Submission by Privacy International, Data Privacy Brazil Research Association and Internet Lab in advance of the third periodic report of Brazil on the implementation of the International Covenant on Civil and Political Rights during the 138th session of the UN Human Rights Committee

Introduction

This joint submission by Privacy International, Data Privacy Brazil Research Association and Internet Lab is for the 138th Session of the UN Human Rights Committee that will take place between 26 June 2023 and 28 July 2023 in relation to Brazil's compliance with the International Covenant on Civil and Political Rights (ICCPR).

Privacy International (PI) is a non-governmental international organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Data Privacy Brazil Research Association (DPBR) is a Brazilian non-profit civil society organization that promotes the protection of personal data and other fundamental rights in the face of the emergence of new technologies, social inequalities, and power asymmetries. The organisation has a multidisciplinary team from different Brazilian regions that develops public interest research, technical briefs, analytical texts on emerging issues, and training sessions with decision-making agents and society in general.

INTERNETLAB (IL) is an independent research centre that aims to foster academic debate around issues involving law and technology, especially internet policy. IL conducts interdisciplinary impactful research and promotes dialogue among academics, professionals and policymakers. IL follows an entrepreneurial non-profit model, which embraces the pursuit of producing scholarly research in the manner and spirit of an academic think tank. As a nexus of expertise in technology, public policy and social sciences, IL's research agenda covers a wide range of topics, including privacy, freedom of speech, gender and technology.

This joint submission focuses on our concerns regarding the use of education technologies (EdTech) in Brazil and its implications on the right to privacy under Article 17 ICCPR. Considering this, the submission discusses the use of facial recognition technologies in educational settings, issues with procurement pertaining to EdTech, concerns with artificial intelligence (AI), and general regulatory failings in Brazil. We also specifically address allegations that educational technology websites and applications, which were endorsed and used by the education authorities of Minas Gerais and São Paulo, harvested and sold data collected in the context of online educational activities provided to children during the COVID-19 pandemic raised in paragraph 23 of the List of Issues.[1]

Recommendations

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

In light with the information and analysis contained in the sections below, we recommend the Human Rights Committee call on Brazil to:

- Adhere to its international and national human rights standards to uphold the right to privacy and the rights of the child pertaining to EdTech;
- Ban the use of facial recognition technology (FRT) in educational settings given its disproportionality, security risks, inaccuracies and discriminatory biases and illegality of processing of children's biometric data;
- Ban the profiling and targeting of children for advertising purposes using classroom EdTech platforms;
- Implement safeguards to prevent data exploitation by EdTech platforms and companies to ensure data minimisation, appropriate data retention and deletion in line with Brazil's data protection law [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018];
- Ensure that robust human rights due diligence processes (including data protection and child right's impacts assessments) are in place, that include within their scope the early stages of the design and development of an EdTech technology, as well as stages of deployment and use. Details of the processes in place should be made public and available for review;
- Ensure that EdTech that uses AI is regulated to reduce the harms associated with AI, including making their algorithms transparent and allow systems to be auditable;
- Adhere to formal public procurement processes when awarding a contract to an EdTech company and put in place formal documentation governing the partnership;
- Provide training to educators and public administrators in data protection legislation and digital protection of children and adolescents – including, continuous training courses to enhance administrators' digital literacy and enable them to evaluate the use of digital technologies beyond usability;
- Ensure that the use of EdTech is regulated in line with Brazil's data protection framework [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018] and that the Data Protection Authority regulates the use of children's data in line with the LGPD.

Education Technologies (EdTech) and their rise in Brazil

EdTech describes technology or software that can be used in educational settings which involves the electronic processing of users' data, in particular children's data.[2] This includes software used for behaviour management, for education administration purposes and software used to assist with teaching lessons and educational materials.[3] It also includes the use of facial recognition technology (FRT) which is being increasingly implemented in educational settings such as schools.

The use of EdTech in Brazil has been rapidly expanding under Brazil's Plano Nacional de Educação (PNE – National Education Plan) which included several goals to encourage technologies to provide digital equipment and resources to schools, and to digitise the management of public schools and the departments of education in the states, federal districts, and municipalities.[4]

Furthermore, in response to the Covid-19 pandemic with the need for remote learning and virtual classrooms, the use of EdTech has accelerated further. Before the pandemic only 21%

[2] Privacy International, 'EdTech Needs Schooling', https://privacyinternational.org/campaigns/edtech-needs-schooling
[3] Ibid.
[4] Plano Nacional de Educação (PNE) (National Education Plan), 2014, https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13005.htm

of schools in Brazil provided remote learning activities rising to 51% in 2020.[5] By the end of 2020, 45% of public schools and 76% of private schools in Brazil already had implemented systems for remote learning.[6] Since then municipalities all over Brazil are increasingly interested in acquiring technologies for educational purposes, such as virtual learning tools and educational robotics.[7]

Schools in Brazil are also increasingly using digital systems to organise student information for administrative purposes. According to a survey: 85% of schools use digital systems to manage information associated with student registration, such as name, address, telephone number, and date of birth; 82% of schools use digital systems to manage data concerning student attendance and grades; 46% of schools use digital systems to manage data on students' physical condition and health, such as weight, height, and allergies; 59% of schools use digital systems to manage teacher- and staff-performance evaluation results and; 71% of schools use digital systems to manage data on the school's budget.[8]

These are extremely data intensive technologies that rely on the collection, analysis, retention and processing of children's, their families', and teachers' data. Where children's data or highly sensitive data is involved, for example biometric data, additional protections are required. However, we are seeing failings in the state's regulatory framework governing data pertaining to EdTech resulting in violations of Article 17 ICCPR.

Furthermore, the involvement of non-state actors with user's data, in this case, the involvement of private companies, is also interfering with individual's privacy under Article 17 ICCPR. For example, procurement is not in accordance with human rights standards, and we are seeing unfettered access to individual's data for purposes beyond education, to serve their economic interests.

The use of Facial Recognition Technologies in Educational Settings

The use of FRT in educational settings has been rolled out in Brazilian public schools, with initiatives across different regions of the country. INTERNETLAB (IL) conducted research to identify how Brazilian public schools adopt facial recognition policies, mapping the degree of expansion, forms of use and common practice.[9] Fifteen cases were identified across different regions of the country.[10] The research explored similarities and differences between these cases including analysis of whether policies were in place; whether impact assessments were conducted; whether there was civil society participation; how facial recognition was being used; the process of procuring companies; and data protection practices.

Findings

Regarding the implementation of FRT in educational settings local authorities claimed it was for optimising school management including addressing school evasion and for security

[5] Centro Regional para o Desenvolvimento da Sociedade da Informação (Cetic.br)., TIC Educação 2019, Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nas Escolas Brasileiras 12,https://cetic.br/media/docs/publicacoes/2/20201123090444/tic_edu_2019_livro_eletronico.pdf, pg 25.
[6] Ibid.
[7] Open Knowledge Brazil, Querido Diário (2023): Panorama #1: Radar das tecnologias na educação nos municípios, https://queridodiario.ok.org.br/educacao/relatorio/1
[8] Centro Regional para o Desenvolvimento da Sociedade da Informação (Cetic.br), TIC Educação 2020 - Edição COVID-19 metodologia adaptada. Coletiva de Imprensa [Slides], 31 August 2021, https://cetic.br/media/analises/tic_educacao_2020_coletiva_imprensa.pdf
[9] Internet Lab, 'Surveillance Technologies and Education: Mapping Facial Recognition Policies in Brazilian Public Schools', 2023, https://internetlab.org.br/wp-content/uploads/2023/03/Educacao-na-mira-EN-02.pdf
[10] (i) Tocantins (TO); (ii) Mata de São João (BA); (iii) Fortaleza (CE); (iv) Jaboatão dos Guararapes (PE); (v) Águas Lindas (GO); (vi) Goiânia (GO); (vii) Morrinhos (GO); (viii) Betim (MG); (ix) Rio de Janeiro (RJ); (x) Angra dos Reis (RJ); (xi) Itanhaém (SP); (xii) Potirendaba (SP); (xiii) Santos (SP); (xiv) Porto Alegre (RS); (xv) Xaxim (SC).

purposes. They argue that using facial recognition saves staff time by automating tasks such as managing absences, tracking the number of required food and supplies in classrooms. Public officials also assert that facial recognition can prevent tampering with attendance records, enable reporting to the Guardianship Council (***Conselho Tutelar***) about students, and facilitate the management of social protection policies like the Family Allowance (***Programa Bolsa Família***) based on attendance. The implementation of facial recognition is also being used to prevent unauthorised individuals from entering and protecting school property.[11]

Within fourteen out of fifteen of the Brazilian States FRT was implemented by public authorities at municipal level through public contracts signed with national companies that offer technology services. In most of the cases identified, the implementation of the technology is still in the initial testing phases, not covering the entire municipal or state education network.[12]

FRT has been fully implemented in three municipalities: Betim, Jaboatão dos Guararapes, and Goiânia. In three other cases (Xaxim, Morrinhos, and Tocantins), the technology is still in its initial testing stages and does not cover the entire municipal or state education network. Unfortunately, there is insufficient information available about the degree of implementation of facial recognition policies in the municipalities of Angra dos Reis (RJ), Águas Lindas (GO), Itanhaém (SP), and Mata de São João (BA).[13]

Within the three municipalities it has been implemented, all of the 69 elementary school units in the city have FRT in place. In Goiânia, the facial recognition system is already in full use in municipal educational units, but technical adjustments are still needed to integrate the facial recognition system into the school management system. According to the Municipal Department of Education and the Agency of Innovation and Educational Technology, 336 school units have the infrastructure and access to the school management system of facial recognition. In Jaboatão dos Guararapes, 125 municipal elementary schools (from 1st to 9th grade) already have facial biometrics systems.[14]

IL found that no municipalities or states reported conducting human rights impact assessment studies or analysing potential risks of discrimination associated with facial recognition software before implementing the projects. Some municipalities that have made progress in implementing facial recognition claim that the technology has a high accuracy rate. However, one municipality highlighted cases where the system incorrectly recorded a student's attendance.[15]

While public administrators assert that the implementation of facial recognition was driven by demands from the educational community, only two municipalities (Itanhaém and Jaboatão dos Guararapes) indicated some level of civil society participation in the project development.[16]

Regarding data protection practices, it was observed that the equipment collected students' biometric data, stored it within the system's database and used it for attendance records. The treatment of data upon students' departure from educational institutions varies across municipalities: in some cases, the data remains stored within the Department of Education, while in others, the biometric data is removed from the database. As one of the stated purposes for facial recognition is to prevent school dropouts, the data is shared, in some cases, with the Guardianship Council (***Conselho Tutelar***) when a student's frequent absence from the school becomes a concern. Public authorities also mentioned data sharing

[11] Internet Lab, 'Surveillance Technologies and Education: Mapping Facial Recognition Policies in Brazilian Public Schools', 2023, https://internetlab.org.br/wp-content/uploads/2023/03/Educacao-na-mira-EN-02.pdf
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid.
[16] Ibid.

among educational managers and with the public administration to enhance the execution of education-focused public policies.[17]

Human Rights Implications

We believe the use of facial recognition technology within educational settings in Brazil violates Article 17 ICCPR. The use of FRT in educational settings is intended to address existing challenges such as overcrowded classrooms, insufficient funds for school meals, school evasion and violence. However, using FRT to address these issues raises significant issues regarding proportionality and necessity of the invasion of privacy under Article 17 ICCPR. Less privacy invasive measures could clearly be adopted to address these challenges without processing children and adolescent's highly sensitive biometric data.

The Committee on the Rights of the Child within their General Comment no.25 has specifically noted that "any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and 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; nor should it 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".[18]

Furthermore, there is potential for discriminatory biases within facial recognition systems, particularly towards marginalised groups. Numerous studies have highlighted how these technologies are less accurate when it comes to non-male or non-white individuals, as they are often trained on datasets lacking gender diversity, racial representation, and cultural records.[19] In addition to accuracy concerns, there are other issues to consider, such as security incidents that may lead to unauthorized access, theft, loss, or misuse of the stored data which can lead to violations under Article 17 ICCPR.

Furthermore, some schools disclosed that data collected by FRT processes could be shared with other public institutions for example, with the Guardianship Council, for matters regarding school evasion. Civil society representatives within Brazil have expressed concerns about the effectiveness of facial recognition in addressing these challenges faced by Brazilian public schools. The causes of problems like overcrowded classrooms are deeply rooted in structural issues within Brazil's education system, which cannot be easily solved through technology alone. The same applies to school evasion, a complex issue influenced by factors such as lack of public transportation, violence against children and teenagers, child labour, and poverty. Therefore, the use of FRT is not a proportionate and reasonable measure to address these issues.

There is currently no specific legislation in Brazil, at the federal, state, or municipal level, that specifically regulates the use of facial recognition or biometric recognition technologies, particularly in the field of education.[20] At the local level, budget laws allocate funds for the education sector, but there are no specific programs or actions related to the development, procurement, and maintenance of facial recognition technologies in schools. The municipality of Mata de São João (BA) is the only exception, as it has established guidelines through municipal laws that govern the treatment of personal data (Municipal Decree No. 162, April 1st, 2022) and the security of municipal information (Municipal Policy for Information Security). However, it is important to note that, like other locations, Mata de São João has

[17] Ibid.
[18] Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', CRC/C/GC/25, 2 March 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[19] Privacy International, 'Facial Recogniton'. https://privacyinternational.org/learn/facial-recognition
[20] Internet Lab, 'Surveillance Technologies and Education: Mapping Facial Recognition Policies in Brazilian Public Schools', 2023, https://internetlab.org.br/wp-content/uploads/2023/03/Educacao-na-mira-EN-02.pdf

not provided any information regarding the conduction of risk studies before or during the implementation and use of facial recognition technology.

We recommend the Human Rights Committee call on Brazil to:

- Ban the use of of facial recognition technology (FRT) in educational in educational settings given its disproportionality, security risks, inaccuracies and discriminatory biases and illegality of processing of children's biometric data.

Allegations that educational technology websites and applications, which were endorsed and used by the education authorities of Minas Gerais and São Paulo, harvested and sold data collected in the context of online educational activities provided to children during the COVID-19 pandemic[21]

In May 2022, research conducted by Human Rights Watch (HRW) found that seven educational websites in Brazil were extracting and sharing children's data to third-party companies using tracking technologies designed for advertising.[22] The websites tracked the physical location and users' activities outside of the website, as well as having access to the student's phone contact list and ability to download personal details about family and friends. The websites included Estude em Casa, Centro de Mídias da Educação de São Paulo, Descomplica, Escola Mais, Explicaê, MangaHigh, and Stoodi. An eighth website, Revisa Enem, also sent children's data to a third-party company, without using ad-specific trackers.

The report found that seven Brazilian websites recommended for remote learning during the pandemic by São Paulo and Minas Gerais, (the two most populous states in the country): (i) carried out surveillance of students' online activities beyond the intended use of the platform; that (ii) none of these websites allowed users to decline being tracked; and (iii) the data collected was not transparent to children and teenagers all of which led to a violation of Article 17 ICCPR.

In response to the 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. This suggests that sufficient due diligence and human rights impact assessments were not conducted by Brazilian authorities. Before the report was published Escola Mais did not respond to requests for comment and only after media reports the company subsequently removed from its website all student-facing links to its online learning platform.[23]

Also, in response to these findings, the education secretariat of Minas Gerais removed all ad tracking from its websites.[24] However, the São Paulo education secretariat continues to endorse the use of the education websites that improperly harvest children's data and did not respond to HRW questions. This shows that the national General Personal Data Protection Law (does not provide sufficient protections for children using EdTech and

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

[22] Human Rights Watch, 'How Dare They Peep into My Private Life? Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic', 25 May 2022, https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

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

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

highlights the lack of consideration of human rights standards through which Brazil is signatory to.

Privacy International conducted a technical analysis of the research methods used by HRW, including the types of analysis (static and dynamic) that were performed on the platforms to understand the conclusions that were drawn and the extent of harms. PI has previously conducted similar types of analysis on various websites and applications to find that companies were relying on some form of tracking within their services.[25]

A static analysis of applications using tools such as Exodus Privacy can provide several insights into the privacy and security practices of apps such as the collection of sensitive user data; a list of third parties with whom data is shared; vulnerabilities within the app's code and the permissions that the app requests within the owner's device. It analyses an app's code and identifies its capabilities and which functions, or instructions may be executed when the app is running. This analysis is conducted without the need for user interaction and is primarily a useful tool to help users make informed decisions about what they can expect from an app without having to interact with it. The more permissions are requested from an app and the more trackers it uses, the higher the risk to privacy.

A dynamic analysis of an application's traffic allows for the person conducting the research to see all data exchanges being done within the app under realistic conditions. This means one can see what data is leaving the analysed device and with whom it's being shared with. This method provides insight into what is happening to data within the apps, which is extremely useful to complement and cross-check a (broader and more uncontextualized) static analysis.

A static analysis of websites using Blacklight provides an instant insight into the capabilities of a website regarding seven widely documented types of tracking technologies: Canvas fingerprinting, cookies, Meta (formerly Facebook), pixel events, key logging, third party trackers and session recorders.

The Adtech (Advertising Technology) ecosystem relies on a complex network of data brokers, ad networks, and other intermediaries, usually with no direct explicit connection to the applications or websites where they are present. The inherent opaqueness of this ecosystem makes it extremely difficult to understand and control what data is being collected, how it's being processed/used, by whom and who the data is being shared with, again interfering with the right to privacy.

Within PI's submission to the 41st session of the Universal Period Review of Brazil we highlighted other examples of EdTech platforms and companies that were collecting, and processing of user's data causing significant interferences with Article 17 ICCPR.[26] These examples included IP.TV[27] (a company responsible for the creation of EdTech mobile applications in Brazil used within the states of Amazonas, Paraná, Pará and Sao Paulo) and Google Workspace (a collaborative tool for teachers and students has been widely implemented throughout the Brazilian education system in schools across all states and the Federal District).[28]

---

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

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

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

[28] Secretaria de Estado de Educação do Amazonas (SEDUC), 'Professores e alunos da rede estadual podem ativar e-mail institucional para ajudar no ensino remoto', 22 February 2021,

General Comment no.16 on Article 17 ICCPR specifically states that "every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination".[29]

When personal data is envisaged to be processed by an EdTech platform, there should be transparency regarding the data processing activities and safeguards around how that data is used including how long the data will be retained and what will be done with users' data when the partnership ends.

Not only does this interfere with Article 17 ICCPR but also interferes with other rights including the rights contained with the Convention on the Rights of the Child. The UN Committee on the Rights of the Child within its General Comment 25 recommended State parties 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".[30] It also sets that "Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children (..) misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity".[31]

Overall, our analysis allows us to support allegations presented in the HRW report, that educational technology websites and applications, endorsed and used by the education authorities of Minas Gerais and São Paulo, and that most of the mentioned platforms were complicit in facilitating some form of student tracking, whether this was intentional or not.

We recommend the UN Human Rights Committee call on Brazil to:

- Ban the profiling and targeting of children for advertising purposes using classroom EdTech platforms.
- Implement safeguards to prevent data exploitation by EdTech platforms and companies to ensure data minimisation, appropriate data retention and deletion in line with Brazil's data protection law [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018.
- Ensure that robust human rights due diligence processes (including human rights, data protection and child right's impacts assessments)[32] are in place, that include within their scope the early stages of the design and development of an EdTech technology, as well as stages of deployment and use. Details of the processes in place should be made public and available for review.

---

http://www.educacao.am.gov.br/gestores-professores-e-alunos-da-rede-estadual-podem-ativar-e-mail-institucional-para-ajudar-no-ensino-remoto/; Freedom of Information Act Request, Protocol nº 00080000386202140, Governo do Estado do Maranhão, 21 October 2017, Parceria entre Governo e Google Brasil disponibiliza 13 mil vagas para revisão do Enem a estudantes da rede pública. Ouça: https://www.ma.gov.br/agenciadenoticias/?p=202953; SEI Process nº 030029/002262/2020.

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

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

[31] Ibid, para 103.

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

Artificial Intelligence (AI) in EdTech and educational settings

EdTech in Brazil can also use artificial intelligence which has additional risks to human rights.[33] EdTech platforms may use AI to recommend students educational content based on test results with the intention to expediate learning, as well as software that uses AI to autonomously correct students' essays. AI can also be used more generally in educational settings for example, within the recent security program being piloted in the State of Paraná, that is seeking to use AI to enhance security in schools. The AI technology will be used to analyse images from security cameras for "unusual behaviour" and then communicate this with authorities.[34] There is a real risk that the use of new AI tools in educational settings without the appropriate safeguards will have a negative impact on human rights, including the right to privacy.

In addition to risks to users' privacy discussed above, through the tracking, generating, processing of data, there are also risks of discrimination through the inaccuracies and biases that AI algorithms are built upon. AI systems can therefore exacerbate existing inequalities and cause further harm to individuals in vulnerable positions. For example, when AI is used in educational settings in Brazil, there is a danger of perpetuating existing inequalities and discrimination such as those linked to lower educational attainment associated with greater income inequality, which is a persistent issue in Brazil.[35] The risks of AI when used on children are also exacerbated due to their physical, psychological, social, and emotional developmental stage.

EdTech that uses Algorithms and other decision-making processes should be open to scrutiny and challenge by being auditable. The ability to audit technologies is essential to provide adequate oversight and redress. For example, if a technology has led to a result that is later challenged in court or used as evidence, the proper administration of justice requires the technology to be entirely auditable.[36] Data Privacy Brazil Research Association's (DPBR) current project 'AI in the classroom: models of participation for the school community' explores the employment of technologies that use AI for educational purposes.[37] With the aim of proposing a participatory model for auditing AI in educational settings which involves the entire school community, especially students, their families, and educators.

A legal framework to regulate AI was recently introduced by the Brazilian House through the Artificial Intelligence Bill. However, the Bill received negative feedback and was considered by some as a "deregulation bill" rather than a legal framework.[38] In response to concerns a Senate working group was established formed of a group of legal experts, members of academia, companies, and Brazil's national data protection watchdog. [39] A public

[33] Privacy International, 'Artificial Intelligence', https://privacyinternational.org/learn/artificial-intelligence.
[34] See Celepar, "Com inteligência artificial, Celepar torna escolas do Paraná mais seguras", 27 March 2023, https://www.celepar.pr.gov.br/Noticia/Com-inteligencia-artificial-Celepar-torna-escolas-do-Parana-mais-seguras#:~:text=Com%20intelig%C3%AAncia%20artificial%2C%20Celepar%20torna%20escolas%20do%20Paran%C3%A1%20mais%20seguras,-A%C3%A7%C3%A3o%20integra%20Programa&text=A%20seguran%C3%A7a%20em%20escolas%2C%20no,solu%C3%A7%C3%A3o%20para%20as%20institui%C3%A7%C3%B5es%20escolares
[35] Committee on the Rights of the Child examines report of Brazil, 22 September 2015, https://www.ohchr.org/en/press-releases/2015/09/committee-rights-child-examines-report-brazil
[36] Privacy International, 'Safeguard for Public-Private Surveillance Partnerships', December 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf.
[37] Data Privacy Brazil, "AI in the classroom: models of participation for the school community", https://www.dataprivacybr.org/en/projeto/ai-in-the-classroom-models-of-participation-for-the-school-community/
[38] Wilson Centre, "AI Regulation Still Lagging in Brazil", 2023, https://www.wilsoncenter.org/blog-post/ai-regulation-still-lagging-brazil
[39] iapp, "Brazil's AI commission to deliver final report", 2022, https://iapp.org/news/a/brazils-ai-commission-to-deliver-final-report/

consultation process[40] was conducted and was followed by a written report which was published in December 2022, with recommendations on how Brazil should regulate AI.[41] The report's recommendations have three main focal points: citizens' rights, the categorisation of risks, and the governance measures and administrative sanctions that must be activated when the regulation is not adhered to.[42]

We recommend the UN Human Rights Committee call on Brazil to:

- Ensure that EdTech that uses AI is regulated to reduce the harms associated with AI including making their algorithms transparent and allow systems to be auditable.

Procurement of EdTech in Brazil

The procurement of EdTech by Brazilian authorities raises significant concerns which have implications for user's privacy. Research shows that during the Covid-19 pandemic schools chose platforms and resources for remote learning based on which was most cost effective, which does not guarantee the best interests of the child or protection of human rights. Technology companies and EdTech start-ups have been influencing local government and schools to "test" their products in small municipalities.[43]

EdTech platforms and programs in Brazil have been obtained through cooperation agreements, bidding processes or through donations. Cooperation agreements can be used in Brazil when both parties have a common interest, which should be aligned with public interest and does not allow a transfer of resources to be permitted. However, companies that provide EdTech platforms and tools, can generate profit through data processing and therefore do not require direct monetary payment to generate profit. Therefore, in this case, data transfer should be understood as a transfer of resources.[44]

For example, Google Classroom was implemented through a donation made by the company Empresa Ensinar Tecnologia Educacional LTDA.[45] According to the Department of Education, the criteria used in deciding what software to use was that the Google service was free of charge.[46]

The UN Special Rapporteur on the Right to Education has highlighted regarding the mining of data on, students, families and communities, as well as educators and other staff in educational settings, child specific privacy and data protection laws; child's rights impact assessments before adopting digital technologies in education and due diligence with private providers to ensure that the technology they recommend for online learning protects children's privacy and data protection rights.[47]

---

[40] Privacy International, 'Submission to the Commission of Jurists on the Brazilian Artificial Intelligence Bill', https://privacyinternational.org/advocacy/4984/submission-commission-jurists-brazilian-artificial-intelligence-bill

[41] See https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4

[42] Ibid.

[43] See "Municípios lançam edital para contratar edtechs no ensino público", Folha de S. Paulo, 2 February 2022, https://www1.folha.uol.com.br/empreendedorsocial/2022/02/municipios-lancam-edital-para-contratar-edtechs-no-ensino-publico.shtml

[44] It is important to highlight that, in terms of consumer protection, the Brazilian Superior Court of Justice recognised that the consumption relationship exists even when the service provided is free of charge. This is because remuneration must be understood in a broad way, in order to include the indirect gain of the supplier. Rapporteur Min. Nancy Andrighi, Superior Court of Justice, REsp nº 1.193.764, Electronic Official Gazette, 8 August 2011.

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

[46] Freedom of Information Act Request, Protocol nº 00080000386202140.

[47] Human Rights Council, 'Report of the Special Rapporteur on the right to education on the impact of the digitalization of education on the right to education', A/HRC/50/32, 19 April 2022,

We recommend the UN Human Rights Committee call on Brazil to:

- Adhere to formal public procurement processes when awarding a contract to an EdTech company and put in place formal documentation governing the partnership.
- Provide training to educators and public administrators in data protection legislation and digital protection of children and adolescents – including, continuous training courses to enhance administrators' digital literacy and enable them to evaluate the use of digital technologies beyond usability.

Legislative failings

It is evident the acquisition of EdTech is not specifically regulated and that human rights and data protection standards are not being upheld by the Brazilian State. The Brazilian government and relevant agencies such as the National Data Protection Authority need to fulfil their obligations to uphold the right to privacy while using these technologies.

At international level Brazil has ratified several international human rights treaties. At national level Brazil's Constitution of the Federative Republic of Brazil 1998 (FC)[48] guarantees fundamental rights including privacy and data protection. The ***Estatuto da Criança e do Adolescente*** (ECA)[49] (Child and Adolescent Statute) 1990, regulates the rights of children and adolescents which includes the right to privacy under Article 17.

Brazil's data protection law, [Lei Geral de Proteção de Dados Pessoais (LGPD) 2018][50] came into force in 2020 (for general provisions) and 2021 (for administrative sanctions). According to Article 14 of the LGPD, the processing of personal data of children and adolescents should be carried out in their best interest, with specific and explicit consent of at least one parent or legal guardian. In Brazil, a child is any person under 12 years old, while an adolescent is anyone between 12 and 18 years old.[51] This distinction is important when interpreting Article 14, Paragraph 1, since it demands that consent should be given by parents or legal guardians only when children's data are processed. This consent related to children's data is not demanded when data collection is necessary to contact parents or legal guardians, as long as the data are used one single time and not stored, or for children's protection. In this case, data shall not be shared with third parties without consent from the parents (Article 14, Paragraph 3).

Information about the kind of data collected should be published "in a simple, clear and accessible way" both to the understanding of parents and guardians, and to the understanding of children and adolescents. The Law states that data controllers shall not condition children's participation in games, internet applications or other activities on the provision of personal data beyond what is strictly necessary for the activity (Article 14, Paragraph 4). It is noteworthy that implementation guidelines should still be published by the National Data Protection Authority, but its formulation was not included in the authority's regulatory agenda for the biennium 2023-2024.

The National Policy on Digital Education, instituted by bill 14.533, was sanctioned in January 2023 by the President. As part of this policy, digital education must be included in schools'

https://www.ohchr.org/en/documents/thematic-reports/ahrc5032-impact-digitalization-education-right-education

[48] Constituição da República Federativa do Brasil de 1988 – Constitution of the Federative Republic of Brazil (FC) 1998.

[49] Estatuto da Criança e do Adolescente (ECA) 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

[50] Lei Geral de Proteção de Dados Pessoais (LGPD) 2018, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; An English version is available at: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

[51] Article 2, Estatuto da Criança e do Adolescente (ECA) 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

curriculum, entailing the development of a critical view towards the use of technology and awareness of digital rights (Article 3, III and IV).

The 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." [52] Laws should be updated to specifically support enforcement and compliance in digital environments.[53]

We recommend the UN Human Rights Committee call on Brazil to:

- Adhere to its international and national human rights standards to uphold the right to privacy and the rights of the child pertaining to EdTech.
- Ensure that the use of EdTech is regulated in line with Brazil's data protection framework [(Lei Geral de Proteção de Dados Pessoais (LGPD) 2018] and that the Data Protection Authority regulates the use of children's data in line with the LGPD.

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