



# ADVANCING CHILDREN'S DIGITAL RIGHTS IN MEXICO



# Advancing Children's Digital Rights in Mexico

**April 2023**

**Lead Author:** Claudia May Del Pozo

**Co-author:** Larissa Gus

**Contributors:** Rodrigo Félix, Geraldine Loaeza, and Constanza Gómez Mont

**Designer:** Nicté Cabañas Segura

**With the support of:** José Roberto Mejía

## Acknowledgments

The British Embassy in Mexico and C Minds' Eon Resilience and AI for Good Labs thank the following people for their time and participation in the forum: Amy Clemitshaw, Deputy Ambassador of the United Kingdom to Mexico, Senator Josefina Vázquez Mota, President of the Commission on the Rights of Childhood and Adolescence, and Deputy Ana Lilia Herrera Anzaldo, President of the Commission on the Rights of Children and Adolescents.

For their valuable time and input, they also thank the forum contributors and speakers: **Ana Cecilia Pérez**, Co-Founder and Director of Capa 8; **Anahiby Becerril Gil**, Cybersecurity Specialist; **Angie Contreras**, Member of Cultivando Género; **Erika Salas**, Academic Specialist in Education in Mexico; **Jen Persson**, Director of DefendDigitalMe; **Jimena Mora**, Senior Corporate Attorney at Microsoft's Cybercrime Unit; **María Cristina Capelo**, Latin America Security Policy Leader at Meta; **Michael Murray**, Director of Regulatory Strategy and Policy Projects at the Information Commissioner's Office in the United Kingdom; **Pilar Ramírez**, Vice President for National Capacity Development at the International Center for Missing and Exploited Children; **Sonia Livingstone**, Director of the UK Digital Futures Commission; **Teresita Poblete**, Consultant in the Promotion and Protection Area of the Inter-American Children's Institute (IIN) of the Organization of American States (OAS); **Valeria Geremía**, Executive Coordinator of the Network for Children's Rights in Mexico (REDIM); **Yolanda Martínez**, General Director of the GovStack Initiative at the International Telecommunication Union (ITU); **Sharon Bissell** for her guidance; and the four girls and boys who were anonymously interviewed.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of C Minds, the British Embassy in Mexico, or the forum contributors and speakers.



# INDEX

<b>Introduction .....</b>	<b>4</b>
<b>The Mexican Context .....</b>	<b>6</b>
<b>Positive regulatory experiences in the United Kingdom.....</b>	<b>10</b>
<b>Experiences of companies including GovTech .....</b>	<b>19</b>
<b>Learnings from children’s perspectives on the digital world .....</b>	<b>24</b>
<b>Recommendations for Mexico .....</b>	<b>26</b>
<b>Conclusion.....</b>	<b>32</b>
<b>The organizations behind the forum and brief.....</b>	<b>34</b>
<b>References .....</b>	<b>35</b>

# INTRODUCTION

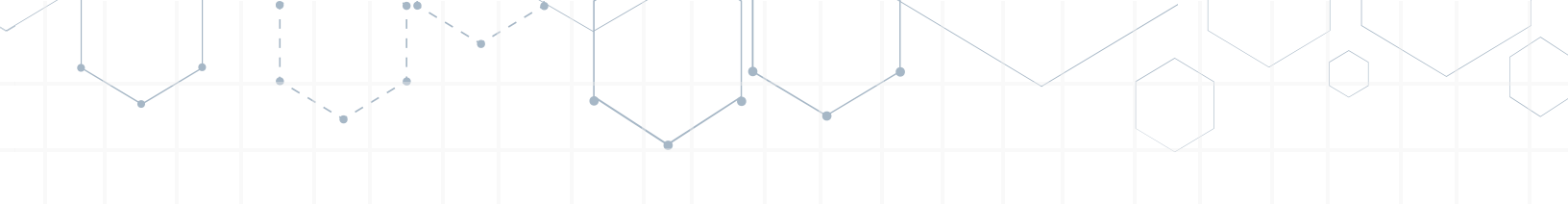
The rapid advancement of technology and the growing use of the Internet have transformed people's lives across the globe as they become everyday tools, especially impacting girls and boys who are born into a highly digitised environment. In fact, it is estimated that one in three Internet users is under the age of 18, a proportion that may be even higher in low- and middle-income countries (UNICEF, n.d). However, this transformation has also created new challenges and vulnerabilities that need to be addressed and mitigated to ensure a safe experience for girls and boys, maximising their opportunities to learn, participate, and create. This perspective should not only be reflected in the design of products and services but should also permeate public policy under the umbrella of Children's Digital Rights (CDR).

As more minors access the Internet, online platforms and applications, and the widespread adoption of Artificial Intelligence (AI) systems increases, the relevance of this issue is growing. However, discussions and actions regarding CDR tend to focus on high-income countries, including the United States, Canada, the European Union, and the United Kingdom.

In order to promote the recognition, protection, and promotion of these same

rights in Mexico, the British Embassy in Mexico and C Minds, through its Eon Resilience Lab and AI for Good Lab, have joined forces to foster more dialogues on this topic in the country and encourage the exchange of knowledge and best practices with institutions in the United Kingdom. On March 14th, they organised the Forum for Children's Digital Rights, inaugurated by the Deputy Ambassador of the United Kingdom in Mexico, Amy Clemitshaw, and both Presidents of the Commissions that work on children's and adolescents' rights from the Senate, Senator Josefina Vázquez Mota, and from the Chamber of Deputies, Deputy Ana Lilia Herrera Anzaldo. In this space and subsequent conversations, 16 experts from Mexico and the United Kingdom participated in discussions on education, privacy, cybersecurity, human rights, and children's rights (see page 1 for a detailed list), along with 4 girls and boys who were interviewed to gather their opinions, concerns, and the actions they take to make the digital world a safer place.

This report summarises the information shared at the forum and subsequent spaces, complemented by independent research presented in small boxes. It includes the opinions, inputs, and recommendations of experts from various fields who participated



in the forum, which was divided into three areas:

- 1 The regulatory approach from the United Kingdom**
- 2 The perspective and actions of the international industry**
- 3 The lessons learned and recommendations for Mexico**

This document seeks to accelerate understanding and dialogue regarding the challenges and highlight good international practices, as well as provide public policy recommendations to strengthen the protection of the CDR in Mexico. It is primarily intended for legislators and autonomous government bodies, as well as public and private human rights protection agencies. Additionally, this report aims to benefit civil society organizations, institutions, and associations specialising in

the topic, providing them with information and recommendations that indicate the various existing opportunities to address the aforementioned challenges from the public and private sectors.

While this report does not claim to be exhaustive or prescriptive, it aims to be a valuable tool for taking action in Mexico to protect and uphold children's digital rights.

# THE MEXICAN CONTEXT

Mexico has numerous regulatory frameworks<sup>1</sup> that protect CDR but the constant evolution of technology and the emergence of new challenges to ensure their online safety require a constant reevaluation of this legislation and its update to address new opportunities and risks.

In Mexico, generally speaking, the violation of CDR is related to the security and privacy of minors online. This includes exposure to online situations that endanger their privacy, security, and integrity, such as cyberbullying, lack of privacy of personal data, and exposure to sexting, among others. When discussing connectivity in Mexico, it is also important to address the digital divide that limits access to technology and digital resources, increasing children's vulnerability in the digital world.

## a. Security and privacy

In Mexico, there have been reports of numerous cyber incidents against girls, boys, and adolescents related to sexual assault, cyberbullying, and disappearances (Human Rights Commission, 2020). According to the Committee of the Convention for the Elimination of all Forms of Discrimination against Women (CEDAW, 2017), girls are twice as likely to be victims of cyberbullying than boys<sup>2</sup>. In Mexico, data from the Cyberbullying Module (MOCIBA, 2019) indicates that online harassment significantly affects children and adolescents between the ages of 12 and 19, making them the second most affected group<sup>3</sup>. It is important to consider the implications of these attacks, such as psychological problems, feelings of insecurity and fear, suicidal thoughts, and even suicide. Anahiby Becerril points out that knowledge of the existing legal framework and reporting to the relevant authorities are crucial steps in protecting children. One of the main issues is the lack of reporting as families do not know whom to turn to or feel ashamed.

<sup>1</sup> Among them: General Law on the Rights of Girls, Boys, and Adolescents, Article 101 bis of the Federal Attorney for the Protection of Girls, Boys, and Adolescents; Law of Science and Technology, Article 65; Federal Telecommunications and Broadcasting Law, Article 2; Declaration of Alert for Violence against Women and Girls.

<sup>2</sup> Committee on the Elimination of Discrimination against Women, General Recommendation No. 36 (2017) on the right of girls and women to education, CEDAW/C/GC/36, 27 November 2017, paragraphs 70 and 71.

<sup>3</sup> Secretariat of Citizen Security of Mexico City, Department of Information Systems and Cyber Investigation of the Sub-Secretariat of Police Investigation and Intelligence, undated official communication, 10 December 2020.

Among the actions that Mexico is taking to protect children online is the creation of the Cyber Police [see Box 1]. Some actors, such as Angie Contreras from Cultivando Género, believe that the impact of these initiatives

could be improved by collaborating with specialised civil society organizations in these issues.

### Box 1. Cyber Police: Measures to address the priority challenge in Mexico

The Cyber Police, implemented by the Federal Telecommunications Institute, is a unit responsible for preventing and combating online crimes in every Mexican state. Its activities include monitoring and tracking the public Internet network to identify any criminal activity that may endanger the safety and assets of the population. According to [Volume II of the Annual Report on Digital Violence Against Women in Mexico City](#) by the Human Rights Commission (2020), the Cyber Police has carried out various actions relevant to the safety of girls and boys. These actions include preventive talks to raise awareness among the population about safe browsing practices, digital civility, reporting culture, and the responsible use of ICT.

In this regard, the National System for Integral Family Development (DIF) has carried out various campaigns to promote online safety, combat misinformation, prevent risks associated with digital platforms, encourage the creation of secure passwords, promote the use of parental control, and ensure a safe return to classes. In the educational field, the DIF participated in the forum called "Online Education during a Health Emergency and the Risks Faced by Children and Adolescents," delivering talks to 360 teachers from the Aprende y Crea DIFerente program. Support has also been provided to the Transgender Childhood community and their families given incidents in digital media. Additionally, Cyber Police personnel has received comprehensive training with a gender and human rights focus, as well as in promoting a violence-free life for women and girls.





Teresita Poblete highlighted some successful initiatives implemented in Mexico, such as "[Internet Seguro](#)" (Safe Internet), a joint initiative of the Mexican Government and various private and public organization [Box 1]. Cyber Police: Measures to address the priority challenge in Mexico ns aimed at promoting Internet safety for children, teenagers, mothers, fathers, and caregivers. Some experts also mentioned that the Senate is currently holding conversations to protect children from online pornographic content.

Despite the progress made in Mexico on this matter, experts like Angie Contreras and activist/academic Erika Salas, a doctoral student at the Institute of Legal Research at the National Autonomous University of Mexico (UNAM) in the field of children's digital rights, emphasize the importance of continuing discussions and sharing best international practices. They argue that **it is necessary to move away from punitive and restrictive approaches that seek to block and censor content and access, and instead prioritize holistic regulatory approaches.** They advocate for approaches

that recognize both the importance of online content for children and the need to mitigate risks, while respecting the agency and rights of children and adolescents. As Anahiby Becerril puts it, "We do not refuse to teach a child how to read because they might come across an inappropriate book."

Valeria Geremia, Executive Coordinator of the Network for Children's Rights in Mexico (REDIM), pointed out that in Mexico, regulation often leaves this responsibility up to mothers, fathers, and caregivers. However, this is in a context of very low digital literacy rates, meaning adults are not always capable of supporting their children in ensuring a safe online experience. They may not even be aware of the implications of using technology or the different settings to reduce exposure to risk. In response to this reality, organizations like Cultivando Género are creating resources such as the [Guide for the Prevention and Support of Digital Violence for Adolescents](#), with the support of INDELA (2023). However, as Sonia Livingstone comments, **it is important to shift the pressure and responsibility from children, adolescents, and their parents back to the state and businesses**, as has been done in the United Kingdom.

## Digital divide

The digital divide in Mexico is also a factor that undermines children's rights, as there is a structural barrier that limits their participation in technology. These limitations are exacerbated by inequalities in the access to and use of ICTs, both among states and between urban and rural areas. Ana Cecilia Pérez comments that digital inclusion



can democratize access to education and technological platforms, but it is important to address the access gap that exists in the population. Girls, in particular, experience these inequalities more severely due to the gender digital divide in the country (Human Rights Commission, 2020). During her participation, Valeria Geremia pointed out that "in Mexico, in 2021, less than 30% of children and adolescents between the ages of 6 and 17 still do not have access to the Internet at home, according to the National Survey on Availability and Use of Information Technologies in Households (ENDUTIH) 2021. However, when it comes to Internet access at home or outside the home (smartphones, schools, web cafes, etc.), **the percentage of girls and boys who connected to the Internet in 2021 rises to 78.7%.**"

It is therefore crucial to take measures to protect children from exposure to online situations that endanger their privacy, security, and integrity, as well as to ensure their safe access to technology and digital resources. To achieve this, it is important

to learn about initiatives and regulatory frameworks that have been successfully implemented across the world in order to identify possible actions for Mexico. The following section explores regulatory advances in the protection of CDR in the United Kingdom, which may serve as inspiration for implementing actions in the Mexican context.



# POSITIVE REGULATORY EXPERIENCES IN THE UNITED KINGDOM

**“In the past the protection of children online typically involved excluding them from this world, but today the value of online resources and opportunities for the learning, growth, and development of children is a reality that cannot be ignored. The current approach focuses more on finding solutions that allow children to make the most of the online world while mitigating risks”,** stated Sonia Livingstone, Director of the Commission on Digital Futures, during the forum.

This was the goal of the Information Commissioner's Office, the Data Protection Authority in the United Kingdom, when creating the [Children's Code](#) (2021), also known as the **Age Appropriate Design Code**. As explained by Michael Murray, Head of Regulatory Strategy and Regulatory Projects and Resident Expert on Children's Privacy at the Information Commissioner's Office (ICO), it is a code of practice that applies to all information society services that are likely to be accessed by children in the United Kingdom<sup>4</sup>. This is in stark contrast to the Children's Online Privacy Protection Act (COPPA) in the United States, which

applies only to services directed at children. This key difference in scope makes the Code for Children one of the most advanced legislations in the world regarding children's rights.

The code of practice is based on the [United Nations Convention on the Rights of the Child](#) (UNCRC) of 1989, designed to create an open, transparent, and safer place for children to play, explore, and learn online. It is based on existing data protection laws, specifically the [General Data Protection Regulation](#) (GDPR) of the United Kingdom, which came into effect in September 2020. The code sets out 15 interconnected standards or practices [See Box 2].

<sup>4</sup> Any person under the age of 18.

## Box 2.

# The 15 Standards of the Children's Code by the ICO

1. **“Best interests of the child:** The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.
2. **Data protection impact assessments (DPIA):** Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.
3. **Age-appropriate application:** Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.
4. **Transparency:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.
5. **Detrimental use of data:** Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions, or Government advice.
6. **Policies and community standards:** Uphold your own published terms, policies, and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).
7. **Default settings:** Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).
8. **Data minimisation:** Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children

separate choices over which elements they wish to activate.

9. **Data sharing:** Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
10. **Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.
11. **Parental controls:** If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.
12. **Profiling:** Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).
13. **Nudge techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.
14. **Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.
15. **Online tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns."

After a year and a half of the Children's Code implementation, the results showed positive changes in companies' behaviour, with 46% considering themselves fully compliant. As shown in Box 3 below, the largest social media companies have also taken steps towards compliance. However, recently, there has been a decrease in the percentage of companies that have made changes. Murray explains that this could be because companies have already implemented the easier changes and are now facing the more difficult ones related to their business model, such as disabling default profiling or using age-verification to restrict access to inappropriate services for children. Alternatively, he says some companies may be waiting for evidence of compliance action from the ICO before making more challenging changes to their business model.

### Box 3. Shift in focus of major social media companies <sup>5</sup>

**Google** has disabled ads for users under 18 and **TikTok** has made the profiles of users under 18 private by default. **Snapchat**, **Instagram**, and **Epic Games** are improving parental controls; Epic has changed its approach regarding users under 13, and **Meta** is developing new age verification systems to improve the identification of accounts belonging to minors and the appropriateness of content based on age.

"As children, their mothers, and fathers tend not to complain," Murray explained, "we knew we would have to monitor this code in a different way. The ICO decided to be more proactive, and in September 2021, we started sending letters to over 60 organizations to ask them what they were doing to comply with the code. In addition, to encourage compliance, the ICO is adjusting its working methods, engaging directly with the design community, in addition to its traditional disclosure to Data Protection Officers and senior management of organizations. It has also made available a series of practical guides, templates, and self-assessment tools, in addition to offering individual audits, guidance, and certification schemes."

Taking an active role in the internationalization of codes to protect CDR, the UK, through the ICO and other organizations, is working with other regulators in the UK, the European Union, and the United States to support the development of similar codes. It is also working with international standard-setting organizations in age verification standards, including the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE). As Jen Persson, Founder of the UK non-governmental organization DefendDigitalMe, noted, **it is essential to create international guidelines based on universal human rights frameworks for these online tools that have no geographical boundaries.**

Among these transnational collaborations, the UK participated in the [UN General Comment No. 25 \(2021\)](#) [See Box 4],

<sup>5</sup> According to the information shared by Michael Murray during the Children's Digital Rights Forum.

developed in collaboration with the 5Rights Foundation, a prominent actor in the field of CDR in Great Britain. The resource section of the website includes an adaptation of the General Comment to the language and understanding of children to promote their awareness of their own rights. In fact, Livingstone highlights the importance of involving children in these conversations, pointing to the Global Kids Online organization dedicated to gathering global evidence on children's online rights, opportunities, and risks.

As mentioned by Murray, it is increasingly popular to create adoption guidelines to accompany new public policies, which is what the Digital Futures Commission led by the 5Rights Foundation is doing, collaborating with researchers, policymakers, children, and designers in the United Kingdom. One of their practical tools is a set of Children's Rights by Design tools (2023) called "Playful by Design" [see Box 5] for companies designing digital services used by children everywhere.

#### **Box 4. UN General Comment No. 25 on the rights of children in relation to the digital environment**

"In this general comment, the Committee explains how States parties should implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment."

"It is based on the Committee's experience in reviewing States parties' reports, its day of general discussion on digital media and the rights of girls and boys, jurisprudence of human rights treaty bodies, recommendations of the Human Rights Council and the special procedures of the Council, two rounds of consultations with States, experts, and other stakeholders on the conceptual note and advanced draft, and an international consultation with 709 girls and boys living in a wide variety of circumstances in 28 countries from various regions." (UN, 2021)



## Box 5. Children's Rights Design Tool "Playful by Design" by the Digital Futures Commission and 5Rights Foundation

The [Playful by Design](#) tool a free resource for creating digital products for children, made up of three components:

- Principle cards guide the design process by embedding CDR considerations into digital products and services to meet certain objectives.
- Prompt cards provide questions to focus on player experiences and design alternatives, turning ideas into actions.
- Playboards allow for a flexible use of the cards, whether working in groups or individually.



**This tool can be used at any stage of the design process and by anyone involved in product development and design.**

One of the new strategies that the British organization DefendDigitalMe has been exploring in collaboration with the Child Rights International Network (CRIN) is data encryption, as described in the report "[Privacy and Protection: A child rights approach to encryption](#)" (2023) [See Box 6].

The United Kingdom has also participated in a Council of Europe Committee, working on Convention 108, which supports legislation and guidance on data protection for its 46 member states, as well as for observers and participants in the council, such as Mexico. In 2020, the Commission developed the "[Guidelines on Data Protection of Children and Adolescents in an Educational Environment](#)" (Advisory Committee on the

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) [See Box 7], with the aim of creating a safe, transparent, and fair digital environment. These guidelines were adopted the same year.

Persson mentions the importance of focusing these regulations on the educational sphere, explaining that inappropriate data processing practices by e-learning platforms, opaque automated decision-making, and misuse of learning analytics can undermine data protection and privacy rights. In the case of children and adolescents, this can have significant and long-term social, economic, and professional consequences, not taking into



account their evolving capacities. She also highlights three major privacy risks related to collecting educational data: firstly, the fact that data generation from an early age can have consequences later in life; secondly, the fact that this data tells not only the story of the student but also that of its family and home; and thirdly, the large ecosystem of technology and education companies involved, generating implications about what and who has access to the educational

system. As Bianca Wylie, a Canadian public technology advocate, noted in May 2020: **“technology procurement is one of the biggest democratic vulnerabilities today.”** For this reason, Livingstone emphasizes the need for all companies with digital services targeted at children to carry out proactive CDR impact assessments before launching their solutions.

### Box 6. Privacy and protection: A child rights approach to encryption

“A debate is currently underway regarding encryption and public safety, with a focus on the fight against online child sexual exploitation and abuse. This discussion is often experienced as a divide between a child protection approach and a civil liberties focus. This report, co-published by CRIN and DefendDigitalMe, is a response to this divide, based on a recognition of the full complexity of how encryption affects children’s lives. Its aim is to set out principles for an approach to encryption that recognises and respects the full range of their rights.

The report argues that :

1. There should be no generalised ban on encryption for children.
2. Interventions engaging encryption must consider and address specific political, economic, social, and cultural contexts.
3. Restrictions on qualified children’s rights such as privacy must be necessary and proportionate. They should be sufficiently clear and precise, limited to achieving a legitimate goal and the least intrusive way of doing so.
4. Policy-making should address the role of business, including by requiring more transparency around how platforms prevent and remedy violations of children’s rights.
5. Children must have access to justice for all violations of their full range of rights in the digital environment, including where encryption is engaged.” (Child Rights International Network and DefendDigitalMe, 2023)

Furthermore, given the growing and widespread adoption of Artificial Intelligence (AI) systems for educational purposes, Persson explains that the Council of Europe is also exploring these emerging technologies and their impacts on human rights<sup>6</sup>, analysing what is changing for children in the digital environment, and publishing "[AI and Education: A Critical View through the Lens of Human Rights, Democracy and the Rule of Law](#)" (Holmes, et al.) in 2022 [See Box 8]. As AI systems automate measurements to assess children's behavior, achievement, and progress based on generated data, we must carefully consider what kind of interactions we allow computers and companies to make decisions about and then create information that teachers read, which gives some indication of a child's profile.

Finally, Persson points out that the risks of datafication and surveillance in education can have a punitive effect on society, illustrating some of the challenges by presenting a case from Brazil, where facial recognition tools were used to identify school absenteeism and deduce welfare payments from families accordingly (Association for Progressive Communications et al., 2019). Regarding the role of the state in relation to the impact of the business sector on children's rights, Persson recommends United Nations General Comment No. 16 (2013), which establishes obligations. She also invites decision-makers to consider whether data protection is sufficient to protect human rights, democracy, and the rule of law in an educational environment.

<sup>6</sup> Emerging technologies and emerging harms to human rights: 1) Technology: a) Biometrics, emotional and behavioral control (facial detection and recognition, fingerprints), b) Automated and opaque decision-making and unexplainable artificial intelligence; 2) Personal: a) Influence (mood, attention, mental health), b) Long-term effects and datafication, c) Quality education and pedagogy; 3) Geopolitical: a) State control and sovereignty of systems, b) Surveillance: technology of origin and data transmission, c) Unequal distribution and impact on labor (raw material production, data cleansing).

### Box 7. Council of Europe Convention 108 - Guidelines on Data Protection of Children and Adolescents in an Educational Environment

"The introduction of digital tools to the classroom [...] opens up the school gates to a wide range and high volume of stakeholders who interact with children's everyday activities. The majority of the devices and applications, software and learning platforms, adopted in educational settings are developed by private, commercial actors.

The Guidelines on Children's Data Protection in an Educational Setting aim at supporting organisations and individuals in the context of education to respect, protect and fulfil the data protection rights of the child in the digital environment, within the scope of Article 3 of the modernised Convention 108 (more commonly referred to as "Convention 108+"), and in accordance with the Council of Europe instruments including the Guidelines on Children in the Digital Environment Recommendation." (Advisory Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2021)

### **Box 8. AI and Education: A Critical View through the Lens of Human Rights, Democracy and the Rule of Law, by the Council of Europe**

“Artificial intelligence (AI) is increasingly having an impact on education, bringing opportunities as well as numerous challenges. These observations [...] to the commissioning of this report, which sets out to examine the connections between AI and education (AI&ED) [...] seen through the lens of the Council of Europe values of human rights, democracy, and the rule of law; and it provides a critical analysis of the academic evidence and the myths and hype.

The Covid-19 pandemic school shutdowns triggered a rushed adoption of educational technology, which increasingly includes AI-assisted classrooms tools (AIED). This AIED, which by definition is designed to influence child development, also impacts on critical issues such as privacy, agency and human dignity [...]. But AI&ED is not only about teaching and learning with AI, but also teaching and learning about AI (AI literacy), addressing both the technological dimension and the often-forgotten human dimension of AI.” (Council of Europe, 2022)

# EXPERIENCES OF COMPANIES INCLUDING GOVTECH



During the second session of the forum, with the participation of Yolanda Martínez, General Leader of the GovStack Initiative; Pilar Ramírez, Vice President of Capacity Development at the International Center for Missing and Exploited Children (ICMEC); Jimena Mora, Senior Corporate Lawyer in the Cybercrime Unit at Microsoft; and María Cristina Capelo, Security Policy Manager for Latin America at Meta, presentations were given on initiatives and actions taken by these companies that take into account the need to reduce risks and protect CDR. In order to continue informing the conversation about best practices to protect human rights, the following summary (Table 1) was prepared with the initiatives presented at the forum:

## Govstack

Implementation strategy for government digitization

**What is it?** A platform that focuses on digitising procedures and services in governments. Via various strategies such as technical specifications, a playbook, capacity development, and a digital marketplace for open-source solutions, it seeks to facilitate the development of digital services in governments and promote the use of reusable components to save time and resources..

**What actions do they implement and what impact can they have on human rights?** They seek to improve the quality and effectiveness of services related to children's rights, such as education, healthcare, and child protection. Additionally, by offering technical specifications and open-source solutions, Govstack helps ensure that online services are secure and designed with the privacy and data security of children in mind.

**Yolanda Martínez, General Leader of the GovStack Initiative:**  
*"It's not just about protecting data but also about taking care of all aspects related to how information is used, how it connects with other things, and whether guardians or the people accessing the services have given their consent."*

## ICMEC

International  
Center for  
Missing and  
Exploited  
Children

**What is it?** The organization works worldwide on two fundamental issues: combating child abuse and sexual exploitation, as well as searching for missing girls and boys. Their mission includes promoting mechanisms for rapid location, such as the Amber Alert, to facilitate immediate action regarding missing children.

**What actions do they implement, and what impact can it have on human rights?** They focus on the prevention and addressing of online child sexual abuse. By empowering girls, boys, and adolescents to protect themselves and report online harassment and sexual abuse, their right to a violence-free life and protection in the digital world is promoted. Additionally, they train authorities to investigate and prosecute technology-using sexual offenders, protecting the rights of girls, boys, and adolescents to justice and the redress of harm.

**Pilar Ramírez, Vice President of Capacity Development:** *"Many countries around the world tell us, 'We need your support to have the best technological tools for conducting investigations in the deep web'"*

## Microsoft Digital Crimes Unit

**What is it?** Microsoft's Digital Crimes Unit is an international team of technical, legal, and business experts that has been combating cybercrime since 2008. They share knowledge with other Microsoft teams to enhance product security, discover evidence for criminal referrals, and take legal actions to disrupt cybercriminal activity.

### **What actions do they implement, and what impact can it have on human rights?**

- The unit focuses on combating cybercrime and protecting minors online. They identify and pursue criminals and provide evidence for legal actions. Additionally, they provide resources to educate children on safe online navigation and protecting their digital privacy and security.
- They design secure products from the earliest stages through a series of processes and tools that allow development teams to identify and address security risks from the initial design and development phases.
- They created the e-book called "[How to Protect Your Children and Adolescents from Online Risks? A Cybersecurity Guide for Parents.](#)" which contains information and recommendations to help minors navigate safely in the digital world and provides advice on what to do in case they become victims of any type of online attack.

**Jimena Mora, Senior Corporate Lawyer:** *"The issue of digital security is becoming increasingly sensitive. I believe there is not a single government or industry that does not intend to protect the most vulnerable populations, such as girls and boys, in the best possible way."*



## Meta

### User protection security area

**What is it?** An area designed to work with experts from different countries to address the safety of Meta's service users.

### **What actions do they implement, and what impact can it have on human rights?**

- They have developed a process to directly apply the UN Convention on the Rights of the Child to the products and experiences built by Meta. They created Meta's Best Interests of the Child Framework, which summarizes the standard of "Best Interests of Children and Adolescents" into six key considerations that product teams can refer to throughout the development process. A combination of internal research and input from global data protection regulators was used to create this framework. Recognising and involving young people and families worldwide using their products.
  1. Creating safe and appropriate environments for young people.
  2. Promoting the autonomy of young people while considering the rights and responsibilities of parents and guardians.
  3. Prioritising the well-being and safety of young people over business objectives and interests.
  4. Supporting the privacy of young people in product decisions.
  5. Empowering young people, parents, and guardians to understand and exercise their data rights.

The adoption of this approach helps build products for youth that support their well-being and rights while promoting consistency across different jurisdictions and product teams. Additionally, it is a project that undergoes continuous evaluation through expert consultation, user research, and co-creation.

- They work in collaboration with expert organizations, authorities, and industry partners, such as the NCMEC, to develop tools and resources to protect girls, boys, and adolescents. An example of this is Take it down, a platform that combats the non-consensual dissemination of intimate images.
- They have implemented default configurations and notifications in their applications and platforms to protect the privacy and security of girls, boys, and adolescents. These tools include immediate interaction to report inappropriate activity and parental supervision.

# LEARNINGS FROM CHILDREN'S PERSPECTIVES ON THE DIGITAL WORLD

Throughout this report, reflections and actions have been shared to make the digital world a safer space for children. However, it is of utmost importance that these reflections also come from children themselves, as they face an increasingly digitised world. For this section, interviews were conducted with four individuals aged 9, 12, 15, and 17. Although this was not a representative or exhaustive sample, the aim was to understand their opinions, concerns, and the actions they take to ensure safety when using the Internet, from which the following learnings emerged:

## 1. Children are aware that there are risks on the Internet, but they don't always know what they are.


Children have some level of awareness of the existence of risks online, but often they do not know what the potential threats are. They may be aware that they should not talk to strangers online, but many times the only reason they refrain from doing so is because their parents told them not to.

## 2. In many cases, children learn about Internet by experience.

Children often understand the risks only when they encounter them or after a certain amount of time using the Internet. As one of the interviewees shared, *"The Internet is like a city, and the more time you spend in a city, the better you know its risks and limits."*

## 3. Learning about safe Internet use is considered a privilege, as not all children have access to resources and education on this topic.

Access to quality educational resources and information on safe Internet use can depend on factors such as geographical location, socioeconomic status, parents' time and digital literacy, and the availability of technology in the community. Children living in rural areas or low-income communities may have less access to quality educational resources and information on safe Internet use compared to those living in urban areas or more affluent communities.



**4. Intermittent teaching on online responsibility topics in schools can be more harmful than beneficial.**

Indeed, it gives them the mistaken impression that everything they need to know will be taught to them by the school, as may be the case with other more traditional subjects. For this reason, among others, they do not necessarily seek to understand more about risks and safe approaches via the Internet itself.

**5. The responsibility of protecting children online often falls on mothers, fathers, and caregivers, which can be counterproductive due to individual contexts.**

It is not always possible for mothers, fathers, and caregivers to effectively ensure safe Internet use due to a variety of factors. These factors include lack of time and lack of information, in line with low levels of digital literacy in the country. Cultural or religious values that influence their approach to online supervision, as well as different levels of time and resources available to safely accompany children on the Internet should also be considered.

# RECOMMENDATIONS FOR MEXICO

This section offers suggestions to support the process of protecting children's digital rights. These recommendations emerged from forums, conversations, and subsequent interviews with a total of 13 experts (see the acknowledgments section on page 1 for more details), mainly from Mexico. The experts addressed topics such as cybersecurity, children's digital rights, online protection, online security policies, among

other relevant subjects, throughout the months of February and March 2023.

These suggestions are not only intended to guide government action, but also to encourage deeper and more critical reflections to identify and propose possible multisectoral actions that can contribute to protecting and respecting the rights of minors at all times

1. Conduct innovative governance exercises as inputs for future regulation focused on children's digital rights.
2. Strengthen the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP).
3. Update Mexico's Federal Penal Code to include crimes committed online and in virtual worlds.
4. Include physical and mental well-being in the regulations and guidelines of the Federal Telecommunications Institute (IFT).
5. Create and strengthen official reporting mechanisms for online situations.
6. Designing and requiring impact assessments for public procurement processes related to digital education solution.
7. Include the topic of Digital Rights in the curriculum from an early age and develop education and training programs and campaigns on the safe and responsible use of the Internet for society as a whole.
8. Promote the recognition of girls', boys', and adolescents' agency.
9. Facilitate collaboration and conversation spaces to promote digital rights in Mexico and create resources.
10. Promote research related to the use of Artificial Intelligence and digital rights.
11. Promote Mexico's participation in international spaces on digital rights and the adaption of lessons-learned to the country.

## Recommendations for Mexico

### 1. Conduct innovative governance exercises as inputs for future regulation focused on children's digital rights.

In order to create a law to protect children's digital rights, as countries like the United Kingdom have done, the authors recommend that the relevant entities such as the Ministry of the Interior (SEGOB), the National Human Rights Commission (CNDH), the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), the Senate's and Chamber of Deputies' Commissions on the Rights of Children and Adolescents, and the Federal Telecommunications Institute (IFT) carry out exercises to generate input for its possible creation and implementation, in order to ensure that the law has the desired impact. To achieve this, it is important to involve as many stakeholders as possible in conversations that address multiple issues.

In particular, they could carry out public policy prototypes. These are processes in which a regulatory proposal is drafted in collaboration with organizations and experts in the relevant fields. Companies are then invited to voluntarily adopt the framework via a program that accompanies them in doing so. This

allows for the obtention of first-hand learnings about the proposal in order to adjust it for the desired impact. Moreover, regulatory sandboxes can also be carried out, where government agencies work with companies to explore the application of an existing law to innovative applications and business models that do not fit within the intended scope of the law. Through this process, the law can be adjusted to ensure its relevance over time.

### 2. Strengthen the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP)

As the European Union, the United Kingdom, Brazil, and other countries have done, it is crucial to update the law on personal data protection to reflect new technological advancements and the risks they pose to society, particularly to its most vulnerable, such as children and adolescents. The Senate or the Chamber of Deputies could draw inspiration from the General Data Protection Regulation (GDPR) to align Mexican law with the highest international standards.

To achieve this, the government could put together a roundtable or consultation mechanisms involving experts from the industry, academia,

civil society organizations, judicial authorities, parents, guardians, children, adolescents, and other subject matter experts to provide a comprehensive approach to the strengthening of Mexico's current data protection legislation.

### **3. Update Mexico's Federal Penal Code to include crimes committed online and in virtual worlds**

The Federal Penal Code does not currently recognize crimes committed online or in virtual worlds. Here is an example of the limited scope of the Code and its potentially negative impact on children's rights: while there are penalties for the promotion of child pornography, these penalties do not apply if the material is digital. Updating the Code to the digital era could not only punish those who violate children's rights online but also deter cybercriminals from carrying out various actions, thus mitigating the risks faced by children and adolescents online.

For this reason, it is urgent for the Senate and the Chamber of Deputies to update the Federal Penal Code, with the support of institutions such as the Attorney General's Office (FGR), INAI, IFT, as well as experts from different sectors, working with professionals focused on cybersecurity and the impact of this issue on children.

### **4. Include physical and mental well-being in the regulations and guidelines of the Federal Telecommunications Institute (IFT)**

While the IFT's regulations and guidelines cover privacy and the use of personal data, they could be strengthened by also including the topics of physical and mental well-being, holding the organization more holistically responsible for the impact that the services or products they approve can have on children and adolescents.

To achieve this, the General Guidelines Applicable to Radio and Television Programs Broadcasting News (Public Broadcasting System of the Mexican State, 2017) can be explored, taking into account the considerable complexity involved in taking responsibility for the content shared on the Internet.

### **5. Create and strengthen official reporting mechanisms for online situations**

Around the world, Internet users often face online challenges individually. To promote collaboration between citizens and the government in addressing these challenges, institutions such as the FGR, SEGOB, CNDH, INAI, and IFT could jointly design, implement, and promote official mechanisms accessible to girls, boys, and adolescents, that enable them to report online situations. It is important to ensure that the reporting channels are secure, practical, and

include the option for anonymity.

Furthermore, effective protection measures should be implemented to prevent and address situations of online violence and harassment. This may include establishing helpline numbers, developing technological tools for reporting, and training specialised teams to handle cases of cyberbullying and grooming.

## **6. Designing and requiring impact assessments for public procurement processes related to digital education solution**

As shared by consulted experts, public procurement processes can be an essential tool for strengthening human rights. Indeed, contracted digital solutions can expose children and adolescents in Mexico to new or increased dangers, particularly in terms of privacy and security. It is therefore essential to ensure a selection process that prioritizes the mitigation of these risks.

In this regard, the Ministry of Education (SEP) in conjunction with the National Institute for the Evaluation of Education (INEE), both at the local and federal levels, could implement impact assessments for digital education solutions intended to be acquired through these processes. This could help promote compliance with minimum human right protection standards (based on international best practices) and to promote equity and inclusion

in their implementation. This approach could contribute to using technology as a tool for quality education and the development of a responsible and critical digital citizenship.

## **7. Include the topic of Digital Rights in the curriculum from an early age and develop education and training programs and campaigns on the safe and responsible use of the Internet for society as a whole**

As online platforms and digital applications are increasingly used in the classroom, it is important to accompany this transition with training on the responsible and safe use of these new spaces. Considering the ubiquity of digital media in everyday life, it is crucial to create learning spaces for children, with thematic guidelines generated by the Ministry of Education in collaboration with other entities such as the Data Protection Authority and specialised organizations. Important topics could include privacy, prevention of cyberbullying, digital literacy, cybersecurity, digital civics, and digital hygiene, as well as digital coexistence.

Additionally, to improve online safety and foster the responsible use of Internet, it is important to have not only one generation but an entire population aware of the risks that individuals can face online. Special attention should be dedicated to those who guide and accompany the development of minors, with special programs for teachers and awareness tools for parents and guardians.



## **8. Promote the recognition of girls', boys', and adolescents' agency**

Recent advances in Mexico regarding human rights seem to lean towards a punitive and censorious approach, which is contrary to international best practices that seek to mitigate risks through the promotion of safe Internet use for minors—a perspective taken and promoted by the United Kingdom. This second perspective is more aligned with the current reality of Internet use among children in Mexico, as it has become an integral part of their lives and development. Eliminating this resource could have drastic impacts on their ability to integrate into society.

The authors recommend that any conversation or initiative on the topic of human rights includes the voices of girls and boys, whether through roundtable discussions, consultations, anonymous exercises, etc., to incorporate their perspective and recognize them as key actors in this conversation. Additionally, awareness and education campaigns could be created to encourage the active participation and defense of their rights through collaborative efforts of SEGOB, SEP, CNDH, and civil society organizations focused on protecting human rights.

## **9. Facilitate collaboration and conversation spaces to promote digital rights in Mexico and create resources**

In order to identify and promote the most appropriate approaches to protect digital rights, institutions such as SEGOB, CNDH, SEP, INAI, as well as state human rights commissions and civil society organizations, could create and facilitate spaces aimed at exploring how to ensure the protection of minors' digital rights without limiting their capacity to fully participate in the digital society. It is recommended that these events be held regularly (in person or online), occasionally including international actors to promote the exchange of best practices regarding digital rights. From there, groups can be formed to create a wide range of resources similar to those published by the United Kingdom.

In this regard, it will be important to cover topics such as privacy protection, digital security, freedom of expression, access to information, and the digital divide, among others. This can be achieved through the organization of forums, roundtable discussions, conferences, workshops, and other events that encourage active participation and collaboration among different stakeholders, where good practices and successful experiences in protecting digital rights can be shared, with the aim of positively impacting the ecosystem and public policy.

## **10. Promote research related to the use of Artificial Intelligence and digital rights**

The conversation surrounding children's safe use of the Internet and digital platforms from a rights perspective is just beginning to consider the impact of Artificial Intelligence systems on the protection of their rights, as demonstrated by the case of the United Kingdom. Considering that these technologies are increasingly permeating everyday life regardless of age, with the widespread adoption of generative AI tools such as ChatGPT, it is urgent to identify risks and create mitigation measures.

In this regard, funding could be provided through the National Council of Science and Technology (CONACYT), in collaboration with other institutions such as INEGI, SEP, national universities, and the Ministry of Infrastructure, Communications, and Transportation (SICT), to carry out research on the topic of digital rights, linking it to these new technological developments. This research could be applied and conducted in close collaboration with the government so that the latter can leverage the results to improve policies and strategies for the prevention and protection of minors in the digital realm.

## **11. Promote Mexico's participation in international spaces on digital rights and the adaption of lessons-learned to the country**

While Mexico participates in some international conversations on digital rights, it may be important to strengthen its presence via decision-makers from the aforementioned institutions, as well as civil society, to contribute the national context and perspective to the creation of international norms and guidelines and to leverage the lessons-learned. In this regard, it will be important for Mexican participants to generate public resources to share and disseminate international best practices, interesting use cases, and explore possible collaborations to replicate them in Mexico.

This replication would need to take into account the local reality and context, so it is recommended that this type of exercise be carried out with the support of highly capable local organizations in terms of analysing practices and cases and implementing them in a contextualised local manner. This type of exercise has already been successfully conducted with the United Kingdom in topics such as artificial intelligence, open banking, and mobility, to mention a few examples.

# CONCLUSION

In the last decades, the Internet has transitioned from being a military innovation to becoming an omnipresent tool in the lives of all individuals. While Internet usage was already prevalent among minors, the pandemic further immersed them in its use, enabling the continuation of their education and communication with others. As a result, the conversation about CDR accelerated internationally, recognising the importance of granting minors access to online platforms and tools, as it promotes their education, growth, and full immersion in society. However, the Internet can be a dangerous place for the unwary, especially for children. A person's "digital footprint" can be as easily traceable as their physical footsteps, making it a priority to explore new ways to protect them from online risks, taking into account that these vary depending on age, gender, online exposure, and other factors. This lack of exposure is particularly notable in Mexico, where 30% of minors do not have Internet access at home, but many have access to it from other locations.

While Mexico is currently working on various initiatives, it is important to strengthen the prioritization of this issue by generating more initiatives to protect children in their daily online activities, learning from international best practices and the global evolution of protection perspectives, industry approaches, and the voices of children

themselves. In this sense, it is necessary to implement measures that recognize the agency and children's digital rights, while also protecting their privacy and security in online and digital environments, fostering a culture of healthy digital coexistence.

As demonstrated in this report, high-income countries are the ones primarily focusing on achieving a balance between accessibility and security on the Internet for children, such as the United Kingdom, which has numerous resources, guidelines, and, since 2021, a law called the "Children's Code," based on international best practices such as the 2016 GDPR and the 1989 United Nations Convention on the Rights of the Child. This proposal is highly innovative as it focuses not so much on prohibiting children's access to the Internet but rather on seeking safe ways and channels for them to take advantage of all online content.

It is also interesting to consider the approaches of the private industry and engage in dialogue to design appropriate solutions to risks. Digital companies and startups play a crucial role in protecting children's digital rights because of the reach and use their products can have in the hands of children. Security is an aspect that must be considered from the design of any product, especially nowadays considering the vast amount of information generated by and

shared through them. It is therefore essential for these companies to take measures to ensure the privacy and protection of user data, especially for the most vulnerable, such as children.

As mentioned earlier, the participation of all stakeholders is crucial for wider reach and impact. It is important to involve the voices of children to consider their reality, the challenges they face online, their purposes for using digital platforms, their perspective on different solutions, their understanding of possible challenges, and many other topics. At the same time, it is important to empower them to have agency in this matter, complementing the crucial role played by parents, caregivers, and the education sector.

Lastly, the recommendations presented in this report are intended to be considered by decision-makers in Mexico, as well as other countries in Latin America and the Caribbean, contributing to regional and

global conversations in order to improve the protection of CDR and ensure they have access to a safe and equitable digital environment. As Ana Cecilia Pérez mentioned, "Education is fundamental to make the Internet a safe, kind, and respectful place for everyone."



# THE ORGANIZATIONS BEHIND THE FORUM AND BRIEF

## C Minds

C Minds is a Mexican think-and-do-tank led by women that works on the development and responsible use of frontier technologies for the social good in Latin America. C Minds' Eon Resilience Lab is specifically dedicated to preparing people for an uncertain and digital future, seeking inclusive digital transformation. In addition, C Minds' AI for Good Lab explores the applications of AI for social impact. The organization promoted and developed the national AI strategy in Mexico, positioning the country as one of the top 10 in the world to have an AI strategy. They founded and coordinated the National Artificial Intelligence Coalition, IA2030Mx. At the beginning of the pandemic, they collaborated with the Inter-American Development Bank (IDB) to create a guide to support schools in the region in safely and responsibly adopting virtual modalities, as well as a report for Ministries of Education and data authorities in Latin America, recommending public policies to support schools in this process. They are also researching the potential impact of augmented reality technology for education.

## British Embassy in Mexico

We develop and maintain long-standing relationships between the UK and Mexico. We support a range of British interests in Mexico and work together through a number of bilateral programmes, through our political, trade and prosperity sections, covering areas of interest to the UK and Mexico. We also provide consular services at our Embassy in Mexico City and our Consulate in Cancun. Our Department for International Trade (DIT) offices in Monterrey and Guadalajara support British companies trading in Mexico and Mexican companies investing in the UK.



British Embassy  
Mexico City

# REFERENCES

Association for Progressive Communications (APC), Article 19, and Swedish International Development Cooperation Agency (SIDA), 2019. *Artificial intelligence: Human rights, social justice and development*. Global Information Society Watch. Available at: [https://giswatch.org/sites/default/files/gisw2019\\_web\\_brazil.pdf](https://giswatch.org/sites/default/files/gisw2019_web_brazil.pdf)

Child Rights International Network and DefendDigitalMe, 2023. *Privacy and protection: a children's rights approach to encryption*. Child Rights International Network and DefendDigitalMe. Available at: <https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/63c9173dc9ac2348a1d9eac7/1674123078909/Privacy+and+Protection+-+CRIN+DefendDigitalMe+encryption+report.pdf>

Comisión de Derechos Humanos, 2020. *Violencia digital contra las mujeres en la Ciudad de México*. Informe Anual 2020, Volumen 2. Comisión de Derechos Humanos. Available at: <https://cdhcm.org.mx/wp-content/uploads/2021/06/Informe-anual-2020-Vol-II-Violencia-digital-contra-las-mujeres.pdf>

Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, 2020. *Children's data protection in an education setting - Guidelines*. Council of

Europe. Available at: <https://edoc.coe.int/en/children-and-the-Internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html>

Digital Futures Commission and 5Rights Foundation, 2023. *Playful by Design Toolkit*. Digital Futures Commission and 5Rights Foundation. Available at: <https://digitalfuturescommission.org.uk/playful-by-design-toolkit/>

INEGI, 2021. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH)*. INEGI. Available at: <https://www.inegi.org.mx/programas/dutih/2021/>

Information Commissioner's Office (ICO), 2020. *Age-appropriate design: a code of practice for online services*. Information Commissioner's Office. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>

Montgomery, E., Koros, E., n.D. *Meta's Best Interests of the Child Framework*. TTC Labs by Meta. Available at: <https://www.ttclabs.net/news/metas-best-interests-of-the-child-framework>

UNICEF, n.D. *Child Rights in the Digital Age*. UNICEF. Available at: <https://www.unicef-irc.org/research/child-rights-in-the-digital-age/>



UNICEF Comité Español, 2006. *Convención sobre los derechos del niño*. UNICEF. Available at: <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>

United Nations Human Rights (UNHR), Office of the High Commissioner, 1989. *Convention on the Rights of the Child*. UNHR. Available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

United Nations Human Rights (UNHR), Office of the High Commissioner, 2021. *General comment no.25 (2021) on children's rights in relation to the digital environment*. UNHR. Available at: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

Holmes, W., Persson, J. and Chounta, I-A., et al., 2022. *Artificial intelligence and education - A critical review through the lens of human rights, democracy and the rule of law*. Council of Europe. Available at: <https://book.coe.int/en/education-policy/11333-artificial-intelligence-and-education-a-critical-view-through-the-lens-of-human-rights-democracy-and-the-rule-of-law.html>



