PRIVACY
INTERNATIONAL

30 June 2022

Privacy International's submission to the Commission of Jurists on the Brazilian Artificial Intelligence Bill

Introduction

Privacy International (PI)[1] is an international non-profit, non-governmental organisation that conducts research 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 recognises that Artificial Intelligence (AI) has the potential to revolutionise societies in many ways. However, as with any scientific or technological advancement, there is a real risk that the use of new tools by states or corporations will have a negative impact on human rights, including the right to privacy. This is of further concern when such technologies are used on individuals with protected characteristics such as children.

AI is becoming increasingly common in schools[2], as part of teaching[3], in classrooms[4], and as part of the administrative running of schools[5]. What has not kept pace has been appropriate safeguards, despite an increasing body of evidence around the potential harms of AI systems[6] and the particularly vulnerable situation of children.

PI's submission will focus on highlighting the potential harms associated with the use of AI within schools and the additional safeguards and precautions that should be taken when implementing AI in educational technology. The use of AI in education technology and schools has the potential to interfere with the child's right to education and the right to privacy which are upheld by international human rights standards that Brazil has ratified. There is a positive obligation to ensure that an appropriate legal framework is in place to protect individuals from such human rights

[1] PI is an international non-governmental organisation that campaigns against companies and governments who exploit individuals' data and technologies. PI employs specialists in their fields, including technologists and lawyers, to understand the impact of existing and emerging technology upon data exploitation and our right to privacy. Available at: https://privacyinternational.org/

[2] Available at: https://www.gminsights.com/industry-analysis/artificial-intelligence-ai-in-education-market

[3] Available at: https://xenoss.io/blog/ai-edtech-startups

[4] Available at: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv

[5] Available at: https://www.classcharts.com

[6] Available at: https://www.mckinsey.com/business-functions/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence

abuses. The relevant standards include the UN Convention on the Rights of the Child (UN CRC)[7], the UN Convention on Civil and Political Rights and the UN Convention (UN ICCPR)[8] and the UN Convention on Economic, Social and Cultural Rights (UN ESCR).[9] There also soft law measures such as the Abidjan Principles that provide human rights guidance for States to provide public education and to regulate private involvement in education. Furthermore, the impact of the digitalisation of education, which includes the use of AI, has been a recent thematic focus of the UN Special Rapporteur on the Right to Education, Koumbou Boly Barry, in their report the "Impact of the digitalization of education on the right to education".[10]

The Impact of AI in Schools on Children's Rights

Firstly, PI would highlight that the use of AI in schools will have direct impact on children's enjoyment of their fundamental rights, who by default, have the right to additional measures of protection as is required by their status as minors.[11]

The Special Rapporteur on the Right to Education has highlighted that the digitalisation of education brings serious risks to human rights, including the right to education. Some risks are the exact opposite of potential benefits such as heightened exclusion instead of improved access, standardisation instead of personalised teaching, enhanced stereotypes instead of diversity, reduced autonomy, and freedom instead of creativity and participation, and data mining for the benefits of a few at odds with the public interest.[12] Furthermore, the use of AI systems schools and education technology can exacerbate these issues further and directly interfere with children's privacy and lead to potential discrimination and limit access to education.

Right to Privacy

AI systems require the generation, collection, processing, and retention of mass amounts of personal data and therefore directly interferes with the right to privacy. Article 17 UN ICCPR upholds the right to privacy, providing that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence and that everyone has the right to the protection of the law against such interference or attacks. Article 16 UN CRC provides that the

[7] Ratified by Brazil in 1990.
[8] Ratified by Brazil 1992.
[9] Ratified by Brazil 1992.
[10] A/HRC/50/32 UN General Assembly Human Rights Council, 'Impact of the digitalization of education on the right to education Report of the Special Rapporteur on the right to education, Koumbou Boly Barry', (19 April 2022).
[11] Preamble, UN CRC.
[12] A/HRC/50/32 UN General Assembly Human Rights Council, 'Impact of the digitalization of education on the right to education Report of the Special Rapporteur on the right to education, Koumbou Boly Barry', (19 April 2022) at para 3.

child shall not be subjected to arbitrary or unlawful interference with his or her privacy and that the child has the right to the protection of the law against such interference or attacks. In its general comment No. 25 (2021), the Committee on the Rights of the Child underlined that children had a right to privacy in the digital space, which was vital for protecting their agency, dignity and safety.[13] The right to privacy encompasses the physical and psychological integrity of a person, and can, therefore, embrace multiple aspects of the person's physical and social identity. Any interference with the right to privacy must be proportionate, necessary and in accordance with the law. Considering the vast amounts of data that AI systems in schools can collect, including potentially sensitive data, or which make inferences about a child, have the potential to significantly impact on their right to privacy. People are often unable to fully understand what kinds and how much data devices, networks, and platforms generate, process, or share. Furthermore, how data is collected and used is often far from transparent, with, in some cases, total opacity and disrespect for the right to privacy and the principle of meaningful consent.

Freedom from Discrimination

AI by design uses identification, profiling, and automated decision-making which can lead to unfair, discriminatory, or biased outcomes.[14] This can occur for several reasons and at many levels in AI systems and they are often difficult to detect and mitigate. Often, the quality of the data and biases within it are the source of potential discrimination and unfair treatment. People can therefore be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain groups of people. The right of the child not to be subject to discrimination is provided in Article 2 UN CRC provides that States shall take all appropriate measures to ensure that the child is protected against all forms of discrimination and that in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.

Right to Education

When discrimination occurs, this can lead to exclusion, which can ultimately interfere with the child's right to education. The right to education is provided in Articles 13 and 14 UN ICESCR and Articles 28 and 29 UN CRC. This is of significant concern as the quality of education a child receives,

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

[14] PI, 'Artificial Intelligence'. Available at: https://privacyinternational.org/learn/artificial-intelligence

their attainment in school, even ultimately their dropping out of school, can have significant consequences across the course of a child's life.[15]

Recommendations

PI recommends that the legislation should fully take into consideration Brazil’s obligations as provided by the international human rights legal frameworks and integrate it into their plans for the use of AI in education. PI recommends the legislation include:

- The introduction and use of digital technology in a thoughtful, learner-focused and age-appropriate way to improve the availability, accessibility, acceptability and adaptability of education for all.[16]

- State regulation and oversight of the use of technology in education by establishing norms and standards, complying with human rights norms and ensuring high quality, relevant and pluralistic content and adequate safeguards.

- Creating a statutory obligation for public bodies, including schools, to perform a Human Rights Impact Assessment to consider the legality, necessity, and proportionality of any systems. This impact assessment must include a necessity assessment to clearly demonstrate that recourse to a particular technology is necessary to achieve defined goals, rather than a mere advantage. As part of this assessment, any projected positive effects of a technology should be assessed through a collection of independent evidence sources and comparative practices.

- Ensuring child rights impact assessments and data privacy audits are conducted before adopting digital technologies in education.

- The requirement for due diligence processes to ensure that the technology they recommend for online learning protects children’s privacy and data protection rights; and provide guidance to educational institutions to ensure that data privacy clauses are included in contracts signed with private providers.[17]

[15] Available at: https://www.copenhagenconsensus.com/publication/brazil-perspectives-education

[16] A/HRC/50/32 UN General Assembly Human Rights Council, ‘Impact of the digitalization of education on the right to education Report of the Special Rapporteur on the right to education, Koumbou Boly Barry’, (19 April 2022) at para 96(a).

[17] A/HRC/50/32 UN General Assembly Human Rights Council, ‘Impact of the digitalization of education on the right to education Report of the Special Rapporteur on the right to education, Koumbou Boly Barry’, (19 April 2022) at para 100(c).

- Clear information and transparency by requiring all relevant information on the use of AI in schools must be made publicly available, and actively ensure parents and children are informed and consulted before systems are implemented or contracts entered in to.

Specific Types of AI Systems

Facial Recognition Technology

Facial recognition typically refers to systems which collect and process data about a person's face. These systems are highly intrusive because they rely on the capture, extraction, storage or sharing of people's biometric facial data -often in absence of explicit consent or prior notice.[18] It can be used to identify, authenticate/verify or categorise an individual. For example, facial recognition may be used by individuals to unlock their devices, authorise payments or sign up for services. This process relies on the facial image of a single individual being captured and compared to an existing image that individuals have already provided and verifying that it is them requesting access (this is what's referred to as 'one to one' matching).[19] The kind of biometric data collected by facial recognition is extremely sensitive, and the potential for abuse is extremely high. It is an extremely intrusive form of surveillance and can seriously undermine our freedoms and have significant impact on our enjoyment of human rights.[20] Moreover, facial recognition has persistently been shown to have biased recognition rates, returning poorer results when trying to recognise black people.[21]

Despite the serious risks, around the world schools have begun to introduce facial recognition in classrooms, including in Brazil.[22] It appears that one facial recognition company operated in 19 out of 26 Brazilian states as of November 2021.[23]

One of the justifications for the use of facial recognition technology in schools in Brazil has been for the purpose of monitoring the attendance of students at schools without the need to take roll call. Similar justification for it use was found in Sweden, where a facial recognition company claimed they were able to save 10 minutes per lesson compared to traditional methods of taking attendance.[24] Ultimately, this resulted in the company being taken to court and the Swedish DPA

[18] PI, 'Facial Recognition'. Available at: https://privacyinternational.org/learn/facial-recognition
[19] Ibid.
[20] Ibid.
[21] Available at: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology
[22] Available at: https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/)
[23] Available at: https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/)
[24] Available at: http://pages.tieto.com/rs/517-ITT-285/images/SummaryFutureClassroom.pdf

ruled that the use of facial recognition in the school violated data protection law and resulted in the company being fined.[25]

In Brazil, the system was rolled out without informing parents or students in advance, this lack of information has been reported in at least two public schools in Mata de São João.[26]

There are also AI systems, which incorporate facial recognition that claim to recognise whether a student's behaviour is inappropriate, such as proctoring software[27] and facial recognition software which claims to be able to identify whether a child is paying attention[28] or if they're bored.[29]

As a result of issues that have arisen with the use of facial recognition technology and harms caused, the use of facial recognition in schools is currently under investigation in the UK,[30] has already been prohibited in Sweden[31] and New York[32] and restricted in China.[33] Therefore, there is increasing recognition globally that facial recognition technology in schools is extremely invasive, posing significant risk to a child's privacy and consequently a growing trend towards banning its use in schools.

Recommendations

PI believes that AI systems that use facial recognition technology, should be banned from use in schools.

Other types of AI used in Educational Technology

PI would further highlight that facial recognition is not the only form of AI already being implemented in schools.

[25] Available at: http://www.tommasoricci.consulting/2019/08/21/first-gdpr-fine-in-sweden-facial-recognition-at-school/

[26] Available at: https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/)

[27] Available at: https://www.legalcheek.com/2020/08/proctoring-problems-bar-students-urinate-in-bottles-and-buckets-over-fears-online-exams-will-be-terminated/

[28] Available at: https://interestingengineering.com/chinese-school-uses-facial-recognition-technology-to-make-students-pay-attention

[29] Available at: https://www.inputmag.com/tech/intel-classroom-ai-student-surveillance-facial-recognition

[30] Available at: https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk

[31] Available at: http://www.tommasoricci.consulting/2019/08/21/first-gdpr-fine-in-sweden-facial-recognition-at-school/

[32] Available at: https://www.nyclu.org/en/news/ny-ignoring-ban-facial-recognition-schools

[33] Available at: https://www.bbc.co.uk/news/world-asia-49608459

For example, there are AI adaptive learning platforms that claim to challenge students based on each student's perceived strengths and weaknesses and predict future academic performance based on underlying patterns and relationships.[34] As well as AI learning and assessment tools that claim to help teachers track student performance and engagement, automate assignment scoring and personalise curriculum needs for each student.[35] There are also companies which claim to use AI to design seating plans for school classrooms based on children's behavioural records.[36] Therefore, there is a wide range of education technologies designed to directly teach and assess children; to manage children's behaviour and to take on administrative tasks.

AI systems used in schools will require a vast volume of sensitive data related to children such as children's names, addresses, educational attainment, even their behavioural records. Information which, traditionally, might only be available to a student's teacher, is now held by a huge volume of companies, increasing the potential risks for exploitation and abuse for financial gain, compromise through poor security.

These types of educational technologies that use AI, can directly interfere with children's access to education. For example, if a student is assessed using an adaptive AI system with a poorly trained algorithm with an inherit bias, their given grade could be generated based on the student's name or address, rather than their answers. This could have substantial consequences for their future academic potential, unfairly limiting their progression or achievements. This a problem that has been repeatedly found with AI systems. A similar situation occurred when Amazon attempted to build an AI system to review people's resumes to automate hiring. However, due to the historic bias in hiring, the data the system was trained on managed to create a system biased towards hiring men.[37] Rather than reducing discrimination, the AI system reinforced it.

Recommendations

PI believes that AI systems that result in biased and discriminatory practices that could directly interfere with a children's access, however, recognises it is extremely difficult to understand which AI systems are biased and in what ways.[38] Therefore, it is vital for any AI legislation to:

[34] Available at: https://assess.com/adaptive-testing/

[35] Ibid.

[36] Available at: https://www.classcharts.com

[37] Available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[38] Available at: https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency

- Require that algorithms and other decision-making processes deployed in a schools should be transparent and open to scrutiny and challenge. Therefore, they must be auditable. The ability to audit technologies is particularly essential in order 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.

- Require that, as part of any procurement process for use in a public service, the assessment of different systems should compare their levels of discriminatory bias. If discriminatory bias is identified, it should be rectified, and if it cannot be rectified, the technology should not be deployed. This should be required for deployment in public services before a contract is awarded.

Public-Private Partnerships in Education

The use of AI in schools frequently involves schools outsourcing and contracting with private companies. While an attractive way to improve education, public-private partnerships raise major concerns for the realisation of human rights. PI has repeatedly seen partnerships between private companies and public bodies, which fail to meet basic standards of transparency[39] [40], accountability[41], oversight[42]. They frequently fail to use appropriate procurement processes[43], and don't meet appropriate standards of legality, necessity or proportionality[44].

The Special Rapporteur on the Right to Education regrets that education is perceived by some as a market with great potential for profit and that some companies are global businesses without interests in or a deep understanding of the contexts in which they operate. They do not seek to promote the interests of learners, but to maximise profit.[45]

[39] PI, 'All roads lead to Palantir'. https://privacyinternational.org/report/4271/all-roads-lead-palantir
[40] Available at: https://www.tedic.org/voto-electronico-falta-de-claridad-testeo-tsje
[41] Available at: https://theintercept.com/2018/06/27/thomson-reuters-defends-its-work-for-/; https://www.reuters.com/article/us-china-tech-surveillance-trfn-idUSKBN2BM1EE
[42] Available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf and https://www.computerweekly.com/news/4500243244/UK-government-pays-150m-to-Raytheon-to-settle-e-Borders-dispute
[43] Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E
[44] PI, "Thousands of Cameras" - a citizen response to mass biometric surveillance'. Available at: https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-biometric-surveillance
[45] A/HRC/50/32 UN General Assembly Human Rights Council, 'Impact of the digitalization of education on the right to education Report of the Special Rapporteur on the right to education, Koumbou Boly Barry', (19 April 2022) at Para 57.

The Special Rapporteur refers to the useful guidance provided by the Abidjan Principles in this respect.[46] The Abidjan Principles set out a useful compilation of existing standards that can help to navigate the issue.[47] When considering the provision of resources to eligible private institutions, the Abidjan Principles list substantive, procedural and operational requirements that States must strictly observe.

Furthermore, the Special Rapporteur also highlighted the need for consideration of the State's obligations under the UN Guiding Principles on Business and Human Rights, that provide the duty to protect against human rights abuses by all actors in society, including businesses. This means that States must prevent, investigate, punish and redress human rights abuses that take place in domestic business operations. In the Guiding Principles, it is recommended that States set clear expectations that companies domiciled in their territory or jurisdiction respect human rights in every country and context in which they operate. Business enterprises must prevent, mitigate and, where appropriate, remedy human rights abuses that they cause or to which they contribute. These principles apply to all States and business enterprises, transnational and others, regardless of their size, sector, location, ownership or structure.

Recommendations

- PI recommends that any AI legislation must pay particular attention to the relationship between public-private partnerships. Private actors should ensure human rights-based approach to their practices, therefore the AI bill should reference full abidance to the Abidjan Principles, in particular the adoption of rules and regulations for the private sector in this area, and to the UN Guiding Principles on Business and Human Rights.

- Companies providing AI technologies to schools should be required to waive commercial confidentiality and make their technologies fully auditable by any third party, to enable understanding of:

  1. What data the company and its technology have access to;

  2. How the technology analyses the data and draws conclusions (including disclosure of algorithm parameters) and;

[46] UN Sustainable Development Goals. Available at: https://sdgs.un.org/goals

[47] The Abidjan Principles. Available at: https://www.abidjanprinciples.org/en/principles/overview

3. What role the technology performs in the public authority's decision- making process. Such information should be available for public scrutiny prior to contracting.

- If details of the workings of a particular technology cannot be disclosed for specified and valid grounds of serious commercial harm to the company, an independent oversight body bound by duties of confidentiality should be granted full access to all details of the technology required to establish those details.

- It should also be noted that all forms of redress codified in this legislation, should not be overly burdensome to allow for children and their families to seek redress. This means that:

1. The burden should be on the body deploying AI to ensure appropriate redress for all those affected if an algorithmic harm comes to light after an AI system has been deployed.

2. Having recourse to courts or other senior judicial systems is often not a viable option for individuals affected by isolated uses of a technology, especially considering that abuse can be difficult to establish through traditional justice mechanisms. AI deployments should require a clear mechanism (whether existing or new) for complaints handling and enforcement of sanctions for violations of the policy (including pointing to an appropriate independent oversight body able to investigate and provide redress). These redress mechanisms and responsible entities should be suited to the nature of the technology, its intended purpose and identified impacts. They should assign responsibilities and redress obligations to both the state and the company involved, and ought to adhere to the eight "effectiveness criteria" set out in UN Guiding Principle 31[48]. That said, any redress provisions must not bar access to courts or other established judicial mechanisms. They must strike the right balance between accessibility of redress and compliance with the rule of law.

3. Redress should not be time limited. Instead, the process should allow for children to grow older and take retrospective action, as harms may not be clear for many years. These kinds of invasions of privacy often create time shifted risks, for example, a data breach at an AI company which processed disciplinary records that later leads to a child being rejected for a job. Or an AI company inferring something about a child, information which is sold on to a third-party company, which leads to a child having higher insurance premiums later in life.

[48] Available at: https://globalnaps.org/ungp/guiding-principle-31/)

For further information on adequate safeguards in the kinds of public/private partnerships common in the use of AI by public bodies, including schools, please refer to PI's Safeguards for Public-Private Surveillance Partnerships[49], which provides further information on relevant and vital safeguards.

[49] PI, ‘Safeguards for Public-Private Surveillance Partnerships’. Available at: https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships