <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens> (accessed July 13, 2021).

²⁴³ Darren Davidson, “Facebook targets ‘insecure’ young people to sell ads,” *Australian*, <http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ado16eee7d7a61c3c30c909fa6>.

²⁴⁴ Facebook, “Comments on Research and Ad Targeting,” April 30, 2017, <https://about.fb.com/news/h/comments-on-research-and-ad-targeting/> (accessed July 13, 2021).

²⁴⁵ Facebook tracks people on its website and app by using its own internal tools. For an explanation, see: Aaron Sankin and Surya Mattu, “I Scanned My Favorite Social Media Site on Blacklight And It Came Up Pretty Clean. What’s Going On?” *The Markup*, October 1, 2020, <https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on> (accessed July 13, 2021).

²⁴⁶ Surya Mattu and Colin Lecher, “Applied for Student Aid Online? Facebook Saw You,” *The Markup*, April 28, 2022, <https://themarkup.org/pixel-hunt/2022/04/28/applied-for-student-aid-online-facebook-saw-you> (accessed May 5, 2022).

As described in the previous section, children are at heightened risk of being influenced by behavioral advertising on social media sites like Facebook, where the lines between organic and commercial content are blurred and advertisements take up significant real estate in the News Feed.

In April 2021, Reset Australia, an advocacy group, reported that Facebook offered advertisers the ability to target their ads to approximately 740,000 children in Australia, and to target children as young as 13 determined by Facebook to be interested in smoking, extreme weight loss, and gambling, for as little as AU\$3.03.²⁴⁰ A Facebook spokesperson said that the company reviews all ads before and after they run, and that advertisers must comply with Facebook’s policies and local laws.²⁴¹

The news outlet the *Australian* reported in 2017 that a leaked Facebook document showed the company telling advertisers that it could judge when teenagers were feeling “insecure” and “worthless,” and offering advertisers the ability to target ads at the moment when young people “need a confidence boost.” The document, which stated that the company held data on 1.9 million *Australian* high schoolers, included an analysis on how young people express their emotions at different points during the week.²⁴² In response, Facebook first released a statement to the *Australian* in which it apologized and said it would undertake disciplinary measures;²⁴³ it released a second statement that said the article’s premise was misleading, that it does not offer tools to target people based on their emotional state, and that the document was commissioned research that was never used to target ads and was based on anonymous and aggregated data.²⁴⁴

Not including Facebook’s own app and website, Human Rights Watch detected 62 EdTech products with embedded Facebook tracking technologies.²⁴⁵ Of these, 22 apps had installed Facebook’s SDKs, giving the company the ability to access children’s personal data, and 37 websites were found transmitting children’s data to Facebook through ad trackers, third-party cookies, and the Facebook Pixel.

Facebook Pixel

Human Rights Watch found 30 EdTech websites sending their users’ data to Facebook through a specific tracking technology known as the Facebook Pixel. This technology collects information about what students and teachers do on these sites and sends this data back to Facebook. This can be used by the EdTech website to later target them with ads on Facebook and Instagram.

Facebook can also retain and use this data for its own advertising purposes, although it is not always clear what these purposes are.²⁴⁶ The Facebook Pixel allows Facebook to track people across the internet, and build user profiles on people – even matching them and their data to their respective Facebook or Instagram profiles, if they have one, and even if they are not logged into Facebook at the time when they were accessing a website with an embedded Facebook Pixel.²⁴⁷ As noted previously in this report, the Facebook Pixel could also enable the company to collect personal data and create shadow profiles on people who have never used their services or signed up for an account.

²⁴⁷ Ibid. Facebook describes the pixel as “The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts.” See: Facebook, “Facebook Pixel: Implementation,” <https://web.archive.org/web/20210713213425/https://developers.facebook.com/docs/facebook-pixel/implementation> (accessed July 13, 2021); see also: Surya Mattu et al., “How We Built a Meta Pixel Inspector,” *The Markup*, April 28, 2022, <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector> (accessed May 5, 2022).

Of the 30 EdTech websites found by Human Rights Watch to be sending data to Facebook through Facebook Pixel, 27 are websites specifically designed for use by children, and all were government-recommended for online learning. Facebook could use such data to profile children and target behavioral advertisements at them.

Product	Country	Child specific?
Educ.ar	Argentina	Yes
Education Perfect: Science	Australia: Victoria	Yes
DragonLearn	Brazil: São Paulo	Yes
Mangahigh	Brazil: São Paulo	Yes
Descomplica	Brazil: São Paulo	Yes
Escola Mais	Brazil: São Paulo	Yes
Explicaê	Brazil: São Paulo	Yes
Stoodi	Brazil: São Paulo	Yes
StoryWeaver	Canada: Quebec	Yes
CBC Kids	Canada: Quebec	Yes
Dropbox	Colombia	No
Khan Academy	India: Uttar Pradesh, Pakistan, Nigeria, South Africa	Yes
WeSchool	Italy	Yes
Study Sapuri	Japan	Yes
Z-kai	Japan	Yes
eboard	Japan	Yes
Asahi Shimbun	Japan	No
Daryn Online	Kazakhstan	Yes
iTest	Kazakhstan	Yes
Learn Smart Pakistan	Pakistan	Yes
Sabaq Foundation	Pakistan	Yes
EBS	Republic of Korea	Yes
ExamenulTau	Romania	Yes
Kinderpedia	Romania	Yes
Miro	Romania	No
ȘcoalăIntuitext	Romania	Yes
Moscow Electronic School	Russia	Yes
Siyavula	South Africa	Yes
PaGamO	Taiwan	Yes
ST Math	US: Texas	Yes

In July 2021, Facebook announced that advertisers would no longer be able to use Facebook's full suite of detailed targeting capacities when targeting children; instead, advertisers would be limited to targeting children based on their age, gender, and location.²⁴⁸ The announcement came two months after 44 state attorneys general in the US wrote to Facebook CEO Mark Zuckerberg asking him to abandon his plans to create an Instagram service for children under the age of 13, citing social media's detrimental effect on the health and well-being of children and the company's track record of having "historically failed to protect the welfare of children on its platforms."²⁴⁹

Facebook did not commit to limiting its own collection, profiling, and targeting of children for its own purposes. Its new policy does not protect children from advertisements targeted to people "living in this location," "recently in this location," or "traveling in this location," as well as to infer further sensitive information about children as described in Chapter 2.²⁵⁰

When reached for comment, Facebook did not acknowledge that they receive data from the EdTech products listed by Human Rights Watch, and said that it was their customers' responsibility to comply with their policies and applicable laws that prohibit the collection of children's data.²⁵¹

For children aged 13-17 with a user account with one of Facebook's services, the company said that it "does not use data from our advertisers' and partners' websites and apps to personalize [ads] to people under 18," and also confirmed that advertisers can only target ads to children aged 13-17 based on age, gender, and location. Facebook also said that children under 13 were not authorized to sign up for an account to use its products, and therefore if the company "were to inadvertently receive data relating to a child under 13, there would not be an authorized Meta user account for that child to which the data could be connected."²⁵²

An internal document written by Facebook's privacy engineers on the Ad and Business Product team and published by *Vice* in April 2022 suggests that the company struggles to understand and track how people's data are shared and used inside of its own systems. "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose,'" the document said.²⁵³ In response to the internal document, Facebook said that the document did not demonstrate non-compliance with privacy regulations, because it did not describe the company's processes and controls to comply with privacy regulations.²⁵⁴

²⁴⁸ Facebook, "Giving Young People a Safer, More Private Experience," July 27, 2021, <https://web.archive.org/web/20210729194429/https://www.facebook.com/business/news/facebook-is-changing-how-advertisers-can-reach-young-people> (accessed August 10, 2021); Facebook, "About Advertising to Young People," Facebook Business Help Center, <https://web.archive.org/web/20210728001952/https://www.facebook.com/business/help/229435355723442> (accessed July 28, 2021).

²⁴⁹ National Association of Attorneys General, "Letter Re: Facebook's Plans to Develop Instagram for Children Under the Age of 13," May 10, 2021, https://ag.ny.gov/sites/default/files/naag_letter_to_facebook_-_final.pdf (accessed August 2, 2021).

²⁵⁰ Facebook, "Use Location Targeting," Facebook Business Help Center, <https://www.facebook.com/business/help/365561350785642?id=176276233019487> (accessed August 2, 2021).

²⁵¹ Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022.

²⁵² Ibid.

²⁵³ Lorenzo Franceschi-Bicchieri, "Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document," *Vice*, April 26, 2022, <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes> (accessed May 5, 2022).

²⁵⁴ Ibid.

Google

Mr. Google has sucked in a beastly amount of information during these days.

—Pere Nieto, primary school teacher, Barcelona, Spain²⁵⁵

Google holds unparalleled dominance over the world's digital advertising market. According to public data, the company has been the global market leader in online advertising for over a decade, commanding a 27.5 percent share of digital ad spending in 2021.²⁵⁶ In turn, advertising contributes to the majority of Google's business; in 2020, it reported that 80 percent of its total annual revenue, or US\$147 billion, was earned by its ads business.²⁵⁷

Google's considerable control over online advertising is reinforced by the overwhelming market dominance of its other services, which have become essential to how most people participate in life online. Google is by far the most widely used search engine in the world; over 92 percent of all internet queries worldwide are done through Google, and to "Google" something is synonymous with online search itself.²⁵⁸ As such, the company's algorithms determine what most people see when they search for information on the internet, as well as the digital ads displayed alongside their search results.

Nine of the company's products—Android, Chrome, Gmail, Google Drive, Google Maps, Google Play Store, Google Photos, Google Search, and YouTube—have more than a billion users each.²⁵⁹ Each of these products provides vast amounts of user data back to Google, which analyzes this data to create new insights and information about people that can then be sold to advertisers.²⁶⁰

The company collects data not just from people directly using their services, but from anyone who encounters their tracking technologies embedded across the internet. Google offers infrastructure and developer tools that are popularly used by other companies to build their own websites and apps; many of these tools offer multiple capabilities, including advertising.²⁶¹ When using Google's services, developers provide Google with their users' data.²⁶² Google offers developers the ability to collect users' data through its non-advertising specific tools and integrate it later with its advertising services.²⁶³

255 Human Rights Watch interview with Pere Nieto, primary school teacher, Barcelona, Spain, June 12, 2020.

256 Ethan Cramer-Flood, "Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl," *eMarketer*, May 10, 2021, <https://www.emarketer.com/content/duopoly-still-rules-global-digital-ad-market-alibaba-amazon-on-prowl> (accessed August 9, 2021).

257 Google filing to United States Securities and Exchange Commission (SEC), "Form 10-K, Annual Report for the fiscal year ended December 31, 2020," https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d (accessed August 9, 2021), p. 10.

258 StatCounter, "Search Engine Market Share Worldwide: Aug 2020-Aug 2021," <https://web.archive.org/web/20210908155103/https://gs.statcounter.com/search-engine-market-share> (accessed September 8, 2021).

259 Harry McCracken, "How Google Photos joined the billion-user club," *Fast Company*, July 24, 2019, <https://www.fastcompany.com/90380618/how-google-photos-joined-the-billion-user-club> (accessed September 8, 2021).

260 Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/> (accessed May 5, 2021).

261 Research conducted by AppCensus for the Australian Competition and Consumer Commission found that Google's SDKs—those with advertising and analytics capacities—were embedded in 91 percent of 1,000 of the most popular mobile apps in Australia, and in 72 percent of children's apps. See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_o.pdf (accessed July 9, 2021) pp. 22-26.

262 Google, "How Google uses information from sites or apps that use our services," <https://web.archive.org/web/20210915110048/https://policies.google.com/technologies/partner-sites> (accessed September 15, 2021).

263 For example, Google Firebase Analytics offers developer tools for building and maintaining apps. It was the most prevalent SDK found in EdTech apps analyzed by Human Rights Watch, and is similarly ubiquitous in Android apps worldwide. Firebase also offers developers the capability to use their users' personal data to "gain insight into who your users are, and what actions they're taking inside your app," and to "apply the power of machine learning to predict future user behavior." Once collected and analyzed by Firebase, users' personal data can be sent to and integrated with Google's other advertising services, including Google Ads, AdMob, and Google Marketing Platform. See: Google Firebase, "Products / Engage," <https://web.archive.org/web/20210811171053/https://firebase.google.com/products-engage> (accessed August 11, 2021); Google Firebase, "Integrations," <https://web.archive.org/web/20210811171551/https://firebase.google.com/integrations> (accessed August 11, 2021); Google Firebase, "AdMob and Firebase," April 19, 2022, <https://web.archive.org/web/20220429083336/https://firebase.google.com/docs/admob> (accessed May 5, 2022).

264 Norwegian Consumer Council (“Forbrukerrådet”), “Out of Control,” January 14, 2020, <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/> (accessed June 10, 2021), p. 121. Despite the extreme difficulties of knowing when and what influences Google’s ads ecosystem and its proprietary algorithmic design, researchers and journalists have been working to catalog and analyze its outputs. See: Leon Yin and Aaron Sankin, “Google Ad Portal Equated ‘Black Girls’ with Porn,” *The Markup*, July 23, 2020, <https://themarkup.org/google-the-giant/2020/07/23/google-advertising-keywords-black-girls> (accessed September 15, 2021); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018); Latanya Sweeney, “Discrimination in Online Ad Delivery,” January 28, 2013, <https://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf> (accessed September 15, 2021).

265 Norwegian Consumer Council (“Forbrukerrådet”), “Out of Control,” <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/>, p. 120.

266 As noted in the methodology, several EdTech products offered both app and website versions of their product, in which case Human Rights Watch analyzed both.

267 “Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners’ sites and apps.” See: Google, “How Google uses information from sites or apps that use our services,” <https://web.archive.org/web/20210915110048/https://policies.google.com/technologies/partner-sites> (accessed September 15, 2021).

268 Surya Mattu and Aaron Sankin, “How We Built a Real-time Privacy Inspector,” *The Markup*, September 22, 2020, <https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector> (accessed July 7, 2021); Google Analytics, “Tracking Code Overview,” <https://web.archive.org/web/20200615214845/https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview> (accessed July 7, 2021).

269 These are defined as any network requests that were made to the following Google-owned domains: Google Analytics, Google Tag Manager, DoubleClick, googleadservices.com, googlesyndication.com, and googletagservices.com.

Google’s advertising ecosystem is opaque, and even experts struggle to understand how its algorithms use the data they collect or receive about people to decide what to show them online.²⁶⁴ It is difficult to know how personal data is used within Google’s ecosystem once it is collected, and difficult to distinguish between “where Google as a service provider ends, and where Google as an advertising service begins.”²⁶⁵

Of the 163 EdTech products examined by Human Rights Watch, 131 products (80 percent) were found with embedded tracking technologies built by Google.²⁶⁶ Of these, 63 Android apps (86 percent of the total 73 apps examined) were found with at least one embedded Google SDK, giving the company the ability to access children’s personal data based on the Android permissions also granted to the app. Human Rights Watch observed 100 websites (81 percent of the total 124 websites examined) transmitting children’s data to Google through ad trackers, third-party cookies, and Google Analytics’ ‘remarketing audiences’ feature.

Human Rights Watch also further identified instances in which EdTech products sent or granted access to children’s data directly to Google’s advertising divisions, which Google may use for its own purposes.²⁶⁷

For example, Google Analytics is popularly used for both its analytics and advertising capabilities. Human Rights Watch examined websites identified to be using a tool offered by Google Analytics, called its ‘remarketing audiences’ feature, that allows developers to make custom audience lists based on user behavior and then target ads to those users across the internet using Google Ads and Display & Video 360.²⁶⁸

EdTech products sent or granted access to children’s data to Google, using Google’s advertising-specific tracking technologies

EdTech Type	Tracker	Receiving Domain	Number of EdTech products
Apps	SDK	Google AdMob	14
	SDK	Google Tag Manager	5
Websites	Ad Tracker	googletagmanager.com	64
	Ad Tracker	doubleclick.net	63
	Ad Tracker	googleadservices.com	30
	Ad Tracker	googletagservices.com	7
	Ad Tracker	googleoptimize.com	2
	Cookie	doubleclick.net	42
	Cookie	10499192.fls.doubleclick.net	1
	Google Analytics’ ‘remarketing audiences’ feature	stats.g.doubleclick	52

Of the 73 EdTech apps reviewed in this report, Human Rights Watch found that 17 apps (23 percent) had installed one of Google’s ad-specific SDKs; likewise, out of the total 124 EdTech websites reviewed, 82 websites (66 percent) were found transmitting children’s personal data to Google’s advertising businesses.²⁶⁹

For example, Human Rights Watch found 14 apps granting access to their users' data to Google AdMob by installing the AdMob SDK, "one of the largest global ad networks" that "helps you monetize your mobile app through in-app advertising."²⁷⁰ Ten out of the 14 are apps designed specifically for children's use in education, and their data sharing practices directly impacted children.²⁷¹

Google's advertising policies prohibit targeting children under 13 with behavioral advertising or collection of their personal information for that purpose.²⁷² Google places responsibility on the developer to follow these policies: "You are responsible for ensuring your ads comply with policy where required," but the company does not appear to have a due diligence policy to actively check whether the personal data they receive might be that of children.²⁷³

In August 2021, Google announced that it would no longer allow advertisers to target personalized advertising to children based on their age, gender, or interests.²⁷⁴ However, the company did not preclude advertisers from continuing to use location data to infer sensitive information and target ads to children.²⁷⁵ The company also did not comment on the massive amounts of children's personal data that it has received to date, nor did it commit to limiting its own collection of children's data or its profiling and targeting of children.

Through dynamic analysis, Human Rights Watch detected one EdTech app, e-Pathshala, transmitting details about what children search for within the app to Google. The Indian Education Ministry, who built the app, does not notify its child users that the app is sending what information children seek within their virtual classroom to Google. Indeed, the app has no privacy policy at all.

Neither Google nor e-Pathshala responded to our request for comment.

270 Google AdMob, "Home," <https://admob.google.com/home/> (accessed August 11, 2021); Google Developers, "AdMob," <https://developers.google.com/admob> (accessed August 11, 2021).

271 These apps were: Top Parent, Descomplica, Edmodo, Study Sapuri, (LINE), Özelim Eğitimdeyim, Extramarks, (Naver Band), Newton, Minecraft, (Miro), Kundelik. Apps in parentheses are directed at general audiences; the rest are apps apparently designed for use by children.

272 Google, "Personalized advertising," <https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465> (accessed August 11, 2021); Google, "Ads & made for kids content," https://web.archive.org/web/20210811183721/https://support.google.com/adspolicy/answer/9683742?hl=en&ref_topic=1626336 (accessed August 11, 2021).

273 Google, "Personalized advertising," <https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465>.

274 Mindy Brooks, "Giving kids and teens a safer experience online," post to Google: The Keyword (blog), August 10, 2021, <https://web.archive.org/web/20210810130430/https://blog.google/technology/families/giving-kids-and-teens-safer-experience-online/> (accessed August 10, 2021).

275 In 2018, an AP investigation concluded that Google collects location data from Android users, even if users had set their privacy settings to prevent Google from doing so. The Attorney General of the US state of Arizona subsequently filed a consumer fraud lawsuit against Google in May 2020; newly unredacted documents in May 2021 revealed testimony from Jack Menzel, Google's former Vice President of Product for Maps and current Vice President of Product for ads, that Google infers a user's home and work locations without consent, even when a user has turned off all of their device's location-related settings, and that the only way for Google not to infer a user's home and work locations is to insert "arbitrary locations." Karin Hennessy, Google's product manager for ads privacy and safety, similarly noted during deposition that even if a user opts out of ads personalization, Google still uses the user's real-time location to serve ads to them. See: Ryan Nakashima, "AP Exclusive: Google tracks your movements, like it or not," *Associated Press*, August 13, 2018, <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1afoecb> (accessed August 11, 2021); *State of Arizona Attorney General, Mark Brnovich v. Google LLC*, The Superior Court of the State of Arizona In and For The County of Maricopa, Complaint, May 2021, <https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf> (accessed August 11, 2021), paras. 93, 99; Google, "Personalized Advertising," <https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465> (accessed August 11, 2021).

IV. Failure to Protect

276 Human Rights Watch interview with Priyanka S., 16, Uttar Pradesh, India, August 2, 2021.

277 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 35.

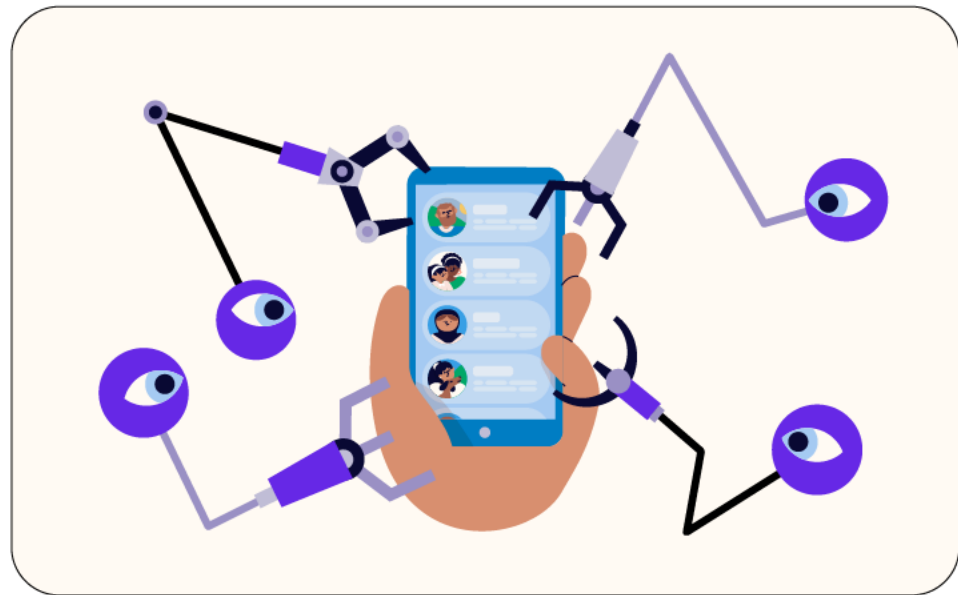
278 United Nations Human Rights Council, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," adopted on July 6, 2011, A/HRC/RES/17/4, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed August 2, 2021); OECD, OECD Guidelines for Multinational Enterprises: 2011 Edition, May 25, 2011, <https://www.oecd.org/daf/inv/mne/48004323.pdf> (accessed August 2, 2021); CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 35.

279 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 36; UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, Principle 13(b).

280 UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, Principles 11, 13.

281 CRC, General Comment No. 16, State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16 (2013), paras. 28, 42; CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 35, 36.

282 CRC, General Comment No. 25, para. 37; CRC, General Comment No. 16, para. 28.



This is scary. Especially us kids, we blindly trust our country, the whole education system, because we don't question these things yet. We don't have enough experience.... As kids, we feel powerless. What can I even do as a kid to stop these companies? That idea itself hurts a lot.

—Priyanka S., 16, Uttar Pradesh, India²⁷⁶

Companies' and Governments' Child Rights Responsibilities

Companies have a responsibility to respect all children's rights, wherever they operate in the world and throughout their operations.²⁷⁷ This is a widely recognized standard of expected corporate conduct, as set out in international human rights standards including the United Nations Guiding Principles on Business and Human Rights, and by the UN Committee on the Rights of the Child.²⁷⁸

Companies' responsibilities encompass preventing their services from being used in ways that cause or contribute to violations of children's rights, even if they were not directly involved in perpetrating abuses.²⁷⁹ These responsibilities hold even when a national government lacks the necessary laws and regulations to sanction such abuses, or is unable or unwilling to protect children's rights.²⁸⁰

Governments are responsible for ensuring that businesses meet these responsibilities.²⁸¹ They have a duty to protect children and their rights, and so should prevent, monitor, investigate, and punish child rights abuses by businesses. Governments are themselves also held responsible for violating children's rights if they have failed to take necessary, appropriate, and reasonable measures to prevent and remedy such violations, or otherwise tolerated or contributed to these violations.²⁸²

When children's rights are violated in an environment of opaque digital systems, businesses' global operations, and complex flows of data and technology between actors and across jurisdictions, children face immense challenges in finding justice. It is difficult for children, much less adults, to obtain evidence, identify perpetrators, or to even know what their rights are and when they have been abused—particularly if they have to act individually and expose themselves to scrutiny to get action from digital service providers.

Governments are obligated to provide effective remedies for violations of children's rights, and companies have a responsibility to put in place processes to remedy rights abuses which they caused or to which they contributed.²⁸³ Remedies should be widely known and readily available to all children; they should involve prompt, thorough, and impartial investigation of alleged violations, and should be capable of ending ongoing violations.²⁸⁴

Child Data Protection Laws

The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care, including legal protections, at all stages of their lives.²⁸⁵

Even as more children spend increasing amounts of their childhood online, most countries in the world do not have modern child data protection laws that would provide protections to children in complex online environments. For example, of the 49 countries examined by Human Rights Watch in this report, 14 countries had no data protection laws at all. Twenty-four countries possessed data protection laws that contained references to children, but these were restricted to the question of who may provide consent to the processing of children's data. Some of these were written at a time when digital technologies and data practices described in this report did not exist. For example, the United States' Children's Online Privacy Protection Act, signed into law in 1998 and subsequently amended, does not provide protections to children aged 13 to 18, nor restrict companies from collecting and using children's data for purposes not in the best interest of the child, including commercial interests and behavioral advertising.²⁸⁶ This domestic law has impacted children's digital experiences worldwide due to the fact that many of the largest and most influential technology companies that provide global services—including the majority of AdTech companies covered in this report—are headquartered in the US.

As a result, technology companies have faced little regulatory pressure or incentive to prioritize the safety and privacy of children in the design of their services. Most online service providers do not offer specific, age-appropriate data protections to children, and instead treat their child users as if they were adults.

The majority of EdTech products examined by Human Rights Watch did not offer data protections specific to children, nor did they provide a high level of privacy by design and default. As noted in this report, of the 163 EdTech products reviewed, 145 (89 percent) engaged in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights.

Of the 74 AdTech companies that responded to Human Rights Watch's request for comment, an overwhelming majority did not state that they had operational procedures in place to prevent the ingestion or processing of children's data, or to verify that the data they did receive comply with their own policies and applicable child data protection laws. Absent effective protections, AdTech companies appear to routinely ingest and use children's data in the same way they do adults' data.

²⁸³ ICCPR, art. 2(3); UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, principles 15, 22.

²⁸⁴ ICCPR, art. 2(3); UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, UN Doc. A/HRC/39/29, August 3, 2018, paras. 50-57; UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/73/348, August 29, 2018, <https://www.undocs.org/A/73/348> (accessed July 22, 2021), para. 39; CRC, General Comment No. 16, State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16 (2013), para. 4 (c); CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 43-49.

²⁸⁵ See: Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990.

²⁸⁶ Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506, <https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm> (accessed May 9, 2022).

287 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 23.

288 Ibid., paras. 28-29; 35-39.

289 CRC, art. 28(1)(a); ICESCR, art. 13 (2)(a).

290 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 11: Plans of Action for Primary Education (article 14 of the International Covenant on Economic, Social and Cultural Rights)," UN Doc. E/C.12/1999/4 (1999), <https://undocs.org/en/E/C.12/1999/4> (accessed July 23, 2021), para. 7.

291 CRC, art. 28(1)(b); ICESCR, art. 13 (2)(b).

292 United Nations, The 2030 Agenda for Sustainable Development, "UN Sustainable Development Goal 4, Target 4.1.: Free Primary and Secondary Education," <https://sdg4education2030.org/the-goal> (accessed May 4, 2022).

293 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 11: Plans of Action for Primary Education (art. 14 of the International Covenant on Economic, Social and Cultural Rights)," para. 6.

294 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 13 (Twenty-first session, 1999) The right to education (article 13 of the Covenant)," UN Doc. E/C.12.1999/10 (1999) <https://undocs.org/E/C.12/1999/10> (accessed October 25, 2021), para. 7.

295 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 103.

296 "The Abidjan Principles—Guiding Principles on the human rights obligations of States to provide public education and to regulate private involvement in education," 2019, <https://www.right-to-education.org/resource/abidjan-principles> (accessed February 22, 2020), principle 4, para. 58.

297 Ibid., para. 59.

298 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 103; OHCHR, "Guiding Principles on Business and Human Rights," 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed April 2, 2021), Principles 1, 13; UN Human Rights Council, Report of the Special Rapporteur on the right to education, "Right to education: impact of the coronavirus disease crisis on the right to education—concerns, challenges and opportunities," UN Doc. A/HRC/44/39 (2020), <https://undocs.org/A/HRC/44/39> (accessed November 9, 2021), para. 84 (j).

The UN Committee on the Rights of the Child states that governments "should review, adopt and update national legislation" to ensure that the digital environment protects children's rights, and that such legislation "should remain relevant, in the context of technological advances and emerging practices."²⁸⁷ Laws should be updated to specifically support enforcement and compliance in digital environments.²⁸⁸

Education

Every child has the right to education. International human rights law makes clear that governments are responsible for ensuring free and compulsory primary education,²⁸⁹ and governments must fulfill an "unequivocal" requirement to ensure the availability of primary education without charge to children, their parents or guardians, and eliminate all direct and indirect costs to children's education.²⁹⁰ Governments must make secondary education progressively available and accessible to all children.²⁹¹ Human Rights Watch calls on states to take immediate measures to ensure that secondary education is available and accessible to all, free of charge. Human Rights Watch also calls on states to make education compulsory through the end of lower secondary school, in line with the Sustainable Development Goals and the political commitments made by all United Nations member states to provide 12 years of free primary and secondary education, with 9 compulsory years of education.²⁹²

Education offered to children needs to "promote the realization of the child's other rights,"²⁹³ placing the best interests of students as a "primary consideration."²⁹⁴

As digital technologies can be used to support children's access to education, the Committee on the Rights of the Child has stated that governments "should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to ... misuse of their personal data, commercial exploitation or other infringements of their rights."²⁹⁵

The Abidjan Principles on the human rights obligations of states to provide public education and to regulate private involvement in education, which are guiding principles adopted in 2019 by a group of independent experts from around the world, state that governments should regulate companies providing ancillary services that enable learning to ensure that their actions facilitate, not obstruct, the right to education.²⁹⁶ They further call on governments to "ban commercial advertising and marketing in public and private instructional educational institutions, and ensure that curricula and pedagogical methodologies and practices are not influenced by commercial interests."²⁹⁷ Where children rely on services from the private market to access their right to education, states should also ensure that private actors do not infringe on children's other rights, including their rights to privacy; to play; to seek, receive, and impart information; to freedom of expression; and to freedom of thought.²⁹⁸

As described in this chapter, some governments made it compulsory for students and teachers to use government-built or endorsed EdTech products during the pandemic. This not only subjected them to the data practices and privacy protections—or lack thereof—of those products, but also made it impossible for children to protect themselves by opting for alternative means to access their right to education.

Students, Parents, and Teachers Operating in Blind Faith

Children, parents, and teachers operated on blind faith that their governments would protect children's rights when providing education online during Covid-19 school closures.

Many children and parents told Human Rights Watch that they did not recall ever being asked for their consent, much less informed how their rights might be protected or affected, when told to adopt specific EdTech products for school.²⁹⁹ Hayley John, a mother of two in Murwillumbah, Australia, said: "I just trusted the school had looked into it. What would we do about it anyway?... We were worried about the tension and uncertainty around this pandemic, so we were trying to make things work."³⁰⁰

But teachers told Human Rights Watch that they were also not informed how the EdTech products they were told to use would protect their students' privacy or told to explain and seek consent from children or their parents.³⁰¹ One secondary school teacher in London, United Kingdom, was told by his school to begin teaching in Google Classroom. But regarding the protection of his students' privacy, he said: "I'm not sure what the school has done.[...] I'm not aware that any student has signed any kind of waiver or consent form. I certainly haven't."³⁰²

Asked whether she had been instructed to seek consent from students and parents, Marie-Therese Exler, a 6th grade teacher in Schleswig-Holstein, Germany, said: "No. I assumed it would be fine and someone else decided over this."³⁰³ A secondary school teacher in Bilbao, Spain, said simply, "If the school's IT team says to use it, it is supposed to be fine."³⁰⁴

Some teachers told Human Rights Watch that their government created accounts for them and their students on EdTech platforms without asking for consent or informing them of the products' privacy practices. Fifth-grade teacher Daniela Andrea Ribeiro Espinoza, in Santiago, Chile, said: "The platforms were activated from the Huechuraba education department. They activated everything and sent us an institutional email, no more. We have never been asked to sign or accept anything."³⁰⁵ When asked whether he was asked to explain or seek consent from his students and their parents, one teacher in Hesse, Germany said: "No. We just got the access code [for the software] and that was it."³⁰⁶

"We don't really understand what's going on with data protection," said a primary school teacher in Barcelona, Spain. "The teachers at my school have accepted it, but it is the feeling that the students and teachers know everyone's home, as they have entered them virtually ... I don't know how it would have worked if someone hadn't wanted to [use the EdTech platform]. Being an extraordinary situation, people have accepted it.... There have been zero clear guidelines from the government or the Department of Education."³⁰⁷

Some teachers expressed concern for their students' data privacy.³⁰⁸ Abby Rufer, an algebra teacher in Texas, US, said that her school district initially did not implement protections for students' privacy. "Teachers were using [an online platform] which has no privacy protection. I was worried because, especially for our kids, this is not safe for them. Sixty to seventy percent of our kids had one primary family member that had been deported or was currently in ICE [US Immigration and Customs Enforcement] holding. So, this is unacceptable, and it is a dangerous situation to put these kids in."³⁰⁹

²⁹⁹ Human Rights Watch interviews with Jordi C., 16, Lleida, Catalonia, Spain, June 11, 2020; Gaetana Pacella, mother, Balvano, Italy, June 19, 2020; mother, Sydney, Australia, June 12, 2020; Bilqis M., mother of two, Hvidovre, Denmark, June 10, 2020; mother, Sidon, Lebanon, June 22, 2020; primary school teacher in Seattle, Washington, United States, June 22, 2020; Pema W., 5th grade mathematics teacher, Dharamsala, India, June 14, 2020.

³⁰⁰ Human Rights Watch interview with Hayley John, Murwillumbah, New South Wales, Australia, June 12, 2020.

³⁰¹ Human Rights Watch interviews with teacher's assistant, Berkshire, Massachusetts, United States, June 10, 2020; Molly Dobkin, primary school teacher, New York, United States, June 7, 2020; Tanja Ilic, teacher, Požarevac, Serbia, July 1, 2020.

³⁰² Human Rights Watch interview with secondary school teacher, London, United Kingdom, June 12, 2020.

³⁰³ Human Rights Watch interview with Marie-Therese Exler, teacher, Kiel, Schleswig-Holstein, Germany, June 3, 2020.

³⁰⁴ Human Rights Watch interview with teacher, Bilbao, Spain, June 12, 2020.

³⁰⁵ Human Rights Watch interview with Daniela Andrea Ribeiro Espinoza, teacher, Santiago, Chile, July 9, 2020.

³⁰⁶ Human Rights Watch interview with #42, teacher, Kassel, Hesse, Germany, June 10, 2020.

³⁰⁷ Human Rights Watch interview with Pere Nieto, teacher, Barcelona, Spain, June 12, 2020.

³⁰⁸ Human Rights Watch interview with teacher, central Iowa, United States, June 18, 2020.

³⁰⁹ Human Rights Watch interview with Abby Rufer, teacher, Dallas, Texas, United States, June 8, 2020.

Companies Failed to Protect

Human Rights Watch found that the data practices of an overwhelming majority of EdTech companies and their products risked or infringed on children's rights. As noted above, companies are responsible for preventing and mitigating abuses of children's rights, including those they indirectly contribute to through their business relationships. Out of 94 EdTech companies, 87 (93 percent) directly sent or had the capacity to grant access to children's personal data to 199 companies, overwhelmingly AdTech, as described in Chapters 2 and 3. In many cases, this enabled the commercial exploitation of children's personal data by third parties, including AdTech companies and advertisers, and put children's rights at risk or directly infringed upon them.³¹⁰

The majority of these companies—79—built and offered educational products designed specifically for children's use. In each of these 80 products apparently designed for use by children, the EdTech company implemented tracking technologies to collect and to allow AdTech companies to collect personal data from children.

Most EdTech companies did not inform children and their parents of how children were secretly surveilled by the online learning platforms they used daily for school. As described in Chapter 2, companies failed to disclose data practices that risked or infringed on children's privacy; 18 companies did not provide a privacy policy at all. As these tracking technologies were invisible to the user, children had no reasonably practical way of knowing the existence and extent of these data practices, much less the impacts on their rights. By withholding critical information, these companies also impeded children's access to justice and remedy.

³¹⁰ Human Rights Watch identified nine companies with products that appear to have protected their users' data and privacy. These were: Stile Education, Math Kids, learn, Prof Multi, Jitsi, Learning Apps, IServ, Visavid, and Learning Outcomes Smart Q.

³¹¹ Ministry of Education and Science of the Republic of Kazakhstan, "Kazakhs will have free access to educational Internet resources" ("Қазақстандықтарға білім беру интернет-ресурстарына тегін кіруге мүмкіндік беріледі"), March 20, 2020, <https://www.gov.kz/memleket/entities/edu/press/news/details/49822?lang=kk> (accessed July 20, 2021).

³¹² Anna Reznik, "Kazakhstani startup has provided everyone with free access to online lessons" ("Казахстанский стартап предоставил всем желающим бесплатный доступ к онлайн-урокам"), Forbes Kazakhstan, April 5, 2020, https://forbes.kz/process/kazhastanskiy_startap_predostavil_vsem_besplatniy_dostup_k_onlayn-urokam (accessed July 20, 2021).

³¹³ Ibid.

³¹⁴ Daryn Online, "Price list for advertising on the Daryn.online website" ("Прайс-лист на размещение рекламы на сайте Daryn.online"), https://web.archive.org/web/20210720061302/https://docs.google.com/spreadsheets/d/1Vz3NkoutAZwtPWqfGb_smdrc_b21kVHS/edit (accessed July 20, 2021).

Case Study: Daryn Online, Kazakhstan

Flush with new users and a captive audience during Covid-19 school closures, EdTech companies faced financial incentives to commercialize children's data and their attention. This was exemplified by Daryn Online, an educational website built by a Kazakh startup, Bugin Soft, which offers classes for students in grades 1 to 12 and claims to be the "Number 1 educational ecosystem in Kazakhstan."

On March 20, 2020, the Kazakhstan Ministry of Education recommended Daryn Online for children's learning during Covid-19 school closures, working with the country's telecommunications providers to zero-rate the website—that is, not charging users for data use when accessing that specific website—to allow students to use it for free.³¹¹ Within days, the website was overwhelmed by 1.5 million new users.³¹² In an interview with Forbes Kazakhstan, 27-year old founder Aibek Kuatbaev said, in astonishment, "we could not imagine such an explosive growth," and that this "organic growth took place with the support of the state."³¹³

By April 1, 2020, the founder sought to monetize the attention of his newfound user base by posting a "Price List for Advertising" on Daryn Online's home page, offering advertisers the opportunity to advertise to his students.³¹⁴ An advertiser could purchase the ability to display an ad banner on the login and registration page—which students had to pass through in order to get to their classes—for 70,000 KZT (US\$164) a day, or 420,000 KZT (US\$985) for a whole week. Advertisers could also purchase the ability to send out a push notification that would appear on the phones of 800,000 users of Daryn Online's study app for 900,000 KZT (US\$2,112).

Human Rights Watch also detected Daryn Online transmitting children’s personal data to Google, CloudFlare, Yandex, and Facebook, and found that the website engaged in intrusive surveillance of its students by installing session recorders and key logging.

Daryn Online discloses in their privacy policy that they may use information about a child and what they do in class—including their search history, messages, and comments to teachers, classmates, or written on their homework—“for advertising and sponsorship purposes,” and provide “anonymous” data to “third parties, as well as to partners and advertisers.”³¹⁵ The company also “reserves the right to download advertisements of other organizations on Daryn.online without the User’s consent.”

Daryn Online did not respond to our request for comment.

Governments Failed to Protect

Because Spain was in a state of emergency, the Ministry of Education communicated [to teachers] that consent for privacy, or data protection, was no longer required ... Privacy and all that has gone into the background completely, but we have done it because the Ministry has said so.

—Secondary school science teacher, Madrid, Spain³¹⁶

With the exception of a single government—Morocco—all governments reviewed in this report failed to protect children’s right to education. Human Rights Watch found that every government endorsed or procured at least one EdTech product that appeared to put at risk or infringed on children’s rights. Similarly, the majority of EdTech products endorsed by governments—145 out of 163, or 89 percent—engaged in data practices that appeared to put children’s rights at risk or directly infringed on them.

Most EdTech products were marketed as free and provided to governments at no direct financial cost. In the process of endorsing these and promoting their wide adoption by schools, teachers, and students, governments offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their fundamental rights to privacy, access to information, and their freedom of thought.

Most governments failed to take measures to prevent or mitigate children’s rights abuses by companies. Few governments appear to have taken child data privacy into consideration in their endorsements of EdTech products. At time of writing, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.

³¹⁵ Daryn Online, “User agreement” (“Қолданушы келісімшарты”), <https://web.archive.org/web/20210308190949/https://daryn.online/qoldanushy-kelisimsharty> (accessed March 8, 2021).

³¹⁶ Human Rights Watch interview with secondary school teacher, Madrid, Spain, June 9, 2020.

One government, Australia (New South Wales), conducted assessments for two of its three EdTech recommendations in June 2020 and October 2021.³¹⁷ These assessments rely on a self-reported questionnaire completed by an EdTech company, and reviewed by a non-profit company owned by state, territory, and Australian Government education ministers.³¹⁸

Human Rights Watch found that two national education ministries and two state-level ministries—Republic of Korea, Australia (Victoria), Germany (Bavaria), and Poland—provided general data privacy guidance to schools relating to online learning.³¹⁹

Governments that did not carry out children’s rights due diligence passed onto children the risks and harms associated with the misuse and exploitation of their personal data, which include security breaches, commercial exploitation, and the use of children’s data by governments, law enforcement, and other actors for purposes that are not directly relevant, necessary, or proportionate to children’s education or their best interests.³²⁰

As noted in Chapter 2, for example, Oracle’s BlueKai was reported to have exposed billions of people’s personal data in one of the largest data security breaches in 2020. Human Rights Watch detected four EdTech products—CBC Kids (Canada), Z-kai (Japan), Notesmaster (Malawi), and EBS (Republic of Korea)—transmitting their students’ data to BlueKai through ad trackers and cookies pointing to the domains **bluekai.com** and **bkrtx.com**, both prior to, and after, the reported data breach.

317 Human Rights Watch email correspondence with Sandie Matthews, Chief Information and Data Officer, New South Wales Department of Education, April 14, 2022.

318 Safer Technologies 4 Schools, “About the ST4S Assessment,” <https://web.archive.org/web/20220313232236/https://st4s.edu.au/general-information/> (accessed May 5, 2022); Education Services Australia, “About Education Services Australia,” <https://web.archive.org/web/20220423212000/https://www.esa.edu.au/about/about-us> (accessed May 5, 2022).

319 Bavarian State Ministry for Education and Culture, “Use online offers in school in a legally compliant manner” (“Online-Angebote rechtssicher in der Schule nutzen”), mebis Infoportal, <https://www.mebis.bayern.de/infoportal/service/datenschutz/recht-ds/apps-im-unterricht/> (accessed September 13, 2021); Republic of Korea Ministry of Education, “Please protect teachers and everyone’s personal information during remote classes!” (“원격수업 시 선생님 교육활동과 모두의 개인정보를 보호해주세요!”), April 9, 2021, <https://www.moe.go.kr/boardCnts/view.do?boardID=340&boardSeq=80261&lev=0&searchType=S&statusYN=W&page=1&s=moe&m=0202&opType=> (accessed September 13, 2021); Australia State Government of Victoria, “Online tools for collaboration and learning,” July 11, 2021, <https://web.archive.org/web/20210423052923/https://www.coronavirus.vic.gov.au/online-tools-collaboration-and-learning> (accessed September 13, 2021); Poland Ministry of Education and Science, “Safe personal data during distance learning - the Personal Data Protection Office for schools” (“Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół”), <https://zpe.gov.pl/a/dane-osobowe-bezpieczne-podczas-zdalnego-nauczania---poradnik-uodo-dla-szkol/D3VP5T8OL> (accessed September 13, 2021). do?boardID=340&boardSeq=80261&lev=0&searchType=S&statusYN=W&page=1&s=moe&m=0202&opType= (accessed September 13, 2021); Australia State Government of Victoria, “Online tools for collaboration and learning,” July 11, 2021, <https://web.archive.org/web/20210423052923/https://www.coronavirus.vic.gov.au/online-tools-collaboration-and-learning> (accessed September 13, 2021); Poland Ministry of Education and Science, “Safe personal data during distance learning - the Personal Data Protection Office for schools” (“Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół”), <https://zpe.gov.pl/a/dane-osobowe-bezpieczne-podczas-zdalnego-nauczania---poradnik-uodo-dla-szkol/D3VP5T8OL> (accessed September 13, 2021).

320 For further examples, please refer to chapter 2 of this report.

Governments Directly Engage in Rights Violations

Many governments directly built and offered their own EdTech products that violated or put at risk children's rights.

Out of the 42 governments that provided online education to children during the pandemic by directly building and offering their own EdTech products, 39 governments produced products that handled children's personal data in ways that may have put at risk or violated their rights, as described in chapters 2 and 3.

Put another way, out of a total 65 EdTech products built or financed by governments, the majority—56, or 86 percent—were found transmitting children's data to AdTech companies.

56 government-built EdTech products sent children's data to AdTech companies

Government	EdTech Product	Has Privacy Policy?
Argentina	Educ.ar	Yes
Brazil (Minas Gerais)	Estude em Casa	No
Brazil (São Paulo)	Centro de Mídias da Educação de São Paulo	Yes
Burkina Faso	Faso e-Educ@tion	No
Cameroon	Distance Learning	No
Canada (Quebec)	CBC Kids	Yes
Canada (Quebec)	Mathies	No
Canada (Quebec)	PBS Learning	Yes
Chile	Aprendo en Línea	Yes
China	Eduyun	No
Colombia	Aprender Digital	No
Côte d'Ivoire	Mon école à la maison	No
Ecuador	Educa Contigo	No
France	Deutsch für Schulen	Yes
France	English for Schools	Yes
Ghana	Ghana Library App	Yes
Guatemala	Mineduc Digital	Yes
India (Maharashtra, National, Uttar Pradesh)	Diksha	Yes
India (Maharashtra, National, Uttar Pradesh)	e-Pathshala	Yes
India (Maharashtra)	e-Balbharti	Yes
Indonesia	Rumah Belajar	Yes
Iran	Shad	No
Iraq	Newton	No
Kenya	Kenya Education Cloud	No
Malawi	Notesmaster	Yes

Malaysia	DELIMA	No
Mexico	@prende 2.0	Yes
Nepal	Learning Portal	No
Peru	Aprendo en Casa	No
Poland	E-podręczniki	Yes
Republic of Korea	EBS	Yes
Republic of Korea	KERIS edunet	Yes
Republic of Korea	Wedorang	Yes
Russian Federation	Moscow Electronic School	Yes
Russian Federation	My Achievements	Yes
Russian Federation	My School is Online	No
Russian Federation	Digital Lessons	Yes
Russian Federation	Russia Electronic School	Yes
Saudi Arabia	iEN	Yes
South Africa	Department of Basic Education website	Yes
Spain (Andalusia)	eAprendizaje	Yes
Spain (Catalonia)	EDU365.cat	Yes
Spain (Catalonia)	Super3	Yes
Spain (National)	Aprendo en Casa	Yes
Sri Lanka	e-Thaksalawa	No
Sri Lanka	Nenasa	Yes
Taiwan	Education Cloud	Yes
Taiwan	Kaohsiung Daxuetang	Yes
Taiwan	Taipei Cooc Cloud	Yes
Thailand	DEEP	Yes
Turkey	Eğitim Bilişim Ağı	No
Turkey	Özelim Eğitimdeyim	Yes
Venezuela	Cada Familia Una Escuela	No
Vietnam	OLM	No
Zambia	e-Learning portal	No
Zambia	Smart Revision	No

Only nine government EdTech products—Educ.ar (Argentina), CBC Kids (Canada), PBS Learning (Canada), Ghana Library App (Ghana), Rumah Belajar (Indonesia), South Africa’s Ministry of Education website (South Africa), EBS (Republic of Korea), KERIS edunet (Republic of Korea), and Wedorang (Republic of Korea)—disclosed in their privacy policies that they collect and use students’ data for advertising. Of these, four government products—Rumah Belajar, the Education Ministry of South Africa’s own website, CBC Kids, and Ghana Library App—explicitly disclosed that they use their students’ data for behavioral advertising purposes.

321 The Education Act, Act 23 of 2011, Part IV, art. 15; Republic of Zambia, Ministry of Education, “Education Sector National Implementation Framework III 2011-2015,” June 2010, https://planipolis.iiep.unesco.org/sites/default/files/ressources/zambia_education_sector_nif_iii_2011_2015_final_draft.pdf (accessed May 16, 2022), p. xvi; Government of Zambia, Free Primary Education Policy of 2002; Government of Zambia, Fifth to Seventh Periodic Reports to the Committee on the Rights of the Child, CRC/C/ZMB/5-7, November 11, 2021, Section H, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2f-C%2fZMB%2f5-7&Lang=en (accessed August 23, 2021), para. 149.

322 Zamtel, “Zamtel Launches E-Learning and Smart Revision Portal,” https://web.archive.org/web/20210823192902/https://www.zamtel.zm/news_elearning.html (accessed August 23, 2021); “Zamtel, ECZ and Ministry of General Education launch e-Learning and Smart Revision portals,” *Lusaka Times*, April 21, 2020, <https://www.lusakatimes.com/2020/04/21/zamtel-ecz-and-ministry-of-general-education-launch-e-learning-and-smart-revision-portals/> (accessed August 23, 2021).

323 Government of Zambia, Ministry of General Education, E-Learning Portal, “Subscription,” <https://web.archive.org/web/20210823165611/https://elearning.co.zm/subscription/> (accessed August 23, 2021); see also: Government of Zambia, Ministry of General Education, E-Learning Portal, “E-Learning,” <https://web.archive.org/web/20210823163825/https://elearning.co.zm/e-learning/> (accessed August 23, 2021).

324 Ministry of General Education, E-Learning Portal, “Grade 10-12 All Subjects,” <https://web.archive.org/web/20210823205605/https://elearning.co.zm/grade-10-12-all-subjects/> (accessed August 23, 2021).

325 Examinations Council of Zambia, Zamtel, Smart Revision, “Grade,” <https://web.archive.org/web/20210823192047/https://www.smartrevision.co.zm/grade.php> (accessed August 23, 2021); see also: “Terms and Conditions,” <https://web.archive.org/web/20210823192347/https://www.smartrevision.co.zm/termsandconditions.php> (accessed August 23, 2021).

Furthermore, Human Rights Watch identified 22 government EdTech products that failed to offer any privacy policy at all, thus keeping their students in the dark about how their governments were handling their intimate data and their privacy.

In contrast, only eight government-built products were found to protect children’s data by not installing any tracking technologies. These were: Juana Manso (Argentina), Biblioteca Digital Escolar (Chile), Jules, MaSpéMaths, and Ma classe à la maison (France), mebis (Germany: Bavaria), NHK for Schools (Japan), and TelmidTICE (Morocco). While few in number, these nine products demonstrate that it is possible for governments to uphold their obligation to protect and promote children’s rights by building and offering digital educational services to children that do not compromise their data and their privacy.

Case Study: Zambia

Children with access to connectivity and capable devices, or whose families made sacrifices to ensure their access, relied on EdTech to attend school online during the pandemic. The economic incentives to monetize their captive attention were illustrated in Zambia, a country which legally guarantees free basic education to every child and has committed to provide free and compulsory primary and secondary education, or grades 1 to 12, in its national education plans.³²¹

Human Rights Watch found that the Zambian government charged primary and secondary students for the online education it provided during Covid-19 school closures. On April 20, 2020, Zambia’s Ministry of General Education launched two websites: the first, e-Learning Portal, offered courses in core subjects for students grades 7 to 12; the second, Smart Revision, provided practice tests to help students in grades 7, 9, and 12 prepare for national examinations.³²²

Both websites required children to pay a monthly subscription fee before they could access learning content. Each course on e-Learning Portal costed ZMW 5 (US\$0.26), although students were nudged by the website’s design toward subscription bundles that were progressively more expensive at higher grades.³²³ For example, the website advertised the option to “Subscribe To All At K35 Only” (at a cost of US\$1.84) for students in grades 10-12, even though only three subjects were available to take—Biology, Chemistry, and Mathematics—that would have costed much less to purchase separately.³²⁴ Smart Revision featured similarly tiered pricing, and charged a monthly fee of ZMW 10 (US\$0.53) for students in grade 7, ZMW 20 (US\$1.05) for grade 9 students, and ZMW 30 (US\$1.58) for students in grade 12.³²⁵

326 Both websites were launched in partnership with Zamtel, the state-owned telecommunications provider and one of the three mobile internet providers in the country. While Zamtel announced that it would zero-rate both websites—that is, to provide free access to these websites by not charging users for data—Human Rights Watch notes that children would realistically first need internet access to even be aware of the government’s websites.

327 The Economist Intelligence Unit, “The Inclusive Internet Index, 2021” <https://theinclusiveinternet.eiu.com/explore/countries/ZM/performance/indicators/affordability> (accessed August 23, 2021).

328 World Bank, “Poverty and Equity Brief: Zambia,” April 2020, https://databank.worldbank.org/data/download/poverty/33E03BB-9722-4AE2-ABC7-AA2972D68AFE/Global_POVEQ_ZMB.pdf (accessed August 23, 2021).

329 PushEngage, “PushEngage,” <https://web.archive.org/web/20210915214533/https://www.pushengage.com/> (accessed September 15, 2021).

330 Salman Parviz, “Schools Set to Open Sept. 5 Amid Pandemic,” *Tehran Times*, September 5, 2020, <https://www.tehrantimes.com/news/452046/Schools-set-to-open-Sept-5-amid-pandemic> (accessed November 16, 2020); Alijani Ershad, “In Iran, poverty and lack of internet make distance learning impossible,” *France24*, April 21, 2020, <https://observers.france24.com/en/20200421-iran-internet-covid19-distance-learning-poverty> (accessed November 16, 2020).

331 Human Rights Watch interview with teacher, Marivan, Iran, May 4, 2020.

332 Government of Iran, Ministry of Education, “Shad,” <https://web.archive.org/web/20211028212342/http://www.shad.ir/> (accessed October 28, 2021).

These fees constituted a direct cost and a financial barrier to education, in addition to the high costs of internet access and devices that students and their families had to pay for before they could even access either of the government’s websites.³²⁶ Access to the internet in Zambia is prohibitively expensive for many, especially for the poorest children and those living in rural areas. According to the Inclusive Internet Index report, Zambia ranks 98 out of 120 countries surveyed in the cost of internet access relative to income.³²⁷ In 2015, 57.5 percent of Zambia’s population lived below the international poverty line of US\$1.90 per day; poverty is estimated to have increased with widespread job losses and rising prices during the pandemic, making the internet even less affordable for most children and their families.³²⁸

Human Rights Watch also detected e-Learning Portal transmitting its students’ personal data to PushEngage, a company offering push notification services “so you can unlock maximum revenue from each visitor,” and Tawk.to, a live chat service, even though the latter function was neither visible nor available for use on e-Learning Portal’s website.³²⁹ Human Rights Watch detected Smart Revision sending students’ personal data to Facebook.

For students relying on these websites to learn core content and prepare for high-stakes national examinations during Covid-19 school closures, submitting to these data practices was an indirect cost levied on them in exchange for their education.

The Zambian government, e-Learning Portal, PushEngage, and Smart Revision did not respond to a request for comment. Tawk.to and Facebook did not acknowledge Human Rights Watch’s finding that they were receiving data from either of these websites, or respond to questions about it.

No Choice

As noted in Chapter 3, this data collection and surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most government-built EdTech platforms did not allow their users to decline to be tracked; most of this surveillance happened secretly, without the child’s knowledge or consent. In such cases, it was impossible for children to opt out of such surveillance and data exploitation without opting out of school and giving up on formal learning altogether during the pandemic.

Some governments made it compulsory for students and teachers to use government-built EdTech platforms, not only subjecting them to the data practices and privacy protections—or lack thereof—of those products, but also making it impossible for children to protect themselves by opting for alternative means to access their right to education.

Teachers in Iran told Human Rights Watch that the government compelled those in public schools to use Shad, an app built by Iran’s Education Ministry for online learning during Covid-19.³³⁰ One teacher said: “The principal called and said that if I do not install the Shad app, I would be recorded as absent. The authorities do not accept teaching in Telegram and WhatsApp.... Students have also been told that if you are not in this app, your score will not be approved and will not be sent to the [school].”³³¹ In October 2021, the Iranian government reported more than 18 million active users of Shad.³³²

Technical analysis of Shad’s code by Human Rights Watch found that the app can collect children’s precise location data, the time of their current location, the child’s last known location, their Wi-Fi SSID, IP address, the child’s contacts, and any saved photos of their contacts.

Iran does not have a data protection law. A Personal Data Protection and Safeguarding Draft Act (“Draft Act”) was first proposed on July 26, 2018, and is still pending review from the Islamic Parliament of Iran as of September 2021; the Draft Act does not contain specific protections for children.³³³

In Turkey, one mother of a 9-year-old child, Rodin, told Human Rights Watch: “Rodin’s teacher forced all these 8-year-old kids to use Facebook. He made Rodin, who was 8 at the time, open a Facebook account, and told him to upload his homework there. Now, the teacher is forcing the kids to use Facebook when they’re taking tests.”³³⁴ Facebook’s terms of service prohibit children under 13 years old from using its services.³³⁵

She continued, “The teacher also asked me to download BiP [a government-mandated messaging app for government and school use during the pandemic] to communicate with him. I’d heard that the app was not secure in terms of data privacy, so I said no. The teacher said, ‘Well, then you can’t communicate with me.’ I didn’t want to download the app, so I told him, ‘I don’t have space on my phone.’ The teacher said, ‘Well, you can’t communicate with me,’ and blocked us all on WhatsApp to prevent all parents from contacting him on secure apps. So, I haven’t been able to talk to him since.”³³⁶

As noted in Chapter 2, the Indian government offered Diksha, an app that claimed to deliver education to over 10 million students in the early days of the pandemic. To drive further adoption, some state-level education ministries set quotas for government teachers to compel a minimum number of students to download the app.³³⁷

Human Rights Watch found that Diksha collects children’s precise location data, including the time of their current location and their last known location. Human Rights Watch also observed Diksha collecting and transmitting children’s AAID to Google, which demonstrates that Diksha shares children’s personal data with Google for advertising purposes.

In these countries, children could not give valid, meaningful consent for the processing of their data by government-mandated EdTech platforms—even if they had been asked—because they could not refuse to use them freely without detrimental effect, and there were no alternative means to access their education.

333 Government of Iran Ministry of Communications and Information Technology, “Draft Protection of Personal Data Law” (“از داده‌های شخصی”), <https://web.archive.org/web/20210611152356/https://www.ict.gov.ir/fa/newsagency/21691/%D9%84%D8%A7%DB%8C%D8%AD%D9%87%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%88%D8%AD%D9%81%D8%A7%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D9%87%D8%A7%DB%8C%D8%B4%D8%AE%D8%B5%DB%8C-%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C%D8%B4%D8%AF> (accessed September 20, 2021); OneTrust DataGuidance, “Iran,” <https://www.dataguidance.com/jurisdiction/iran> (accessed September 20, 2021).

334 Human Rights Watch interview with mother, Istanbul, Turkey, June 11, 2021.

335 Facebook, “Terms of Service,” <https://www.facebook.com/legal/terms> (accessed September 15, 2021), 3(1).

336 Human Rights Watch interview with mother, Istanbul, Turkey, June 11, 2021.

337 Ishita Bhatia, “Remote learning: UP sets target, tells each govt teacher to convince 10 students to download Diksha app,” *Times of India*, November 18, 2020, <https://timesofindia.indiatimes.com/city/meerut/remote-learning-up-sets-target-tells-each-govt-teacher-to-convince-10-students-to-download-diksha-app/articleshow/79268507.cms> (accessed August 24, 2021).

Acknowledgments

This report was researched and written by Hye Jung Han, researcher and advocate in the children's rights division at Human Rights Watch, who also conducted technical static analysis of all EdTech apps, technical analysis of EdTech websites, and data analysis of all EdTech products.

Technical analysis of EdTech websites was also conducted by Gabi Ivens, head of open source research at Human Rights Watch, and guided by Surya Mattu, Senior Data Engineer and Investigative Data Journalist of The Markup. We are particularly grateful to Surya Mattu for his work in building Blacklight, the real-time website privacy inspector built for The Markup, and for his generous assistance and invaluable insights in adapting the tool for Human Rights Watch's website analysis.

Additional technical analysis—both static and dynamic—of eight EdTech apps was conducted by Esther Onfroy, founder of Defensive Lab Agency, who also conducted additional dynamic analysis and ran the data experiments with four children located in Indonesia, India, South Africa, and Turkey. We are extremely grateful to Esther Onfroy for her work, as well as for her generous technical advice and expertise.

Additional interviews were conducted by Marlene Auer, former associate, Europe and Central Asia (ECA); Martha Bernild, associate, Development and Global initiatives; Hanna Darroll, former senior associate, Development and Global Initiatives; Tayla Hall, senior coordinator, Development and Global Initiatives; Anjelica Jarrett, former coordinator, LGBT rights; Aya Majzoub, researcher, Middle East and North Africa (MENA); Devin Milroy, former associate, Global IT; Elin Martínez, senior researcher, children's rights; Seung Kyung Noh, former senior associate, Operations; Catherine Pilishvili, senior coordinator, ECA; Marina Riera Rodoreda, former coordinator, International Justice; Anna Salami, officer, Development and Global initiatives; Kristen Scott, senior associate, Development and Global initiatives; Delphine Starr, former senior coordinator, children's rights; Svetlana Stepanova, senior manager, Development and Global initiatives; Behrouz Tehrani, consultant, MENA; Agnes Tkotz, associate director, Development and Global initiatives; Nicole Tooby, officer, Asia; Frances Underhill, senior manager, Film Festival; and Tenzin Wangmo, officer, General Counsel.

This report was edited by Bede Sheppard, children's rights deputy director at Human Rights Watch. Maria McFarland Sánchez-Moreno, senior legal advisor, and Tom Porteous, deputy program director, provided legal and program reviews. Expert reviews were provided by: Ilaria Allegrozzi, senior researcher, Africa; Jayshree Bajoria, senior researcher, Asia; Julia Bleckner, Asia researcher and health editor; Deborah Brown, senior researcher and advocate, technology and human rights; Eva Cossé, researcher, ECA; Farida Deif, Canada director; Corinne Dufka, associate director, Africa; Anietie Ewang, researcher, Africa; Elvire Fondacci, coordinator, France; Lydia Gall, senior researcher, ECA; Abir Ghattas, director, Information Security; Andreas Harsono, senior researcher, Asia; Saroop Ijaz, senior researcher, Asia; Paula Ini, senior research assistant, Americas; Gabi Ivens, head of open source research; Teppei Kasai, officer, Asia; Chloe King, researcher, MENA; Anastasiia Kruope, assistant researcher, ECA; Linda Lakhdhir, legal advisor, Asia; Elin Martínez, senior researcher, children's rights; Tyler Mattiace, researcher, Americas; Sophie McNeill, researcher, Asia; Santiago Menna, research assistant, Americas; César Muñoz, senior researcher, Americas; Otsieno Namwaya, senior researcher, Africa; Juan Pappier, senior researcher, Americas; Laura Pitter, deputy director, United States; Sunai Phasuk, senior researcher, Asia; Martina Rapido Ragazzino, senior research assistant, Americas; Kartik Raj, researcher, ECA; Mihra Rittmann, senior researcher, ECA; Tara Sepehri Far, senior researcher, MENA; Mary Smith, researcher, Asia; Judith Sutherland, associate director, ECA; Tamara Taraciuk Broner, acting director, Americas; Nathalie Cotrino Villarreal, senior research assistant, Americas; Maya Wang, senior researcher, Asia; Belkis Wille, senior researcher, crisis and conflict; Lina Yoon, senior researcher, Asia; and Hiba Zayadin, senior researcher, MENA.

Acknowledgments

Additional colleagues provided expert review for this report but are not named here for security reasons.

We are grateful to Esther Onfroy and Surya Mattu for providing external expert technical review.

External legal review was provided by Elizabeth Wang, founder of Elizabeth Wang Law Offices.

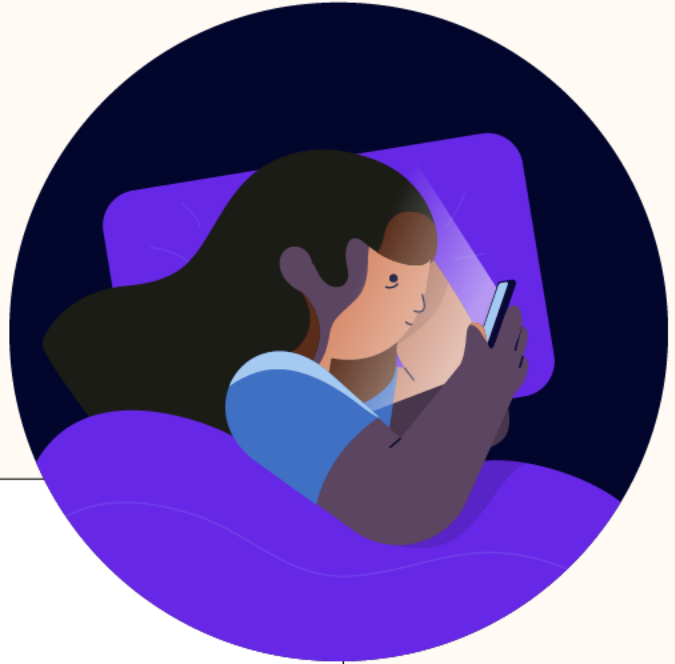
Sakae Ishikawa, senior video editor at Human Rights Watch, Liliana Patterson, senior editor, and Christina Curtis, multimedia deputy director, produced and edited one of the accompanying videos. Priya Sanghvi, content and production strategist, managed the production of a second accompanying video, which was produced and edited by Alejandro Norman, Patrick Scerri, Andrea Devia-Nuño, Erik Righetti, Hanna Lau-Walker, and Min Liu at Hero Studios.

Production assistance was provided by Katherine La Puente, associate, children's rights; Travis Carr, senior publications coordinator; and Fitzroy Hepkins, senior administrative manager. Content strategy, branding, and design was provided by Deroy Peraza, Izabella Stern, Lauren Jones, Pauline Shin, and Rima Desai of Hyperakt; and illustration was provided by Andrea Devia-Nuño at Hero Studios. Design direction and operational support was provided by Grace Choi, director of publications and information design; Les Lim, developer; and Christina Rutherford; senior digital manager.

The campaign supporting this project was led by Amanda Alampi, deputy director, Campaigns and Public Engagement; Ziva Luddy Juneja, acting digital campaigner; Bronte Price, digital engagement strategist; Nailah Ali, senior graphic designer, public engagement; and supported by Andrea Zita, associate; and Naimah Hakim, senior coordinator. Emma Daly, head of the Collaboratory, provided support and guidance.

We thank the four children and their parents who were willing to test out specific EdTech apps recommended by their government in order to verify our findings, and shared their stories with us.

Human Rights Watch thanks the Novo Nordisk Foundation for their support of this project.



“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That
Endorsed Online Learning During the Covid-19 Pandemic

“How Dare They Peep into My Private Life?: Children’s Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic,” is a global investigation of the education technology (EdTech) endorsed by 49 governments for children’s education during the pandemic. Based on technical and policy analysis of 164 EdTech products, Human Rights Watch finds that the majority of these online learning platforms put at risk or infringed upon children’s privacy and other rights, for purposes unrelated to their education.

These products monitored children, harvesting personal data such as who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use. Children, parents, and teachers were largely kept in the dark about these data surveillance practices.

The report finds that governments failed to protect children’s right to education. By endorsing and enabling the wide adoption of EdTech products without adequate safeguards or oversight, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy and access to information, and potentially their freedom of thought.

Children’s reliance on digital services that enable their education will likely continue long after the end of the pandemic. Governments should adopt modern child data protection laws to protect children online. Companies should immediately stop collecting, processing, and sharing children’s data in ways that risk or infringe on their rights.



“Como eles ousam espiar minha privacidade?”

Violações dos direitos das crianças e adolescentes por
governos que endossaram sistemas de aprendizagem on-line
durante a pandemia de Covid-19

Sumário

De segunda a sexta, Rodin, de 9 anos, acorda às 8 da manhã em Istambul, na Turquia. Ele come uma tigela de cereal de chocolate no café da manhã, e sua mãe o lembra, como sempre, de escovar os dentes depois. Às 9 da manhã, ele se conecta à sala de aula e acena para o professor e para os colegas. Ele espera que ninguém perceba que ele está um pouco sonolento, ou que está atrasado na lição de casa.

Durante os intervalos entre as aulas, Rodin lê mensagens de seus colegas no chat e faz rabiscos no quadro branco virtual que seu professor deixa aberto. Ele observa seu melhor amigo desenhar um gato; ele acha que seu amigo desenha muito melhor do que ele. No final da tarde, Rodin abre um site para assistir a aula de matemática televisionada nacionalmente para aquele dia. No final de cada dia, ele publica uma foto de sua lição de casa na página de mídia social de seu professor.

Sem que ele soubesse, um enxame invisível de tecnologias de rastreamento vigia as interações online de Rodin ao longo de seu dia. Em milissegundos após Rodin entrar na sala de aula pela manhã, a plataforma de aulas online de sua escola começa a rastrear a localização física de Rodin – em casa, na sala de estar de sua família, onde ele passou a maior parte de seus dias durante o lockdown da pandemia. A lousa virtual passa informações sobre seus hábitos de rabiscar para empresas de tecnologia da publicidade (AdTechs); quando a aula de matemática de Rodin termina, os rastreadores o seguem para fora de sua sala de aula virtual e para os diferentes aplicativos e sites que ele visita na internet. A plataforma de mídia social que Rodin usa para postar sua lição de casa acessa silenciosamente a lista de contatos de seu telefone e baixa detalhes pessoais sobre sua família e amigos. Algoritmos sofisticados revisam esse tesouro de dados, o suficiente para reunir um retrato íntimo de Rodin para descobrir como ele pode ser facilmente influenciado.

Nem Rodin nem sua mãe sabiam que isso estava acontecendo. Eles só foram informados por seu professor que ele tinha que usar essas plataformas todos os dias para ter sua frequência registrada na escola durante a pandemia de Covid-19.¹

Este relatório é uma investigação global das empresas de tecnologias educacionais (EdTechs) endossadas por 49 governos para a educação de crianças e adolescentes durante a pandemia. Com base na análise técnica de 163 produtos de EdTechs, a Human Rights Watch constatou que o endosso de governos à maioria dessas plataformas de aprendizado on-line colocou em risco ou violou diretamente a privacidade de crianças e adolescentes e outros direitos, para fins não relacionados a sua educação.

A pandemia de coronavírus abalou a vida e o aprendizado de crianças e adolescentes em todo o mundo. A maioria dos países optou por alguma forma de aprendizagem online, substituindo as salas de aula físicas por sites e aplicativos de EdTech. Isso ajudou a preencher lacunas urgentes na oferta de alguma forma de educação para muitas crianças e adolescentes.

Mas na pressa de conectar estudantes a salas de aula virtuais, poucos governos verificaram se as EdTech que eles estavam rapidamente endossando ou contratando para suas escolas eram seguras para as crianças e adolescentes. Como resultado, estudantes cujas famílias tiveram condições financeiras de acessar a internet e dispositivos eletrônicos, ou que fizeram grandes sacrifícios para acessar o ensino remoto, foram expostos às práticas de privacidade dos produtos de EdTech aos quais foram instruídos ou obrigados a usar durante o fechamento das escolas devido à Covid-19.

A Human Rights Watch realizou sua análise técnica dos produtos entre março e agosto de 2021 e, posteriormente, verificou suas conclusões conforme detalhado na seção de metodologia. Cada análise essencialmente é uma fotografia da prevalência e frequência das tecnologias de rastreamento incorporadas em cada produto em uma determinada data neste período. Essa prevalência e frequência podem flutuar ao longo do tempo com base em múltiplos fatores, o que significa que uma análise realizada em datas posteriores poderia registrar variações no comportamento dos produtos.

¹ Entrevista da Human Rights Watch com Rodin R. e sua mãe, em Istambul, Turquia, 11 de junho de 2021. Os nomes de todas as crianças citadas neste relatório foram alterados para proteger sua privacidade.

Dos 163 produtos de EdTech analisados, 145 (89 por cento) pareceriam se envolver em práticas em relação aos dados que colocaram os direitos de crianças e adolescentes em risco, contribuíram para enfraquecer esses direitos ou os violaram ativamente. Esses produtos monitoraram, ou tinham a capacidade de monitorar, crianças e adolescentes, na maioria dos casos secretamente e sem o consentimento das crianças e adolescentes ou de seus pais, mães ou outros responsáveis legais, em muitos casos coletando dados sobre quem são, onde estão, o que fazem durante a aula, quem são seus familiares e amigos e que tipo de dispositivo eletrônico suas famílias tinham condições financeiras de ter para usarem.

A maioria das plataformas de aprendizagem on-line instalou tecnologias de rastreamento que acompanharam as crianças e adolescentes fora de suas salas de aula virtuais e pela Internet ao longo do dia. Algumas ainda coletavam e registravam os hábitos dos estudantes de maneira invisível e impossível de evitar ou deletar – mesmo que os estudantes, seus pais, mães, responsáveis legais e professores estivessem cientes e tivessem o desejo e o conhecimento tecnológico para fazê-lo – sem jogar o dispositivo no lixo.

A maioria das plataformas de aprendizagem on-line enviaram ou concederam acesso a dados de crianças e adolescentes para terceiros, normalmente empresas de tecnologia da publicidade (AdTechs). Ao fazê-lo, elas parecem ter permitido aos algoritmos sofisticados de empresas de AdTech a oportunidade de unir e analisar esses dados para adivinhar as características e interesses pessoais de uma criança ou adolescente, e prever o que ele ou ela poderia fazer e como poderia ser influenciada. O acesso a essas informações poderia então ser vendido para qualquer pessoa – anunciantes, corretores de dados (data brokers) e outros – que buscassem impactar um grupo definido de pessoas com características semelhantes online.

As crianças e os adolescentes são vigiados em escala vertiginosa em suas salas de aula online. A Human Rights Watch observou 145 produtos de EdTech enviando diretamente ou concedendo acesso a dados pessoais de crianças e adolescentes para 196 empresas terceirizadas, em sua maioria esmagadora AdTechs. Em outras palavras, descobrimos que o número de empresas de AdTech que recebiam dados de crianças e adolescentes era muito maior do que as empresas de EdTech que enviavam esses dados a elas.

Alguns produtos de EdTech direcionaram publicidade comportamental a crianças e adolescentes. Ao usar os dados das crianças e adolescentes – extraídos de ambientes educacionais – para direcioná-las com conteúdo personalizado e anúncios que as seguem pela Internet, essas empresas não apenas distorceram as experiências online das crianças e adolescentes, mas também correram o risco de influenciar suas opiniões e crenças em um momento de suas vidas em que sofrem alto risco de manipulação. Muitos outros produtos de EdTech enviaram dados de crianças e adolescentes para empresas de AdTech especializadas em publicidade comportamental ou cujos algoritmos determinam o que as crianças e adolescentes veem online.

Não é possível para a Human Rights Watch chegar a conclusões definitivas sobre as motivações das empresas em promover essas ações, apenas podemos relatar o que observamos nos dados e nas próprias declarações das empresas e governos. Em resposta a solicitações de comentários, várias empresas de EdTech negaram a coleta de dados de crianças e adolescentes. Algumas empresas negaram que seus produtos fossem destinados a crianças e adolescentes, ou enfatizaram que suas páginas de sala de aula virtual destinadas a crianças e adolescentes tinham proteções de privacidade adequadas, mesmo que a análise da Human Rights Watch tenha descoberto que páginas adjacentes às páginas da sala de aula virtual (como a página de login, página inicial ou página adjacente com conteúdo infantil) não tivessem. As empresas de AdTech negaram o conhecimento de que os dados estavam sendo enviados a elas, indicando que, em qualquer caso, era responsabilidade de seus clientes não enviar dados de crianças e adolescentes.

Os governos têm a responsabilidade final sobre o fracasso de proteger o direito das crianças e adolescentes à educação. Com exceção de um único governo – Marrocos – todos os demais governos analisados neste relatório endossaram pelo menos um produto de EdTech que colocou em risco ou prejudicou os direitos de crianças e adolescentes. A maioria dos produtos de EdTech foi oferecida aos governos sem custo financeiro direto para eles; no processo de endossar e garantir sua ampla adoção durante o fechamento das escolas devido à Covid-19, os governos transferiram os verdadeiros custos de fornecer educação on-line para crianças e adolescentes, que sem saber foram obrigadas a pagar por seu aprendizado com seus direitos à privacidade, acesso à informação e potencialmente liberdade de pensamento.

Muitos governos colocaram em risco ou diretamente violaram os direitos de crianças e adolescentes. Dos 42 governos que forneceram educação on-line diretamente para as crianças e adolescentes, criando e oferecendo seus próprios produtos de EdTech para uso durante a pandemia, 39 governos produziram produtos que lidaram com dados pessoais de crianças e adolescentes de maneiras que arriscavam ou violavam seus direitos. Alguns desses governos tornaram obrigatórios para alunos e professores o uso de seus produtos de EdTech, não apenas os sujeitando aos riscos de uso indevido ou exploração de seus dados, mas também impossibilitando que estudantes se protegessem optando por alternativas de acesso à sua educação.

Às crianças e adolescentes, pais, mães ou outros responsáveis, e professores foram negados o conhecimento ou a oportunidade de contestar essas práticas de vigilância de dados. A maioria das empresas de EdTech não divulgou que poderia vigiar crianças e adolescentes por meio de seus dados; da mesma forma, a maioria dos governos não notificou estudantes, pais e professores ao anunciarem seus endossos aos produtos dessas EdTechs.

Em todos os casos, essa vigilância de dados ocorreu em salas de aula virtuais e ambientes educacionais onde estudantes não tinham como se opor. A maioria das empresas de EdTech não permitia que seus alunos se recusassem a ser rastreados; a maior parte desse monitoramento acontecia secretamente, sem o conhecimento ou consentimento da criança ou adolescente. Na maioria dos casos, era impossível para as crianças e adolescentes optarem por não serem vigiadas e não terem seus dados coletados sem abrir mão completamente da educação obrigatória e do aprendizado formal durante a pandemia.

É urgentemente necessário a adoção de medidas de reparação para crianças e adolescentes cujos dados foram coletados durante a pandemia e continuam em risco de uso indevido e exploração. Os governos devem realizar auditorias de privacidade de dados das EdTech endossadas para o aprendizado de estudantes durante a pandemia, remover aquelas que falharem nessas auditorias e notificar e orientar imediatamente as escolas, professores, pais e crianças afetados a fim de evitar coleta e uso indevido de dados das crianças e adolescentes.

De acordo com os princípios de proteção de dados de crianças e adolescentes e as obrigações de direitos humanos das empresas, conforme descrito nos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos, as empresas de EdTech e AdTech não devem coletar e processar dados de crianças e adolescentes para publicidade. As empresas devem inventariar e identificar todos os dados de crianças e adolescentes coletados durante a pandemia e garantir que não processem, compartilhem ou utilizem dados de crianças e adolescentes para fins não educacionais. As empresas de AdTech devem excluir imediatamente quaisquer dados de crianças e adolescentes que tenham recebido; as empresas de EdTech devem trabalhar com os governos para definir regras claras sobre retenção e exclusão de dados de crianças e adolescentes coletados durante a pandemia.

À medida que mais crianças passam cada vez mais parte de sua infância conectadas, sua dependência do mundo online e dos serviços digitais que permitem sua educação continuará por muito tempo após o fim da pandemia. Os governos devem desenvolver, refinar e implementar leis e padrões modernos de proteção de dados para crianças e adolescentes e garantir que as que desejam aprender não sejam obrigadas a abrir mão de outros direitos para fazê-lo.

As crianças e adolescentes devem ser consultados de forma ativa ao longo desses processos, ajudando a construir salvaguardas que protejam o acesso significativo e seguro a ambientes de aprendizagem on-line que ofereçam espaço para que as crianças e adolescentes desenvolvam suas personalidades e suas habilidades mentais e físicas em todo o seu potencial.

Recomendações

Aos governos

- Disponibilizar soluções urgentes para crianças e adolescentes cujos dados foram coletados durante a pandemia e permanecem em risco de sofrer uso indevido e exploração. Para fazer isso deveriam:
 - Realizar auditorias relacionadas à privacidade de dados nas empresas de tecnologia educacional (EdTech) endossadas para o ensino remoto de crianças e adolescentes durante a pandemia, remover aquelas que falharem nessas auditorias e notificar e orientar imediatamente as escolas, professores, pais, mães, ou outros responsáveis, e crianças e adolescentes afetados a fim de evitar nova coleta e uso indevido de dados.
 - Exigir que as empresas de EdTech que falharem nessas auditorias identifiquem e excluam imediatamente quaisquer dados de crianças e adolescentes coletados durante a pandemia.
 - Exigir que as empresas de tecnologia da publicidade (AdTechs) identifiquem e excluam imediatamente quaisquer dados de crianças e adolescentes que tenham recebido de empresas de EdTech durante a pandemia.
 - Prevenir a coleta e o processamento de dados de crianças e adolescentes por empresas de tecnologia para fins de criação e utilização de perfis de usuário, publicidade comportamental e outros usos não relacionados ao propósito de oferecer educação.
- Adotar leis de proteção de dados específicas para crianças e adolescentes que abordem os impactos significativos sobre os seus direitos decorrentes da coleta, processamento e uso de dados pessoais de crianças e adolescentes. Onde já existem leis de proteção de dados de crianças e adolescentes, atualizar e fortalecer as medidas de implementação buscando fornecer uma estrutura moderna de proteção de dados que garanta a proteção de crianças e adolescentes em ambientes on-line complexos.
- Aprovar e implementar leis que garantam que as empresas respeitem os direitos das crianças e dos adolescentes e sejam responsabilizadas se não o fizerem. De

acordo com os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos, essas leis deveriam exigir que as empresas:

- Conduzam e publiquem processos de due diligence sobre o respeito aos direitos das crianças e adolescentes.
- Ofereçam transparência total nas cadeias de fornecimento de dados e relatem publicamente como os dados das crianças e adolescentes são coletados e processados, para onde são enviados, para quem e com que finalidade.
- Forneçam mecanismos adequados a crianças e adolescentes, apropriados à idade, para solucionar e reparar estudantes que sofreram violações de seus direitos; esses mecanismos devem ser transparentes, independentes e implementáveis.
- Exigir avaliações do impacto sobre os direitos das crianças e adolescentes em editais e quaisquer processos de contratação pública para o fornecimento serviços essenciais às crianças e adolescentes por meio da tecnologia.
- Proibir a publicidade comportamental para crianças e adolescentes. Interesses comerciais e publicidade comportamental não devem ser considerados argumentos legítimos para o processamento de dados que violem os interesses de crianças ou adolescentes e seus direitos fundamentais.
- Proibir a criação e utilização de perfis de usuário para crianças e adolescentes. Em circunstâncias excepcionais, os governos podem suspender essa restrição quando for do interesse da criança ou do adolescente e somente se as salvaguardas apropriadas estiverem previstas em lei.

Aos Ministérios e Secretarias de Educação

- Onde a aprendizagem online é adotada como um mecanismo preferencial ou híbrido para fornecer educação, alocar fundos para pagar por serviços que permitam a educação online com segurança, em vez de permitir a venda e comercialização de dados de crianças e adolescentes para financiar os serviços.
- Certificar-se de que quaisquer serviços que sejam endossados ou adquiridos para oferecer educação online sejam seguros para as crianças e adolescentes. Em coordenação com as autoridades de proteção de dados e outras instituições relevantes deveriam:

- Exigir que todas as empresas que prestem serviços educacionais para crianças e adolescentes identifiquem, previnam e mitiguem os impactos negativos sobre os direitos das crianças e adolescentes, inclusive em seus relacionamentos comerciais e operações globais.
- Exigir avaliações de impacto de proteção de dados de crianças e adolescentes de qualquer provedor de tecnologia educacional que busque investimento, aquisição ou endosso público.
- Assegurar que as instituições educacionais públicas e privadas celebrem contratos com fornecedores de EdTechs que incluam proteções de dados de crianças e adolescentes. Não é razoável esperar que crianças e adolescentes celebrem um contrato, nem deve ser válido o consentimento dado por crianças e responsáveis, quando este não pode ser livremente recusado sem pôr em risco o direito da criança e do adolescente à educação.
- Definir e fornecer proteções especiais para categorias de dados pessoais confidenciais que nunca devem ser coletados de crianças e adolescentes em ambientes educacionais, como dados precisos de geolocalização.
- Fornecer canais de denúncia adequados para crianças e adolescentes, apropriados à idade e confidenciais; providenciar ajuda especializada e condições para ação coletiva em idiomas locais para estudantes que buscam justiça e reparação. Tais medidas devem evitar colocar ônus indevido ou responsabilidade exclusiva sobre as crianças e adolescentes ou seus responsáveis ao buscar reparação das empresas, agindo individualmente ou se expondo no processo.
- Desenvolver e promover a alfabetização digital e a privacidade de dados das crianças e adolescentes nos currículos. Fornecer programas de treinamento para funcionários do ministério e das secretarias de educação, professores e outros funcionários de escolas em habilidades de alfabetização digital e proteção da privacidade de dados das crianças e adolescentes, visando apoiar os professores a conduzir o aprendizado on-line de estudantes com segurança.
- Buscar os pontos de vista das crianças e dos adolescentes no desenvolvimento de políticas que protejam seus interesses em ambientes educacionais on-line e engajar significativamente as crianças no aprimoramento dos benefícios positivos que o acesso à Internet e às tecnologias educacionais podem fornecer para sua educação, habilidades e oportunidades.

Às Empresas de Tecnologia Educacional (EdTechs)

- Providenciar soluções urgentes e reparação nos casos em que direitos das crianças e adolescentes foram colocados em risco ou violados pelas práticas de coleta e uso de dados das empresas durante a pandemia. Para fazer isso deveriam:
 - Parar imediatamente de coletar e processar dados de crianças e adolescentes para desenvolver perfil de usuário, publicidade comportamental ou qualquer outra finalidade que não seja estritamente necessária e relevante para a oferta de educação.
 - Parar de compartilhar os dados de crianças e adolescentes para fins desnecessários e desproporcionais à oferta de educação. Nos casos em que os dados das crianças e adolescentes foram divulgados a terceiros para um propósito legítimo, de acordo com os princípios dos direitos das crianças e adolescentes e as leis de proteção de dados, celebrar contratos explícitos com processadores de dados terceiros e aplicar limites estritos ao processamento, uso e retenção dos dados que recebem.
 - Aplicar marcadores específicos para crianças e adolescentes a quaisquer dados compartilhados com terceiros, para garantir que todas as empresas do conglomerado de tecnologia sejam informadas adequadamente de que estão recebendo dados pessoais de crianças e, portanto, obrigadas a aplicar proteções aprimoradas no processamento desses dados.
 - Fazer um inventário e identificar os dados pessoais de crianças coletados durante a pandemia e tomar medidas para garantir que esses dados não sejam mais processados, compartilhados, retidos ou usados para fins comerciais ou outros que não estejam estritamente relacionados à educação infantil.
 - As empresas com produtos EdTech desenvolvidos para uso de crianças e adolescentes deveriam parar de coletar categorias específicas de dados de crianças e adolescentes que aumentam os riscos aos seus direitos, incluindo seus dados de localização precisos e identificadores de publicidade.
- Realizar due diligence dos direitos das crianças e adolescentes visando identificar, prevenir e mitigar o impacto negativo das empresas sobre os seus direitos, inclusive em seus relacionamentos comerciais e operações globais, e publicar os resultados desse processo de auditoria.

- Respeitar e promover os direitos das crianças e adolescentes no desenvolvimento, operação, distribuição e comercialização de produtos e serviços de EdTech. Garantir que os dados de estudantes sejam coletados, processados, usados, protegidos e excluídos de acordo com os princípios de proteção de dados infantis e as leis aplicáveis.
- Desenvolver políticas de privacidade escritas em linguagem clara, adequada para crianças e adolescentes, apropriada à idade. Estas devem ser separadas dos termos legais e contratuais para responsáveis e educadores.
- Providenciar às crianças, adolescentes e seus responsáveis mecanismos de denúncia adequados por idade e buscar remediar abusos de direitos quando ocorrerem. As soluções devem envolver investigações imediatas, consistentes, transparentes e imparciais de supostos abusos, e devem efetivamente acabar com as violações de direitos em questão.

Às Empresas de Tecnologia da Publicidade (AdTechs) e outras empresas terceirizadas que podem receber dados de produtos EdTech

- Fazer um inventário e identificar todos os dados de crianças e adolescentes recebidos por meio de tecnologias de rastreamento que empresas de tecnologia possuem e tomar medidas para excluir esses dados imediatamente e garantir que esses dados não sejam processados, compartilhados ou usados. Para fazer isso deveriam:
 - Identificar todos os aplicativos e sites que instalaram tecnologias de rastreamento e são propriedade de empresas de tecnologia e transmitiram dados do usuário a elas.
 - Destes classificar e criar uma lista de serviços direcionados prioritariamente às crianças e adolescentes, que devem ser monitorados e atualizados periodicamente. Notificar as empresas controladoras desses serviços de que elas precisam fornecer evidências explícitas de que seu serviço não é feito para crianças e adolescentes para terem seu produto removido desta lista.
 - Usando esta lista, as empresas devem revisar e excluir imediatamente quaisquer dados de crianças e adolescentes recebidos de produtos feitos para estudantes.

- Impedir o uso por empresas de tecnologia de tecnologias de rastreamento para vigiar crianças e adolescentes ou qualquer usuário desses serviços desenvolvidos para crianças e adolescentes.
 - Auditar regularmente os dados recebidos e as empresas que os enviam. Excluir ou de outra forma desativar o uso de quaisquer dados de crianças e adolescentes recebidos ou dados de usuários recebidos de serviços desenvolvidos para crianças e adolescentes, quando detectados.
 - Notificar e exigir que empresas e clientes que usam tecnologias de rastreamento identifiquem quaisquer dados de crianças e adolescentes coletados por meio dessas ferramentas com um marcador específico para crianças e adolescentes ou por outros meios, para que os dados marcados possam ser sinalizados e excluídos automaticamente antes da transmissão para empresas terceirizadas.
- Desenvolver e implementar processos eficazes para detectar e prevenir o uso comercial de dados de crianças e adolescentes coletados por meio de tecnologias de rastreamento por empresas de tecnologias
- Realizar due diligence em relação aos direitos das crianças e adolescentes para identificar, prevenir e mitigar o impacto das empresas de tecnologia sobre os direitos das crianças e adolescentes, inclusive em seus relacionamentos comerciais e em todas as operações globais, e publicar os resultados desse processo de auditoria.
- Providenciar às crianças e adolescentes e seus responsáveis mecanismos de denúncia adaptados às crianças e adolescentes e buscar solucionar violações de direitos quando ocorrerem. As soluções devem envolver a investigação imediata, consistente, transparente e imparcial de supostas infrações e devem acabar com as violações em questão.

**EXCELENTÍSSIMA SENHORA ISABELA MAIOLINO (COORDENADORA-GERAL
DE NORMATIZAÇÃO) DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
– ANPD**

**O INSTITUTO BRASILEIRO DE ESTUDOS DE CONCORRÊNCIA, CONSUMO E
COMÉRCIO INTERNACIONAL – IBRAC**, associação civil sem fins lucrativos, inscrita no
CNPJ sob o nº 96.287.453/0001-10, com sede em Rua Cardoso de Almeida, 788, cj. 121 –
Perdizes, CEP 05013-00, São Paulo/SP, vem por meio desta esclarecer que a avaliação
qualitativa e os comentários submetidos via e-mail à Tomada de Subsídios para elaboração da
Agenda Regulatória da ANPD para o biênio 2023-2024, em nome de **MARCELA
MATTIUZZO**, foram submetidos em nome do Ibrac.

O Ibrac é uma entidade privada, sem fins lucrativos, criada em dezembro de 1992, com o
objetivo de promover a realização de pesquisas, estudos e debates sobre temas relacionados à
defesa da concorrência, comércio internacional e consumo.

O interesse em contribuir para o modelo regulatório surgiu do empenho comum dos membros
de Grupo de Trabalho do Comitê de Regulação em buscar a construção de um melhor ambiente
jurídico de proteção de dados pessoais para os agentes econômicos envolvidos. Espera-se,
assim, que as contribuições possam colaborar para a Tomada de Subsídios.

Sendo o que havia para o momento, nos colocamos à inteira disposição desta coordenação para
quaisquer esclarecimentos adicionais.

De São Paulo para Brasília, 31 de agosto de 2022.

TOMADA DE SUBSÍDIOS

Agenda Regulatória ANPD 2023-2024

1. INTRODUÇÃO

Levando em consideração o [Aviso de Tomada de Subsídios nº 03/2022](#), publicado no Diário Oficial da União em 05.08.2022; e o conteúdo da [Nota Técnica nº 31/2022/CGN/ANPD](#), elaborada pela Coordenação-Geral de Normatização da Autoridade Nacional de Proteção de Dados (ANPD) brasileira e disponibilizada no processo nº 00261.001286/2022-93, o Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional – IBRAC vem:

- (i) trazer suas considerações sobre a ordem de priorização sugerida para os temas cuja regulação encontra-se “em andamento” na ANPD, a serem regulados com maior prioridade do que os temas “novos” propostos, conforme já manifestado pela própria Coordenação-Geral de Normatização da ANPD;
- (ii) apresentar suas justificativas para a avaliação qualitativa realizada na Plataforma Participe Mais Brasil, sobre a ordem de priorização dos novos temas a serem regulados pela ANPD no biênio de 2023-2024; e
- (iii) fazer ponderações sobre a regulamentação concomitante de temas de Governança Institucional pela ANPD.

Desde já, esclarecemos que não nos debruçamos sobre o nível de priorização da regulamentação sobre “Dosimetria e aplicação de sanções administrativas” em razão de perda de objeto, tendo em vista a recente publicação do [Despacho de 15 de agosto de 2022](#), que submete à consulta pública a minuta de Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela ANPD.

2. TEMAS EM ANDAMENTO

Com relação aos temas que obrigatoriamente serão incluídos na Agenda Regulatória de 2023-2024 da Autoridade – os quais, atualmente, se encontram em fase de estudo pelo corpo técnico da Autoridade; ou se relacionam a projetos de regulamentação no âmbito da ANPD, incluindo os itens da Agenda Regulatória do biênio 2021-2022 que não foram finalizados –, sugerimos uma possível priorização, seguindo a mesma ordem proposta na Plataforma Participe Mais Brasil, conforme segue abaixo:

- **5 – Muito importante (Urgente e prioritário)**

a) Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O tema é urgente e prioritário, especialmente tendo em vista a ampla discussão sobre o momento de apresentação do referido documento, vez que a redação da Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018 – “LGPD”) prevê duas situações que acabam por gerar insegurança aos controladores: a primeira, no artigo 10, §3º em que o RIPD poderá ser solicitado quando o tratamento de dados pessoais for pautado na base legal de legítimo interesse, o que pode ser entendido como se o documento já necessitasse estar pronto quando da requisição pela ANPD; e, a segunda, no artigo 38, quando a ANPD poderá determinar sua elaboração, indicando que o controlador será previamente notificado para fazê-lo.

Além disso, nos parece importante a emissão de um *template* próprio da Autoridade, que sirva de modelo para os controladores, de modo a dirimir dúvidas e eventuais omissões que temos visto na prática. Assim, a elaboração e disponibilização de regulamento próprio sobre o tema é de extrema importância, a fim de constar as situações obrigatórias e/ou eventuais casos de dispensa, além dos prazos para apresentação e modelo do RIPD.

b) Comunicação de incidentes e especificação do prazo de notificação

Sugerimos a priorização do assunto, de modo que a ANPD defina o que é considerado “risco ou dano relevante”, que justifica a comunicação de incidentes de segurança aos titulares de dados pessoais. Note-se que a recente publicação da [Tomada de Subsídios sobre tratamento de dados pessoais de alto risco](#) pela ANPD faz menção apenas ao critério de “tratamento de dados pessoais de alto risco” previsto na Resolução CD/ANPD/ nº 2, de 27 de janeiro de 2022 (que regulamenta a aplicação da LGPD para agentes de tratamento de pequeno porte), mas é silente sobre a aplicação do mesmo conceito em outras frentes.

Além disso, deve a ANPD: (i) estabelecer em qual prazo o controlador deve comunicar o titular e a própria Autoridade sobre a ocorrência de incidentes de segurança, esclarecendo o que entende por “prazo razoável”, nos termos do §1º do artigo 48 da LGPD, e (ii) qual o prazo para envio da complementação das informações nas situações em que houver comunicação parcial, nos termos do formulário atual disponibilizado no site da ANPD (e que prevê a notificação complementar). Por fim, sugerimos a retirada da comunicação de incidentes por parte do Operador do formulário de comunicação.

c) Transferência Internacional de Dados Pessoais

Considerando que muitos dos agentes de tratamento são organizações que atuam transnacionalmente; que a transferência de dados pessoais para outros países,

atualmente, se insere em um contexto de elevada insegurança jurídica, dada a ausência de parâmetros claros a serem observados; e levando em conta a necessidade de uma harmonização do cenário regulatório brasileiro com os padrões internacionais de fluxos de dados, o tema evidencia-se como urgente e prioritário.

Assim, sugerimos que a ANPD: (i) defina “transferência internacional” e “uso compartilhado de dados pessoais, bem como estabeleça as limitações de cada conceito; (ii) emita seu posicionamento sobre o nível de adequação dos países no mundo; (iii) publique os seus modelos e/ou posicionamentos sobre cláusulas contratuais-padrão, inclusive valendo-se de modelos de países cuja legislação seja amplamente semelhante à brasileira; (iv) dê início à análise das normas corporativas globais das companhias; dentre outras ações relacionadas ao funcionamento de mecanismos de transferência internacional de dados pessoais.

- **4 - Importante (Prioritário - pode esperar a curto prazo)**

- a) Direitos dos titulares de dados pessoais**

Entendemos que a regulamentação sobre o assunto é de grande relevância, razão pela qual merece ser priorizada. Contudo, a nosso ver, a elaboração de uma regulamentação única para a totalidade de direitos de titulares previstos na LGPD pode ser particularmente complexa, considerando os diferentes obstáculos relativos à implementação de cada um dos direitos dos titulares (a exemplo, o direito de portabilidade, cujos obstáculos de implementação são exclusivamente diferentes daqueles relativos ao direito de revogação de consentimento, por exemplo).

Assim, entendemos que a ANPD deverá priorizar a regulamentação da operacionalização básica destes direitos, na medida em que o recebimento de pedidos de titulares para exercício de seus direitos já é uma realidade de diversos agentes de tratamento e ausentes instruções acerca do tema, incluindo: (i) a definição de prazos para atendimento a pedidos de titulares, (ii) os formatos de atendimento aos direitos dos titulares, e (iii) eventuais limitações ao exercício desses direitos, que constituem pontos essenciais para operacionalizar qualquer um dos direitos previstos no art. 18 da LGPD.

Adicionalmente, entendemos que o tópico de “Petição de direitos de titulares”, sugerido como um novo tema a ser regulado pela ANPD, poderia ser endereçado conjuntamente com essa abordagem de “Direitos dos titulares”, tendo em vista que abrange a operacionalização, de forma geral, desses direitos pelos titulares.

- **3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)**

- a) Encarregado de proteção de dados pessoais**

O tema é consideravelmente relevante, especialmente porque a não-indicação de encarregado por agentes de tratamento é passível de sanções administrativas por violação à obrigação legal correspondente, conforme previsto no artigo 41 da LGPD.

Contudo, tendo em vista os recentes posicionamentos da ANPD sobre essa figura – seja através do "[Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais](#)" ou pela [Resolução CD/ANPD nº 02/2022](#), que estabeleceu a hipótese de dispensa do Encarregado para agentes de tratamento de pequeno porte –, entendemos que eventual regulação geral sobre o tema não seria tão prioritária neste primeiro momento, tendo em vista a existência de outras questões que necessitam de maior atenção por parte da Autoridade.

De outro lado, entendemos que seria possível um “afunilamento” regulatório, de modo a priorizar a regulamentação de subtemas específicos dentro desse grande tema, incluindo: (i) atribuições do encarregado; (ii) meios/formas de atuação do encarregado; (iii) terceirização e responsabilização do encarregado e (iv) dispensa e flexibilização de indicação do encarregado.

b) Hipóteses legais de tratamento de dados pessoais

Embora o tema seja dotado de grande relevância para fomentar a cultura de proteção de dados e para orientar os agentes de tratamento, de modo geral, a aplicação de bases legais depende do contexto fático analisado. Neste sentido, entendemos que eventual regulação sobre o assunto não seria tão prioritária para o próximo biênio, em razão da baixa capacidade fiscalizatória, em geral, da ANPD; e da existência de outras questões que necessitam de maior atenção por parte da Autoridade.

De outro lado, entendemos que seria possível um “afunilamento” regulatório, de modo a priorizar a regulamentação de subtemas específicos dentro desse grande tema; ou mesmo a adoção de mecanismos de *soft law* como a publicação de guias e orientações sobre temas como: (i) a aplicabilidade do legítimo interesse, seus requisitos e seus limites; (ii) a base legal de execução de contrato - fases sob o escopo (pré-contratual, pós-contratual e etc.), limites e outros aspectos; (iii) a aplicação da base legal de garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, "g" da LGPD) e (iv) a aplicação de bases legais ao tratamento de dados pessoais de crianças e adolescentes, por exemplo.

c) Larga escala (Resolução CD/ANPD nº 2/2022)

Considerando que “larga escala” é um dos critérios que excluem a configuração de um agente de tratamento como de pequeno porte, impedindo a efetiva flexibilização

do regime de obrigações para esses agentes, a definição desse conceito é o que irá possibilitar que a Resolução CD/ANPD nº 02/2022 possa produzir os efeitos desejados, facilitando a adequação à LGPD por esses agentes de pequeno porte.

Porém, considerando especialmente a recente publicação da [Tomada de Subsídios sobre tratamento de dados pessoais de alto risco](#) pela ANPD, entendemos que o tema já está sendo analisado pela ANPD – e, portanto, uma regulamentação geral sobre o tema não seria tão prioritária neste primeiro momento, tendo em vista a existência de outras questões que necessitam de maior atenção por parte da Autoridade.

d) Cookies

Diante de debates sobre se cookies podem conter dados pessoais identificados/identificáveis; considerando a recente recomendação da ANPD sobre a utilização de cookies no Portal Gov.br (que, a princípio, não representa uma recomendação geral voltada a outros agentes de tratamento); e levando em consideração a manifestação de integrantes técnicos da ANPD em recentes eventos sobre a aplicabilidade de bases legais para a coleta e uso de cookies, entendemos que o tema vem assumindo uma relevância indiscutível nos debates e na produção de conhecimento sobre a privacidade e proteção de dados no Brasil.

Contudo, levando em consideração que o tema não é, a princípio, estrutural para o *enforcement* da LGPD, e considerando a existência de temas de caráter mais urgente que ainda não foram regulamentados pela Autoridade, entendemos que, em um juízo de balanceamento com a capacidade regulatória da ANPD, o tema poderia ser regulamentado a médio prazo.

• 2 - Pouca importância (Neutro - pode esperar a longo prazo)

a) Tratamento de dados pessoais pelos órgãos de pesquisa

Considerando que: (i) o tema possui pouca relevância prática para a maioria dos agentes de tratamento no Brasil, já que seu escopo é restrito aos órgãos de pesquisa, conforme delimitado/definido pela LGPD; e (ii) já existem entendimentos da ANPD sobre o tema, como é possível se verificar pelo estudo técnico publicado pela Autoridade sobre "[A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa](#)", capaz de orientar, ainda que forma preliminar, os órgãos de pesquisa, entendemos que eventual regulação sobre o assunto não deve ser prioritária para o próximo biênio, em razão da existência de outras questões que necessitam de maior atenção por parte da Autoridade.

- **1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação)**

a) Cumprimento do disposto na Lei de Diretrizes e Bases da Educação Nacional (art. 62 da LGPD)

Setores econômicos específicos foram e serão bastante impactados pela LGPD e demais regulamentações sobre privacidade e proteção de dados, sendo o setor da educação um desses setores. No entanto, considerando o tempo de vigência da LGPD, bem como o tempo de atuação da ANPD e temas ainda em aberto para regulamentação, uma vez que setores específicos já possuem regulamentações diversas e autoridades específicas que determinam regulamentações e orientações setoriais, entendemos que o presente tema, ainda que em andamento, não deve ser um foco de regulamentação para a ANPD frente a temas novos e/ou mais urgentes.

b) Dados pessoais sensíveis – Organizações religiosas

Apesar de o presente tema já ser objeto de análise pela ANPD, entendemos que outros temas também já em andamento, bem como novos temas propostos, possuem mais urgência em sua regulamentação, considerando uma análise de proporcionalidade entre o efeito que eventual regulamentação possa ter sobre os titulares e agentes de tratamento quando comparado à eventual não regulamentação do tema.

c) Glossário sobre proteção de dados pessoais

Apesar da relevância da compreensão geral sobre termos e definições relacionados à privacidade e proteção de dados pessoais, entendemos que a própria LGPD traz em seu texto as definições mais relevantes, de forma clara e direta, capazes de orientar a compreensão dos agentes de tratamento e titulares de dados. Além disso, a própria ANPD já publicou e disponibilizou diversos guias e orientações que trazem os conceitos relevantes em aplicação – como um documento de [perguntas frequentes](#) (FAQ), contendo definições de diversos temas. Dessa forma, entendemos não haver necessidade urgente de regulamentação acerca desse tema.

Por fim, ressaltamos que, embora os temas supracitados não tenham sido submetidos à consulta à sociedade, entendemos que é importante criar uma ordem de priorização para sua regulamentação, de modo a garantir que novos temas sejam regulados e contemplados concomitantemente com a continuação desses projetos de regulamentação.

3. TEMAS NOVOS

Com relação aos novos temas que foram propostos pela Autoridade para serem avaliados no próximo biênio referente à Agenda Regulatória de 2023-2024 – os quais foram levantados pela Coordenação-Geral de Normatização por meio de pedidos de acesso à informação, consultas e sugestões recebidos pelos canais de atendimento da Ouvidoria da ANPD, além de processos administrativos que vêm suscitando posicionamentos ou interpretações da LGPD por parte da ANPD e informações de grupos internos da Autoridade –, sugerimos a seguinte priorização, de acordo com a ordem proposta na Plataforma Participe Mais Brasil, conforme segue abaixo:

- **5 – Muito importante (Urgente e prioritário)**

- a) Medidas de segurança técnicas e administrativas (incluindo padrões técnicos mínimos de segurança)**

O tema deve ser considerado prioritário em razão da necessidade de orientar os agentes de tratamento sobre quais são as medidas de segurança esperadas pela ANPD para o efetivo cumprimento da obrigação imposta pelo art. 46 da LGPD, especialmente porque há previsão no artigo 44, parágrafo único, de que os agentes de tratamento devem responder por danos decorrentes da violação da segurança dos dados quando deixarem de adotar tais medidas de segurança.

Apesar de a Autoridade já ter publicado o [Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte](#), tal documento não cuidou de estabelecer quais seriam os "padrões técnicos mínimos" que devem ser adotados pelos agentes de tratamento em geral. Assim, entendemos como necessária a emissão de um guia ou regulamento próprio especificando o que a Autoridade considera por padrões técnicos mínimos a serem adotados, levando em consideração as tecnologias disponíveis e as condições gerais dos agentes de tratamento, de maneira a não engessar o mercado.

Adicionalmente, sugerimos a utilização de eventuais parceiros de certificação, que possuem reconhecimento/prática internacional (como, por exemplo, ISO27001); e parcerias com Cert.br para realização de cursos ou treinamentos sobre segurança da informação.

- **4 - Importante (Prioritário - pode esperar a curto prazo)**

- a) Dados Pessoais Sensíveis – Dados biométricos**

Na medida em que dados biométricos (i) constituem dados pessoais sensíveis, dotados de proteção especial pela LGPD e (ii) são utilizados de forma difundida em

diferentes operações de tratamento (reconhecimento facial, impressão digital, etc.), é importante que a ANPD oriente agentes de tratamento quanto ao manuseio dessa categoria de dados, evitando seu uso indiscriminado e potenciais violações ao princípio de não-discriminação previsto na LGPD.

Destacamos que a LGPD tampouco é clara quanto ao conceito de dados biométricos, o qual merece ser esclarecido, em especial considerando que já tem se observado decisões judiciais se valendo de definições sobre dados biométricos em lei nacional de forma complementar à definição de dados sensíveis pela LGPD.

A exemplo, a legislação nacional já conta com uma definição para "atributos biométricos", ainda que restrita ao âmbito de compartilhamento de dados entre entidades da administração pública federal (Decreto 10046/2019, art. 2, II), que já foi inclusive emprestada pela jurisprudência de forma complementar à definição de dados sensíveis pela LGPD, a qual não define expressamente o que são dados biométricos (Ação Civil Pública 1090663-42.2018.8.26.0100, Foro Central Cível, 37ª Vara Cível, Juíza Lívia Martins Trindade Prado, Distrib. 30/08/2018).

Assim, ainda que a regulamentação acerca do tema não seja urgente, sua priorização é importante para garantir segurança jurídica para o tratamento de dados sensíveis biométricos, cuja definição ainda não é clara, e cujo uso pode ser invasivo aos direitos de personalidade dos titulares.

b) Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (exceções de aplicação da LGPD: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais)

A elaboração e publicização de opiniões ou recomendações da ANPD sobre as exceções do art. 4º, inciso III da LGPD é importante dado o atual vácuo legislativo para o tratamento de dados nos cenários dispensados da aplicação da Lei. Neste cenário, a orientação da Autoridade é especialmente relevante, uma vez que a LGPD vem sendo utilizada como instrumento para inviabilizar a garantia de acesso a informações, na forma da Lei (dificultando solicitações de autoridades policiais e de outros órgãos relacionados, por exemplo).

Além disso, considerando as recentes movimentações sobre o tema – através do Projeto de Lei nº 1.515/2022 (PL da LGPD Penal), por exemplo –, entendemos que é de fundamental importância estabelecer maior alinhamento e clareza sobre as limitações de aplicação da LGPD no âmbito da segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, de maneira a garantir o alinhamento com as novas regras. Nesse sentido, entende-se relevante o posicionamento institucional da ANPD a respeito do assunto, de forma prioritária.

a) Regras de boas práticas e de governança

De acordo com o artigo 50 da LGPD, os controladores e operadores poderão formular regras de boas práticas e de governança no âmbito de suas competências. A complexidade e especificidade de determinados setores e atividades de tratamento corroboram para a importância da elaboração de orientações de boas práticas, capazes de auxiliar os agentes de tratamento em suas atividades de tratamento de dados pessoais.

Embora exista uma certa autonomia privada na elaboração de normas de governança pelos agentes de tratamento, considerando que existe uma demanda da sociedade por direcionamentos sobre essas regras de boas práticas e de governança – especialmente sobre a adoção de guias orientativos que fomentem a cultura de proteção de dados pessoais no país –, entendemos que seria possível um “afunilamento” regulatório, de modo a priorizar a regulamentação de subtemas específicos dentro desse grande tema, tais como: (i) quais são os critérios; e (ii) qual será o procedimento que a ANPD adotará para reconhecer/validar as regras de boas práticas e de governança criadas pelos agentes de tratamento de dados pessoais.

c) Crianças e adolescentes

Embora existam temas cuja regulamentação deve ser priorizada com mais urgência, o tratamento de dados de crianças e adolescentes deve ser endereçado pela ANPD com certa prioridade, por diferentes razões. Primeiro, ao estabelecer que o tratamento de crianças e adolescentes deve ser guiado pelo “melhor interesse” dos titulares (art. 14, caput), a LGPD não define, em nenhum momento, o que deve ser abarcado nesse conceito. A definição do princípio, portanto, é vital para compreensão da abordagem do tratamento desses dados e proteção dos titulares.

Outro ponto que deve ser endereçado com certa prioridade pela Autoridade é a possibilidade de uso de outras bases legais, além do consentimento, para o tratamento de dados pessoais de menores de idade. Isso porque a LGPD, ao definir que “o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico” de pais ou responsável legal, pode ser interpretada de forma a limitar o tratamento de dados dessa categoria de titular somente por essa base legal – o que, na prática, pode impossibilitar tratamento de dados de crianças para cumprimento de obrigações legais e execução de políticas públicas, por exemplo.

Cumprir destacar que o tema tem sido alvo de um considerável debate doutrinário e até mesmo foi levado à IX Jornada de Direito Civil – que, em seu Enunciado 4796, admitiu a possibilidade de aplicação de outras bases legais além do consentimento para o tratamento de dados pessoais de menores, desde que observado o melhor interesse da criança. Dessa forma, é importante que a ANPD oriente o tema de modo a

garantir maior segurança jurídica ao tratamento de dados de crianças.

Por fim, recordamos que crianças e adolescentes são, por natureza, titulares de dados vulneráveis, cujos dados são cada vez mais sujeitos à exposição com o avanço de novas tecnologias destinadas ao seu público que processam uma gama de dados pessoais (brinquedos, videogames, redes sociais).

Assim, de forma a evitar danos à esfera de personalidade desses sujeitos, e considerando a demanda da sociedade pela regulamentação deste tema, é importante que a ANPD enderece com prioridade o tema.

- **3 – Razoavelmente importante (Neutro - pode esperar a médio prazo)**

b) Registro de operações

A regulamentação do tema se dá em razão da exigência expressa no artigo 37 da LGPD, que prevê que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem. É necessário considerar que o setor privado, influenciado por experiências de outras jurisdições mais maduras e por discussões doutrinárias, desenvolveu ferramentas e técnicas adequadas e de fácil acesso para o registro efetivo das operações de tratamento de dados pessoais – seja por meio de registros escritos simples e manuais ou até mesmo por softwares especializados em privacidade.

Contudo, é fato que apenas pequena parte da comunidade empresarial brasileira tem acesso aos softwares especializados em privacidade. Além disso, ainda que haja o licenciamento de tais ferramentas, é possível notar que grande parte das empresas não compreende a condução dos registros de operação, a necessidade de sua atualização e o que deles devem constar.

Note-se que o descumprimento da referida obrigação poderá ser considerado como uma violação à LGPD e, conseqüentemente, sujeito à aplicação de sanções administrativas. Em razão desses fatores e da falta de clareza sobre os critérios a serem fiscalizados pela ANPD no que diz respeito a esses registros de atividades de tratamento de dados pessoais, fomentando um cenário de insegurança jurídica, entendemos que a regulamentação do tema deve esperar no máximo “médio prazo” para regulamentação.

c) Adequação progressiva de banco de dados

A adequação progressiva de bancos de dados (incluindo bases legadas e bases de dados em geral) é medida relevante para garantir o *compliance* das organizações e evitar sanções administrativas severas durante um regime de transição em que as entidades ainda estão se adequando à LGPD. Por isso, é importante a elaboração de orientações sobre procedimentos, prazos e medidas de segurança sobre o tema.

Contudo, entendemos que eventual regulação sobre o assunto não seria tão prioritária para o próximo biênio, em razão da baixa capacidade fiscalizatória, em geral, da ANPD; e da existência de outras questões que necessitam de maior atenção por parte da Autoridade.

Outra proposta possível seria que a ANPD adotasse mecanismos de *soft law* num primeiro momento com relação a este tema, através da publicação de guias e de boas práticas para orientar os agentes de tratamento sobre limitações de armazenamento, formas de manutenção dessas bases e prazos aplicáveis, quando possível.

d) Boas práticas regulatórias

Considerando “boas práticas regulatórias” como a adoção de procedimentos para a elaboração de regulamentos pautados em outras experiências, cumpre frisar que o tema possui sua relevância relacionada ao desenvolvimento de um ambiente de proteção de dados estruturado, de modo a contribuir para a padronização e aprimoramento dos atos normativos das entidades responsáveis, com cooperação entre diferentes instâncias técnicas, maior qualificação dos subsídios técnicos e melhor gestão do estoque regulatório.

Neste sentido, e considerando que existe uma demanda da sociedade por direcionamentos sobre boas práticas regulatórias – especialmente para dirimir eventuais incongruências na uniformização de conceitos da LGPD e na aplicação de obrigações relevantes da LGPD por diversas autoridades e órgãos reguladores –, entendemos que a regulamentação do tema pela Autoridade é razoavelmente importante para o próximo biênio.

• 2 – Pouca importância (Neutro - pode esperar a longo prazo)

a) Compartilhamento de dados pelo poder público

Levando em consideração que a ANPD publicou, em janeiro de 2022, um Guia Orientativo sobre “[Tratamento de Dados Pessoais pelo Poder Público](#)”, sob a perspectiva do Ibrac enquanto entidade privada sem fins lucrativos, entendemos que a regulação do tema de compartilhamento de dados pelo Poder Público não é urgente e/ou prioritária para o próximo biênio, devendo-se priorizar a regulamentação de outras questões que necessitam de maior atenção por parte da Autoridade.

b) Termos de compromisso com agentes de tratamento

Ao nos referirmos a “termos de compromisso com agentes de tratamento” como os instrumentos que poderão ser celebrados para eliminar irregularidades, incertezas

jurídicas ou situações contenciosas no âmbito de processos administrativos pela ANPD, de acordo com o previsto no Decreto-Lei nº 4.657/1942 (conforme redação do art. 55-J, XVII da LGPD), entendemos que eventual regulação sobre o assunto não deve ser prioritária para o próximo biênio, em razão da baixa capacidade fiscalizatória, em geral, da ANPD; e da existência de outras questões que necessitam de maior atenção por parte da Autoridade.

- **1 – Nenhuma importância (Não há ou há pouca necessidade de regulamentação)**

a) Saúde

Setores econômicos específicos foram e serão bastante impactados pela LGPD e demais regulamentações sobre privacidade e proteção de dados, sendo o setor da saúde um desses setores. No entanto, considerando o tempo de vigência da LGPD, bem como o tempo de atuação da ANPD e temas ainda em aberto para regulamentação, uma vez que setores específicos já possuem regulamentações diversas e autoridades/órgãos reguladores específicos que determinam regulamentações e orientações setoriais, entendemos que o presente tema não deve ser um foco de regulamentação para a ANPD, sendo mais recomendável a priorização de temas mais abrangentes, em vez de temas que focam em setores, mercados ou nichos específicos.

b) Educação

Setores econômicos específicos foram e serão bastante impactados pela LGPD e demais regulamentações sobre privacidade e proteção de dados, sendo o setor da educação um desses setores. No entanto, considerando o tempo de vigência da LGPD, bem como o tempo de atuação da ANPD e temas ainda em aberto para regulamentação, uma vez que setores específicos já possuem regulamentações diversas e autoridades/órgãos reguladores específicos que determinam regulamentações e orientações setoriais, entendemos que o presente tema não deve ser um foco de regulamentação para a ANPD, sendo mais recomendável a priorização de temas mais abrangentes, em vez de temas que focam em setores, mercados ou nichos específicos.

c) Inteligência Artificial

A princípio, é necessário esclarecer que entendemos que o tema deve possuir influência da ANPD em sua regulamentação, visto que seria uma das autoridades com maior competência temática de assumir a regulação da Inteligência Artificial ("IA") a nível nacional em razão dos impactos que o uso dessa tecnologia traz para o tratamento

de dados pessoais.

Contudo, acreditamos que o Ministério da Ciência, Tecnologia e Inovações (MCTI), responsável pela publicação da Estratégia Brasileira de Inteligência Artificial - EBIA, também deve indicar publicamente se o tema da Inteligência Artificial deverá ser regulado de maneira setorial, assim como é o tema da Segurança Cibernética – o que tornaria a IA competência de agências e autoridades de todos os setores.

Não obstante, mesmo que caiba à ANPD somente a regulação da IA no setor da proteção de dados, é importante levar em consideração o baixo nível de maturidade do tema no Brasil, sob pena de que eventual regulação traga o risco de criação de entrave à evolução tecnológica. Portanto, neste momento inicial de regulamentação da IA no Brasil, entendemos que a Autoridade não deve priorizar a regulamentação sobre a utilização de IA, mas sim participar de forma ativa nos debates de regulação do uso dessa tecnologia (o que pode ocorrer, inclusive, via debates de outros temas prioritários, como *age gating*, por exemplo).

d) Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade

De início, propomos que este tema seja regulado "concomitantemente" pela ANPD, tendo em vista que já vem sendo tratado pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). Caso contrário, entendemos que eventual regulamentação do tema pela ANPD não seria prioritária neste primeiro momento, tendo em vista a existência de outras questões que necessitam de maior atenção por parte da Autoridade.

Ademais, cumpre notar que as diretrizes que a ANPD formulará como contribuição à construção da Política Nacional de Proteção de Dados Pessoais e da Privacidade ("Política") não apresentam necessidade de regulamentação, uma vez que as diretrizes configurariam apenas um auxílio ao Ministério da Ciência, Tecnologia e Inovações (MCTI), ministério competente para a efetiva formulação da Política.

4. GOVERNANÇA INSTITUCIONAL

Por fim, com relação aos temas de governança institucional indicados pela ANPD – incluindo a atualização do Regimento Interno e a regulamentação de Planejamento e Estratégia Institucional da ANPD 2024-2026, Plano de Dados Abertos e Código de Ética e Conduta da ANPD –, entendemos que tais temas não são submetidos à consulta pública, por disporem de matéria relativa à gestão administrativa e ao funcionamento das unidades da ANPD.

Contudo, propomos que temas institucionais sejam regulados "concomitantemente" pela Autoridade, de maneira a não prejudicar a atividade

regulatória dos temas “em andamento” e “novos” indicados anteriormente (especialmente levando em consideração que tais temas de governança institucional não passam por consultas e audiências públicas).

September 6, 2022

Waldemar Gonçalves Ortunho Júnior
President-Director of the National Data Protection Authority (ANPD)
Palácio do Planalto
Praça dos Três Poderes, 70150-900
Brasília, Brazil

Dear Mr. Ortunho,

The Information Technology Industry Council (ITI) is the primary voice, advocate and thought leader for the global information and communications technology (ICT) industry. Our 80 member companies include the world's leading innovation companies, headquartered worldwide and value chains distributed around the globe. Our member companies are leading Internet services and e-commerce companies, wireless and fixed network equipment manufacturers and suppliers, computer hardware and software companies, and consumer electronics and technology companies.

We would like to congratulate ANPD's initiative to open a call for initial input to the Authority's Regulatory Agenda for 2023-2024. This action demonstrates ANPD's commitment to listening to stakeholders' considerations and ensuring greater predictability and transparency in the Authority's regulatory processes. ITI recently submitted its perspectives through the Participa + Brasil platform.

While we appreciate the opportunity to comment on ANPD's forward-looking agenda, we want to emphasize the importance of completing the ANPD's existing workstreams, such as regulating international data transfers, and taking into consideration ongoing legislative and other initiatives. For example, we would like to reiterate our understanding that there are several legislative and conceptual discussions in Brazil around the regulation of artificial intelligence (AI), for which there are several relevant bills being discussed in Congress and an active Commission of Legal Scholars. While we do not believe that ANPD should prioritize regulating AI in the short to medium term (as demonstrated by our score of 2), if ANPD is considering pursuing AI regulations, we strongly encourage close coordination with ongoing discussions in Congress and the Commission to ensure that any efforts do not result in conflicting regimes

Thank you very much for your consideration. We respectfully make ourselves available to further discuss our contributions to the Open Call for Initial Input.

Sincerely,



Husani Durans de Jesus
Senior Manager of Policy for the Americas, ITI

C.c:

Directors Joacil Basilio Rael, Nairane Farias Rabelo Leitão, Arthur Pereira Sabbat, Miriam Wimmer
Board of Directors
National Data Protection Authority
Palácio do Planalto
Praça dos Três Poderes, 70150-900
Brasília, Brazil

6 de setembro de 2022

Ilmo.
Waldemar Gonçalves Ortunho Júnior
Diretor-Presidente
Autoridade Nacional de Proteção de Dados
Palácio do Planalto, Praça dos Três Poderes
70150-900 Brasília, Brazil

A Sua Excelência o Senhor Diretor-Presidente da Autoridade Nacional de Proteção de Dados Waldemar Gonçalves Ortunho Júnior,

O Information Technology Industry Council (ITI) é a voz primordial, defensor e um dos principais líderes na indústria global de tecnologia da informação e comunicações (TIC). Nossas 80 empresas membro incluem as principais empresas mundiais de inovação, com sedes ao redor do mundo e cadeias de valor distribuídas em todo o planeta. Nossas empresas membro são líderes de serviços de Internet e e-commerce, fabricantes e fornecedores de equipamentos sem fio (wireless) e de rede fixa, empresas de hardwares e softwares, e empresas de tecnologia e eletrônicos voltadas para consumidores.

Nós gostaríamos de parabenizar a iniciativa da ANPD em submeter à Tomada de Subsídios a Agenda Regulatória da Autoridade para o biênio 2023-2024. Essa iniciativa demonstra o compromisso da ANPD em ouvir as considerações de todas as partes interessadas e garantir maior previsibilidade e transparência no processo regulatório da Autoridade. O ITI submeteu recentemente suas contribuições através da Plataforma Participa + Brasil.

Se por um lado nós apreciamos a oportunidade de comentar a futura agenda da ANPD, gostaríamos de enfatizar a importância da conclusão de trabalho existentes pela ANPD, como a regulamentação da transferência internacional de dados pessoais, e de levar em consideração iniciativas legislativas e outras em andamento. Por exemplo, gostaríamos de reforçar o nosso

entendimento de que discussões legislativas e conceituais em torno de inteligência artificial (IA) têm acontecido no Brasil. Existem diversos projetos de lei que versam sobre o tema em tramitação no Congresso brasileiro, bem como foi criada uma Comissão de Juristas específica sobre IA. Embora não acreditemos que a ANPD devesse priorizar a regulamentação de IA no curto e médio prazo (como demonstrado pelo valor '2' atribuído na nossa contribuição), caso a Autoridade esteja considerando se debruçar sobre a regulação de IA, incentivamos fortemente que a ANPD coordene seus esforços estreitamente com as discussões em andamento no Congresso e na Comissão de Juristas para garantir que quaisquer deliberações não resultem em regimes conflitantes.

Desde já agradecemos a sua consideração e respeitosa e nos colocamos à disposição da ANPD para discutir de forma mais aprofundada nossas contribuições à Tomada de Subsídios.

Atenciosamente,



Husani Durans de Jesus
Gerente Sênior de Políticas Públicas para as Américas
Information Technology Industry Council (ITI)

CC:

Diretores Joacil Basilio Rael, Nairane Farias Rabelo Leitão, Arthur Pereira Sabbat, Miriam Wimmer
Conselho Diretor
Autoridade Nacional de Proteção de Dados
Palácio do Planalto
Praça dos Três Poderes, 70150-900
Brasília, Brasil

Tomada de Subsídios da ANPD

Agenda Regulatória 2023-2024 ([Formulário](#))

Prazo: 31/08/2022

Introdução

A proposta resulta da conciliação entre importância, prioridade e impacto do respectivo tema para as empresas e para o sistema de proteção de dados.

5 – Muito importante (Urgente e prioritário)

6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)

10. Boas Práticas Regulatórias

Temas muito importantes para regulação urgente

Os temas selecionados como “muito importantes”, e, portanto, que merecem regulação urgente e prioritária pela ANPD, são aqueles que reconhecemos como estruturantes para permitir a evolução e o amadurecimento de práticas de mercado e que, ao mesmo tempo, favorecem consolidação do sistema de proteção de dados.

Assim, o estabelecimento das diretrizes para a Política Nacional de Proteção de Dados e o estabelecimento das boas práticas regulatórias em proteção de dados permitirão a ANPD a exercer sua regulação responsiva em diálogo com os setores regulados dentro de balizas socialmente reconhecidas. A partir dessas molduras regulamentares, será possível avançar com segurança e previsibilidade na regulamentação de outros pontos específicos da LGPD.

A Política é fundamental para apoiar no reconhecimento de temas socialmente relevantes na agenda nacional de proteção de dados, no amadurecimento de boas práticas no mercado e para fomentar o diálogo entre agentes de tratamento, sociedade civil, autoridades públicas e titulares de dados. As boas práticas regulatórias devem buscar a harmonização e integração entre atos normativos produzidos pela ANPD e outras entidades reguladoras, de modo com que haja coordenação efetiva entre os diversos comandos regulatórios. Ademais, é fundamental a garantia da participação social e medidas de transparência e diálogo contínuos no transcurso do processo regulatório, bem como a consolidação das técnicas de regulação a partir de evidências.

4 – Importante (Prioritário – pode esperar a curto prazo)

14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)

11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)

16. Diálogo institucional entre a ANPD e entidades supervisoras do SFN

Temas importantes que devem ter regulação priorizada no curto prazo

Opiniões e recomendações sobre as exceções do inciso III do Art. 4º da LGPD: O tratamento de dados pessoais – inclusive de dados sensíveis – para apoio a iniciativas de combate à fraude e para a proteção da vida ou da incolumidade física de clientes é prática essencial para as empresas do setor. São necessárias cooperações com autoridades de segurança e autoridades reguladoras, que exigem das instituições reguladas o tratamento de dados para garantir o bom andamento de atividades de segurança pública, de investigação e repressão de infrações penais e a higidez e confiança social no Sistema Financeiro Nacional. Portanto, é importante que a ANPD

7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	regulamente de forma prioritária a maneira como irá conduzir a emissão de opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do art. 4º da LGPD, com especial garantia de que tais opiniões e recomendações emergjam de um diálogo contínuo com as entidades do setor produtivo. Medidas e padrões de segurança: A regulamentação das medidas e padrões mínimos de segurança deve levar em conta as práticas e regulações setoriais existentes, e as competências normativas complementares da ANPD com demais órgãos reguladores. Para o sistema financeiro nacional, por exemplo, estão em vigor normas específicas que determinam medidas e padrões de cibersegurança que precisam ser acolhidos e reconhecidos para se evitar antinomias e excessivo custo de conformidade. Citamos, apenas a título de exemplo, a Resolução nº 4.893/21, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Diálogo institucional ANPD e SFN: Recomendamos, ainda, na condição de tema para ação prioritária pela ANPD, o estabelecimento de diálogo institucional entre a autoridade e as entidades normativas e supervisoras do Sistema Financeiro Nacional, a exemplo do Conselho Monetário Nacional (CMN), do Banco Central do Brasil e da Comissão de Valores Mobiliários, com o objetivo de promover a uniformização e convergência regulatória em temas como (i) comunicação de incidentes como dados pessoais no âmbito do Sistema de Pagamentos Brasileiro (SPB); (ii) segurança cibernética; (iii) contratação de serviços em nuvem e transferência internacional de dados; (iv) Open Finance e o direito de portabilidade no sistema financeiro; (v) papel dos agentes de tratamento de dados pessoais no âmbito do SFN quando atuam para no âmbito do Open Finance, ou cumprimento obrigação legal ou regulatória, a exemplo das hipóteses de controladoria singular, conjunta, operador e sub-operador. Peticionamento do titular de dados: A ausência de procedimento explícito em relação ao peticionamento dos titulares perante a ANPD, eventualmente atribuindo-se prazos para a autoridade se manifestar e maior clareza nos procedimentos, inclusive na forma de engajamento com os agentes de tratamento, é medida prioritária e que recomendamos a regulamentação no curto prazo.
3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	
8. Dados Pessoais Sensíveis – Dados biométricos (Art. 5º, II da LGPD)	Temas razoavelmente importantes que devem ser regulamentados no médio prazo Dados pessoais sensíveis – dados biométricos: Reconhecemos a relevância do tema, com amplo espaço para amadurecimento das práticas de mercado, inclusive com a criação de arranjos especializados de autorregulação sobre o assunto. O uso de dados pessoais sensíveis em respeito à LGPD e outras normas, a exemplo de regulações expedidas pelo Banco Central do Brasil, é prática que vem se consolidando no mercado financeiro para combater fraudes, validação de identidades e proteção dos usuários de serviços financeiros. Ademais, esse tema poderá receber atenção específica quando da regulamentação itens da agenda
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)	
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	

	regulatória atual, a exemplo do relatório de impacto à proteção de dados (RIPD), bases legais e outros poderão vir regulamentados de forma prioritária, a exemplo das medidas e padrões de segurança. Termos de compromisso: Recomendamos a regulamentação do tema no médio prazo, após a definição das diretrizes da Política Nacional de Proteção de Dados e das Boas Práticas Regulatórias. Compartilhamento de dados pelo Poder Público: Aqui servimo-nos de argumentação semelhante. Entendemos que a ANPD pode endereçar melhor o compartilhamento e uso compartilhado de dados pelo Poder Público no âmbito de suas orientações, guias e estudos técnicos.
2 – Pouca importância (Neutro - pode esperar a longo prazo)	
1. Crianças e adolescentes (Art. 14 da LGPD)	Temas cuja regulação pode ocorrer no longo prazo Crianças e adolescentes: O tratamento de dados pessoais de crianças e adolescentes deve seguir as normas da LGPD e de legislações especiais aplicáveis, a exemplo do Estatuto da Criança e do Adolescente. Ao apontarmos esse tema como merecedor de regulação no longo prazo não estamos minimizando sua importância, mas que entendemos haver disciplinamento mínimo e razoável no ordenamento jurídico para se garantir o melhor interesse desses titulares de dados pessoais. Ademais, as regulamentações de outros temas prioritários da LGPD, a exemplo do relatório de impacto e das medidas de segurança, também servirão para robustecer a proteção dos direitos de titulares de dados menores de 18 anos. Adequação de banco de dados: A regulamentação da adequação progressiva de banco de dados deve seguir-se ao amadurecimento das boas práticas de mercado, em especial com a definição adequada das bases legais e sua aplicabilidade às atividades de tratamento em diversos setores da economia. Assim, recomendamos que os dados legados recebam tratamento regulatório para a sua adequação no longo prazo. Registro de operações: A definição da forma e conteúdo dos registros de atividades de tratamento de dados pode ser regulamentada no longo prazo, em uma abordagem flexível que acolha práticas de mercado. Regras de boas práticas e governança: A regulamentação das regras de boas práticas e governança é tema que deve se seguir após a conclusão de aspectos fundamentais do sistema nacional de proteção de dados pessoais, a exemplo da Política Nacional, das Boas Práticas Regulatórias e temas que já constam na agenda regulatória atual, como as bases legais e o relatório de impacto à proteção de dados (RIPD). Ademais, vemos a necessidade de se avançar em temas como padrões e medidas de segurança da informação e a consolidação da cooperação entre a ANPD e reguladores e supervisores do Sistema Financeiro Nacional. No transcurso da regulamentação desses e outros pontos, a ANPD poderá acompanhar junto aos setores regulados a evolução de suas regras setoriais de boas práticas e a consolidação de governanças de dados mais robustas, conforme mercado e sociedade aprendam com as
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)	
12. Registro de Operações (Art. 37 da LGPD)	
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)	

	experiências no tratamento de dados pessoais. Recomendamos que, quando da regulamentação futura das regras de boas práticas e governanças, a ANPD já tenha consolidado precedentes importantes sobre como o mercado pode formular diretrizes e orientações e a forma como esses documentos podem ser legitimados junto ao órgão e demais titulares de dados interessados. No longo prazo, as entidades representativas do setor produtivo já terão conduzido alguns trabalhos relevantes, acompanhados pela ANPD, na busca de denominadores comuns sobre práticas de tratamento de dados de agudo interesse social, a exemplo de tratamento de dados para combate à fraude, uso de dados biométricos, segurança da informação e cooperação para investigações. A maturação desse processo será importante para o surgimento de ecossistemas de autorregulação mais robustos em favor dos direitos dos titulares e da inovação, tornando o trabalho de longo prazo da ANPD para a sua regulamentação uma atividade que pode extrair da experiência setorial para produzir normas mais efetivas.
1 – Nenhuma importância (Não há ou há pouca necessidade de regulamentação)	
5. Inteligência Artificial	Temas cuja regulação necessidade de regulamentação pode ser avaliada no longo prazo Inteligência Artificial: Entendemos que o tema de inteligência artificial é bastante amplo e ainda está sujeito a debates legislativos importantes, a exemplo das propostas de lei em trâmite no Congresso Nacional. Ademais, não está claro na tomada de subsídios da ANPD qual dimensão da inteligência artificial poderia ser objeto de regulamentação pela autoridade. Nesse sentido, recomendamos que esse tema não seja incorporado à agenda regulatória neste momento. Ademais, a LGPD, em especial em seu artigo 20 e outros pontos, e outras normas como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e regulações prudenciais setoriais do Sistema Financeiro Nacional já endereçam aspectos relevantes da governança de modelos das instituições financeiras e assemelhadas.

Tomada de Subsídios da ANPD

Agenda Regulatória 2023-2024 ([Formulário](#))

Prazo: 31/08/2022

Introdução

A proposta resulta da conciliação entre importância, prioridade e impacto do respectivo tema para as empresas e para o sistema de proteção de dados.

5 – Muito importante (Urgente e prioritário)

6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)

10. Boas Práticas Regulatórias

11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD).

Temas muito importantes para regulação urgente

Os temas selecionados como “muito importantes”, e, portanto, que merecem regulação urgente e prioritária pela ANPD, são aqueles que reconhecemos como estruturantes para permitir a evolução e o amadurecimento de práticas de mercado e que, ao mesmo tempo, favorecem consolidação do sistema de proteção de dados.

Assim, o estabelecimento das diretrizes para a Política Nacional de Proteção de Dados e o estabelecimento de diretrizes gerais de boas práticas regulatórias em proteção de dados permitirão a ANPD a exercer sua regulação responsiva em diálogo com os setores regulados dentro de balizas socialmente reconhecidas. A partir dessas molduras regulamentares, será possível avançar com segurança e previsibilidade na regulamentação de outros pontos específicos da LGPD.

A Política é fundamental para apoiar no reconhecimento de temas socialmente relevantes na agenda nacional de proteção de dados, no amadurecimento de boas práticas no mercado e para fomentar o diálogo entre agentes de tratamento, sociedade civil, autoridades públicas e titulares de dados. As boas práticas regulatórias devem buscar a harmonização e integração entre atos normativos produzidos pela ANPD e outras entidades reguladoras, de modo com que haja coordenação efetiva entre os diversos comandos regulatórios. Ademais, é fundamental a garantia da participação social e medidas de transparência e diálogo contínuos no transcurso do processo regulatório, bem como a consolidação das técnicas de regulação a partir de evidências.

Medidas e padrões de segurança: A regulamentação das medidas e padrões mínimos de segurança deve levar em conta as práticas e regulações setoriais existentes, e as competências normativas complementares da ANPD com demais órgãos reguladores. Para o sistema financeiro nacional, por exemplo, estão em vigor normas específicas que determinam medidas e padrões de cibersegurança que precisam ser acolhidos e reconhecidos para se evitar antinomias e excessivo custo de conformidade.

Existe uma dificuldade em se alcançar um padrão básico de “higiene cibernética”, em especial para aferir um grau mínimo de segurança em fornecedores e parceiros. Onde uma visão normativa mínima e horizontal entre os diferentes seguimentos de negócio contribuiria como processo de adequação do mercado com mitigação de riscos e prejuízos decorrentes de ataques em quantidade crescente, devido em muitos casos a baixa adequação de padrões mínimos de cibersegurança.

4 – Importante (Prioritário – pode esperar a curto prazo)

14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)

8. Dados Pessoais Sensíveis – Dados biométricos (Art. 5º, II da LGPD)

Temas importantes que devem ter regulação priorizada no curto prazo

O tratamento de dados pessoais – inclusive de dados sensíveis – para apoio a iniciativas de combate à fraude e para a proteção da vida ou da incolumidade física de clientes é prática essencial para as empresas do setor. São necessárias cooperações com autoridades de segurança e autoridades reguladoras, que exigem das instituições

7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	reguladas o tratamento de dados para garantir o bom andamento de atividades de segurança pública, de investigação e repressão de infrações penais e a higidez e confiança social no Sistema Financeiro Nacional. Portanto, é importante que a ANPD regulamente de forma prioritária a maneira como irá conduzir a emissão de opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do art. 4º da LGPD, com especial garantia de que tais opiniões e recomendações emergjam de um diálogo contínuo com as entidades do setor produtivo. Dados pessoais sensíveis – dados biométricos: Reconhecemos a relevância do tema, mas entendemos haver espaço para amadurecimento das práticas de mercado, inclusive com a criação de arranjos especializados de autorregulação sobre o tema. O uso de dados pessoais sensíveis em respeito à LGPD e outras normas, a exemplo de regulações expedidas pelo Banco Central do Brasil, é prática que vem se consolidando no mercado financeiro para combater fraudes, validação de identidades e proteção dos usuários de serviços financeiros. Ademais, esse tema poderá receber atenção específica quando da regulamentação de temas que já estão colocados na agenda regulatória atual, a exemplo do tema das bases legais, do relatório de impacto à proteção de dados (RIPD) e temas que poderão vir regulamentados no médio prazo, a exemplo das medidas e padrões de segurança. Peticionamento do titular de dados: A ausência de procedimento explícito em relação ao petitionamento dos titulares perante a ANPD, eventualmente atribuindo-se prazos para a autoridade se manifestar e maior clareza nos procedimentos, inclusive na forma de engajamento com os agentes de tratamento, é medida prioritária e que recomendamos a regulamentação no curto prazo.
3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	
	Temas razoavelmente importantes que devem ser regulamentados no médio prazo
12. Registro de Operações (Art. 37 da LGPD)	Registro de operações: A definição da forma e conteúdo dos registros de atividades de tratamento de dados pode ser regulamentada no médio prazo, em uma abordagem flexível que acolha práticas de mercado.
*. Diálogo institucional entre a ANPD e entidades supervisoras do SFN 3. Adequação progressiva de banco de dados (Art. 63 da LGPD) 9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)	Diálogo institucional ANPD e SFN: Recomendamos, ainda, na condição de tema “razoavelmente importante”, o estabelecimento de diálogo institucional entre a ANPD e as entidades normativas e supervisoras do Sistema Financeiro Nacional, a exemplo do Conselho Monetário Nacional (CMN), do Banco Central do Brasil e da Comissão de Valores Mobiliários, com o objetivo de promover a uniformização e convergência regulatória em temas como (i) comunicação de incidentes como dados pessoais no âmbito do Sistema de Pagamentos Brasileiro (SPB); (ii) segurança cibernética; (iii) contratação de serviços em nuvem e transferência internacional de dados; (iv) Open Finance e o direito de portabilidade no sistema financeiro, dentre outros. Dados legados: A regulamentação da adequação progressiva de banco de dados deve seguir-se ao amadurecimento das boas práticas de mercado, em especial com a definição adequada das bases legais e sua aplicabilidade às atividades de tratamento em diversos setores da economia. Assim, recomendamos que os dados legados recebam tratamento regulatório para a sua adequação no longo prazo. Termos de compromisso: Recomendamos a regulamentação do tema no médio prazo, após a definição das diretrizes da Política Nacional de Proteção de Dados e das Boas Práticas Regulatórias.
2 – Pouca importância (Neutro - pode esperar a longo prazo)	
1. Crianças e adolescentes (Art. 14 da LGPD)	Temas cuja regulação pode ocorrer no longo prazo

	Crianças e adolescentes: O tratamento de dados pessoais de crianças e adolescentes deve seguir as normas da LGPD e de legislações especiais aplicáveis, a exemplo do Estatuto da Criança e do Adolescente. Ao apontarmos esse tema como merecedor de regulação no longo prazo não estamos minimizando sua importância, mas que entendemos já haver disciplinamento razoável no ordenamento jurídico para se garantir o melhor interesse desses titulares de dados pessoais. Ademais, as regulamentações de outros temas prioritários da LGPD, a exemplo do relatório de impacto e das medidas de segurança, também servirão para robustecer a proteção dos direitos de titulares de dados menores de 18 anos. Compartilhamento de dados pelo Poder Público: Aqui servimo-nos de argumentação semelhante. Entendemos que a ANPD pode endereçar melhor o compartilhamento e uso compartilhado de dados pelo Poder Público no âmbito de suas orientações, guias e estudos técnicos. Regras de boas práticas e governança: A regulamentação das regras de boas práticas e governança é tema que deve se seguir após a conclusão de aspectos fundamentais do sistema nacional de proteção de dados pessoais, a exemplo da Política Nacional, das Boas Práticas Regulatórias e temas que já constam na agenda regulatória atual, como as bases legais e o relatório de impacto à proteção de dados (RIPD). Ademais, vemos a necessidade de se avançar em temas como padrões e medidas de segurança da informação e a consolidação da cooperação entre a ANPD e reguladores e supervisores do Sistema Financeiro Nacional. No transcurso da regulamentação desses e outros pontos, a ANPD poderá acompanhar junto aos setores regulados a evolução de suas regras setoriais de boas práticas e a consolidação de governanças de dados mais robustas, conforme mercado e sociedade aprendam com as experiências no tratamento de dados pessoais. Recomendamos que quando da regulamentação futura das regras de boas práticas e governanças, a ANPD já tenha consolidado precedentes importantes sobre como o mercado pode formular diretrizes e orientações e a forma como esses documentos podem ser legitimados junto ao órgão e demais titulares de dados interessados. No longo prazo, as entidades representativas do setor produtivo já terão conduzido alguns trabalhos relevantes, acompanhados pela ANPD, na busca de denominadores comuns sobre práticas de tratamento de dados de agudo interesse social, a exemplo de tratamento de dados para combate à fraude, uso de dados biométricos, segurança da informação e cooperação para investigações. A maturação desse processo será importante para o surgimento de ecossistemas de autorregulação mais robustos em favor dos direitos dos titulares e da inovação, tornando o trabalho de longo prazo da ANPD para a sua regulamentação uma atividade que pode extrair da experiência setorial para produzir normas mais efetivas.
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)	
1 – Nenhuma importância (Não há ou há pouca necessidade de regulamentação)	
5. Inteligência Artificial	Temas cuja regulação necessidade de regulamentação pode ser avaliada no longo prazo Inteligência Artificial: Entendemos que o tema de inteligência artificial é bastante amplo e ainda está sujeito a debates legislativos importantes, a exemplo das propostas de lei em trâmite no Congresso Nacional. Ademais, não está claro na tomada de subsídios da ANPD qual dimensão da inteligência artificial poderia ser objeto de regulamentação pela autoridade. Nesse sentido, recomendamos que esse tema não seja incorporado à agenda regulatória dos próximos anos. Ademais, a LGPD, em especial em seu artigo 20 e outros pontos, e outras normas como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e regulações prudenciais setoriais do Sistema Financeiro Nacional já endereçam aspectos relevantes da governança de modelos das instituições financeiras e assemelhadas.



DEFENSORIA PÚBLICA
DO ESTADO DO RIO DE JANEIRO

Ofício nº 15/NUDECON-PDP/2022 Rio de Janeiro, 30 de agosto de 2022.
(favor mencionar o número deste ofício ao responder)

DA: DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

NUDECON - Núcleo de Defesa do Consumidor

Departamento de Proteção de Dados Pessoais

Rua São José, 35 - 13º Andar - Terminal Garagem Menezes Côrtes, Centro, Rio de Janeiro/RJ, CEP: 20010-020 - Telefone: (21) 2868-2100, ramal 303

e-mail: nudecon.dadospessoais@defensoria.rj.def.br

PARA: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD

Esplanada dos Ministérios, Ministério da Economia, Bloco C, 2º andar, Brasília/DF, CEP: 70.297-400

e-mail: presidencia@anpd.gov.br

Ref.: Agenda Regulatória 2023/2024

Exmo. Sr. Waldemar Gonçalves Ortunho Júnior

DD. Diretor-Presidente da ANPD,

Os Defensores Públicos abaixo assinados, no uso de suas atribuições legais, respaldados nos arts. 5º, LXXVI, da Constituição da República, 178, IV, alínea “a”, da Constituição Estadual, 128, X, da Lei Complementar Federal nº 80/94, e 87, III, da Lei Complementar Estadual 06/77,

Considerando que a Constituição da República, em seu art. 5º, inciso LXXIV, impôs ao Estado o dever de prestar assistência jurídica integral e gratuita aos que comprovarem insuficiências de recursos, outorgando à Defensoria Pública a



função essencial à justiça de promover a orientação jurídica, os direitos humanos e a defesa, em todos os graus, judicial e extrajudicial, dos direitos individuais e coletivos, de forma integral e gratuita, aos necessitados (art. 134, da Constituição da República);

Considerando o fato do Núcleo de Defesa do Consumidor da Defensoria Pública – NUDECON – ser órgão da Defensoria Pública do Estado do Rio de Janeiro, criado especificamente para a defesa dos interesses e direitos protegidos pelo Código de Defesa do Consumidor, conforme a Deliberação CS nº 78/2011, devendo ser garantido o seu acesso a informações indispensáveis para a assistência jurídica integral e gratuita dos consumidores hipossuficientes ou em situação de vulnerabilidade, conforme garantia do art. 128, inciso X, da Lei Complementar 80/94, assegurando inclusive a prerrogativa de requisição de documentos necessários para o exercício de sua atribuição;

Considerando que o papel de proteção do consumidor pela Defensoria Pública, também está previsto na legislação específica de sua organização, sendo uma de suas funções institucionais “exercer a defesa dos direitos e interesses individuais, difusos, coletivos e individuais homogêneos e os direitos do consumidor, na forma do inciso LXXIV do art. 5º da Constituição Federal”, como previsto no inciso VIII do art. 4º da Lei Complementar nº 80/94;

Considerando que na legislação estadual há disposições no mesmo sentido, entre elas, a Constituição do Estado do Rio de Janeiro, que prevê como uma de suas funções institucionais o patrocínio dos “direitos e interesses do consumidor lesado” (art. 179, § 3º, V, alínea f), e o disposto no art. 22, § 3º, da Lei Complementar Estadual nº 6/77, pelo qual “aos Defensores Públicos incumbe também a defesa dos direitos dos consumidores que se sentirem lesados na aquisição de bens e serviços”;



Considerando que a Constituição da República prevê em seu artigo 5º, inciso LXXIX o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais;

Considerando que as Leis ns. 12.414/11 (Lei do Cadastro Positivo), 12.527/11 (Lei do Acesso à Informação), 12.965/14 (Marco Civil da Internet) e 13.709/2008 (Lei Geral de Proteção de Dados) introduziram no sistema brasileiro normas positivadas de proteção de dados pessoais e acesso à informação;

Considerando que, dentre as atribuições da Autoridade Nacional de Proteção de Dados (ANPD) previstas no artigo 55-J, da LGPD, estão “editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade” (inciso XIII) e “ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante” (inciso XIV);

Considerando o início do planejamento da agenda regulatória para o biênio 2023/2024, com a chamada da sociedade civil para tomada de subsídios através da plataforma *Participa+Brasil*¹;

Considerando que a Defensoria Pública do Estado do Rio de Janeiro, enquanto integrante do Sistema Nacional de Defesa do Consumidor, contribuiu para a formatação da agenda regulatória do biênio 2023/2024 através da plataforma indicada no item anterior, opinando acerca da importância dos temas pré-definidos pela ANPD;

Considerando que, além dos temas pré-definidos pela ANPD, a Defensoria Pública do Estado do Rio de Janeiro entende oportuno opinar sobre outros temas de interesse dos titulares de dados pessoais enquanto consumidores, para além dos 2000 caracteres disponibilizados na plataforma *Participa+Brasil*,

¹ [A Agenda Regulatória da ANPD para o biênio 2023–2024 já está em fase de planejamento — Português \(Brasil\) \(www.gov.br\)](#). Acesso em 29 de agosto de 2022.



OFICIAM

a V. Exa. para sugerir outros temas de relevância para integrar a agenda regulatória do biênio 2023/2024, submetendo-os à apreciação desta Agência Reguladora e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, consoante as justificativas que seguem:

- 1) Dados pessoais tornados públicos pelos titulares para fins de prestação da tutela jurisdicional, em virtude do princípio constitucional da publicidade dos atos judiciais (art. 7º, § 4º, LGPD; art. 93, IX, da CRFB) – Plataformas de compilação de informações processuais – Finalidades das empresas que prestam o serviço e das parceiras comerciais – Tema 1.141 do STF.**

Justificativa: A Defensoria Pública do Estado do Rio de Janeiro entende relevante a regulamentação da matéria, inicialmente em razão da própria relevância da questão constitucional e do reconhecimento da existência de repercussão geral pelo Supremo Tribunal Federal quando da apreciação dos requisitos de admissibilidade do Recurso Extraordinário com Agravo nº 1.307.386/RS, em que são partes as empresas Potelo Sistemas de Informação Ltda. – ME (plataforma Escavador), Goshme Soluções para a Internet Ltda. – ME (plataforma JusBrasil) e Google Brasil Internet Ltda., evidenciando a litigiosidade do tema.

Importante asseverar também que, dentre os princípios regentes da atividade de tratamento de dados pessoais, estão a finalidade, a adequação e a necessidade (art. 6º, I, II e III, da LGPD), motivo pelo qual o princípio da publicidade dos atos judiciais deve ser ponderado com o direito fundamental à proteção de dados pessoais, máxime quando a publicidade do ato judicial importa em publicização dos dados pessoais para além da finalidade almejada pelo seu titular, qual seja, a prestação da tutela jurisdicional.

A partir do momento em que as empresas que coletam, compilam e disponibilizam informações processuais não atuam apenas no interesse do



titular do dado pessoal, mas, principalmente, em seus interesses comerciais², portanto, com finalidade distinta daquela vislumbrada pelo titular do dado pessoal e que resultou na publicidade de seus dados, mister se faz regulamentar a questão para proteção dos dados pessoais dos titulares, impedindo que a compilação das informações processuais de processos públicos atinja finalidade distinta e viole os dados pessoais dos jurisdicionados brasileiros.

2) Uso compartilhado de dados pessoais (art. 5º, XVI, LGPD) – Empresas do mesmo grupo econômico com finalidades distintas – Dados pessoais e dados sensíveis tratados com base legal no consentimento (art. 7º, I, e art. 11, I, e § 3º, da LGPD).

Justificativa: Ainda objetivando a observância dos princípios da finalidade, adequação e necessidade, revela-se oportuno e importante regulamentar as hipóteses em que os dados pessoais dos titulares são compartilhados entre as empresas do mesmo grupo econômico, haja vista que a principal base legal para tratamento é o consentimento do titular enquanto consumidor e para a finalidade inicial por ele vislumbrada, não autorizando o tratamento de seus dados pessoais para finalidade diversas e que digam respeito aos demais objetos empresariais das outras empresas do mesmo grupo econômico.

A importância da questão ganha maior vulto quando se observa este compartilhamento entre empresas que tratam dados pessoais sensíveis, como os dados de saúde do titular, o que revela não apenas a violação do princípio da finalidade, como a possibilidade de manipulação de dados excessivos com vistas ao interesse lucrativo do grupo econômico, com a possibilidade de perfilamento, segmentação de mercado, discriminação, precificação, predição de consumo, o que se deve impedir.

² Ver os Termos de uso, Políticas de Privacidade e Modelos de Negócios objetivados pelas empresas em:
[Escavador - Seu assistente jurídico](#)
[Jusbrasil - Informação Jurídica que Transforma](#)
[Google](#)



- 3) **Autoridades com poder legal de requisição e órgãos integrantes do Sistema Nacional de Defesa do Consumidor (arts. 105 e 106, CDC) – Defensorias Públicas³, Ministérios Públicos, Procons – Prerrogativa de requisição de informações no interesse do titular de dados pessoais enquanto consumidor, para efetivação do direito de petição e de acesso à justiça (art. 5º, XXXV e LXXIV, CRFB e art. 2º, VI, e art. 18, §§ 1º e 8º, LGPD) – Prazos para soluções de reclamação ao controlador (art. 55-J, V, LGPD).**

Justificativa: Visando ao efetivo acesso à justiça e à assistência jurídica a serem assegurados ao titular de dados pessoais enquanto consumidor, na tutela de seu direito fundamental à proteção de dados pessoais e do seu direito de petição, os Órgãos de Defesa do Consumidor integrantes do Sistema Nacional têm a prerrogativa de requisitar informações e solicitar documentos, sem os quais a assistência jurídica resta inviabilizada.

Desta feita, mister se faz regular o exercício da prerrogativa de requisição tanto das autoridades com poder legal de requisição quanto dos órgãos integrantes do SNDC, fixando-se prazo para resposta às requisições e a respectiva sanção pelo descumprimento da solicitação.

Outrossim, mostra-se importante a regulamentação da norma do art. 55-J, V, da LGPD, fixando-se o prazo para solução das reclamações dirigidas pelo titular ao controlador e a respectiva sanção a ser aplicada pela ANPD para a hipótese de descumprimento.

- 4) **Compartilhamento de dados sensíveis de saúde entre pessoas jurídicas de direito público (SUS) e de direito privado (saúde suplementar) – Art. 27, da LGPD.**

Justificativa: O uso compartilhado de dados sensíveis de saúde deve objetivar única e tão somente o interesse do titular, e, por tal razão, deve o titular ser previamente informado sobre todos os detalhes da operação de compartilhamento, para que possa exercer o seu direito de escolha e

³ Vide STF, ADI 6.852 em [Supremo Tribunal Federal \(stf.jus.br\)](https://stf.jus.br). Acesso em 29 de agosto de 2022.



consentir validamente com fundamento na autodeterminação informativa, impedindo que o uso compartilhado atenda apenas aos interesses empresariais e lucrativos das empresas que operam no sistema de saúde suplementar, como perfilamento, precificação segmentada, discriminação e indução de consumo.

Por tais razões, revela-se a importância da inclusão do art. 27, da LGPD, na agenda regulatória do setor econômico de Saúde, ampliando a regulamentação dos arts. 11, § 4º, e 13, da LGPD, sugerida no item 15 da tomada de subsídios da Plataforma *Participa+Brasil*.

- 5) Contratos internacionais firmados entre lojas de aplicativos e desenvolvedores – Aplicação da lei brasileira de proteção da privacidade e dos dados pessoais – Ineficácia das disposições que elegem a legislação e jurisdição estrangeiras – Vedação a objetos contratuais que contrariem a CRFB, o MCI e a LGPD (art. 3º, LGPD; art. 11, MCI; art. 17, LINDB) ou afastem a competência da Justiça brasileira (art. 21, incisos II e III, do CPC c/c do art. 2º, da Lei nº 7.347/85, e do art. 101, I, do CDC).**

Justificativa: Via de regra, os contratos firmados entre os desenvolvedores de aplicações de internet e as grandes empresas de tecnologia, que oferecem essas aplicações nas chamadas “lojas de aplicativos” aos consumidores brasileiros, estes, destinatários finais dos produtos, preveem em suas cláusulas a aplicação da legislação estrangeira e a adoção da jurisdição internacional para a solução de conflitos⁴.

Todavia, quando o tratamento dos dados pessoais atrai a legislação brasileira (art. 3º, LGPD, e art. 11, MCI), as lojas de aplicativos e os desenvolvedores devem observar a legislação nacional, seja porque a legislação estrangeira não pode ser aplicada sob pena de ofender a soberania nacional (art. 17, LINDB), seja por se tratar de matéria de ordem

⁴ Vide, como exemplos:

[Apple Developer Program License Agreement \(Portuguese - Brazil\)](#). Acesso em 29 de Agosto de 2022.
[Google Play](#). Acesso em 29 de agosto de 2022.



pública a possível violação do direito fundamental à proteção de dados pessoais de brasileiros ou de pessoas sujeitas à soberania e à jurisdição brasileira.

Por consequência, as aplicações de internet desenvolvidas e colocadas à venda nas lojas de aplicativo para o mercado brasileiro devem obedecer à legislação nacional de proteção da privacidade e dos dados pessoais, motivo pelo qual tanto as grandes empresas de tecnologia quanto os desenvolvedores não podem colocar à disposição do mercado brasileiro produtos ou serviços que violem a Constituição da República, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet, a Lei Geral de Proteção de Dados, e as demais leis protetivas dos titulares de proteção de dados pessoais.

Essa é uma das questões debatidas pela Defensoria Pública e pelo Ministério Público do Estado do Rio de Janeiro na ação civil pública em trâmite na 2ª Vara Empresarial da Capital sob o nº 0062675-25.2022.8.19.0001⁵, sendo certo que o Supremo Tribunal Federal, no âmbito da apuração de ilícito penal no inquérito de combate à desinformação nº 4.781/DF⁶, reconheceu a aplicação da lei brasileira e a soberania nacional às aplicações de internet desenvolvidas por empresas estrangeiras e que chegam ao Brasil através das lojas de aplicativos, mediante contratos internacionais.

Assim, a matéria assume grande importância a merecer a devida atenção na agenda regulatória desta Autoridade Nacional, com o fito de reafirmar a soberania nacional e a aplicação da lei brasileira.

⁵ [inicial_acp_assinado_assinado_assinado_assinado.pdf \(mprj.mp.br\)](#). Acesso em 29 de agosto de 2022.
[Portal de Serviços \(tjrj.jus.br\)](#). Acesso em 29 de agosto de 2022.

⁶ [Supremo Tribunal Federal \(stf.jus.br\)](#). Acesso em 29 de agosto de 2022.

[Leia a íntegra da decisão que determinou o bloqueio do Telegram no Brasil | Política | G1 \(globo.com\)](#). Acesso em 29 de agosto de 2022.

[DecisaoTelegram20mar.pdf \(stf.jus.br\)](#). Acesso em 29 de agosto de 2022.



DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

Sendo estas as sugestões da Defensoria Pública do Estado do Rio de Janeiro, e certos do atendimento que ora se faz necessário, os defensores públicos signatários aproveitam a oportunidade para apresentar a V. Exa. protestos de elevada estima e consideração.

Atenciosamente,

Eduardo Chow de Martino Tostes
Defensor Público - NUDECON

[REDACTED]

Thiago Henrique Basilio
Defensor Público - NUDECON
Mat. nº 949.573-0

Adriana Araujo João
Defensora Pública - NUDECON

[REDACTED]

TOMADA DE SUBSÍDIOS - AGENDA REGULATÓRIA 2023-2024

Considerações Preliminares:

A Câmara Brasileira de Economia Digital (“Câmara-e.net”) gostaria de saudar a Autoridade Nacional de Proteção de Dados (“ANPD”) pela importante iniciativa de lançar a esta tomada de subsídios para o colher contribuições da sociedade sobre os temas a serem inclusos na Agenda Regulatória referente ao biênio 2023-2024. A presente entidade concorda integralmente com a perspectiva da ANPD de que a Agenda Regulatória é um instrumento essencial para fins de organização, planejamento e execução das ações de normatização pela Autoridade, bem como para possibilitar o acompanhamento, pela sociedade e pelos agentes regulados, do processo normativo, garantindo maior publicidade, previsibilidade, transparência e segurança jurídica. No ímpeto de contribuir para esses objetivos, a Câmara-e.net oferece respeitosamente suas considerações gerais acerca da tomada de subsídios, bem como sugestões para aprimoramento.

Como destacado na [Nota Técnica nº 31/2022/CGN/ANPD](#), a Agenda Regulatória da ANPD, referente ao biênio 2021-2022, foi publicada por meio da [Portaria nº11/2021](#). No referido ato normativo foram elencados dez temas que deveriam ser iniciados no processo de normatização dentro daquele período, sendo que, pelo [Relatório de Acompanhamento e Execução da Agenda Regulatória para o biênio 2021-2022](#), divulgado em julho de 2022, ficou evidenciado que, apesar de alguns temas terem tido o processo de normatização devidamente iniciado, cinco deles ainda precisam ter o processo finalizado, são eles: (1) estabelecimento de normativos para aplicação do art. 52 e seguintes da Lei Geral de Proteção de Dados Pessoais (“LGPD”) - norma de sanção e dosimetria; (2) comunicação de incidentes e especificação do prazo de notificação; (3) relatório de impacto à proteção de dados pessoais; (4) encarregado de proteção de dados pessoais; e (5) transferência internacional de dados pessoais.

A Câmara-e.net reconhece os esforços desta Autoridade no que tange à conclusão da normatização da maioria dos temas elencados na Agenda Regulatória do biênio 2021-2022, contudo, considerando o início de mais um ciclo normativo, é importante frisar a necessidade de priorização da finalização dos processos normativos dos temas iniciados no biênio 2021-2022 em relação aos temas que forem eleitos para o biênio 2023-2024. Em adição, visando aumentar a previsibilidade, a transparência e a segurança jurídica, a Câmara-e.net sugere que na Agenda Regulatória referente ao biênio 2023-2024 haja previsão também de prazo para finalização do processo normativo de cada um dos temas ou, alternativamente, nos moldes do Relatório mencionado, que haja indicação de previsão para: o termo de abertura de projeto de regulamentação, a tomada de subsídios, a consulta interna, a análise de impacto regulatório, a consulta pública e audiência pública, a análise jurídica e a deliberação pelo Conselho Diretor.

A Câmara-e.net ainda entende que alguns dos temas trazidos pela ANPD na presente tomada de subsídios já estariam abarcados em temas presentes na Agenda Regulatória do Biênio 2021-2022. Nesse sentido, entendemos que a temática do direito de peticionamento pelo titular de dados pessoais (art. 18, § 1º da LGPD) deve ser devidamente abordada pela resolução que tratará dos direitos dos titulares dos dados pessoais. Da mesma

forma, seria importante que os “termos de compromisso” com agentes de tratamento (Art. 55-J, XVII da LGPD) sejam devidamente abordados na normativa que versará sobre a aplicação do art. 52 e seguintes LGPD.

Outra questão que gostaríamos de destacar é a necessidade de priorização, pela ANPD, da normatização de temas estruturantes gerais, diminuindo-se assim as incertezas quanto ao mais adequado cumprimento da LGPD, para que posteriormente possa se discutir a aplicação em setores econômicos específicos. Depois sejam regulamentados temas específicos, bem como de setores econômicos especializados. Em contraponto, ressalta-se a importância da normatização de boas práticas regulatórias, um norteador para as atividades da Autoridade.

Por fim, antes de passar propriamente à classificação dos temas abaixo, destacamos alguma preocupação com o formato apresentado para tomada de subsídios que podem levar a uma distorção na avaliação das contribuições apresentadas, tendo em vista que alguns dos temas, muito embora sejam importantes, não devem ser - no momento - objeto de estudo e regulamentação pela ANPD, tal como inteligência artificial, temática que ainda é objeto de tramitação legislativa. Neste sentido, cabe elucidar que as notas, atribuídas aos assuntos pela Câmara-e.net, tomaram como base a noção de prioridade, caracterizada, de forma crescente, por: (1) desnecessidade ou pouca necessidade de regulamentação, (2) necessidade de regulamentação a longo prazo, (3) necessidade de regulamentação a médio prazo, (4) necessidade de regulamentação a curto prazo e (5) necessidade de regulamentação urgente e prioritária.

Legenda da Classificação:



TEMA	CLASSIFICAÇÃO	JUSTIFICATIVA
1. Crianças adolescentes (Art. 14 da LGPD)	5	O tratamento de dados pessoais de crianças e de adolescentes é um tema que exige urgente e prioritária normatização, não só por sua evidente relevância, mas especificamente pela falta de clareza quanto às bases legais que podem ser utilizadas para esse tipo de tratamento, bem como sobre qual seria o recorte etário para aplicabilidade da Seção III da LGPD.

2. Regulação - Setor econômico de Educação	2	Entende-se que a regulação do setor econômico da educação pode esperar a longo prazo para normatização, para que haja a priorização da de temas mais gerais e de maior impacto, bem como para que haja tempo hábil para o desenvolvimento e amadurecimento de boas práticas pelo setor.
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)	1	Considerando a passagem de quase dois anos desde que a LGPD entrou em vigor, a temática de adequação progressiva de banco de dados perdeu relevância, sendo assim-, entende-se que o tema não é prioridade.
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)	3	Entendemos que boas práticas e de governança são absolutamente essenciais para a plena adoção da LGPD pela sociedade. Nesse sentido, a adoção de guias orientativos pela ANPD poderá ser uma ação bastante positiva da Autoridade, no sentido de orientar a sociedade na melhor aplicação da lei. Preocupa, no entanto, a edição de normativos que venham a limitar os princípios assegurados na LGPD de <i>accountability</i> dos agentes de tratamento, com suas respectivas avaliações de risco e adoção de salvaguardas cabíveis.
5. Inteligência Artificial	1	Apesar da importância inegável da temática, entende-se que os sistemas de inteligência artificial não devem ser objeto de normatização pela ANPD, especialmente enquanto não houver lei aplicável ao tema. Neste sentido, destaca-se que atualmente a Comissão de Juristas Responsável por Subsidiar a Elaboração de Minuta de Substitutivo aos Projetos de Lei sobre Inteligência Artificial (“CJUSBIA”) ainda está redigindo e consolidando os subsídios para instruir as discussões legislativas sobre o tema.. É importante ressaltar que um dos pontos a serem definidos pelo substitutivo é se haverá (ou não) um órgão responsável pela regulamentação da inteligência artificial, quais seriam suas atribuições, se esse órgão deveria ser centralizado ou não, etc.

6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)	3	2
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	4	Entende-se que a temática de peticionamento do titular de dados deveria ser um aspecto da regulamentação específica sobre direitos dos titulares, e não deverá ser endereçada como um item autônomo na agenda regulatória. A resolução que tratará dos direitos dos titulares dos dados pessoais já é tema integrante da Agenda Regulatória de 2021-2022 e deverá efetivamente ser uma prioridade na atuação da Autoridade, tendo em vista os inúmeros desafios enfrentados por agentes de tratamento na falta de clareza sobre a implementação dos direitos dos titulares previstos na LGPD.
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)	3	Entende-se que o tema necessita de normatização a médio prazo, isso porque seria importante ter orientações da Autoridade sobre os contextos nos quais a coleta de dados sensíveis seria legítima, especialmente de dados biométricos no contexto de autenticação do titular para evitar os altos índices de fraude atualmente enfrentados por muitos agentes de tratamento.
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)	3	Como ressaltado acima, entende-se que o tema deveria ser tratado juntamente com a normativa que versará sobre a aplicação do art. 52 e seguintes LGPD, constante da Agenda Regulatória de 2021-2022. Isso porque é importante que haja a possibilidade de celebração de termo de compromisso com os agentes de tratamento, como uma alternativa à eventual imposição de sanção administrativa pela ANPD, nos processos administrativos decorrentes dos seus poderes fiscalizatório e sancionador.. Nesse sentido, apesar da indicação de que a normatização do tema pode esperar a médio prazo, salienta-se que essa relevância aumentará caso o tema não seja abordado no processo normativo que busca regulamentar a dosimetria das sanções administrativas.
10. Boas Práticas Regulatórias	5	Compreende-se o tema como urgente e prioritário, tendo em vista que normas que orientem boas práticas regulatórias são

		extremamente relevantes para aprimorar a organização, planejamento e execução das ações de normatização, bem como para aumentar a qualidade, a transparência, a tecnicidade e previsibilidade do processo normativo, gerando maior segurança jurídica aos administrados.
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)	3	Entende-se que a temática pode esperar a médio prazo para regulamentação, mas que sua relevância aumenta com a finalização da normativa que versará sobre a aplicação do art. 52 e seguintes LGPD. Ressalta-se, contudo, o entendimento de que a ANPD não deve estabelecer padrões técnicos mínimos de segurança, porquanto cabe ao agente de tratamento adotar as medidas que entenderem adequadas às suas atividades e necessidades. Ademais, o estabelecimento de padrões mínimos engessaria a própria evolução das medidas de segurança em constante desenvolvimento.
12. Registro de Operações (Art. 37 da LGPD)	1	É o entendimento da Câmara-e.net que a temática de registro de operações não deve ser objeto de normativa pela ANPD, dado que deve ficar a cargo dos agentes de tratamento a definição dos seus processos de registro. Porém, poderia a Autoridade disponibilizar guias orientativos para fins de instrução pautados em modelos internacionais de referência.
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	5	Entende-se o tema como prioritário e urgente, especialmente considerando casos recentes que dizem respeito à temática, a exemplo do processo fiscalizatório instaurado pela presente Autoridade para apurar a adequação da Portaria RFB nº 167/2022 à LGPD.
14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)	1	Entende-se que a ANPD não deve emitir quaisquer opiniões técnicas ou recomendações sobre a temática, tendo em vista que a LGPD deferiu à temática reserva de lei específica, nos termos do art. 4º, inciso III, §1º.
15. Regulação - setor econômico de Saúde (Art. 11, § 4º; Art. 13 da LGPD)	2	Entende-se que a regulação do setor econômico da saúde pode esperar a longo prazo para normatização, para que haja a priorização de temas mais gerais e de maior impacto, bem como o

		decorso de tempo necessário para o desenvolvimento e amadurecimento de boas práticas pelo setor.
--	--	--

CONTRIBUIÇÕES DA BRASSCOM EM RESPOSTA À TOMADA DE SUBSÍDIOS DA ANPD SOBRE SUA AGENDA REGULATÓRIA PARA O BIÊNIO 2023-2024

Agosto de 2022

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (TIC), entidade que congrega empresas fornecedoras de software, aplicações de Internet, soluções e serviços de TIC e que tem como missão trabalhar em prol do desenvolvimento do setor, disseminando seu alcance e potencializando seus efeitos sobre a economia e o bem-estar social, parabeniza a Autoridade Nacional de Proteção de Dados (ANPD) pela abertura de tomada de subsídios visando à coleta de contribuições da sociedade para a elaboração da Agenda Regulatória para o biênio 2023–2024.

De início, entendemos como relevante esclarecer que a atribuição das notas concedidas aos temas listados levou em consideração a necessidade iminente ou não da regulamentação desses assuntos pela ANPD neste próximo biênio, porém não significa que as matérias que receberam notas baixas não tenham importância para os associados da Brasscom. As notas atribuídas, portanto, tiveram como critério a relevância do tema somada à prioridade regulatória em termos de prazo. Alguns assuntos, por exemplo os relacionados à regulação setorial, como educação e saúde, receberam notas baixas, eis que, apesar de serem considerados importantes, em nosso entendimento, não existe uma urgência para a sua regulamentação no momento. No entanto, é oportuno informar que a Brasscom também considerou que alguns tópicos listados não deveriam ser regulamentados pela ANPD, pelos diversos motivos que exploramos abaixo.

Por oportuno, ressaltamos a importância de que os processos regulatórios dos temas da Agenda Regulatória 2021-2022 sejam priorizados àqueles que serão definidos para o biênio 2023-2024. O objetivo, para tanto, é direcionar os esforços conforme a agenda regulatória do contexto

atual, conferir tempo hábil para que todos os atores possam contribuir de forma efetiva e com a técnica necessária para os assuntos ainda pendentes de regulamentação.

Sendo assim, de forma complementar às respostas que apresentamos através da Plataforma Participa + Brasil, a Brasscom, a fim de pontuar essas questões adicionais, respeitosamente apresenta à ANPD seus comentários.

TOMADA DE SUBSÍDIOS SOBRE AGENDA REGULATÓRIA DA ANPD PARA O BIÊNIO 2023-2024 ¹		
1. Crianças e adolescentes (Art. 14 da LGPD)	Nota 5	A Brasscom entende que é um assunto de extrema relevância, pela própria natureza do tema, pela dificuldade de compreensão das regras aplicáveis às crianças e aos adolescentes, bem como das bases legais admissíveis pela legislação brasileira no tratamento dos dados pessoais desses titulares. Logo, existe urgência em sua regulamentação, de modo a conferir maior segurança jurídica aos agentes de tratamento que realizem suas atividades utilizando dados de crianças e adolescentes.
2. Regulação - Setor econômico de Educação	Nota 1	Existem alguns pontos na LGPD, de aplicabilidade geral, que ainda não foram regulamentados pela ANPD. Tendo em vista a limitação de pessoal da Autoridade, a Brasscom entende que temas mais básicos de implementação da LGPD devem ser

¹ Avalie os temas segundo grau de importância, sendo:

- 1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação)
- 2 - Pouca importância (Neutro - pode esperar a longo prazo)
- 3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)
- 4 - Importante (Prioritário - pode esperar a curto prazo)
- 5 - Muito importante (Urgente e prioritário)

		priorizados, deixando para uma oportunidade futura os processos de regulamentação voltados para setores específicos, como a Educação.
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)	Nota 1	Esse tema se apresenta extremamente complexo pela sofisticação técnica que envolve, sendo difícil antecipar e/ou endereçar em um ato normativo todas as problemáticas que dele podem decorrer, não apresentando relevância para ser regulamentado no próximo biênio e sequer para ser regulamentado, tendo em vista o decurso do tempo desde a aprovação da LGPD.
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)	Nota 2	A uniformização das regras de boas práticas e de governança, ainda que mínimas, é desafiadora e absolutamente relevante para uma ampliação na plena adoção da LGPD e o acultramento da sociedade. No entanto, entendemos que tal uniformização não deve vir pela via normativa, e sim por construção setorial, refletindo as especificidades dos setores e respectivos modelos de negócios envolvendo o tratamento de dados pessoais. Esse tema é relevante para fins de conscientização da forma de tratamento adequado dos dados pessoais, razão pela qual iniciativas educacionais da ANPD serão mais eficazes do que a regulamentação propriamente dita do tema.
5. Inteligência Artificial	Nota 1	A LGPD, em seu artigo 20, conferiu atribuição à ANPD para a discussão específica sobre inteligência artificial, mais especificamente sobre decisões automatizadas. Entretanto, falta clareza a respeito da amplitude regulamentar da Autoridade para tratar desta e das múltiplas dimensões inerentes ao tema. O assunto é de extrema relevância, porém, vem sendo discutido no Poder Legislativo Federal, fórum próprio para um debate mais amplo e estruturado do assunto. Portanto, entendemos que, enquanto não houver um marco legal próprio da inteligência artificial, não deveria a ANPD priorizar esse tema na sua agenda regulatória.

6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)	Nota 3	Embora exista uma dificuldade de compreensão do que deveria ser abordado em uma Política Nacional de Proteção de Dados Pessoais, entendemos que, como as diretrizes podem trazer a delimitação e direcionamento sobre o tratamento de dados pessoais, em especial, para fins de políticas públicas e compartilhamento de dados pessoais oriundos do Poder Público, devem ser consideradas um assunto razoavelmente importante e que merecem atenção da ANPD no próximo biênio.
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	Nota 5	Esse tema já foi levado ao conhecimento da ANPD pela Brasscom anteriormente e se apresenta extremamente importante. Todavia, consideramos ser um tema inseparável do “exercício dos direitos dos titulares”, assunto já inserido na Agenda Regulatória da ANPD do biênio 2021-2022. Os associados da Brasscom se deparam com inúmeras dúvidas e dificuldades no atendimento de pedidos de titulares que geram insegurança jurídica do mercado quanto aos requisitos necessários para o exercício legítimo de um direito e a forma de atendimento adequado aos pedidos formulados. Dentre as principais questões, estão (i) a maneira segura de conferir a autenticidade a um pedido formulado por um titular; (ii) os limites, em especial, do direito de acesso; (iii) possibilidade ou não de recusa de pedidos quando excessivos e repetitivos; (iv) na hipótese de direito exercido por terceiros, qual o detalhamento que deve ser exigido na procuração para se atender corretamente o pedido, evitar fraudes e/ou incidentes de segurança, dentre diversas outras. Logo, de fundamental importância e prioridade regulatória estão, conjuntamente, tanto o peticionamento do titular, como a forma de exercício e limites dos seus direitos.
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)	Nota 4	A dificuldade de se compreender o conceito de dados biométricos, os limites e possibilidades de sua utilização restringem demasiadamente a atividade dos agentes de tratamento, mais uma vez, pela insegurança jurídica que gera. A coleta da biometria é de fundamental importância para se evitar fraudes e uma salvaguarda relevante para a

		segurança do titular. Deste modo, é um tema que precisa ser regulamentado pela ANPD no biênio 2023-2024 com considerada prioridade.
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD) – “TAC”	Nota 5	Antes de a Brasscom indicar a classificação regulatória do assunto, é necessário trazer à atenção da ANPD sobre o termo utilizado nesta Tomada de Subsídios. Embora a ANPD tenha trazido expressão “compromisso” da LGPD (artigo 55-J, inciso XVII), esse assunto foi abordado no Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD (RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021), quando se utilizou a expressão “Termo de Ajustamento de Conduta”, em seu artigo 44. Deste modo, para evitar equívocos de interpretação e facilitarmos a compreensão da Lei e da atuação da ANPD, sugerimos que seja utilizada a expressão já consagrada na Resolução nº1/2021 da ANPD. De todo modo, como é um assunto relacionado ao processo fiscalizatório, tema que foi regulamentado pela Autoridade e que, inclusive possui consulta pública aberta no tocante à dosimetria da sanção administrativa, entendemos que é um assunto de relevância para ser regulamentado no biênio 2023-2024.
10. Boas Práticas Regulatórias	Nota 5	O estabelecimento de boas práticas regulatórias na ANPD é fundamental para a compreensão ampla da atividade regulamentar da Autoridade e para o atendimento dos princípios constitucionais que regem a Administração Pública, em especial, os princípios da publicidade (transparência), da impessoalidade e eficiência na atuação administrativa. A demonstração dos passos a serem seguidos e dos aspectos considerados pela ANPD acerca de um assunto a ser regulamentado pela Autoridade amplia a participação democrática na construção do ato normativo. Um exemplo de boas práticas regulatórias a ser considerado é o da ANATEL que, em seu guia, aborda quando e quais são os instrumentos utilizados - por exemplo, o Relatório de Impacto Regulatório, a Tomada de

		Subsídios, a Consulta Pública - como meios de coleta de informações e solicitação de esclarecimentos da sociedade, bem como os objetivos por ele alcançados no processo regulatório, o que confere segurança jurídica àqueles afetados e/ou interessados no tema. Deste modo, considerando o momento de detalhamento normativo da LGPD, a edição de um Guia de Boas Práticas Regulatórias tem uma relevância considerável para a agenda regulatória do próximo biênio.
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)	Nota 2	Na definição de padrões mínimos de medidas técnicas e administrativas existem diversas variáveis no tocante ao tratamento de dados pessoais que devem ser considerados, como, por exemplo, a natureza dos dados tratados, as características específicas do tratamento segundo os agentes de tratamento e o estado atual da tecnologia. A edição de regulamento no tema poderá engessar um assunto que está em constante evolução ante os desafios que o tratamento de dados atualmente enfrenta. Portanto, a Brasscom entende ser oportuna a atuação educacional da ANPD neste assunto com a elaboração de guias orientativos pautados em referências internacionais como melhores práticas em segurança da informação.
12. Registro de Operações (Art. 37 da LGPD)	Nota 3	Entendemos que o registro das operações é um assunto a ser tratado internamente por cada corporação ou agente de tratamento, e que diz respeito à observância do princípio de prestação de contas, com reflexos diretos na responsabilização. Não seria recomendável, portanto, que o tema fosse regulamentado pela ANPD na medida em que os agentes de tratamento devem ter liberdade para desenvolver os seus processos internos, inclusive o de registro de operações, que melhor se adequem às suas estruturas, ou ter a liberdade de opção dentre as soluções disponíveis no mercado. Contudo, para fins de instrução, a ANPD poderia disponibilizar guias orientativos para que possam servir como diretrizes ao mercado nesse tema.

13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	Nota 4	Esse assunto está em grande evidência no momento, pois há inúmeras discussões relevantes e atuais sobre aspectos que envolvem o tema, como, por exemplo, a polêmica de privatização ou não do Serpro, o Projeto de Lei nº 2224 (de dados abertos), a nova Portaria da Receita Federal do Brasil nº 167/2022 (sobre o compartilhamento tratados pelo SERPRO com terceiros). A relevância dessa temática foi, ainda, reforçada com a Nota Técnica nº 68/2022 da ANPD que pouco esclareceu em quais condições poderia ocorrer o compartilhamento de dados pessoais pelo poder público, inclusive a realização das comunicações atreladas cabíveis. Sendo assim, ante a falta de clareza e a insegurança que o desconhecimento dessa matéria gera nos administrados, é importante sua regulamentação pela ANPD no próximo biênio.
14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)	Nota 1	Considerando que o artigo 4º da LGPD traz exceções à sua aplicabilidade, a Brasscom entende não ser cabível a regulamentação do tema pela ANPD que, portanto, carece de competência regulamentar da matéria. Referido assunto vem sendo trabalhado em projetos de lei em tramitação no Congresso Nacional, esfera apropriada para sua abordagem e concretização.
15. Regulação - setor econômico de Saúde (Art. 11, § 4º; Art. 13 da LGPD)	Nota 1	Nesse aspecto, apresentamos os mesmos argumentos trazidos para o tópico “2” acima, no sentido de que a LGPD ainda carece de regulamentação em temas básicos, antes de setores específicos, como a Saúde, serem normatizados pela ANPD. Considerando a limitação de pessoal da ANPD e a necessidade de um melhor amadurecimento do tema, é um assunto que pode aguardar a regulamentação futura da Autoridade.

**À COORDENAÇÃO-GERAL DE NORMATIZAÇÃO DA AUTORIDADE NACIONAL
DE PROTEÇÃO DE DADOS (CGN/ANPD)**

São Paulo, 31 de agosto de 2022

**Ref. Tomada de Subsídios para elaboração da Agenda Regulatória da ANPD para o
biênio 2023-2024**

Prezadas e prezados,

O Idec - Instituto Brasileiro de Defesa do Consumidor é uma associação de consumidores, sem fins lucrativos, independente de empresas, partidos ou governos. Fundada em 1987 em São Paulo/SP, sua missão é a defesa dos consumidores, na sua concepção mais ampla, representando-os nas relações jurídicas de qualquer espécie, promovendo a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica. Desde a sua fundação, o Idec tem atuado na defesa do consumidor, com uma incidência ativa para a aprovação de importantes leis consumeristas, tais como o Código de Defesa do Consumidor, em 1990.

Considerando seu histórico de [atuação no setor de proteção de dados pessoais](#), o Idec vem apresentar suas contribuições para a Tomada de Subsídios para elaboração da Agenda Regulatória da ANPD para o biênio 2023-2024¹.

¹ Contribuíram com as respostas: Luã Cruz, Juliana Oms e Camila Leite Contrí.

Avalie os temas segundo grau de importância, sendo:

1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação)

2 - Pouca importância (Neutro - pode esperar a longo prazo)

3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)

4 - Importante (Prioritário - pode esperar a curto prazo)

5 - Muito importante (Urgente e prioritário)

Contribuição do Idec - Instituto Brasileiro de Defesa do Consumidor

Temas	Grau de importância				
	1	2	3	4	5
1. Crianças e adolescentes (Art. 14 da LGPD)					
2. Regulação - Setor econômico de Educação					
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)					
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)					
5. Inteligência Artificial					
6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)					
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)					
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)					
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)					

10. Boas Práticas Regulatórias	1	2	3	4	5
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)	1	2	3	4	5
12. Registro de Operações (Art. 37 da LGPD)	1	2	3	4	5
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	1	2	3	4	5
14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)	1	2	3	4	5
15. Regulação - setor econômico de Saúde (Art. 11, § 4º; Art. 13 da LGPD)	1	2	3	4	5

Sobre quais outros temas (4-importantes ou 5-muito importantes) você gostaria que a ANPD considerasse na elaboração da próxima Agenda Regulatória? Favor, justificar a necessidade.

1. Regulação do setor econômico de Finanças, com foco na análise de crédito (Art. 7º, X; Art. 20 da LGPD)

A análise de crédito, intensiva em dados e tratamento automatizado, já possuía diversos problemas, em especial de transparência e explicabilidade na pontuação de crédito e limites abertos de quais dados e fatores podem constituir-la, que merecem atenção da ANPD, especialmente pela regulação do art. 20.

O inciso X do art. 7º criou uma nova hipótese de tratamento indeterminada. A autorização é aberta e não conta com critérios e deveres específicos. O conceito não está definido por outra legislação, de modo que uma ampla gama de atividades podem ser consideradas para a “proteção ao crédito”, como observado na pesquisa TIC Empresas 2021. Este uso abrangente de informações creditícias, justificado pela genérica base legal, pode implicar riscos ao titular, como tratamentos com finalidades abusivas e discriminatórias.

Assim, essa base legal precisa ser estritamente regulada para estabelecer deveres e responsabilidades adicionais para agentes de tratamento, como ocorre no caso do legítimo

interesse, bem como para definir parâmetros de quais dados e para quais finalidades pode ser utilizados (em remissão à lei do cadastro positivo).

2. Regulação - setor econômico de Saúde (Art. 11, § 5º; da LGPD)

A ANPD já colocou em consulta a prioridade da regulação do setor econômico de saúde, tópico que defendemos como absolutamente prioritário devido à sensibilidade dos dados e a diversos acontecimentos recentes, incluindo vazamentos relevantes de dados de saúde no âmbito do próprio Ministério da Saúde.

Entretanto, no tema "Regulação em Saúde" foi destacada somente a regulação do §4º do art. 11 da LGPD, que nos parece insuficiente para endereçar (1) os desafios práticos do setor e (2) e de forma completa as normas dispostas na LGPD, sendo também necessário regular o §5º.

Este parágrafo dispõe sobre a vedação à seleção de risco, já consagrada de certa maneira na regulação setorial, mas ainda meritória de atenção desta e. autoridade.

3. Regulação do direito à portabilidade e interoperabilidade (art. 40)

O Art. 2º, inciso VI, dispõe que um dos princípios que regem a Lei Geral de Proteção de Dados é a livre concorrência. Desta maneira, a legislação tem também a função de não criar barreiras à entrada e ao desenvolvimento de concorrentes ao mercado, atentando a questões de proteção de dados aliada à viabilização de medidas que promovam a competitividade. Uma das disposições centrais sobre o tema é o exercício dos direitos de interoperabilidade e portabilidade de dados, que podem reduzir a assimetria de poder das grandes plataformas e permitir o desenvolvimento de novos modelos de negócio, que, potencialmente, podem ser até mais protetivo para os consumidores. Desta maneira, o Idec entende que o artigo 40 é central para ser regulado no próximo biênio.

São Paulo, 31 de agosto de 2022.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Ref.: Tomada de Subsídios nº 03/2022

Envio por correio eletrônico

O **GOOGLE BRASIL INTERNET LTDA.** ("Google") pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 06.990.590/0001-23, com sede na Avenida Brigadeiro Faria Lima, nº 3.477, 18º andar, Itaim Bibi, São Paulo/SP, vem, respeitosamente, por meio de seus procuradores, informar que, na data de hoje, apresentou suas contribuições à Tomada de Subsídios nº 3/2022. A participação foi feita a partir de login pertencente a advogada que aqui subscreve e conforme consta em comprovante em anexo. O Google aproveita ainda para, tal qual facultado pela Autoridade, apresentar material extra no qual traz insumos sobre as classificações dadas aos temas indicados.

Atenciosamente,



Amanda Moreira Kraft
OAB/SP 383.864

1. COMPROVANTE PARTICIPAÇÃO TS 03/2022

 Presidência da República Participa +Brasil

Tomada de Subsídios para elaboração da Agenda Regulatória da ANPD para o biênio 2023-2024

Órgão: Autoridade Nacional de Proteção de Dados

Status: Ativa

Abertura: 05/08/2022

Encerramento: 31/08/2022

Contribuições Recebidas: 118



RESUMO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), inaugurou um novo regime jurídico referente ao tratamento de dados pessoais no país e introduziu novos conceitos, direitos e obrigações ao estruturar nacionalmente um sistema efetivo de proteção de dados pessoais.

A referida lei estabeleceu as competências da ANPD, dentre os quais destacam-se zelar pela proteção dos dados pessoais e a editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade.

Para tanto, a ANPD faz uso da Agenda Regulatória, instrumento de planejamento que agrega as ações regulatórias prioritárias e que serão objeto de estudo ou de tratamento pela Autoridade para o seu período de referência. A Agenda Regulatória busca conferir maior publicidade, previsibilidade, transparência e eficiência para o processo regulatório da ANPD, possibilitando o acompanhamento pela sociedade e trazendo maior segurança jurídica na relação com os agentes regulados.

Neste sentido, para dar continuidade ao projeto de elaboração da Agenda Regulatória para o biênio 2023-2024, pretende-se realizar consulta à sociedade para amparar a elaboração da Agenda Regulatória para o biênio 2023-2024.

Esta consulta tem objetivo de identificar temas considerados relevantes pela sociedade para estudos e/ou regulamentação sobre proteção de dados pessoais pela ANPD.

Para tanto, as contribuições à pesquisa devem ocorrer, exclusivamente por meio da Plataforma Participa + Brasil, em forma de avaliação qualitativa aos temas abaixo descritas.

Para opinar deve-se fazer cadastro e estar logado na plataforma.

Caso deseje compartilhar relatórios, imagens ou outros anexos, favor enviar para o e-mail normatizacao@anpd.gov.br, durante o período em que esta consulta estiver ativa.

Por e-mail serão aceitos apenas anexos, com materiais complementares às respostas fornecidas. **Não serão aceitas respostas às perguntas através do e-mail.**

Para contribuir, avaliar os temas segundo grau de importância, sendo:

1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação)

2 - Pouca importância (Neutro - pode esperar a longo prazo)

3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)

4 - Importante (Prioritário - pode esperar a curto prazo)

5 - Muito importante (Urgente e prioritário)



Presidência da República

 **Participa +Brasil**

NOTA TÉCNICA

Nota Técnica

[Baixar em PDF](#) - Tamanho do arquivo: 163,55 KB

AVISO TOMADA DE
SUBSÍDIOS

AVISO TOMADA DE SUBSÍDIOS

[Baixar em PDF](#) - Tamanho do arquivo: 46,34 KB

REGISTRE SUA OPINIÃO

Avalie os temas segundo grau de importância, sendo:

- 1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação)
- 2 - Pouca importância (Neutro - pode esperar a longo prazo)
- 3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)
- 4 - Importante (Prioritário - pode esperar a curto prazo)
- 5 - Muito importante (Urgente e prioritário)

	1 Sem importância	2	3	4	5 Muito importante
1. Crianças e adolescentes (Art. 14 da LGPD)	☐	☐	☐	☐	☒



Presidência da República

Participa +Brasil

4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)					
5. Inteligência Artificial					
6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)					
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)					
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)					
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)					
10. Boas Práticas Regulatórias					
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)					
12. Registro de Operações (Art. 37 da LGPD)					
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)					
14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)					



■
Presidência da República

 Participa +Brasil

Sobre quais outros temas (4-importantes ou 5-muito importantes) você gostaria que a ANPD considerasse na elaboração da próxima Agenda Regulatória? Favor, justificar a necessidade.

Não há.

2000 caracteres

Sua opinião já foi registrada em 31/08/2022



[SOBRE](#)

[CONSULTAS
PÚBLICAS](#)

[OPINE AQUI](#)

[ÓRGÃOS
PÚBLICOS](#)

[COLEGIADOS](#)

[AUDIÊNCIAS
PÚBLICAS](#)

[AJUDA PARA
USUÁRIOS](#)

[NAVEGAÇÃO](#)

[FALE
CONOSCO](#)



2. MATERIAL EXTRA À CONTRIBUIÇÃO



CONTRIBUIÇÕES À TOMADA DE SUBSÍDIOS PARA ELABORAÇÃO DA AGENDA REGULATÓRIA DA ANPD PARA O BIÊNIO 2023-2024

O **GOOGLE BRASIL INTERNET LTDA.** ("Google") pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 06.990.590/0001-23, com sede na Avenida Brigadeiro Faria Lima, nº 3.477, 18º andar, Itaim Bibi, São Paulo/SP agradece o espaço de manifestação ofertado pela Tomada de Subsídio da Autoridade Nacional de Proteção de Dados ("ANPD") para a elaboração de sua Agenda Regulatória do biênio de 2023-2024. A empresa gostaria ainda de enaltecer a iniciativa da Autoridade em aprofundar o debate democrático na definição de temas prioritários de forma aberta.

Como já pontuado em outras oportunidades de diálogo, a missão do Google é tornar as informações do mundo universalmente acessíveis e úteis. No cumprimento desse compromisso, o Google investe continuamente no desenvolvimento de tecnologias visando fazer da internet um ambiente seguro, no qual a privacidade esteja sempre em primeiro lugar. Faz parte do nosso compromisso manter nossas políticas atualizadas de acordo com os parâmetros da Lei Geral de Proteção de Dados ("LGPD") e em cumprimento às leis locais de modo a garantir que os dados pessoais protegidos pela legislação sejam tratados sempre de forma segura e transparente.

Aliado aos valores exercidos internamente e com seus parceiros, o Google acredita na construção conjunta de uma regulamentação que atenda as diretrizes de proteção de dados, mas que esteja em sintonia com o desenvolvimento tecnológico. A ANPD selecionou temas que são de grande relevância para os titulares e para o mercado de modo geral, havendo alguns deles que se acredita demandarem uma resposta mais célere por parte da Autoridade. Dessa forma, tal como já foi submetido no sistema de participação disponibilizado ao público, o Google aproveita a oportunidade para apresentar breves considerações sobre suas avaliações e reproduz sua classificação completa de prioridade.

Tema	Classificação ¹	Comentário
1. Crianças e Adolescentes (Art. 14 da LGPD)	5	A regulamentação do tratamento de dados pessoais de crianças e adolescentes é de extrema relevância em face do grau de compreensão diverso desses titulares quanto ao uso de suas informações por terceiros. Dentre os temas que merecem detalhamento estão, dentre outros, as distinções entre os tratamentos de dados de crianças e de adolescentes; a utilização das demais bases legais previstas na LGPD, que não o consentimento; e o que serão considerados “esforços razoáveis”, para fins do §5º, art. 14 da LGPD.
5. Inteligência Artificial	5	O acelerado desenvolvimento e uso de tecnologias de inteligência artificial (IA) vêm gerando inúmeros debates regulatórios e a elaboração de novos regramentos ao redor do mundo. No Brasil, o tema já é alvo de projeto de lei específico em estágio avançado de tramitação, no âmbito do Congresso Nacional. Nesse contexto, é fundamental que a ANPD avance na regulamentação do assunto da perspectiva da proteção de dados pessoais e, em particular, da aplicação da LGPD. Tais diretrizes servirão de base para o desenvolvimento de outras regras que venham a ser necessárias para a disciplina de sistema de IA.
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, §2º; Art. 50, §3º; Art. 51, da LGPD)	4	Trata-se de um instrumento fundamental de co-regulação e para que o setor privado assuma um papel mais pró-ativo na proteção de dados pessoais. Nesse sentido, diversos setores e entidades já vêm adotando esse tipo de instrumento no Brasil. A ANPD pode apoiar o fortalecimento desses esforços, ao reconhecer exemplos bem-sucedidos nessa área e ao definir incentivos concretos aos setores e entidades que decidam investir nesse instrumento.
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	4	A ANPD já fixou algumas diretrizes para o peticionamento do titular de dados pessoais ² , no entanto a regulamentação deste tópico pode oferecer mais clareza sobre como eventuais demandas dos titulares podem ser solucionadas diretamente com os controladores, sem

¹ A classificação atribuída aos temas obedece aos mesmos parâmetros definidos na Tomada de Subsídios, isto é, de 1 (para temas com nenhuma ou pouca necessidade de regulamentação) a 5 (para temas urgentes e/ou prioritários).

² Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contr-controlador-de-dados. Acesso: 31.08.2022.

		qualquer necessidade de intervenção da Autoridade. Nesse sentido, as novas regras podem colaborar para a efetividade do art. 18 da LGPD como um todo.
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)	4	A despeito da importância do assunto, a LGPD não supriu integralmente a necessidade de disciplina do tema. Dúvidas e debates têm ocorrido - não apenas no Brasil - envolvendo o próprio alcance do conceito de dados biométricos e a distinção entre diferentes tipos de tratamento que utilizam dados biométricos ³ .
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)	4	Embora o art. 46 da LGPD determine que a adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas devam acontecer desde o momento da concepção do produto ou serviço até a sua execução, a norma não traz nenhuma diretriz sobre quais os padrões técnicos mínimos devem ser empregados. Desse modo, é importante que haja um trabalho da ANPD, em conjunto com o mercado, inclusive para que sejam compreendidas as diferentes realidades vivenciadas. A regulação para a fixação de parâmetros de segurança deve observar não só a natureza das informações tratadas, como também as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis.

³ Parte desse debate e dos desafios colocados está sumarizado em: <https://dfj.emnuvens.com.br/dfj/article/view/1007>. Acesso: 31.08.2022.

ANEXO – REPRODUÇÃO CLASSIFICAÇÃO COMPLETA DE TEMAS

Temas	1	2	3	4	5
1. Crianças e Adolescentes (Art. 14 da LGPD)					X
2. Regulação - Setor econômico de Educação		X			
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)			X		
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, §2º; Art. 50, §3º; Art. 51, da LGPD)				X	
5. Inteligência Artificial					X
6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)		X			
7. Peticionamento do titular de dados pessoais (Art. 18, §1º da LGPD)				X	
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)				X	
9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)			X		
10. Boas Práticas Regulatórias				X	
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)				X	
12. Registro de Operações (Art. 37 da LGPD)			X		
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)		X			
14. Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD (Art. 4, §3º da LGPD)	X				

Temas	1	2	3	4	5
15. Regulação - setor econômico de Saúde (Art. 11, §4º; Art. 13 da LGPD)		X			
Sobre quais outros temas (4-importantes ou 5-muito importantes) você gostaria que a ANPD considerasse na elaboração da próxima Agenda Regulatória? Favor, justificar a necessidade.					
Não há.					

3. DOCUMENTAÇÃO GOOGLE

SUBSTABELECIMENTO

Eu Giovanna Bruno Ventre, brasileira, solteira, advogada, OAB/SP 361.659, procuradora regularmente constituída para representar **GOOGLE BRASIL INTERNET LTDA.** ("Google") pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 06.990.590/0001-23, com sede na Avenida Brigadeiro Faria Lima, nº 3.477, 18º andar, Itaim Bibi, São Paulo/SP, substabeleço, com reserva de iguais poderes, **Beto Ferreira Martins Vasconcelos**, [REDACTED], inscrito na OAB/SP sob o n. 172.687, **Luís Felipe Valerim Pinheiro**, [REDACTED], inscrito na OAB/SP sob o n. 198.242, **Ivo da Motta Azevedo Corrêa**, [REDACTED], inscrito na OAB/SP sob o n. 207.069, **Eduardo Xavier**, [REDACTED], inscrito na OAB/SP sob o n. 207.671, **Felipe de Paula**, [REDACTED], inscrito na OAB/SP sob o n. 237.080, **Wellington Márcio Kubliskas**, brasileiro, solteiro, advogado, inscrito na OAB/SP sob o n. 224.392, **Ana Luísa Ferreira Pinto**, [REDACTED], inscrita na OAB/SP sob o n. 345.204, **Sofia Rodrigues Silvestre Guedes**, [REDACTED], inscrita na OAB/SP sob o n. 413.183, **Amanda Moreira Kraft**, [REDACTED], inscrita na OAB/SP sob o n. 383.864, **Julia Maria Lillo do Nascimento**, [REDACTED], inscrita na OAB/SP sob o n. 425.697, **Rodolfo da Costa Arruda Silva**, [REDACTED], inscrito na OAB/SP sob o n. 440.949, **Natalia Pereira Lana**, [REDACTED], inscrita na OAB/SP 429.767, **Pâmela de Andrade Stempluk**, [REDACTED], inscrita na OAB/SP sob o n. 376.490, **Túlio de Medeiros Jales**, [REDACTED], inscrito na OAB/RN nº 13.767, **Sofia Motta e Pralon**, [REDACTED], inscrita na OAB/SP sob o n. 461.077, **Dhaniel Poletto Cavassana**, [REDACTED], portador do RG n. [REDACTED], **Pedro Henrique Souza Santos**, [REDACTED], portador do RG n. [REDACTED], **Rebeca Faustino Vieira da Silva**, [REDACTED], portadora do RG n. 5 [REDACTED], **Paulo Vitor de Oliveira Nunes**, [REDACTED], portador do RG n. 6 [REDACTED], **Morena Marconi Fonseca Santos**, [REDACTED], portadora do RG n. [REDACTED], todos integrantes do escritório **XAVIER, VASCONCELOS, VALERIM, CORRÊA, DE PAULA SOCIEDADE DE ADVOGADOS**, com endereço profissional à Alameda Santos, 234, 5º andar, Conjunto 505, Cerqueira Cesar, em São Paulo/SP, e endereço eletrônico contato@xvvadvogados.com.br, os poderes outorgados por Google os poderes da cláusula "ad judicium et extra", especialmente para os fins de representá-la em todos os atos referentes à participação na Tomada de Subsídios nº 03/2022 da Autoridade Nacional de Proteção de Dados - ANPD.

31/08/2022

São Paulo, 31 de agosto de 2022.

DocuSigned by:

Giovanna Ventre

5CF4EAE31C8442A...

Giovanna Bruno Ventre

Autores: Rony Vainzof, Henrique Fabretti, Marcella Costa e Tatiana Bauer

Tomada de subsídio - Agenda Regulatória 2023-2024

ESCOPO:	Contribuição para a Tomada de Subsídios Nº 3/2022 sobre a Agenda Regulatória de 2023-2024 da ANPD	
DESCRIÇÃO:	Submissão de contribuição acerca da:	
	(1) avaliação de relevância dos temas indicados pela ANPD (15 temas distribuídos em 11 eixos temáticos);	
	(2) sugestão de temas relevantes não contemplados pela ANPD (2000 caracteres).	
	a) indicação de relevância considerando visão setorial de negócio;	
	b) parâmetros a partir de benchmarking internacional;	
	c) avaliações consideraram pautas regulatórias da ANPD.	
PRAZO:	Encerramento em 31/08/2022	
Legenda:	Nº propostas/temas	
ANPD Proposta de temas	Lista de novos temas apresentados pela ANPD com base em levantamento de informações e de experiências nacionais e internacionais, bem como avaliação qualitativa dos temas.	15
ANPD Temas Obrigatórios	Temas que atualmente se encontram em fase de estudo pelo corpo técnico da ANPD ou, ainda, que se relacionam aos projetos de regulamentação no âmbito da ANPD, incluindo os itens da Agenda Regulatória do biênio 2021-2022 que não foram finalizadas.	17
ANPD Concluídos	Temas elencados na Agenda Regulatória 2021-2022 que já foram concluídos	4
OBA Sugestões	Lista de novos temas sugeridos a partir de benchmarking nacionais e internacionais, pauta regulatória da ANPD e avaliação de pertinência e relevância dos temas.	20

Autores: Rony Vainzof, Henrique Fabretti, Marcella Costa e Tatiana Bauer

TOMADA DE SUBSÍDIOS - AGENDA REGULATÓRIA ANPD 2023-2024

ID	SITUAÇÃO	EIXO TEMÁTICO	TEMA	FUNDAMENTO LGPD	RELEVÂNCIA (1-5)	JUSTIFICATIVA
I	ANPD Proposta de temas	Direito dos titulares	Peticionamento do titular de dados pessoais	Art. 18, § 1º	5 - Muito importante (Urgente e prioritário)	O tema é de grande importância, considerando a atuação das empresas representadas pela Fecomercio nos setores de comércio de bens, serviços e turismo do Estado de SP e a alta probabilidade dessas empresas manterem contato direto com os titulares dos dados. Embora já haja página específica sobre o assunto no site da ANPD, espera-se que a Autoridade aborde aspectos sobre as requisições a serem feitas por titulares acerca de seus direitos em maior grau de detalhe podendo, inclusive, trazer parâmetros para os direitos dos titulares contemplados no art. 18 e seguintes da LGPD.
II	ANPD Proposta de temas	Governança e Boas Práticas	Regras de boas práticas e de governança	Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51	5 - Muito importante (Urgente e prioritário)	O tema é de grande importância, já que se relaciona com os princípios de segurança e prevenção previstos no art. 6º, VII e VIII da LGPD. Espera-se que a ANPD indique parâmetros do que a Autoridade espera dos agentes de tratamento em relação à observância destes dois princípios, em linha com o que dispõe o art. 50, §2º da LGPD. A partir de medidas educativas, e não normativas, será possível aos agentes de tratamento definir medidas mais assertivas em termos de governança em proteção de dados, além de aumentar a segurança jurídica para sua adoção. Nesse sentido, a adoção de guias orientativos pela ANPD poderá ser uma ação bastante positiva da Autoridade, no sentido de orientar a sociedade para melhor aplicação da lei.
III	ANPD Proposta de temas	Tratamento de Dados pelo Poder Público	Compartilhamento de dados pelo poder público	Art. 25	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Apesar de não se tratar de um tópico aplicável à realidade da Fecomercio e/ou das empresas representadas, como agentes de tratamento, o tema é razoavelmente importante tendo em vista o impacto que o tratamento e a disponibilidade de dados por pessoas jurídicas de direito público pode gerar para procedimentos ligados às atividades rotineiras e burocráticas que envolvem a prática empresarial, por exemplo, cumprimento de obrigações legais perante Órgãos Públicos.
IV	ANPD Proposta de temas	Tratamento de Dados Pessoais	Crianças e adolescentes	Art. 14	4 - Importante (Prioritário - pode esperar a curto prazo)	Compreende-se que este tema englobaria o direcionamento acerca da viabilidade de aplicação de outra base legal, que não o consentimento, para o tratamento de dados pessoais de crianças. O assunto pode tangenciar atividades da Fecomercio e/ou das empresas representadas, razão pela qual entendemos ser importante. Ademais, diante das construções doutrinárias recentes (Enunciado ID 4796 da IX Jornada de Direito Civil), o tema ganha ainda mais relevância para determinação de posição pela ANPD.
V	ANPD Proposta de temas	Fiscalização	Termos de compromisso com agentes de tratamento	Art. 55-J, XVII	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Tema importante para trazer mais clareza quanto ao procedimento mencionado, porém, considerando que sua aplicação dependerá do envolvimento do agente de tratamento em uma fiscalização/processo administrativo da ANPD, a definição de relevância ponderou aplicabilidade à curto prazo x urgência para a Agenda regulatória.
VI	ANPD Proposta de temas	Governança e Boas Práticas	Opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do Art. 4º da LGPD	Art. 4, § 3º	2 - Pouca importância (Neutro - pode esperar a longo prazo)	Por não se tratar de um tópico aplicável à realidade da Fecomercio e/ou das empresas representadas, por se referir ao tratamento de dados pessoais realizado para fins exclusivos de a) segurança pública, b) defesa nacional, c) segurança do Estado ou d) atividades de investigação e repressão de infrações penais, avaliamos este tema como sendo de pouca relevância neste momento.
VII	ANPD Proposta de temas	Política Nacional de Proteção de Dados Pessoais e da Privacidade e CNPD	Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade	Art. 55-J, III	4 - Importante (Prioritário - pode esperar a curto prazo)	Compreende-se que as diretrizes contempladas na Política Nacional de Proteção de Dados Pessoais e de Privacidade poderão servir de parâmetro para construção/revisão de documentos de governança internos da Fecomercio e/ou das empresas representadas, razão pela qual categorizamos este tema como sendo importante.
VIII	ANPD Proposta de temas	Regulação	Boas Práticas Regulatórias	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Compreende-se que este tema englobaria a indicação de quais documentos ou práticas serão consideradas (ou até mesmo priorizadas) pela ANPD no âmbito de uma fiscalização. Tendo em vista que a Fecomercio e as empresas representadas estão sujeitas a fiscalizações da Autoridade, categorizamos este tema como sendo importante.

IX	ANPD Proposta de temas	Segurança da Informação	Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança)	Art. 46	4 - Importante (Prioritário - pode esperar a curto prazo)	O tema traz grande importância especialmente se abordado sob a ótica de privacy by design, além de sua utilidade para o esclarecimento de medidas exigíveis em relações com terceiros (como em cláusulas contratuais) e outras recomendações relacionadas para a própria Fecomércio e/ou para as empresas representadas.
X	ANPD Proposta de temas	Regulação, setores econômicos específicos	Saúde	Art. 11, § 4º Art. 13	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	A interpretação da vedação contida no artigo 11, §4º sobre a comunicação ou o uso compartilhado entre controladores de dados sensíveis referentes à saúde com o objetivo de obter vantagem econômica, mostra-se como um item de grande importância para as empresas representadas pela Fecomércio, especialmente aquelas do setor de saúde. No entanto, a LGPD ainda carece de regulamentação em temas básicos, antes de setores específicos, como a Saúde, serem normatizados pela ANPD. Considerando essa limitação, é um assunto que pode aguardar a regulamentação futura da Autoridade.
XI	ANPD Proposta de temas	Regulação, setores econômicos específicos	Educação	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Os serviços prestados na seara da Educação enfrentam desafios importantes relacionados ao tratamento de dados, como compartilhamento e base legal, especialmente por envolver dados pessoais de crianças e adolescentes. Foi categorizado como razoavelmente importante, por considerarmos que alguns desses desafios já estão contemplados em outros eixos temáticos da Agenda da ANPD (item IV acima, por exemplo).
XII	ANPD Proposta de temas	Tratamento de dados pessoais	Registro de Operações	Art. 37	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Considerando insumos estrangeiros acerca do conteúdo dos registros de atividades de controladores e operadores, entende-se que seja um tema relevante, mas que pode esperar a médio prazo para ser regulamentado.
XIII	ANPD Proposta de temas	Tratamento de dados pessoais	Dados Pessoais Sensíveis - Dados biométricos	Art. 5º II	4 - Importante (Prioritário - pode esperar a curto prazo)	O tema é avaliado como importante na medida em que sua utilização em processos de identificação e autenticação, assim como outras aplicações de reconhecimento facial são parte da realidade das atividades recorrentes de muitas empresas e entidades, incluindo as empresas representadas.
XIV	ANPD Proposta de temas	Tratamento de dados pessoais	Adequação progressiva de banco de dados	Art. 63	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	O tema é razoavelmente importante pois apresenta risco regulatório baixo, na medida em que a lei traz os princípios e as bases legais para o tratamento de dados pessoais que também servem de diretriz para a adequação dos bancos de dados usados pela Fecomércio e/ou pelas empresas representadas.
XV	ANPD Proposta de temas	Direito Digital e Tecnologias	Inteligência Artificial	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Considera-se um tema importante, diante da crescente utilização em projetos de data analytics, algoritmos e desenvolvimentos de tecnologias presentes nos modelos de negócios atuais e, no entanto, a existência de dúvidas relevantes quanto ao risco aos titulares e a conformidade com a LGPD.
I	ANPD Temas obrigatórios	Direito Digital e Tecnologias	Cookies	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	x
II	ANPD Temas obrigatórios	Direito dos titulares	Direitos dos titulares de dados pessoais	NA	5 - Muito importante (Urgente e prioritário)	x
III	ANPD Temas obrigatórios	Fiscalização	Dosimetria e aplicação de sanções administrativas	Art. 52 Art. 53	5 - Muito importante (Urgente e prioritário)	x
IV	ANPD Temas obrigatórios	Segurança da Informação	Comunicação de incidentes e especificação do prazo de notificação	Art. 48	5 - Muito importante (Urgente e prioritário)	x
V	ANPD Temas obrigatórios	Transferência Internacional	Transferência Internacional de Dados Pessoais	Capítulo V	5 - Muito importante (Urgente e prioritário)	x
VI	ANPD Temas obrigatórios	Tratamento de dados pessoais	Tratamento de dados pessoais pelos órgãos de pesquisa	Art. 7º, IV Art. 11, I, 'c' Art. 13	4 - Importante (Prioritário - pode esperar a curto prazo)	x
VII	ANPD Temas obrigatórios	Tratamento de dados pessoais	Dados pessoais sensíveis - Organizações religiosas	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x

VIII	ANPD Temas obrigatórios	Tratamento de dados pessoais	Relatório de Impacto à Proteção de Dados Pessoais	Art. 4º, §3º Art. 5º, XVII Art. 10, §3º Art. 32 Art. 38 Art. 55-J, XIII	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
IX	ANPD Temas obrigatórios	Tratamento de dados pessoais	Encarregado de proteção de dados pessoais	NA	5 - Muito importante (Urgente e prioritário)	x
X	ANPD Temas obrigatórios	Tratamento de dados pessoais	Hipóteses legais de tratamento de dados pessoais	Art. 7º Art. 11	5 - Muito importante (Urgente e prioritário)	x
XI	ANPD Temas obrigatórios	Tratamento de dados pessoais	Larga escala	Art. 4º, §3º, da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XII	ANPD Temas obrigatórios	Tratamento de dados pessoais	Cumprimento do disposto na Lei de Diretrizes e Bases da Educação Nacional	Art. 62	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XIII	ANPD Temas obrigatórios	Tratamento de dados pessoais	Glossário sobre proteção de dados pessoais	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XIV	ANPD Temas obrigatórios	Governança Institucional	Regimento Interno	Art. 55-G, § 2º	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XV	ANPD Temas obrigatórios	Governança Institucional	Planejamento e Estratégia Institucional da ANPD 2024-2026	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XVI	ANPD Temas obrigatórios	Governança Institucional	Plano de Dados Abertos	Decreto 8777/2016	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
XVII	ANPD Temas obrigatórios	Governança Institucional	Código de Ética e Conduta da ANPD	NA	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	x
I	ANPD Concluído	Governança Institucional	Regimento Interno	Art. 55-G, § 2º		x
II	ANPD Concluído	Governança Institucional	Planejamento e Estratégia Institucional da ANPD 2021-2023	NA		x
III	ANPD Concluído	Fiscalização	Processo de Fiscalização e Processo Administrativo Sancionador	Art. 52 Art. 53		x
IV	ANPD Concluído	Tratamento de dados pessoais	Proteção de dados e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos	Art. 55-J, XVIII		x
I	OBA Sugestões	Tratamento de Dados Pessoais	Tratamento de dados pessoais em relações de trabalho	NA	5 - Muito importante (Urgente e prioritário)	O tema é relevante por ser unanimidade entre as entidades privadas. Orientações necessárias sobre bases legais aplicáveis e temas como medicina do trabalho, monitoramento do colaborador, trabalho remoto e uso de tecnologias no ambiente do trabalho.

II	OBA Sugestões	Segurança da Informação	Anonimização	Art. 12 § 3º	4 - Importante (Prioritário - pode esperar a curto prazo)	Conforme art. 12, §3º da LGPD, resta pendente a disposição de padrões e técnicas em processos de anonimização e verificações acerca de sua segurança. Sua importância se aplica ao tratamento para pesquisas (art. 7º, IV e 11, II 'c'), estudos na área de saúde pública (art. 13), hipóteses associadas ao término do tratamento (art. 16, II e IV) e direitos dos titulares (art. 18, IV e art. 18 §6º).
III	OBA Sugestões	Segurança da Informação	Comunicação de incidentes - risco ou dano relevante	Art. 48	4 - Importante (Prioritário - pode esperar a curto prazo)	Embora tenha sido indicado que a pauta "Comunicação de incidentes e especificação do prazo de notificação" dispensa consulta (Nota técnica nº 31/2022/CGN/ANPD), não está claro se a consulta abordará os requisitos e aspectos referentes a riscos ou danos relevantes. Assim, entende-se pela importância do tema.
IV	OBA Sugestões	Tratamento de Dados Pessoais	Compartilhamento de dados COM o poder público	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Necessidade de orientações sobre como balancear o atendimento às solicitações/compartilhamentos com a exigência de que agentes públicos estejam adequados à lei.
V	OBA Sugestões	Direito Digital e Tecnologias	Decisão automatizada	Art. 20	4 - Importante (Prioritário - pode esperar a curto prazo)	Definições do que constitui decisão tomada unicamente com base em tratamento automatizado (direito dos titulares, art. 20 da LGPD). Ainda, o tema abarca orientações para atividades de perfilamento e sua conformidade à LGPD.
VI	OBA Sugestões	Governança e Boas Práticas	Teste de balanceamento	Art. 7º Art. 10 Art. 11	4 - Importante (Prioritário - pode esperar a curto prazo)	Considerando que em notas técnicas emitidas pela ANPD exigiu-se a elaboração de teste de balanceamento, é importante que os agentes de tratamento tenham orientações quanto aos critérios de elaboração e casos aplicáveis.
VII	OBA Sugestões	Regulação em Setores Econômicos	Marketing direto	NA (duvida pra baixo)	4 - Importante (Prioritário - pode esperar a curto prazo)	O tema traz importância já que é uma prática amplamente utilizada pelo mercado, incluindo as empresas representadas. Assim, sugere-se direcionamento de limites e orientações para o tratamento de dados pessoais na área de marketing, já que esse aspecto é abordado de forma específica também no cenário internacional.
VIII	OBA Sugestões	Regulação em Setores Econômicos	Oferta de produtos e serviços a usuários de redes sociais (targeting)	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Embora tenha sido indicado "Cookies" como tema obrigatório (Nota técnica nº 31/2022/CGN/ANPD), não há esclarecimento quanto aos aspectos que serão abrangidos. Assim, é necessário que sejam estabelecidos os limites e as orientações com relação às técnicas e formas como os dados são tratados e manipulados para essa finalidade (targeting).
IX	OBA Sugestões	Fiscalização	Crítérios para considerar faturamento do grupo econômico como base de cálculo para aplicação de sanções administrativas de multa	Art. 52, §4º	4 - Importante (Prioritário - pode esperar a curto prazo)	Apesar de existir consulta pública aberta pela ANPD sobre norma de dosimetria, o que engloba a questão dos critérios de faturamento, este é um tema relevante e recorrente nas entidades privadas no âmbito de uso de Normas Corporativas Globais, bem como no tocante à aplicação de multas. Assim, sugere-se direcionamentos e boas práticas especialmente quanto ao compartilhamento e armazenamento de dados pessoas intragrupo.
X	OBA Sugestões	Tratamento de Dados Pessoais	Definição do conceito de grupo econômico	Art. 33, II, c Art. 52, II Art. 52, § 4º	4 - Importante (Prioritário - pode esperar a curto prazo)	Apesar de existir consulta pública aberta pela ANPD sobre norma de dosimetria, o que engloba a questão dos critérios de faturamento, este é um tema relevante e recorrente nas entidades privadas no âmbito de uso de Normas Corporativas Globais, bem como no tocante à aplicação de multas. Assim, sugere-se direcionamentos e boas práticas especialmente quanto ao compartilhamento e armazenamento de dados pessoas intragrupo.
XI	OBA Sugestões	Direito Digital e Tecnologias	Monitoramento de indivíduos	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Aplicável de modo geral e com mais intensidade em determinados setores econômicos, necessárias orientações sobre limites de legalidade e atendimento à lei (ex.: monitoramento por vídeo, geolocalização, rastreamento, apps – colaboradores, pacientes). É importante também ao considerarmos a prática de trabalho de casa (home office) por funcionários de diversas empresas.
XII	OBA Sugestões	Governança e Boas Práticas	Privacidade por concepção (Privacy by Design) e privacidade por padrão (Privacy by Default)	Art. 46, § 2º	4 - Importante (Prioritário - pode esperar a curto prazo)	Embora tenha sido indicado que a pauta "Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança)" dispensa consulta (Nota técnica nº 31/2022/CGN/ANPD), não há esclarecimento quanto aos aspectos que serão abrangidos. Assim, entende-se pela importância de que já se defina os aspectos específicos do tema para nortear as atividades de tratamento de dados pela Fecomércio e/ou pelas empresas representadas.
XIII	OBA Sugestões	Direito Digital e Tecnologias	Serviços em nuvem (cloud computing) e/ou uso de servidores estrangeiros	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Bases legais, limites e recomendações. É importante tendo em vista o grande uso desses serviços no mercado, inclusive pela Fecomércio e pelas empresas representadas.

XIV	OBA Sugestões	Governança e Boas Práticas	Transparência	Art. 6º, VI; Art. 9º; Art. 8º; Art. 10, § 2º; Art. 40; Art. 50, I 'd'	4 - Importante (Prioritário - pode esperar a curto prazo)	Em acompanhamento às decisões e notas técnicas emitidas pela ANPD no âmbito de suas investigações, identifica-se que são feitas exigências quanto ao atendimento do princípio da transparência, especialmente no que tange ao Aviso de Privacidade. Assim, denota-se a importância de que a ANPD publique orientações aos agentes de tratamento sobre o tema de transparência, a exemplo do que é feito no âmbito internacional (ex: EDPB)
XV	OBA Sugestões	Regulação em Setores Econômicos	Tratamento de dados pessoais no setor da saúde	NA	4 - Importante (Prioritário - pode esperar a curto prazo)	Além dos arts. 11, §4º e 13, há necessidade de orientações aplicáveis ao tratamento de dados pessoais no setor de saúde, incluindo por exemplo data health analytics, medicina preditiva e compartilhamento entre agentes interconectados do setor. Consta na Proposta que o tema Saúde deve constar obrigatoriamente da Agenda Regulatória e, assim, englobaria o tema desse item.
XVI	OBA Sugestões	Segurança da Informação	Pseudonimização	Art. 13 §4º	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Necessidade de orientações quanto aos padrões e técnicas para que os dados sejam considerados pseudonimizados. Importância e relevância foram definidas considerando a possibilidade do tema ser abordado na pauta "Anonimização".
XVII	OBA Sugestões	Regulação em Setores Econômicos	Comunicação ou uso compartilhado de dados pessoais sensíveis entre controladores com o objetivo de obter vantagem econômica	Art. 11, § 3º	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Conforme consta no Art. 11, § 3º, tal prática poderá ser objeto de vedação ou de regulamentação pela ANPD e, dessa forma, deve ser incluído na Tomada de Subsídios. Esse tema é relevante pois pode afetar a Fecomércio e/ou as empresas representadas, mas pode esperar no médio prazo.
XVIII	OBA Sugestões	Direito dos titulares	Prazo para atendimento ao titular e validação de identidade	Art. 19, § 4º	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Embora tenha sido indicado que a pauta "Direito dos titulares" dispensa consulta (Nota técnica nº 31/2022/CGN/ANPD), não há esclarecimento quanto aos aspectos que serão abrangidos. Assim, entende-se pela importância de que já se defina mecanismos aptos e direcionamentos específicos para verificar a identidade do titular no momento da requisição e prazos para atendimento de direitos dos titulares de dados pessoais, considerando inclusive o previsto no art. 19, §4º sobre a disposição de prazos para setores específicos.
XIX	OBA Sugestões	Direito dos titulares	Portabilidade	Art. 18, V Art. 40	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Embora tenha sido indicado que a pauta "Direito dos titulares" dispensa consulta (Nota técnica nº 31/2022/CGN/ANPD), não há esclarecimento quanto aos aspectos que serão abrangidos. Assim, indica-se como sugestão de tema a regulamentação pela ANPD acerca dos padrões de interoperabilidade para fins de portabilidade, com base no art. 18, V e art. 40 da LGPD.
XX	OBA Sugestões	Direito dos titulares	Direito de acesso	Art. 18, II Art. 40	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)	Embora tenha sido indicado "Direito dos titulares" como pauta obrigatória (Nota técnica nº 31/2022/CGN/ANPD), não há esclarecimento quanto aos aspectos que serão abrangidos. Assim, indica-se como sugestão de tema a orientação da ANPD quanto à interpretação do direito de acesso para seu atendimento pelos agentes de tratamento (art. 18, II e art. 19 LGPD), bem como sobre padrões de interoperabilidade para fins de livre acesso (art. 40 LGPD).

Autores: Rony Vainzof, Henrique Fabretti, Marcella Costa e Tatiana Bauer

Benchmarking OBA			
Benchmarking setorial		Benchmarking internacional	
Setor	Internacional	País-DPA	Resultados
Indústria alimentícia		EU - EDPB	Guidelines European Data Protection Board (europa.eu)
Saúde e farmácia	Guidance Notes Health and Pharma DataGuidance	WP 29 (endorsed by EDPB)	Endorsed WP29 Guidelines European Data Protection Board (europa.eu)
Marketing	Guidance Notes Marketing DataGuidance	Argentina - Agencia de Acceso a la Información Pública	Normativa Argentina.gob.ar
Telecomunicações	Guidance Notes Telecomm/Maketing DataGuidance	UK - ICO	Guide to Data Protection ICO
Bancário	Guidance Notes Financial DataGuidance	ES - AEPD	Guías AEPD
Transporte	Guidance Notes Automotive DataGuidance	IE - DPC	For Organisations Data Protection Commissioner
Educação	Guidance Notes Education DataGuidance	FR - CNIL	Lignes directrices et recommandations de la CNIL CNIL

Autores: Rony Vainzof, Henrique Fabretti, Marcella Costa e Tatiana Bauer

CONFORME INFORMADO EM NOTA TÉCNICA, A ANPD REALIZOU OS SEGUINTE BENCHMARKINGS:

Benchmarking ANPD	
Benchmarking setorial	Benchmarking internacional
Foi realizado benchmarking em relação às agências reguladoras do país, dentre elas:	Foi realizado benchmarking internacional, buscando consolidar as principais tendências regulatórias de outras autoridades de proteção de dados pelo mundo, tendo sido pesquisadas:
1) Agência Nacional de Transportes Terrestres (ANTT)	1) Information Commissioner's Office (ICO)
2) Agência Nacional de Saúde Suplementar (ANS)	2) Agencia Española de Protección de Datos
3) Agência Nacional de Telecomunicações (Anatel)	3) Unidad Reguladora y de Control de Datos Personales
4) Agência Nacional de Aviação Civil (Anac)	4) Commission Nationale de l'Informatique et des Libertés.
5) Agência Nacional de Energia Elétrica (Aneel)	
6) Agência Nacional de Transportes Aquaviários (Antaq)	
7) Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP)	
8) Agência Nacional do Cinema (Ancine)	
9) Agência Nacional de Águas e Saneamento Básico (ANA)	
10) Agência Nacional de Vigilância Sanitária (Anvisa).	

**MANIFESTAÇÃO CONJUNTA DA ASSOCIAÇÃO BRASILEIRA DE CRÉDITO DIGITAL (ABCD)
E ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS (ABIPAG)
TOMADA DE SUBSÍDIOS DA ANPD SOBRE AGENDA REGULATÓRIA 2023-2024**

Assunto: Tomada de subsídios da ANPD sobre a agenda regulatória 2023-2024.

Prazo: 31/08/22

Protocolo: Plataforma Mais Brasil e no e-mail normatizacao@anpd.gov.br

Objetivo:

A presente manifestação pretende avaliar os temas sugeridos pela ANPD (elencados abaixo), para a construção da agenda regulatória da autoridade (2023-2024), considerando os seguintes graus de importância: 1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação); 2 - Pouca importância (Neutro - pode esperar a longo prazo); 3 - Razoavelmente importante (Neutro - pode esperar a médio prazo); 4 - Importante (Prioritário - pode esperar a curto prazo); 5 - Muito importante (Urgente e prioritário).

1. Crianças e adolescentes (Art. 14 da LGPD)

3 - Razoavelmente importante (Neutro - pode esperar a médio prazo)

Embora as atividades de tratamento de dados de crianças e adolescentes demandem maior grau de proteção e orientações mais robustas da ANPD, entende-se que há normas de caráter geral que se mostram mais prementes, por se aplicarem a maior número de setores econômicos e envolverem volume considerável de atividades de tratamento. Ademais, já existem normas gerais como o

	ECA, Código Civil e CDC que trazem diretrizes no tema.
2. Regulação - Setor econômico de Educação	2 - Pouca importância (Neutro - pode esperar a longo prazo) Há normas de caráter geral que se mostram mais urgentes, pois se aplicam a maior número de setores econômicos e envolvem volume considerável de atividades de tratamento.
3. Adequação progressiva de banco de dados (Art. 63 da LGPD)	2 - Pouca importância (Neutro - pode esperar a longo prazo) Espera-se maior maturidade em relação a tópicos basilares, como incidentes, bases legais e modelos de RIPD e LIA, para que se possa avançar nos temas de adequação de bancos de dados. Todavia, a padronização nas diretrizes de banco de dados é positiva e traz maior segurança jurídica.
4. Regras de boas práticas e de governança (Art. 50, caput; Art. 50, § 2º; Art. 50, § 3º; Art. 51, da LGPD)	5 - Muito importante (Urgente e prioritário). Para que agentes de tratamento garantam a governança institucional no que tange à proteção de dados, mostra-se necessária a criação de instruções mais objetivas e a

	definição de alguns conceitos basilares. Cita-se, como exemplo, conceitos como “alto risco”, “larga escala”, “volume de operações” e “probabilidade de danos para os titulares”. Ademais, a definição de regras de boas práticas de governança se aplica como atenuante na norma de aplicação de sanções, sendo relevante a sua regulação para conferir maior segurança jurídica e estimular a cultura de proteção de dados.
5. Inteligência Artificial	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo) Atualmente, o Projeto de Lei nº 21/2020¹ que visa regulamentar o tema da Inteligência Artificial, encontra-se em trâmite no Legislativo Federal (já aprovado em uma das Casas Legislativas). Entende-se que o avanço da discussão a nível legislativo demandará planejamento a médio prazo pela ANPD. Isso porque, no texto em discussão, não há previsão de nova autoridade responsável pelo tema. Assim, nos moldes da União Europeia, entende-se relevante que a ANPD conduza as discussões, assegurando que a futura Lei seja publicada em conformidade com a LGPD. A fim de evitar diretrizes não harmônicas, a regulação deste tópico precisa estar diretamente vinculada ao avanço do debate no legislativo, que se mostra premente.

¹ <https://www.camara.leg.br/propostas-legislativas/2236340>

	Propõe-se que os enfoques dentro do tema sejam: i) a regulação do art. 20 da LGPD sobre direito de revisão de decisões exclusivamente automatizadas, diferenciando-as de processos operacionais automatizados; ii) aspectos concorrenciais e não-discriminatórios no uso de IA, sobretudo em relação a usuários profissionais; e iii) proporcionalidade regulatória ao risco que a IA oferta aos titulares de dados.
6. Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 55-J, III da LGPD)	5 - Muito importante (Urgente e prioritário). O estabelecimento dessas diretrizes permitirá à ANPD o exercício de suas competências principalmente em setores não regulados, considerando a existência de uma série de diretrizes aplicáveis a setores regulados tal qual o setor financeiro e de pagamentos, com as quais deve haver harmonização.
7. Peticionamento do titular de dados pessoais (Art. 18, § 1º da LGPD)	5 - Muito importante (Urgente e prioritário). O atual procedimento para o peticionamento do titular de dados junto à ANPD carece de algumas ferramentas específicas para os agentes de tratamento. Por exemplo, agentes Controladores não contam com fluxo próprio

	de acompanhamento, devendo, para tanto, realizar cadastro por meio de pessoa física (não havendo possibilidade de cadastro de pessoa jurídica). Isso significa dizer que os Controladores precisam habilitar indivíduos específicos para o acompanhamento de processos, sob o risco da perda de informações (por exemplo, em caso de problemas no cadastro pessoal ou desligamento do responsável). Ainda, observa-se que não há homogeneidade de prazos para manifestação dos agentes na ocasião do acionamento do titular à ANPD, sendo desejável que haja prazos específicos e definidos para tanto. Em resumo, o peticionamento do titular de dados pessoais demanda alguns aprimoramentos que visam, primordialmente, mitigar riscos, sobretudo para agentes de tratamento, garantindo os objetivos de fiscalização, melhorias regulatórias e educação pretendidos pela ANPD. Assim, sugerimos: (i) adoção de plataforma com interface mais intuitiva e que permita o cadastro de pessoas jurídicas, a fim de possibilitar o acompanhamento de peticionamentos em face da empresa; (ii) confecção de cartilha/guia com instruções procedimentais claras
--	--

	sobre a forma como a ANPD desenvolverá o recebimento e as tratativas das petições dos titulares; (iii) padronização de prazos específicos de resposta pelos Controladores a titulares; (iv) análise e adoção urgente das medidas propostas, a fim de resguardar melhores práticas em relação ao atendimento dos direitos dos titulares, fortalecendo a construção da governança nacional em proteção de dados pessoais.
8. Dados Pessoais Sensíveis - Dados biométricos (Art. 5º, II da LGPD)	5 - Muito importante (Urgente e prioritário). Considerando: (i) a natureza desses dados; (ii) as limitações em termos de proteção de dados; (iii) os processos inerentes ao setor financeiro, a exemplo do <i>onboarding</i> de novos clientes e de prevenção à fraude de crédito; e (iv) o avanço do processo de identificação digital dos cidadãos, a atuação da ANPD mostra-se essencial na determinação de melhores práticas relacionadas ao uso de dados biométricos. Inclusive, diretrizes nesse sentido podem auxiliar na construção de processos mais assertivos.

9. Termos de compromisso com agentes de tratamento (Art. 55-J, XVII da LGPD)	2 - Pouca importância (Neutro - pode esperar a longo prazo) Mostra-se necessário o estabelecimento de diretrizes objetivas para temas fundamentais na aplicação da LGPD (por exemplo, uso de bases legais, padronização de prazos de resposta pelos Controladores a titulares e modelos de RIPD e LIA), antes de regular os termos de compromisso com agentes de tratamento.
10. Boas Práticas Regulatórias	4 - Importante (Prioritário - pode esperar a curto prazo) Tal qual o estabelecimento de diretrizes para a Política Nacional de Proteção de Dados Pessoais, a disciplina sobre as boas práticas regulatórias implica na regulação de setores não regulados e no diálogo direto da ANPD com os setores econômicos regulados, avançando na harmonização entre a LGPD e as demais normas aplicáveis a setores regulados.
11. Medidas de segurança, técnicas e administrativas, incluindo padrões técnicos mínimos de segurança (Art. 46 da LGPD)	2 - Pouca importância (Neutro - pode esperar a longo prazo) Considerando que há setores (a exemplo do financeiro) que contam com a existência de

	normas específicas sobre o tema, entende-se que a discussão no âmbito da ANPD pode ser precedida por pautas de cunho mais basilar (a exemplo dos dados biométricos). Assim, em razão da urgência de outros temas, a prioridade para o presente item é menor.
12. Registro de Operações (Art. 37 da LGPD)	1 - Nenhuma importância (Não há ou há pouca necessidade de regulamentação) Não há a necessidade, a curto prazo, de regulação neste tópico, sobretudo porque esta discussão pode impactar as estruturas já estabelecidas pelas empresas até o momento. Sugere-se, em alternativa, que a ANPD disponha de orientações (guias) sobre o tema.
13. Compartilhamento de dados pelo poder público (Art. 25 da LGPD)	2 - Pouca importância (Neutro - pode esperar a longo prazo) Há normas de caráter geral que se mostram mais prementes, na medida em que se aplicam a maior número de setores econômicos e envolvem volume considerável de atividades de tratamento.
14. Opiniões técnicas ou recomendações referentes às exceções	2 - Pouca importância (Neutro - pode esperar a longo prazo)

previstas no inciso III do Art. 4º da LGPD (Art. 4, § 3º da LGPD)	Há normas de caráter geral que se mostram mais prementes, na medida em que se aplicam a maior número de setores econômicos e envolvem volume considerável de atividades de tratamento.
15. Regulação - setor econômico de Saúde (Art. 11, § 4º; Art. 13 da LGPD)	3 - Razoavelmente importante (Neutro - pode esperar a médio prazo) De um lado, os dados de saúde são dados pessoais sensíveis, exigindo atuação mais rápida da ANPD em estabelecer as limitações. De outro, há normas de caráter geral que se mostram mais prementes, na medida em que se aplicam a maior número de setores econômicos e envolvem volume considerável de atividades de tratamento.
<u>Sobre quais outros temas (4-importantes ou 5-muito importantes) você gostaria que a ANPD considerasse na elaboração da próxima Agenda Regulatória? Favor, justificar a necessidade.:</u> Realizar uma regulação específica para o Tratamento de Dados Pessoais de Alto Risco. <u>Justificativa:</u> Na visão da ABCD e ABIPAG, a regulação aplicável ao tratamento de Dados Pessoais deve ser proporcional ao risco da atividade de tratamento, de modo que cumpre aos agentes de tratamento que realizarem atividades de alto risco observar obrigações adicionais relacionadas à proteção de dados, tais como: (i) conferir direito de acesso não-discriminatório às infraestruturas; (ii) viabilizar a revisão de decisões de moderação; (iii) assegurar a portabilidade de dados; e (iv) disponibilizar relatórios de transparência. Tais	

direitos são fundamentais para os titulares de dados exercerem sua autodeterminação informativa e reduzir sua dependência de prestadores de serviços incumbentes, em um cenário de baixa possibilidade de portar de plataforma.

Considera-se alto risco a ocorrência de uma série de critérios cumulativos, dentre os quais: (i) o tratamento massivo de dados, que envolva mais de **45 milhões de titulares** localizados em território nacional, nos termos da regulação de plataformas da União Europeia (*Digital Markets Act*² e *Digital Services Act*³); e (ii) tratamento de atividades em setor não-regulado.

A agenda regulatória da ANPD para o biênio 2023-2024 mostra-se uma grande oportunidade para regular operações de tratamento de alto risco, com fundamento nos artigos 50 e 55-J, XIII da LGPD, de modo que a ANPD possa focar sua fiscalização nas operações que possam gerar mais danos relevantes aos titulares de Dados Pessoais, a partir de uma metodologia de riscos de privacidade e proteção definidas, como os modelos de excelência das autoridades de proteção de dados do México (INAI)⁴ e da Espanha (AEPD).⁵

Isso deve ocorrer para além da mera regulação das exceções ao regime flexível de tratamento por agentes de pequeno porte, tal qual em curso atualmente, de forma que haja uma **regulação aplicável a todos que se enquadrem como alto risco**.

Classificação:

5 - Muito importante (Urgente e prioritário)

Ademais, são temas relevantes para a Agenda Regulatória de 2023-2024:

² <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=pt>

³ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

⁴ [https://www.google.com/url?sa=t&source=web&rct=j&url=https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%25C3%25ADa%20de%20An%25C3%25A1lisis%20de%20Riesgo%20BAA\(Junio2015\).pdf&ved=2ahUKEwj2emyrO75AhWruZUCHYakCHoQFnoECACQAQ&usg=AOvVaw35WI9y_qfKRZcFul-veJNg](https://www.google.com/url?sa=t&source=web&rct=j&url=https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%25C3%25ADa%20de%20An%25C3%25A1lisis%20de%20Riesgo%20BAA(Junio2015).pdf&ved=2ahUKEwj2emyrO75AhWruZUCHYakCHoQFnoECACQAQ&usg=AOvVaw35WI9y_qfKRZcFul-veJNg)

⁵ <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluaciones-impacto>

i) elaboração de Guia sobre a utilização de bases legais pelos agentes de tratamento, contribuindo com a cultura de proteção de dados pessoais no país. Os agentes de tratamento ainda possuem dificuldades em entender os contornos das bases legais e os critérios para a sua utilização, bem como as exigências que eventualmente trazem. Por exemplo, a base legal de proteção ao crédito é uma inovação brasileira e os agentes de tratamento não têm quaisquer referências internacionais para saber os limites do uso desta base legal. Exemplos práticos dos mais diversos mercados seriam muito úteis, por exemplo, da saúde, educação, setor público, financeiro, dentre outros;

Classificação:

4 - Importante (Prioritário - pode esperar a curto prazo)

ii) elaboração de modelos e orientações para a construção do Relatório de Impacto de Proteção de Dados (RIPD) e o LIA (teste de balanceamento de legítimo interesse).

Classificação:

4 - Importante (Prioritário - pode esperar a curto prazo)

iii) padronização de prazos de resposta pelos Controladores a titulares.

Classificação:

4 - Importante (Prioritário - pode esperar a curto prazo)