

unicef
for every child

ARTIFICIAL INTELLIGENCE GOVERNANCE IN MOTION:

A rapid global review of AI regulation and its implications for children's rights

ACKNOWLEDGEMENTS

This rapidreviewwasauthoredbySabine Witting, Laura Berton, and Emma Day, Tech Legality.

Thereview was commissioned by UNICEF to supportthework of the ChildProtection Programme and Child Rights and Business teams. Josianne Galea Baron, Programme Specialist, Business Engagement and Child Rights, and Afrooz Kaviani Johnson, Child Protection Specialist, oversaw its development and provided technical oversight and guidance to the authors, with support from Ida Hyllested, Senior Adviser, and Stephen Blight, Senior Adviser.

Sincere appreciation is extended to Steven Vosloo and Miles Hastie, UNICEF Innocenti Global Office of Research and Foresight; Alexandra Chernyavskaya, UNICEF East Asia and the Pacific Regional Office; and Henrietta Ridley, UNICEF Digital Core, who provided helpful inputs and comments on earlier drafts.

This review reflects information available as of April 2025. While the authors have endeavoured to verify the accuracy and timeliness of the sources included, subsequent legislative and regulatory amendments may not be reflected.

Cover photo: ©UNICEF/UN0221433/LeMoyne

Suggested citation: United Nations Children's Fund, 'Artificial Intelligence Governance in Motion: A rapid global review of AI regulation and its implications for children's rights', UNICEF, New York, October 2025.

TABLE OF CONTENTS

Abbreviations and Acronyms....4
Executive Summary....5

01. Context 9

02. Objective & Methodology 12
2.1 Objective 13
2.2 Methodology 13
2.2.1 Limitations 13

03. International and Regional AI Guidance 15
3.1 OECD AI Principles (2019, updated in 2024)
3.2 ....17 G20 AI Principles (2019)
3.3 ....18 Santiago Declaration to Promote Ethical AI in Latin America
3.4 and the Caribbean (2023)
3.5 ....18 UNGA AI Resolution (2024) ....18 Council of
3.6 Europe Framework Convention on AI and Human Rights,
3.7 Democracy and the Rule of Law (2024)
3.8 ....19 AU Continental AI Strategy (2024)
....20 Global Digital Compact (2024)
....21 ASEAN Guide on AI Governance and Ethics (2024) 21

04. National Approaches to AI Regulation 22
4.1 Countries with AI-Specific Regulation 23
4.1.1 Risk-based approach (EU) 23
4.1.2 State-managed approach (China) 26
4.2 Countries without AI-Specific Legislation 29
4.2.1 Using existing legal frameworks to address AI-related risks (UK) 29
4.2.2 Government-led AI development with minimal regulation (India) 32

05. Key Findings and the Way Forward 35

ABBREVIATIONS AND ACRONYMS

AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
AU	African Union
CoE	Council of Europe
CRIA	Child Rights Impact Assessment
DSA	European Union Digital Services Act 2022
EdTech	Education Technology
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	European Union General Data Protection Regulation 2016
GenAI	Generative Artificial Intelligence
HRIA	Human Rights Impact Assessment
NCSC	United Kingdom National Cyber Security Centre
SDGs	Sustainable Development Goals
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly
UNICEF	United Nations Children's Fund
US	United States of America

EXECUTIVE SUMMARY

"States parties should ensure that national policies relating to children's rights specifically address the digital environment, and they should implement regulation, industry codes, design standards and action plans accordingly, all of which should be regularly evaluated and updated. Such national policies should be aimed at providing children with the opportunity to benefit from engaging with the digital environment and ensuring their safe access to it."[1]

Artificial Intelligence (AI) is becoming a key component of processes and systems across both the private and public sectors worldwide, shaping children's present and future experiences. As AI continues to evolve, there is an urgent need for responsible governance and regulation to address the risks and opportunities associated with its growing role in children's lives.

With an overall goal of informing ongoing efforts to strengthen AI regulation from a child rights perspective, this rapid review aims to:

1. Provide an **overview of international and regional AI frameworks and guidance** to better understand current approaches to AI regulation and governance at both levels; and
2. Identify and describe **current regulatory approaches on AI in four national jurisdictions,** analysing how regulators have addressed **the impact of AI on children** within their regulatory framework.

This review also serves as an input into UNICEF's broader guidance on AI for children,[2] which should be consulted for specific recommendations.

KEY FINDINGS

Of the eight **international** and **regional** AI frameworks and guidance reviewed, three make no explicit reference to children's rights or other vulnerable groups. Even if children are covered tangentially, this omission highlights a significant gap in addressing a key group of rights-holders.

While **national** regulatory approaches are unique and do not neatly fit into categories, this review identifies two broad categories, with corresponding regulatory trends:

1. **Countries with AI-specific legislation,** either adopting a risk-based approach or a state-managed model; and

1 United Nations Committee on the Rights of the Child, General comment General comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25, paragraph 24.

2 UNICEF's Policy Guidance is currently being updated. The updated version will be available in late 2025. See: https://www.unicef.org/innocenti/projects/ai-for-children.

2. **Countries without AI-specific legislation,** relying instead on existing frameworks or promoting government-led AI development with minimal regulation.

These trends are illustrated through examples from the European Union (EU), China, the United Kingdom (UK), and India reviewed as of April 2025. Among them, the EU AI Act explicitly recognises children as a vulnerable group, while China's legal framework includes specific references to children across various regulations and guidelines. In contrast, the UK's AI regulatory framework and guidance makes few explicit references to children and other vulnerable groups, instead relying on related frameworks for protections. India's framework contains no AI-specific provisions tailored to children or other vulnerable groups.

Importantly, this reflects regulatory trends as of April 2025 and may quickly become outdated due to the fast-evolving nature of AI regulation. The categorisation of trends is not exhaustive, and the recent enactment of many regulations means their impact on children remains uncertain, particularly as key guidelines and standards are still under development.

THE WAY FORWARD

The rapid review illustrates that countries around the world are taking **vastly different regulatory approaches** – aiming to maximise its benefits while minimising potential harms. As most AI regulations are newly adopted, and enforcement is only just beginning, it is too early to identify 'best practice' examples or recommend a specific regulatory approach. However, as the regulatory landscape evolves, **continuous scrutiny** will be essential to ensure that emerging approaches remain **responsive, evidence-based,** and aligned with **human rights and children's rights laws.** A proactive approach to regulation – balancing innovation with strong safeguards to protect the most vulnerable members of society, such as children – is necessary in ensuring that AI technologies support rather than undermine children's rights.



© UNICEF/UNI813019/Vu Le Hoang

Table 1 Snapshot of regulatory categories and trends

1. Countries with AI-specific legislation Countries which have enacted either comprehensive legislation for all AI technologies (commonly referred to as a 'horizontal approach') or legislation for specific AI technologies (also known as a 'vertical approach')	1.1 Risk-based approach Categorises AI based on the risk posed for society. High-risk applications carrying a higher compliance burden than low-risk applications, and certain types of AI technologies are prohibited altogether.	**Example: EU** The EU AI Act (2024) is the world's first AI regulation to apply a **comprehensive/horizontal, risk-based approach**. It establishes a regulatory framework to ensure the safety and trustworthiness of AI technologies by categorising applications by risk level and imposing stricter regulations and oversight on higher-risk systems. The EU AI Act recognises children as a vulnerable group by, for example, prohibiting AI systems that exploit age-related vulnerabilities and classifying certain uses of AI in education as high-risk. Examples of other countries with a similar approach: South Korea's Basic AI Act,[3] Brazil Draft AI Act.[4]
	1.2 State-managed approach Include measures of enhanced state management of AI, such as registration of AI with the government, content moderation, and output filtering/ management.	**Example: China** China's regulatory approach to AI can be described as a **vertical, state-managed approach** with strong enforcement and licensing restrictions for developers. The primary objective is to guide the development of AI in ways that support the Government's strategic priorities, particularly in enhancing the management of information ecosystems, to promote social cohesion, stability, and contribute to national efforts in advancing AI and technological innovation. The Chinese legal framework makes specific reference to children by, for example, requiring algorithmic recommendation service providers to fulfil their obligation of protecting children online and requiring the use of effective measures to prevent children from overly relying on or becoming 'addicted' to generative AI services. Example of another country applying a State-managed approach: Russia.[5]

3 Jethani et al., The Closing Act of 2024: South Korea's AI Basic Act, Tech Law Policy, 20 January 2025.

4 Atanasovska/Ribeli, Brazil's AI Act: A New Era of AI Regulation, GDPR local, 26 February 2025.

5 GINC, Russian's National AI Strategy.

<table>
<tr>
<td rowspan="2">2. Countries without AI-specific legislation

Countries which are relying on existing legal frameworks to tackle AI-risks or that complement existing legal frameworks with non-binding principles and standards</td>
<td>2.1 Using existing legal frameworks to address AI-related risks</td>
<td>Example: UK

The UK has taken a sectoral approach to AI regulation by using existing legal frameworks on data protection, consumer protection, cybersecurity, privacy, non-discrimination and others to address various AI-associated risks, instead of developing an AI-specific legal framework.

The UK's AI strategy makes few explicit references to children and other vulnerable groups. Such considerations are addressed indirectly through broader legislation, including data privacy, online safety, human rights, and anti-discrimination laws.

Examples of other countries with a similar approach: Singapore,[6] South Africa.[7]</td>
</tr>
<tr>
<td>2.2 Government-led AI development with minimal regulation</td>
<td>Example: India

India's approach to AI regulation is rooted in its view of AI as a 'kinetic enabler'[8] for the growth of its technology ecosystem and a catalyst for national development. Regulation is deliberately 'light touch' and sectoral (privacy, healthcare, banking, IT etc.), reflecting its philosophy of avoiding horizontal AI-specific legislation that could hamper innovation.

There are no AI-specific provisions tailored to children and other vulnerable groups. However, relevant data protection laws provide potentially significant protections for children and, to some extent, vulnerable groups in the context of data processing, which will directly impact AI development and deployment.

Examples of other countries with a similar approach: Saudi Arabia,[9] United Arab Emirates.[10]</td>
</tr>
</table>

6 Chng/Jones, Global AI Governance Law and Policy: Singapore, IAPP, February 2025.

7 De Wet, South Africa: The approach to regulating AI compared with the EU, VDT, 29 October 2024.

8 The Times of India, India's AI programme to be kinetic enabler to achieve $1 trillion digital economy: Rajeev Chandrasekhar, 13 October 2023.

9 Saudi Data & AI Authority, Vision 2030.

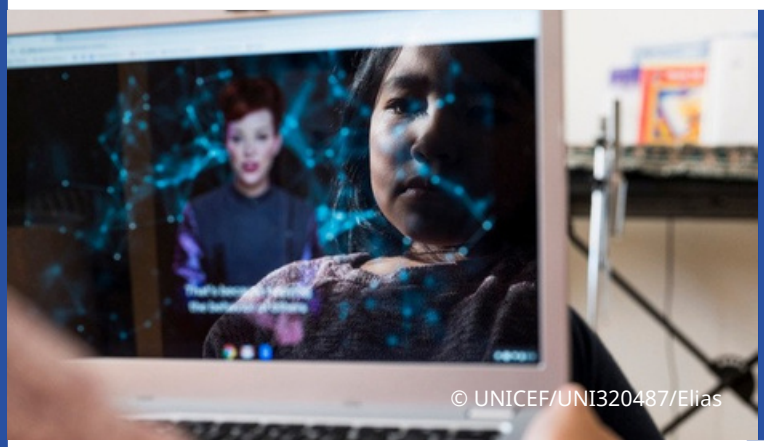
10 Hayward, Gulf governments take 'business friendly' approach to AI regulation, Pinsent Masons, 24 May 2024.



01

CONTEXT

© UNICEF/UNI782594/Exodus


© UNICEF/UNI320487/Elias

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[11]

Artificial Intelligence (AI) is becoming a key component of processes and systems across both private and public sectors worldwide, shaping children's present and future experiences.[12]

Today, children interact with AI across multiple facets of their daily lives – through smart toys, virtual assistants, video games, chatbots, and adaptive learning software. Algorithms curate the content they consume, suggesting what videos to watch, which news articles to read, what music to listen to, and even who to connect with online. AI-driven automated decision-making systems also have a significant, though often less visible, impact on children's lives. These systems influence crucial aspects such as access to education, healthcare quality, social welfare distribution, and even housing applications affecting their families. [13]

AI presents immense opportunities for children and society. It can support progress toward the Sustainable Development Goals (SDGs), from reducing poverty to combatting climate change. AI has the potential to create growth and employment and generate social and environmental value, such as creating new income streams for communities (SDG 1 and SDG 10) and improving agricultural practices (SDG 2).

By consolidating information obtained from diverse sources, such as official reports, news and social media, AI can assist governments and NGOs monitor risks in real time and respond effectively.[14] AI providers can also play a positive role in children's development and wellbeing. For example, AI can aid children's education and development, from early learning to virtual mentoring and school management. AI-driven adaptive learning platforms can provide personalised learning experiences, tailored towards each student's unique needs. AI-enabled systems can improve health outcomes by supporting diagnoses, triage, and treatment recommendations[15] – particularly valuable in isolated areas where teachers and doctors are scarce.

Despite these immense opportunities, AI raises concerns about equity and inclusion, particularly for children in low- and middle-income country contexts who may face exclusion from its benefits, widening existing digital and socioeconomic divides. Further, unrepresentative or biased data used to train AI technologies can lead to amplified discrimination and exclusion. This can affect children as

11 OECD, Recommendations of the Council on Artificial Intelligence, OECD/LEGAL/0449, 2024.

12 UNICEF, Policy guidance on AI for children, 2021, p. 7.

13 Ibid

14 ITU/Deloitte, AI for Good Impact Report, 2024, p. 41.

15 UNICEF, Policy guidance on AI for children, 2021, p. 21.

a collective if they are not considered in training data, or specific groups of children, such as when facial recognition software is trained on data of children with lighter skin tones and then shows higher error rates for children with darker skin tones. The lack of transparency in AI decision-making processes and the speed of deployment makes it difficult to identify and rectify such biases, further compounding the risk of discrimination.[16] This can negatively impact children in a range of contexts, including public welfare benefits, access to justice, and healthcare.[17]

Another type of AI with significant impact on children is Generative AI (GenAI), a specialised application of deep learning which can generate realistic content.[18] GenAI is not only capable of writing poetry and creating design features, but can also produce exploitative content such as child sexual abuse material or sexualised 'deepfakes'.[19] Children have also been using GenAI to create virtual friends.[20] While these can provide tailored educational support or act as play and creative partners, they also pose serious risks of harm – including manipulation, exposure to inappropriate or harmful content, and sexual exploitation.[21]

AI can also pose a risk to children depending on the context in which it is deployed. For example, live facial recognition software deployed in public spaces can be used for mass surveillance and assist governments to target people, including children, based on their ethnicity or political opinion.

As AI continues to evolve, there is an urgent need for responsible governance and regulation to address the risks and opportunities associated with its growing role in children's lives.

Against this background, international bodies and consortia, such as the OECD, the G7, the Council of Europe, and the UN, have developed international guidance to ensure responsible development of AI. At the national level, governments are beginning to introduce regulations to create an enabling environment for the responsible development, deployment, and use of AI, while also aiming to harness its developmental and economic benefits.

As an example, the OECD AI Observatory currently hosts over 1,000 AI policy initiatives from 69 countries, including territories such as the EU,[22] and a privately-run global AI tracker contains information about the AI regulation status of more than 195 countries.[23] In 2025, the Global Privacy Assembly's annual conference, the key forum for data protection authorities worldwide, has the overarching theme of 'AI in our daily lives'. While these authorities play a central role in data governance for AI, many countries are mandating separate regulators to oversee AI development and deployment, making cross-regulatory collaboration increasingly essential.

The development of national AI regulatory frameworks often reflects common themes, such as human rights, fairness, privacy and data governance, safety, transparency, competition through innovation, and accountability. However, countries diverge considerably in both their motivations for regulation and their approaches. These differences extend to how they protect individual rights, and whether they consider the specific vulnerabilities of groups such as children.

16 World Bank Group, Global Trends in AI Governance. Evolving Country Approaches, 2024, p. 23.
17 UNICEF, Policy guidance on AI for children, 2021, p. 22.
18 ITU/Deloitte, AI for Good Impact Report, 2024, p. 2.
19 NCMEC, Generative AI CSAM is CSAM, 2024.
20 See applications such as: Replika or Anima: AI Friend.
21 UNICEF, Beyond algorithms: Three signals of changing AI-child interaction, 23 May 2025.
22 OECD, National AI policies & strategies, accessed 15 April 2025.
23 Raymond Sun, Global AI Regulation tracker, accessed 15 April 2025.



02

OBJECTIVE & METHODOLOGY

© UNICEF/UNI552370/Dejongh

2.1 OBJECTIVE

With an overall goal of informing ongoing efforts to strengthen AI regulation from a child rights perspective, this rapid review aims to:

1. Provide an **overview of international and regional AI frameworks and guidance** to better understand current approaches to AI regulation and governance at both levels (see Part 3); and

2. Identify and describe **current regulatory approaches on AI in four national jurisdictions,** analysing how regulators have addressed **the impact of AI on children** within their regulatory framework (see Part 4).

This review also serves as an input into UNICEF's broader guidance on AI for children,[24] which should be consulted for specific recommendations.

2.2 METHODOLOGY

This rapid review has been conducted through desktop research. The **international and regional** instruments were selected based on their influence in national law-making processes, as well as their regional relevance.

While **national** regulatory approaches are unique and do not neatly fit into categories, this review identifies two broad categories, with corresponding regulatory trends, for clarity. These trends are illustrated through examples from the EU, China, the UK, and India.

The EU and China were selected as regulatory examples of **AI-specific legislation**, with the EU being the first region to adopt a 'horizontal' AI regulation and China the first country to adopt 'vertical' AI regulation. The UK was chosen for its **sector-based approach** to AI regulation, using current regulators' expertise. India was selected for viewing AI as an enabler for national development, with regulation playing a supportive role.

2.2.1 Limitations

This review has important limitations. Firstly, **AI regulation is a very fast-moving field, with regulatory trends changing in the span of a few months**. As such, the findings presented here reflect the state of regulatory trends as of April 2025. These may quickly become outdated, particularly the legislative examples drawn from specific jurisdictions.

Secondly, **categories of AI regulatory trends are fluid and not clear-cut**. While this review proposes a certain categorisation, it does not capture all existing trends, nor do the examples from specific jurisdictions fit neatly into each category. For example, some countries have adopted voluntary risk assessments and AI ethics principles, which is another trend within the broader non-AI specific regulatory approach. Despite these nuances, the categories selected for this review were considered most representative of the current AI regulatory landscape.

24 UNICEF's Policy Guidance is currently being updated. The updated version will be available later in 2025. See: https://www.unicef.org/innocenti/projects/ai-for-children.

Thirdly, **since these regulations were enacted recently**, it is too early to evaluate their impact – positive or negative – on children's lives.

Finally, **some regulatory frameworks are highly reliant on accompanying guidelines and standards**, which might not have been drafted or adopted yet. Therefore, this review is only a reflection of the current state of regulation, acknowledging that key parameters for scope and/or interpretation of the legal framework will most likely change on a national level in the coming months and years.



© UNICEF/UN0654904/Taylor



03

INTERNATIONAL AND REGIONAL AI GUIDANCE

© UNICEF/UN0678713/Filippov

In recent years, the international community has increasingly recognised the transformative power of AI on societies, economies and our collective future. Acknowledging the importance of transnational alignment in AI regulation, various international and regional bodies have developed guidance. While most of this guidance is non-binding – with the exception of the Council of Europe's Convention on AI – it addresses many of the same themes found in national frameworks, including human rights, fairness, privacy and data governance, safety, transparency, competition, and accountability. These international and regional guidance provide an important framework in establishing areas of consensus and common ground.

Table 2 provides an overview of the international and regional guidance, which is discussed in more detail in the subsequent sections.

Table 2 Overview of international and regional AI guidance

Guidance	Region	Type	Date	Mention of children's rights
OECD AI Principles	38 OECD Member [25] s	Non-binding	2019, updated 2024	No explicit mention of children's rights or other vulnerable groups
G20 AI Principles	G20 Members[26]	Non-binding	2019	No explicit mention of children's rights or other vulnerable groups
Santiago Declaration to Promote Ethical Artificial Intelligence in Latin America and the Caribbean	20 countries from Latin America and the Caribbean	Non-binding	2023	No explicit mention of children's rights or other vulnerable groups
UNGA Resolution on AI	193 UN Member States[27]	Non-binding	2024	Refers to people 'in vulnerable situations', which includes children

25 OECD, Members and partners, accessed 15 April 2025.

26 G20, Members, accessed 15 April 2025.

27 UN, Member States, accessed 15 April 2025.

Table 2 Overview of international and regional AI guidance (cont.)

Guidance	Region	Type	Date	Mention of children's rights
Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law	15 signatories[28]	Binding* *Convention has not been ratified yet and has hence not entered into force Non-binding	2024	Recognises the importance of the UN Convention on the Rights of the Child in its preamble and requires States parties to take due account of children's specific needs and vulnerabilities
AU Continental AI Strategy	55 AU Member States[29]		2024	Recognises the vulnerability of children and makes dedicated recommendations
Global Digital Compact	193 UN Member States[30]	Non-binding	2024	Explicitly references children's rights, though not in the context of AI. Elaborates on the objective of enhancing international governance of AI for the benefit of humanity
ASEAN Guidance on AI Governance and Ethics	10 ASEAN Member States[31]	Non-binding	2024	Recognises the vulnerability of children in relation to data protection and makes various reference to vulnerable groups in general, including children

3.1 OECD AI PRINCIPLES (2019, UPDATED IN 2024)

The non-binding OECD AI Principles, first adopted in 2019 and updated in 2024, represent the first intergovernmental standard on AI. They advocate for AI that is both innovative and trustworthy, and that upholds human rights and democratic values. The principles emphasise the importance of transparency and explainability, as well as robustness, security, safety and accountability. They recommend that national AI policies focus on investing in research and development, fostering an inclusive AI-enabling ecosystem, shaping an enabling interoperable governance and policy

28 CoE, The Framework Convention on Artificial Intelligence, accessed 15 April 2025.

29 AU, Member States, accessed 15 April 2025.

30 UN, Member States, accessed 15 April 2025.

31 ASEAN, Member States, accessed 15 April 2025.

environment for AI, building human capacity and preparing for labour market and transformation, and enhancing international cooperation for trustworthy AI. While the OECD AI Principles do not explicitly name specific vulnerable groups, such as children, they emphasise the importance of equity, fairness, and inclusivity, ensuring that AI benefits everyone, especially those at risk of exclusion or harm. To date, 47 adherents have signed on to the OECD AI Principles.

3.2 G20 AI PRINCIPLES (2019)

The non-binding G20 AI Principles, adopted in 2019, serve as an extension of the OECD AI Principles, ensuring a broader global commitment to responsible AI governance. Similar to the OECD AI Principles, the G20 AI Principles do not explicitly name vulnerable groups such as children, but promote AI policies that prioritise fairness, inclusivity, and accessibility, which inherently benefit marginalised and at-risk communities. While the OECD principles remain the foundational framework, the G20 endorsement gives them greater international legitimacy, encouraging more countries to adopt human-centric
and ethical AI policies. The OECD AI Principles were initially adopted by OECD members and partner countries. Their reach was significantly expanded when the G20 endorsed them, promoting wider adoption among major economies beyond the OECD, including China, India, and Brazil. The G20 AI Principles encourage G20 members to align their national AI policies with the OECD framework.

3.3 SANTIAGO DECLARATION TO PROMOTE ETHICAL AI IN LATIN AMERICA AND THE CARIBBEAN (2023)

The Santiago Declaration to Promote Ethical Artificial Intelligence in Latin America and the Caribbean (2023), signed by 20 countries from the region, emphasises that AI policies should be grounded in equity, non-discrimination, gender equality, privacy, security, transparency, and accountability. It calls for public policies and legal frameworks to ensure that AI technologies are safe, fair, and sustainable across social, cultural, economic, and environmental dimensions. The declaration emphasises the importance of human oversight, education, and multi-stakeholder collaboration to ensure AI development and deployment align with ethical guidelines. It also calls for proactive governance, recognising that AI-driven changes are evolving rapidly and may require new legal and ethical responses. Another key focus is the importance of engaging private companies, civil society, and academia to ensure inclusive, multisectoral AI governance tailored to the unique challenges of the region.

While children are not explicitly mentioned in the declaration, it places strong emphasis on the need to prevent discrimination, exclusion and gender bias, including structural inequalities, in AI technologies. It also highlights the need to monitor the impact of AI on unemployment in the region, especially for young people and those in vulnerable situations.

3.4 UNGA AI RESOLUTION (2024)

In 2024, the United Nations General Assembly (UNGA) unanimously adopted a landmark resolution promoting 'safe, secure, and trustworthy' AI technologies to benefit sustainable development globally. The resolution emphasises the importance of bridging the digital divide, ensuring equitable access

to AI technologies, and safeguarding human rights throughout the AI lifecycle. It calls upon member states, private sector and civil society to develop regulatory frameworks that uphold these principles, aiming to harness AI's potential while mitigating risks associated with its misuse. The resolution calls upon stakeholders to refrain from or cease the use of AI technologies that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, especially of those who are in vulnerable situations. While children are not specifically mentioned, the text refers to those 'in vulnerable situations', which includes children.

3.5 COUNCIL OF EUROPE FRAMEWORK CONVENTION ON AI AND HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW (2024)

In 2024, the Council of Europe adopted its Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law (CoE AI Convention), which is the first binding international treaty on AI. The CoE AI Convention outlines fundamental principles, such as human dignity, autonomy, equality, non-discrimination, privacy protection, transparency, accountability, reliability, and safe innovation, that AI technologies must adhere to throughout their lifecycle to ensure ethical and responsible use.

States parties must adopt measures to ensure adequate transparency and oversight, enable individuals to challenge AI-based decisions, and offer procedural safeguards for those whose rights and freedoms are significantly impacted by AI.

The CoE AI Convention also provides that AI technologies must undergo continuous risk and impact assessments to evaluate their effects on human rights, democracy, and the rule of law. States parties must implement preventive and mitigation measures to address potential harms. Authorities should have the power to ban or impose moratoria on AI applications that pose unacceptable risks, ensuring that AI development aligns with ethical and legal standards.

The CoE AI Convention recognises the importance of the UN Convention on the Rights of the Child in its preamble and requires States parties to take account of any specific needs and vulnerabilities in relation to respect for the rights of children (Art 18). At the time of writing, the CoE AI Convention has been signed by 15 entities, including ten CoE member states (Andorra, Georgia, Iceland, Liechtenstein, Montenegro, Norway, Republic of Moldova, San Marino, Switzerland and the United Kingdom), four non-CoE member states (Canada, Japan, United States of America, Israel) and the European Union.[32] As these states have only signed, but not ratified the Convention yet, the Convention has not yet entered into force.[33]

32 CoE, The Framework Convention on Artificial Intelligence, accessed 15 April 2025.

33 The Convention will enter into force after five signatories, including at least three Council of Europe member states, have ratified it, see Art 30 (3).

3.6 AU CONTINENTAL AI STRATEGY (2024)

The African Union (AU) Continental AI Strategy is a comprehensive framework that aims to leverage AI for Africa's socio-economic development while ensuring responsible and ethical deployment. The AU Continental AI Strategy proposes a people-centric, development-oriented and inclusive approach to AI. It highlights the need for harnessing AI's benefits for African people, institutions, the private sector and countries, and promoting the competitiveness of the African private sector. It further addresses the risks associated with the increasing use of AI, with attention to governance, inclusion and diversity, human rights, gender equality, dignity, safety, peace and security, information integrity, and sustainable environment and ecosystem, considering African contexts, cultures, and values. The strategy also aims to accelerate AU Member States' capabilities in infrastructure, AI talent and skills, datasets, innovation and research that underpin AI development. foster regional and international cooperation and partnerships, and stimulate public and private investment in AI at national and regional levels.

The AU Strategy recognises the vulnerability of children in the context of AI and makes several recommendations how children can be protected from AI-associated risks, such as data privacy violations; how AI can be used to promote children's access to quality healthcare; and how children can be prepared for the AI workforce through the education system.

Global AI Summit on Africa – Africa Declaration on AI

The Global AISummit on Africa took place between 4-5 April 2025 in Kigali, Rwanda. A key Summit output is the Africa Declaration on AI, which builds heavily on the existing AU strategic frameworks such as the African Union Continental Strategy on AI, Smart Africa AI for Africa Blueprint, AU Data Policy Framework, and the AU Convention on Cybersecurity and Personal Data Protection.

Even though there is no specific mentioning of children, recommendations made by children during a child-led side event were included in the Declaration, namely on the need for safeguards to prevent harm and protect privacy, ethics, transparency, and explainability while prioritising human dignity, rights, freedoms, and environmental sustainability; as well as the need for continent-wide AI education initiatives with curriculum development for youth at all levels.



© UNICEF/UNI715443/Nazir

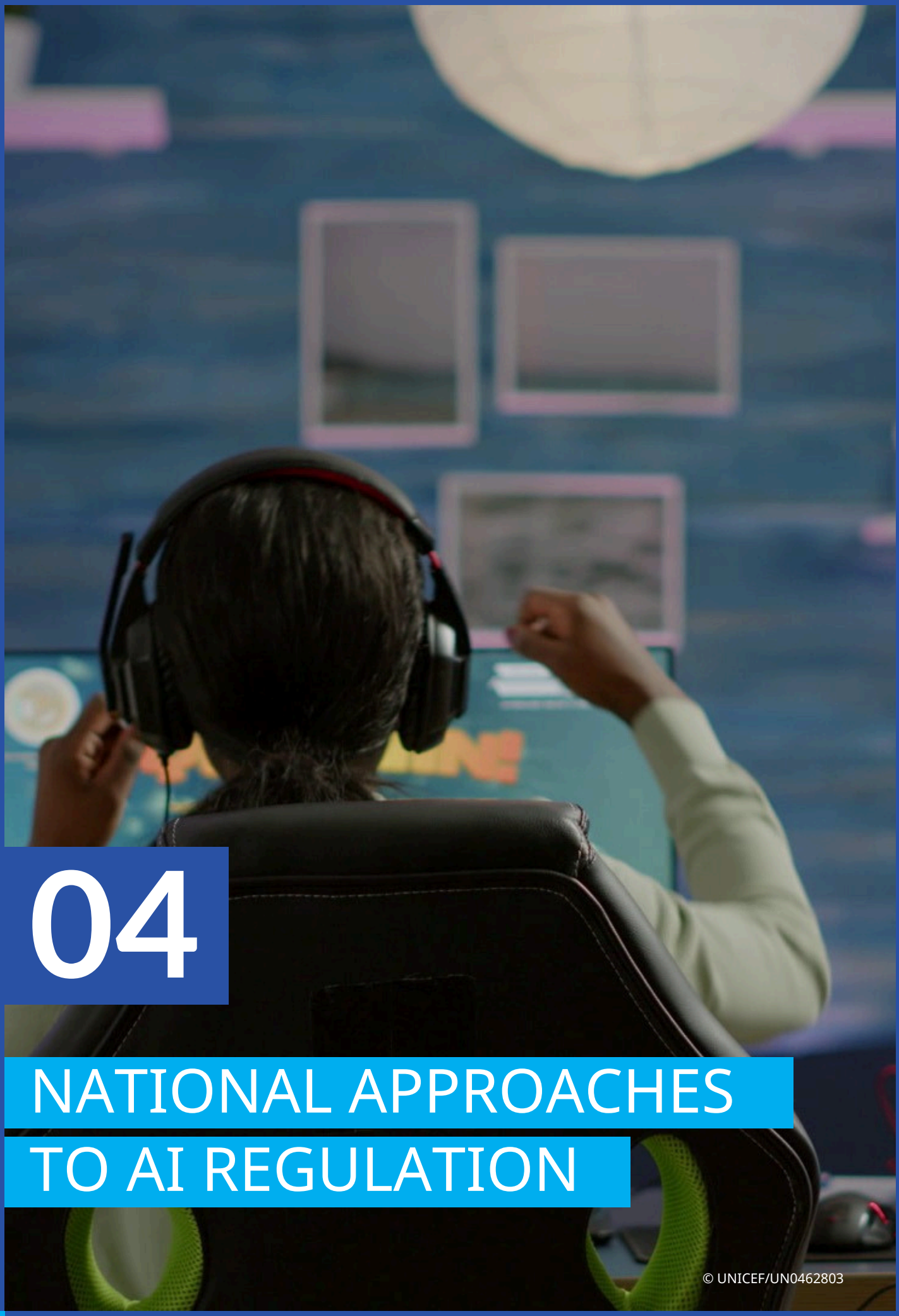
3.7 GLOBAL DIGITAL COMPACT (2024)

In 2024, the United Nations General Assembly adopted the Global Digital Compact, a milestone agreement aimed at shaping an inclusive, open, sustainable, fair, safe and secure digital future for all. It calls on governments, the private sector, civil society, and other stakeholders to collaborate on key areas such as digital inclusion, data governance, online safety, and fostering respect for human rights, including children's rights, in the digital space. The Compact includes five objectives including 'enhancing international governance of artificial intelligence for the benefit of humanity'. While the Compact places emphasis on the rights and safety of children, it does not include specific reference to children in relation to AI.

3.8 ASEAN GUIDE ON AI GOVERNANCE AND ETHICS (2024)

The Association of Southeast Asian Nations (ASEAN) Guide on AI Governance and Ethics serves as a practical guide for organisations to design, develop, and deploy traditional AI in commercial and non-military or dual-use applications. The Guide focuses on encouraging alignment within ASEAN and fostering interoperability of AI frameworks across jurisdictions. It sets out several guiding principles, such as transparency and explainability, fairness and equity, security and safety, robustness and reliability, human-centricity, privacy and data governance, and accountability and integrity. It recommends nurturing of AI talent and upskilling the workforce; supporting AI innovation and promoting investment; and raising awareness on risks and benefits of AI, amongst others.

While children are only explicitly mentioned in the context of data protection, the ASEAN Guide refers to vulnerable individuals in the context of risk assessments, protection from malicious actors and designing AI technologies with human benefit in mind which should not take advantage of vulnerable individuals. It can be assumed that children are considered vulnerable individuals under the ASEAN Guide. An accompanying expanded guide on GenAI was released in January 2025, with more explicit provisions for various types of risks, but not for children.



04

NATIONAL APPROACHES TO AI REGULATION

© UNICEF/UN0462803

4.1 COUNTRIES WITH AI-SPECIFIC REGULATION

Countries with AI-specific regulation have enacted either comprehensive legislation for all AI technologies (horizontal approach) or legislation for specific AI technologies (vertical approach). The horizontal approach is illustrated by the risk-based approach to AI regulation taken by the EU's AI Act, while the vertical approach is represented by China's state-managed AI regulation.

4.1.1 Risk-based approach (EU)



Philosophy

The European Union (EU) AI Act (2024)[34] is the world's first AI regulation to apply a horizontal, risk-based approach. Most obligations under the AI Act will apply after a two-year implementation period (i.e. from 1 August 2026). The EU AI Act introduced a gradation of AI technologies, reaching from prohibited systems to high-risk and low-risk AI technologies. The different risk levels mean more or fewer AI compliance requirements. The EU AI Act reflects the EU's wider digital regulation philosophy and principles which are human centric (protecting EU citizens) and rights-based, with a strong emphasis on accountability and transparency.

With the EU AI Act, the EU aims to take global leadership in setting legal standards for AI, as it did with data privacy through the General Data Protection Regulation (GDPR) and platform regulation via the Digital Services Act (DSA). The GDPR, the DSA and other EU regulations complement the AI Act. The EU believes that providing legal certainty for AI development will allow EU AI developers to flourish while respecting human rights and mitigating AI risks. It should serve as a tool for people, with the ultimate aim of increasing human well-being.



Legislative approach

The EU AI Act establishes a regulatory framework to ensure the safety and trustworthiness of AI technologies within the EU and categorises AI applications by risk level, imposing stricter regulations and oversight on higher-risk systems. The AI Act applies extraterritorially, meaning it impacts providers, deployers, importers, distributors, and manufacturers of AI technologies regardless of their geographic location, provided that the AI system is placed on the market, put into service, or used in the EU. This geographical scope is analogous to other EU digital regulations, such as the GDPR and the DSA.

The EU AI Act **prohibits AI technologies which pose an unacceptable risk** for the public and individuals (Art 5). For example, when AI is used for social scoring (i.e. evaluating or classifying individuals or groups based on social behaviour or personal traits); assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits; compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage; or inferring emotions in workplaces or educational institutions, except for medical or safety reasons, amongst others.

34 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Most obligations focus on **high-risk AI technologies**. AI technologies are considered 'high-risk' in three ways: when the AI system is itself a certain type of product which is already subject to EU regulation;[35] when the AI system is a safety component of a certain type of product which is already subject to EU regulation;[36] and when the AI system meets the description of listed 'high-risk' AI technologies.[37] High-risk systems carry the highest compliance burden, including on robust risk management, data governance, transparency and explainability, accountability, security and technical robustness, AI literacy capacity building for staff as well as users, monitoring and reporting and application of ethical considerations, amongst others (Chapter 3 EU AI Act).

The EU AI Act also contains provisions on 'general-purpose' AI. Providers of general-purpose AI models must ensure a good understanding of their models along the entire AI value chain. They must draw up technical documentation of their models, put in place a copyright policy, and publish a training content summary. In addition, providers of general-purpose AI models posing systemic risks, which may be the case either because they are models with high impact capability[38] or because they have an equivalent impact,[39] must notify those models to the EU Commission, assess and mitigate systemic risks stemming from those models, including via performing model evaluations, reporting serious incidents, and ensuring adequate cybersecurity of these models.



Considerations for children and other vulnerable groups

The EU AI Act **explicitly recognises children as a vulnerable group**. Recital 15 acknowledges that AI can also be 'misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict [....] fundamental rights, including [...] the rights of the child.' In the context of fundamental rights impact assessments, the EU AI Act states that 'children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child [...], both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being' (Recital 28a). While Recitals do not form part of the legally binding text, they are an important rule of interpretation and demonstrate that children and their specific needs were considered in the development of the EU AI Act.

Even though children are not explicitly mentioned in the body of the text, there are multiple provisions which provide protection to children due to their acknowledged vulnerability. As an example, Article 5 (1) (b) EU AI Act prohibits – under specific circumstances – an AI system that exploits vulnerabilities due to age, disability or a specific social or economic situation.

35 See Rauer/Kempf, A guide to high-risk AI systems under the EU AI Act, Pinsent Masons, 13 February 2025: The EU AI Act recognises that AI systems may be an AI system and another form of product at the same time. Where those products are already subject to certain EU regulation, the EU AI Act provides for AI systems constituting such products to be considered 'high-risk' AI systems. This could apply to medical devices, industrial machinery, toys, aircraft or cars, amongst others.

36 Ibid., where an AI system is used as safety component of a product which is subject to certain EU regulation, the EU AI Act provides for AI systems constituting such products to be considered 'high-risk' AI systems. This could apply to safety components in medical devices, toys, rail infrastructure or lifts, amongst others.

37 Ibid., AI systems could also be considered 'high-risk' AI systems if they meet the description of any of the AI systems listed in a further annex to the EU AI Act. The list covers different contexts such as biometrics, education, employment, and access to essential services, amongst others, and adds additional requirements depending on the extent of harm the AI system poses in each specific context.

38 Defined as models with 10^25 floating-point operations, see Art 51(2) AI Act.

39 See Art 51(1) AI Act.

In 2024, the EU Commission published Guidelines[40] for the interpretation of Article 5, clearly stating that children are particularly susceptible to manipulation due to their developmental stage, which limits their ability to assess and understand what is real and the intentions behind AI-driven interactions critically. Children are also particularly vulnerable to forming attachments to AI agents and applications, and are therefore more susceptible to manipulation, exploitation, and what it calls addictive behaviour.

Further, the Guidelines state that children are highly impressionable and may not possess the cognitive maturity to evaluate persuasive content critically or resist certain exploitative practices that aim to keep them dependent on the AI-enabled services. This could, in turn, contribute to the shaping of their values, beliefs and steer behaviours in potentially harmful ways. The significant harm here is both physical and psychological, exacerbated by the children's inability to discern and resist the exploitation and the harmful effects to their development and well-being that may have a long-term impact.[41] Therefore, the EU AI Act prohibits AI technologies which exploit the vulnerability of children due to their age, under specific circumstances.

Further, children must be given special consideration within the AI provider's risk management system (required for high- risk systems) which includes, among other requirements, the completion of a fundamental rights impact assessment (Art 9). Vulnerability is a common concept in the EU AI Act, referred to in multiple other provisions, which gives an opportunity to specifically assess the AI system's impact on children and develop mitigating measures.[42]

Lastly, the EU AI Act classifies specific uses of AI in education as high risk, in particular when used for determining access or admission, for evaluating learning outcomes, for assessing education levels required for admission to an education institution, or for monitoring and detecting prohibited behaviour during tests (see Annex III, AI Act). This approach aims to address many of the most potentially problematic or extreme uses of AI in education.



© UNICEF/UNI658121/Magakoe

40 EU Commission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 2025.

41 Ibid.

42 Malgieri/Rebrean, Vulnerability in the AI Act: Building an interpretation, SSRN, 28 November 2024.

4.1.2 State-managed approach (China)



Philosophy

China's AI regulation has evolved alongside its rise as a cyber-power. Currently ranked second globally in AI investments,[43] China aims to set its own rules over cyberspace while leveraging digital technologies for economic and social goals. Since 2017, AI governance has been a priority, with policies shaping its development in three stages. Initially, China promoted industry self-regulation, encouraging investment and market growth. As cybersecurity policies solidified, national standards emerged to guide industry participation. More recently, regulators have introduced concrete rules for specific industries and technologies, targeting recommendation algorithms for disseminating content, synthetically generated images and video, and generative AI technologies. [44]

China's approach can be described as 'vertical' – focused on specific applications or manifestations of an AI technology – and iterative. China's approach is iterative as it quickly moves to adapt and improve its legislation following new technological developments, such as the 2023 Regulation discussed below. However, China might also be moving to a 'horizontal' AI law soon, aiming to establish a more cross-cutting AI law.[45]

The underlying philosophy of China's AI governance can be described as a state-managed, characterised by strong enforcement and licensing requirements for developers.[46] Regulatory measures are closely aligned with national priorities, particularly in enhancing the management of information ecosystems, promoting social cohesion and stability, and contributing towards national efforts in advancing AI and technological innovation. This strategic focus was evident in China's first regulatory intervention on AI, which targeted the impact of AI on content recommender systems.[47]

China's regulatory measures for GenAI require systems uphold 'socialist core values' and prohibits certain types of content such as content that undermines political stability.[48] Broader regulatory goals include minimising adverse social and economic impacts of AI, creating a conducive environment for becoming a global leader in AI development, and positioning China as a leader in AI governance and regulation.[49]

43 TU/Deloitte, AI for Good Impact Report, 2024, p. 6.

44 Gong/Qu/Dorwart, AI Governance in China: Strategies, Initiatives, and Key Considerations, Bird & Bird, 14 March 2024.

45 Sheehan, China's AI regulation and how they get made, 2024, p. 115.

46 Pessarlay, China updates draft rules governing generative Ai platforms, Coingeek, 16 July 2023.

47 Sheehan, China's AI regulation and how they get made, 2024, p. 111.

48 Art 4, 2023 Interim Measures on Generative AI, which enforce strict security and content control over Generative AI models.

49 Sheehan, China's AI regulation and how they get made, 2024, p. 118.

Legislative approach

China's AI regulatory approach is vertical. Accordingly, the following analysis focuses on three key regulatory measures advanced by the Cyberspace Administration of China, China's primary internet and cyber regulator:

- 2021 Regulation on the Management of Algorithmic Recommendations for Internet Information Providers;
- 2022 Regulation on the Administration of Deep Synthesis Internet Information Services; and
- 2023 Interim Measures on Generative AI, which enforce strict security and content control over Generative AI models.

2021 Regulation on the Management of Algorithmic Recommendations for Internet Information Providers

This 2021 Regulation was China's first regulatory measure on AI. Initially driven by the Cyberspace Administration of China's concern about the role of algorithms in disseminating online information, its scope was extended to other areas in which algorithmic recommender systems are deployed, such as price setting or preparation of work schedules.[50] The regulation requires service providers to 'uphold mainstream value orientation' and 'actively transmit positive energy' (Art 6). It requires platforms to manually intervene in political topics discussed on social media to ensure they reflect government priorities (Art 9) and prohibits the building of algorithms that 'go against ethics and morals' and which induce users to 'become addicted and overconsume' (Art 8). The regulation also grants users new rights, such as the right to turn off algorithmic recommender systems or to delete tags used to personalise recommendations (Art 17).

The 2021 Regulation created an algorithm registry. Developers need to submit information on how the algorithms are trained and deployed, including the data sets they are trained on. They are also required to complete an algorithmic security self-assessment report. A limited version of the registration is made public (Arts 23-30).

2022 Regulation on the Administration of Deep Synthesis Internet Information Services

The 2022 Regulation aims to combat synthetically generated content as a major threat to the information environment in China. It encompasses the use of AI to generate or alter content online, including voice, text, and video (Art 23). The regulation puts forward a set of information controls for providers. Providers must label synthetically generated content that might cause confusion or mislead the public (Art 17), such as services simulating natural persons, or face-swapping applications. They also must take steps to mitigate misuse of the technology, such as requiring users to register with their real names (Art 9). Like the 2021 Regulation, the 2022 Regulation contains some specific content requirements. Deepfake content needs to 'adhere to the correct political direction' and shall not disturb the 'economic and social order' (Art 4). Deep synthesis service providers also need to register their algorithms in an algorithm registry (Art 19).

50 Sheehan, China's AI regulation and how they get made, 2024, p. 111.

2023 Interim Measures on Generative AI

Even though the 2022 Regulation appeared to cover most issues associated with GenAI, especially when it comes to images and videos, the 2023 Interim Measures focused on the large volumes of text produced by GenAI, as well as the general-purpose nature of this technology. The 2022 Regulation was finalised just a few days before the release of ChatGPT, which brought the public's attention to the potential adverse impacts of GenAI models.[51] The development of the 2023 Interim Measures demonstrates China's iterative regulatory approach to AI, quickly adjusting the regulatory framework when the technology evolves.

The Interim Measures state that the provision and use of GenAI shall respect social morality and ethics, including core socialist values, and prohibits content inciting subversion of national sovereignty (Art 4). Article 4 further requires providers to respect the lawful rights and interests of others and prohibits actions that endanger physical or psychological wellbeing. The Interim Measures require service providers to 'employ effective measures to improve the quality of training data and to enhance the data's veracity, accuracy, objectivity, and diversity' (Art 7). Data used to train the GenAI model must have been obtained lawfully (Art 9). Providers are responsible as producers of online information content (Art 9) and must label generated content as such, promptly addressing 'illegal content' through 'effective measures.' These include stopping the generation or transmission of the content, removing it, and correcting it through model optimisation training, and reporting the issue to the relevant authorities (Art 14).



Considerations for children and other vulnerable groups

Various regulations and guidelines make **specific reference to children**. The 2021 Regulation specifically addresses 'minors' affected by algorithmic recommender systems. Article 18 states that providers offering services to minors shall fulfil their obligation of protecting minors online in accordance with the law. This includes facilitating access to information beneficial to their physical and mental health by developing models suitable for minors and providing services suitable for the characteristics of minors. It also prohibits pushing any information that may negatively affect the physical and mental health of minors, such material that could lead to imitation of unsafe behaviours, behaviours violating social morality, or encouraging harmful habits. Additionally, algorithmic recommendation services must not be used to induce minors to become 'addicted' to the internet (Art 18).

The 2023 Interim Measures state that providers shall clarify and disclose the applicable populations, occasions, and uses of their services; guide users to scientifically and rationally understand and lawfully use GenAI technology; and employ effective measures to prevent minors from overly relying on or becoming addicted to GenAI services.

51 Sheehan, China's AI regulation and how they get made, 2024, p. 114.

4.2 COUNTRIES WITHOUT AI-SPECIFIC LEGISLATION

Countries without AI-specific legislation are either using existing legal frameworks to tackle AI-specific risks or relying on non-binding principles and standards. The approach of a country using its existing legal framework to address AI related risks is illustrated by the UK, while India is an example of an approach based on non-binding principles and standards.

4.2.1 Using existing legal frameworks to address AI-related risks (UK)

Philosophy

Since Brexit, the UK strategically adopted an AI regulatory philosophy distinct from that of the EU, prioritising innovation and economic competitiveness rather than embracing the EU's perceived regulatory-heavy approach. In 2023, the UK promoted a 'pro-innovation' strategy[52] seeking to stimulate economic growth whilst endeavouring to position itself into a 'trustworthy AI' global leadership position.

The rationale was based on the rapidly evolving AI landscape, the need for global competitiveness, and fears that legislation would stifle innovation and deter businesses whilst gaining public trust by tackling AI risks with a focus on security and safety. To pursue these ambitions, the UK has taken a sectoral approach relying on the expertise and experience of its current 'high-quality regulators and its strong approach to the rule of law, supported by its technology-neutral legislation and regulations to apply AI principles.'[53]

Legislative approach

The UK's legislative approach to AI regulation currently lacks dedicated horizontal AI legislation, with the recent exception of potential regulations for frontier AI technologies.[54] Instead, the UK's approach involves relying on existing sectoral regulation (and AI-specific guidance), complemented by a principles-based voluntary framework. This hybrid model is said to use existing regulatory expertise while maintaining the flexibility to adapt to a rapidly evolving technological environment.[55]

This governance approach targets the uses and outcomes of AI technologies rather than the technology itself, aligning with the philosophy of promoting innovation.

52 UK Government, National AI Strategy, September 2021; UK Government, A pro-innovation approach to AI Regulation, 3 August 2023. Please note that the UK Government website on which this paper is published now contains a big disclaimer stating "This was published under the 2022 to 2024 Sunak Conservative government". As the current government may pursue different priorities, the approach outlined in these papers might not be reflective of the present government's position.

53 UK Government, A pro-innovation approach to AI Regulation, 3 August 2023.

54 UK Government, Frontier AI Safety Commitments, AI Seoul Summit 2024, 7 February 2025; UK Government, Frontier AI: capabilities and risks – discussion paper, 25 October 2023.

55 Rashid/Kausak, AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications, Hybrid Advances, Vol. 7/2024; World Economic Forum, This timeline charts the fast pace of tech transformation across centuries, 27 February 2023.

Sector-Based Regulation: AI governance is managed through sector-specific regulatory frameworks and guidance covering data privacy, financial services, healthcare, cybersecurity, and competition. The UK does not have one single AI regulator but instead relies on the expertise of its existing sectoral regulators to deal with specific queries and challenges. These regulators' mandates cover the issuance of sectoral AI guidance as necessary.

The UK has a number of authorities responsible for overseeing AI compliance within their respective domains. For example, the Information Commissioner Office oversees data privacy and AI and due to the huge datasets used for training AI and is therefore the de facto AI regulator. The Competition and Markets Authority focuses on market competition and has explicitly addressed AI through its AI strategic update.[56] The National Cyber Security Centre provides cybersecurity guidelines and best practices for secure AI system development with 'secure by design' as its key principle.[57]

In addition to current UK technology-neutral regulation, UK regulators have been encouraged to take into account existing international AI frameworks and to create AI cross-sectoral 'sand boxes'[58] to facilitate cooperation and be more user-friendly – for example, by reducing the need to seek advice from multiple regulators when AI systems span different regulatory domains.

Principles-Based Framework: In addition, the UK government's paper, A pro-innovation approach to AI regulation (March 2023),[59] sets out 'five core principles' guiding AI usage across all sectors:

1. Safety, Security, and Robustness
2. Transparency and Explainability
3. Fairness
4. Accountability and Governance
5. Contestability and Redress

56 UK Government, Competition and Markets Authority AI Strategic update, 29 April 2024.

57 National Cyber Security Centre, Guidelines for secure AI system development, undated.

58 See for example Medical device sandbox, Financial Institutions sandbox, ICO sandbox.

59 UK Government, A pro-innovation approach to AI Regulation, 3 August 2023. In addition, the UK has also set-up the **Department for Science, Innovation and Technology** (DSIT) responsible for some aspects of the UK's government AI strategy and includes (amongst others):

- the **AI Security Institute**, a research organisation within the DSIT;
- an **Office for Artificial Intelligence** (responsible for overseeing implementation of the National AI Strategy) which has been, as of February 2024, integrated within the AI Policy Directorate in DSIT;
- the **Centre for Data Ethics and Innovation,** which is now also part of DSIT and develops tools and techniques that enable responsible adoption of AI in the private and public sectors, in support of DSIT's broader mission to drive innovations that change lives and sustain economic growth;
- the **Digital Regulation Cooperation Forum** (DCRF), constituted of four UK regulators with responsibilities for digital regulation – the Competition and Markets Authority, the Financial Conduct Authority, the Information Commissioner's Office and Ofcom. DCRF's mission is to deliver a "coherent approach to digital regulation for the benefit of people and businesses online". It operates the AI and Digital Hub (i.e. helping businesses with cross-regulatory queries);
- the **AI Standards Hub**, which aims to advance trustworthy and responsible AI with a focus on the role that standards can play as governance tools and innovation mechanisms.

Sectoral regulators will apply the five core principles to existing regulation and may issue additional sectoral guidance, as and when appropriate.

While this legislative structure is designed to support innovation and allow rapid technological developments, it also contributes to a fragmented governance landscape, which may lead to inconsistencies in regulatory interpretation and application.



Considerations for children and other vulnerable groups

Although the UK's five core principles indirectly provide some protection during AI development to children and vulnerable groups, the current AI regulatory framework and guidance makes **few explicit references to children and other vulnerable groups**. Such considerations are addressed indirectly through broader legislation such as the UK General Data Protection Regulation (2016), the Age-Appropriate Design Code[60] (2022), the Online Safety Act[61] (2023), as well as broader human rights obligations and anti-discrimination laws like the Equality Act[62] (2010).

- **Data Privacy:** Protection for children and vulnerable individuals primarily occurs through data privacy obligations, mainly through the Age-Appropriate Design Code which provides guidelines for online services targeting children. The Age-Appropriate Design Code requires privacy-by-design principles, data minimisation, and consideration of children's best interests, implicitly extending to AI-driven systems aimed at children. However, it currently lacks specificity regarding AI applications and does not explicitly refer to AI-specific considerations such as mandatory bias audits, AI-generated misinformation, deepfakes, or transparency regarding AI decision-making processes.
- **Online Safety Act:** One of the main aims of the Online Safety Act is the protection of children from online harms, however, the Act does not explicitly address the unique risks posed by AI, such as algorithmic bias, AI-generated misinformation, deepfakes etc.
- **Equality Act 2010:** The Equality Act prohibits discrimination, harassment, and victimisation across nine protected characteristics, including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation. Accordingly, it does impose some constraints against discrimination by AI technologies. Nonetheless, AI-specific risks for children and vulnerable groups are not addressed.

The UK's approach does not include explicit safeguards tailored specifically to AI impacts on vulnerable groups, such as:

- Mandatory child-specific AI risk assessments.
- Specific categories for AI technologies targeting children and vulnerable groups, such as within education, healthcare, or social service applications.

60 United Kingdom Information Commissioner Office, Age appropriate design: a code of practice for online services, undated.

61 Ofcom, Time for tech firms to act: UK online safety regulation comes into force, 16 December 2024.

62 Equality Act 2010.

More generally, such groups could benefit from requirements of bias audits pre-deployment to prevent discrimination, regulations governing disclosure and transparency of AI-generated content and AI-assistants, clear requirements for human oversight or identification of 'forbidden AI' use cases. Therefore, although children and vulnerable groups benefit from some protection through existing legal frameworks and ethical principles, strengthening explicit safeguards would significantly enhance protection against AI-driven harms. Of note, the UK is one of the first countries to create new AI sexual abuse offences to protect children from perpetrators generating AI images.[63]

4.2.2 Government-led AI development with minimal regulation (India)



Philosophy

India's approach to AI regulation is rooted in its view of AI as a 'kinetic enabler'[64] for the growth of its technology ecosystem and a catalyst for national development.

The Government of India has decided that stringent regulation would stifle innovation and prevent India from reaching a global leadership position. India, therefore, follows a government-driven AI innovation model focusing on the use of AI for economic growth, development of its public services and wider digital transformation (agriculture, healthcare, education etc). Its priorities are the use of AI for national development and strategic positioning within the global AI ecosystem while encouraging regulatory flexibility through privacy-driven[65] regulation. Privacy regulation is a cornerstone of this approach, with legislation designed to protect individual rights without imposing broad, technology-specific constraints.

This philosophy has been reflected in initiatives like the National AI Strategy of 2018,[66] which laid the groundwork for transforming India's economy through emerging technologies, and the IndiaAI Mission,[67] launched in March 2024, which focuses on strategic programs[68] to strengthen the AI ecosystem and which further supports the National AI Strategy by fostering public-private collaboration and infrastructure development.

Globally, India has demonstrated its commitment to responsible AI development by signing the Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet[69] and the Paris Charter on AI in the Public Interest[70] at the AI Action Summit[71] in Paris in February 2025. These actions underscore India's intent to position itself within international norms while prioritising national development goals.

63 UK Government, Britain's leading the way protecting children from online predators, 4 February 2025.

64 The Times of India, India's AI programme to be kinetic enabler to achieve $1 trillion digital economy: Rajeev Chandrasekhar, 13 October 2023.

65 The Government of India has recently been pushing forward new data protection rules that will have a direct impact on digital and AI technologies, explained further in the "Legislative Approach" section below.

66 Government of India, National Strategy for Artificial Intelligence, 2018.

67 Government of India, IndiaAI Mission.

68 The IndiaAI Mission is structured around seven core pillars: Compute, Datasets Platform, Application Development Initiatives, Future Skills, Innovation Center, Startup Financing and Safe & Trusted AI.

69 Statement on inclusive and sustainable Artificial Intelligence for people and the planet, AI Action Summit, 2025.

70 Paris Charter on AI in the Public Interest, 2025.

71 Artificial Intelligence Action Summit, 2025.

Legislative approach

In 2023, the Government of India decided against regulating AI as a technology. Therefore, regulation is deliberately 'light touch' and sectoral (privacy, healthcare, banking, IT etc.), reflecting its philosophy of avoiding horizontal AI-specific legislation that could hamper innovation.

This decentralised approach relies on multiple government agencies instead of a single AI regulator, ensuring that oversight aligns with domain-specific expertise. The current key regulatory bodies for this AI sectoral approach include the National Institution for Transforming India, which deals with AI Policy; the Ministry of Electronics and Information Technology oversees digital governance and personal data protection; and the Telecom Regulatory Authority of India for telecommunications. However, some of the sectoral legislation[72] which underpins this strategy has not yet been fully developed nor implemented, potentially creating an AI vacuum both horizontally and vertically. This stands in contrast to the UK, where the sectoral regulation had been enacted years ago, and the authorities are well versed and experienced in their enforcement. Hence the UK authorities can immediately take the extended scope of their regulations on board in their enforcement practices.

To complement this early-stage sectoral approach, India is developing an AI-specific voluntary AI code,[73] alongside integrating AI-specific provisions into existing frameworks like the Information Technology Act 2000[74] (which deals with digital communication, cybercrime and e-commerce) and in the forthcoming Digital India Act (intended to replace the IT Act), which will regulate the country's online environment and digital data protection policies. These laws will complement the Digital Personal Data Protection Act 2023[75] which was India's first cross-sectoral law on personal data protection. While the Digital Personal Data Protection Act does not address AI directly, such legislation has significant impact on AI technologies development, considering AI technologies' needs for large volumes of personal data.

Finally, the Indian Government is also developing a horizontal 'AI for India-Specific Regulatory Framework' which will consider both the opportunities and risks presented by AI in India. A multi-stakeholder Advisory Group and a Subcommittee on 'AI Governance and Guidelines Development' were formed to create actionable recommendations for AI governance and created a report on AI Governance Guidelines Development[76] which contains the following principles—transparency, accountability, safety, privacy, fairness, human-centred values, inclusivity, and digital governance — and aims to guide ethical AI development, though their implementation remains voluntary and in progress as of March 2025.

72 For examples the Digital Personal Data Protection Rules 2025, which will in effect, implement the Digital Personal Data Protection Act 2023 are still under consultations, see Ministry of Electronics & IT, Draft Digital Personal Data Protection Rules, 2025.

73 Business Standard, IT Ministry finalising voluntary code of conduct, ethics for AI companies, 18 November 2024.

74 Government of India, Information Technology Act, 2000.

75 See Ministry of Electronics & IT, Draft Digital Personal Data Protection Rules, 2025.

76 Government of India, Report on AI Governance Guidelines Development. This report has now been published for public consultation.



Considerations for children and other vulnerable groups

There are **no AI-specific provisions tailored to children and other vulnerable groups**, despite the rapid proliferation of AI-driven technologies like Education Technology (EdTech) platforms and proctoring tools,[77] which are widely used by young adults and students in and beyond India.

However, the Digital Personal Data Protection Act 2023, and its associated Digital Personal Data Protection Rules (Rules) 2025, will provide (as and when implemented) potentially significant protections for children and, to some extent, vulnerable groups in the context of data processing, which will directly impact AI development. The Rules prioritise the protection of children (defined as individuals under 18 years of age) in the digital environment. Key provisions include verifiable parental consent, prohibition of tracking and targeting of children, purpose limitation for use of children's personal data in line with parental consent, data security etc.[78]

Although not directly applicable to AI, additional children and vulnerable groups' protections can be inferred (and applied to AI technologies) from other legislation such as India's Constitution which provides broad protections against discrimination, as well as the Protection of Children from Sexual Offences Act 2012[79] which could be applied to AI-generated content that constitutes CSAM, or the Right to Education Act 2009[80] which ensures equitable access to education and could be used for Ed-Tech to avoid exclusion or biases.

77 The Economic Times, India's edtech market set to reach $29 billion by 2030: report, 17 January 2025.

78 See Ministry of Electronics & IT, Draft Digital Personal Data Protection Rules, 2025.

79 Government of India, The protection of children from sexual offences Act, 2012.

80 Government of India, Right to Education Act, 2009.



05

KEY FINDINGS AND THE WAY FORWARD

© UNICEF/UN0398144/Karimova

Of the eight international and regional AI guidance reviewed, three make no explicit reference to children. Even if children are covered tangentially, this omission highlights a significant gap in addressing a key group of rights-holders. This is a major concern as AI's impact might be more severe for vulnerable groups, including children, by exploiting gaps in their rights protections, limited autonomy, and developmental capacity. The asymmetryinpower,information,and control between children and AI technologies – and those who design and deploy them – makes these impacts more persistent and less visible.

The asymmetry in power, information, and control between children and AI technologies – and those who design and deploy them – makes the impact more severe, persistent, and less visible.

The review also illustrates how national level regulatory approaches differ significantly. While regulating AI development is a primary goal in some countries, others believe that an innovation-centred and business-friendly approach will lead to economic growth and prosperity for all. A country choosing not to regulate AI directly does not automatically mean it does not seek to address any of AI's potential adverse impacts through sectoral regulation. However, the absence of AI-specific regulation does raise questions about how the country intends to address new risks generated by AI and protect rights that may be impacted, in particular for vulnerable groups including children.

To ensure regulatory protection for children's rights in the context of AI, countries without specific AI regulation might rely on related regulatory areas, such as data protection, consumer protection, or online safety laws. However, reliance on such frameworks should depend on a comprehensive assessment that the existing legal framework is indeed capable of preventing and mitigating AI-related impacts comprehensively. Due to the quickly evolving nature of the AI landscape, there is a risk that children's rights and needs fall through the cracks if their protection is scattered across different legal frameworks and is not closely monitored and adjusted if needed. In such cases, it could be worth considering an AI regulator nonetheless to act as a central point of contact and redress, coordinating the use of the different sectoral legislation that may be relevant.

As of the time of writing, none of the approaches reviewed appear to have undertaken a comprehensive assessment of AI technology used by or for the benefit of children and how such technology could impact children from the perspective of their emotional and intellectual developmental stages. This indicates a foundational gap in how states understand the potential impacts of AI on children, which in turn limits their ability to identify the right questions to ask and the appropriate safeguards to implement.

Given that most AI regulatory approaches have only emerged in recent years, it is too early to determine which regulatory approach will ultimately prove most effective in protecting children's rights – AI regulation is truly a field in motion. In this context of AI governance in motion, **continuous research** is essential to monitor and assess the impact of AI regulation on children across different contexts, and to generate lessons learnt and best practices that can inform future policymaking. This need is particularly important as some countries continue to adopt a 'wait-and-see' approach, observing global AI regulation before taking regulatory action. This stance, while understandable, must consider that **AI impacts on children may be harder to undo than to prevent**. In other words, there are inherent risks involved in not regulating the impacts of AI on children, particularly as the technology takes root across multiple domains, activities, and services upon which they depend.

unicef
for every child

Published by UNICEF Child Protection and Business Engagement and Child Rights Teams, Programme Group, 3 United Nations Plaza, New York, NY 10017.
Email: childprotection@unicef.org.
Website: www.unicef.org.

© United Nations Children's Fund (UNICEF) October 2025.