



RIGHTS BY DESIGN: EMBEDDING HUMAN RIGHTS PRINCIPLES IN AI SYSTEMS

2025

DOCUMENT DISCLAIMER

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

Acknowledgements

This report represents a collaborative effort that would not have been possible without the dedication and contributions of numerous individuals. We extend our heartfelt gratitude to all those who played a pivotal role in bringing this research to fruition.

We express our thanks to the research teams, analysts, and contributors who worked on designing, analyzing, and presenting the research in this report. Their commitment to excellence is evident throughout these pages.

We would also like to express our deep gratitude to the following members of the DCO technical team and external experts for their invaluable support, review, feedback, and guidance throughout this process:

Luca Belli, PhD
Professor, FGV Law School, Brazil

Ahmad Bhinder
Policy Innovation Director, DCO

Kevin Muvunyi
Policy Innovation Assistant Manager, DCO

Their expertise and unwavering support have been instrumental in shaping the direction and focus of this report.

TABLE OF CONTENTS

01	Executive Summary	4
1.1	Findings and recommendations	6
1.2	Implications of the findings	10
02	Introduction	11
2.1	Purpose and scope of the report	12
2.2	Importance of human rights in the AI sphere	13
2.3	Responsible AI vs. ethical AI – the relevance of incorporating human rights in the AI concept	17
03	Human Rights and AI: An Overview	18
3.1	Key human rights within the AI ecosystem	19
3.1.1	Right to Privacy	20
3.1.2	Right to non-discrimination	25
3.1.3	Freedom of opinion and expression	26
3.1.4	Right to Work	27
3.1.5	Right to Education	29
3.1.6	Right to Health	31
3.1.7	Right to a Healthy Environment	33
3.1.8	Right to Participate in Cultural Life	34
3.2	International frameworks and standards addressing human rights and AI	36
3.3	DCO Member States' regulatory landscape	39
3.4	Global Discourse on AI and human rights and the DCO Member States	44
04	Conclusions and Recommendations	46
4.1	Conclusions	47
4.2	Policy Recommendations	48
4.2.1	Recommendations for Governments and Policymakers	48
4.2.2	Recommendations for industry stakeholders	51
05	Annex 1 – Methodology	53
5.1	Research approach and design	54
5.2	Data collection methods	55
06	Annex 2 – Bibliography	56

01

EXECUTIVE SUMMARY

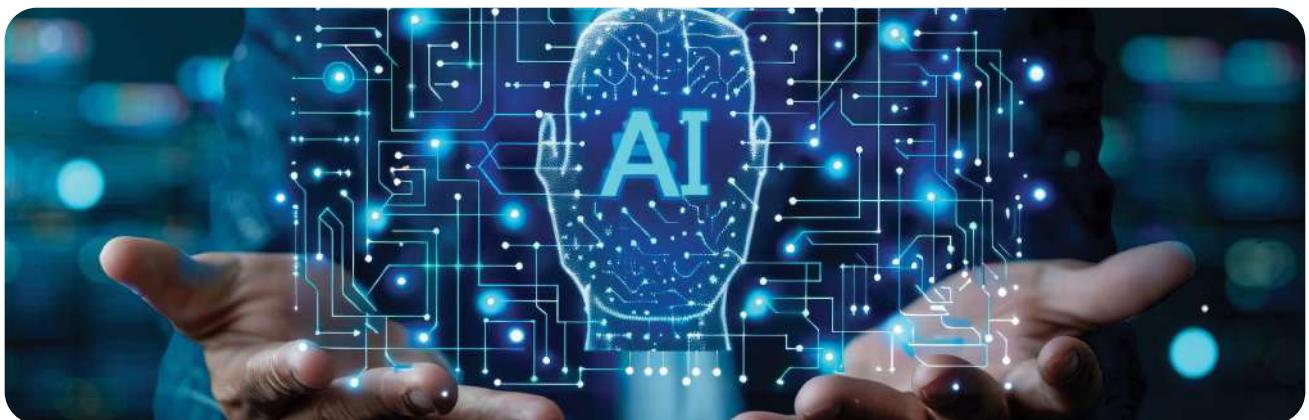
Artificial Intelligence (AI) is central to the **Digital Cooperation Organization (DCO)** agenda, given its profound impact on current and future economic growth and innovation. As one of the most revolutionary technologies of the century, AI's influence continues to expand across sectors and societies.

The DCO recognises AI's fundamental importance for its Member States and promotes its early adoption to foster economic and social progress. Proof of this commitment is the adoption of the **Riyadh AI Call for Action Declaration (RAICA)**, signed by the DCO Member States in 2022,¹ which highlights the importance of using a responsible approach towards the implementation of AI in the public and private sectors to ensure societal and environmental benefit. The RAICA stands as one of the first documents of its kind, demonstrating multiple nations' commitment to fostering AI development with human-centric values at its core.

In line with RAICA commitments, the DCO has prepared this report examining the intersection of AI and human rights globally and within its Member States. The report employs a qualitative and comparative research approach to analyse AI governance frameworks across the DCO Member States, focusing on AI's ethical implications and human rights impacts. From this analysis, AI promises economic and social benefits. However, if not responsibly governed, it has the potential to jeopardise essential human rights. The report concludes that AI's integration into society holds both significant potential and complex risks for human rights within DCO Member States that must be correctly addressed. To set the right parameters, this report compares two similar but not synonymous concepts to better understand what ethical or responsible implications mean. Ethical AI refers to AI systems and technologies filtered through the lens of moral and societal values.¹ On the other hand, responsible AI refers to the practical aspects of AI development and deployment. It focuses on the safety and regulatory compliance of AI uses.²

The report argues that the integration of human rights principles into AI governance is crucial for responsible innovation and individual freedoms in an increasingly digital world that often transcends physical borders. This approach lays a strong ethical foundation for AI development, helping prevent abuses and uphold human dignity. In emerging AI landscapes, it provides a stable basis for future regulations, ensuring alignment with fundamental rights. Moreover, by prioritising human rights, governments can guide the private sector towards the adoption of human-centred ethical AI practices. This rights-centric framework offers the flexibility to adapt to rapidly evolving AI technologies while maintaining robust protections for individual liberties. The principles and guidelines listed in this report reflect a 'soft law' or 'collaborative' approach to regulation and are part of a mix of regulatory approaches that governments should consider.

The findings underscore the urgency for comprehensive, rights-based AI governance frameworks that address diverse contexts and levels of technological advancement within the DCO Member States. Even for countries where AI adoption is limited, proactive policies are crucial, as these technologies are becoming increasingly accessible. The findings and recommendations presented here aim to provide a roadmap for DCO Member States to navigate the complex landscape of AI governance while upholding fundamental human rights principles.



1.1 FINDINGS AND RECOMMENDATIONS

The rapid advancement of AI technology presents both opportunities and significant challenges for human rights protection globally. As AI systems become increasingly embedded in crucial aspects of daily life – from healthcare delivery to criminal justice, from education to employment – their impact on fundamental human rights has become a critical concern for policymakers, technologists, and civil society alike.

The intersection of AI and human rights encompasses various critical issues, including privacy rights in an era of massive data collection, the potential for algorithmic discrimination and bias, the preservation of freedom of expression in automated content moderation systems, and the right to work in an increasingly automated economy. International organisations and national governments worldwide face the challenge of developing governance frameworks that can harness AI's benefits while protecting essential human rights and dignity.

In the context of the DCO Member States, this challenge takes on particular significance due to the diverse levels of technological advancement, regulatory readiness, and digital infrastructure development across nations. The variation in AI readiness among DCO Members States presents both challenges and opportunities for developing comprehensive, culturally sensitive approaches to AI governance that respect human rights while promoting innovation and economic growth.

Key findings

Based on the research conducted throughout this report, these are the most relevant findings:

1. Diverse AI readiness among DCO Member States:



The analysis reveals a wide spectrum of AI readiness among DCO Member States, influenced by factors such as technological advancement, regulatory framework development, and data protection mechanisms. This diversity underscores the need for tailored, yet harmonised approaches to AI governance that consider the unique status of each Member State.

2. Privacy as a key concern:

The research highlights privacy as a primary concern in the context of AI governance. Privacy encompasses multiple dimensions, including physical privacy (affected by surveillance and biometric tracking), decisional privacy (the autonomy to make personal choices without algorithmic interference), mental/psychological privacy (protection of emotional and cognitive states), associational privacy (the right to maintain confidential relationships and associations), behavioural privacy (patterns of daily activities and habits), data privacy, and spatial privacy (movement and presence in various spaces). Data privacy emerges as a particularly critical dimension, serving as an interconnective element that fundamentally influences and intersects with all other privacy domains. By providing the foundational layer through which personal information is collected and processed, data privacy becomes the critical nexus that can either protect or compromise the integrity of physical, decisional, psychological, associational, behavioural, and spatial privacy. The technology's ability to combine seemingly unrelated pieces of information to create detailed outcomes, coupled with its often-opaque decision-making processes, necessitates a comprehensive approach to privacy protection and considers the full spectrum of human privacy rights.



3. Addressing algorithmic bias and discrimination:



This report emphasises the importance of addressing algorithmic bias to prevent discrimination. The absence of concrete legal measures to combat bias in AI systems is an area in which there is significant opportunity for improvement, as it can perpetuate and even exacerbate existing social inequalities. The report calls for more robust legal protection and greater transparency in AI development to ensure fairness and non-discrimination.

4. Navigating AI's impact on freedom of expression:



This report recognises the complex interplay between AI and freedom of expression, particularly in the context of content moderation and censorship. It considers the importance of cultural differences when finding a balance between free speech and addressing harmful content online, which presents a significant challenge globally and for the DCO Member States. The report highlights the need for transparent and accountable AI systems that respect freedom of expression while mitigating the spread of misinformation, harmful and culturally insensitive content, and hate speech.

5. AI's impact on the right to work and education:



The report acknowledges the potential for AI to both create and displace jobs, emphasising the importance of education and skills development to prepare workforces for the changing nature of work. It underscores the need for equitable access to AI-powered education to bridge the digital divide and ensure that the benefits of AI are shared broadly.

6. Limited government focus on AI in healthcare and the environment:



While the private sector and academia demonstrate significant interest in using AI to improve healthcare outcomes and promote environmental sustainability, this report notes a lack of direct government involvement in these areas. The report suggests that increased government support for AI initiatives supporting these policy initiatives could yield substantial benefits for the DCO Member States.

Recommendations

Based on these findings, the report advocates for integrated governance structures that balance innovation with the protection of human rights. The primary recommendation focuses on the need to establish robust national regulatory frameworks that embed human rights principles across all AI applications. These frameworks should ensure transparency, accountability, and consistent enforcement, along with anticipatory protections, such as mandatory human rights impact assessments, oversight bodies, and inclusive policies that incorporate the voices of vulnerable and impacted communities.

The report also highlights the need for international cooperation to provide coherent AI governance standards while respecting local cultural and social contexts. This includes aligning human rights protections across borders through shared impact assessment methodologies, remediation mechanisms, and monitoring systems to track the effects of AI on human rights. Furthermore, industry stakeholders are encouraged to implement human rights review processes within product development and adopt sector-specific standards to address unique human rights challenges.

The success of these initiatives depends on continuous education and capacity-building efforts that engage all sectors of society from the public sector to academia, civil society and the private sector. Educational programmes for government officials, technical training for AI developers, and public awareness campaigns will help ensure that AI systems are developed and deployed with a commitment to human dignity and fundamental rights. Citizens have a fundamental role to play as the main users of AI in their different roles. These efforts described in the report must address citizens, ensuring they are aware of the risks associated with AI and how they can and should make informed decisions when using related applications. Training and education around AI must cover all different stages of a person's life.

The report proposes a multi-tiered approach to human rights-based AI governance, tailored to the different levels of AI readiness among DCO Member States. Key recommendations include:

For countries in the early stages of AI adoption:

1. • Implement comprehensive data protection frameworks to safeguard personal information.
- Engage diverse stakeholders to develop principles-based ethical AI-specific policies and guidelines that embed human rights.

For countries developing initial AI regulatory frameworks:

2. • Focus on market enablement, raising AI awareness, fostering trust in AI, and supporting AI-driven transformation.
- Review current AI policies with a view to explicitly embedding human rights principles, should they be missing.
- Establish mechanisms to address potential human rights violations caused by AI systems. These mechanisms should focus on preventing violations – by deploying tailored communications campaigns to different groups of citizens and stakeholders – and on the reporting (for example, with easy-to-access online and free hotlines to report violations) and enforcement side. To achieve this, countries could establish national or regional AI safety institutes focused on monitoring and mitigating the social and ethical impacts of AI.
- Develop a collaborative process to make sure diverse stakeholders engage and participate in the development of AI regulatory or policy frameworks.

3

For countries with more advanced AI frameworks:

- Promote collaboration between AI policymakers and human rights experts to guarantee that AI regulations have considered and incorporated human rights principles.
- Launch sector-specific initiatives or guidelines to harness AI's benefits in key industries.
- Provide concrete examples and policy steps in the form of guidelines on responsible development and use of AI.
- Establish oversight mechanisms to monitor, report, and mitigate emerging risks, such as developing a quantitative measure to track and assess the implementation status and impact of AI policies and strategies.
- Create accessible grievance procedures to address AI-related human rights violations.

4

For industry stakeholders:

- Actively engage in public-private partnerships to drive human-centric AI innovation and adoption.
- Invest in AI education and training programmes to build a skilled workforce that is aware of human rights risks and importance.
- Foster knowledge sharing and collaboration within the industry.
- Build internal policies that embed ethical AI principles.
- Develop and use relevant tools to identify and address the main risks posed by AI.

By embracing a balanced and comprehensive approach to AI governance, the DCO Member States can unlock AI's transformative potential while safeguarding fundamental human rights. The report's recommendations provide a roadmap for navigating the complex intersection of AI and human rights, paving the way for a future where AI technologies benefit all members of society.

1.2 IMPLICATIONS OF THE FINDINGS

The report's findings have significant implications for the future of AI development and human rights protection across the DCO Member States, as approaches to AI governance vary greatly across nations.

The report emphasises that as AI becomes more integrated into various aspects of society, ensuring its alignment with human rights principles is crucial for fostering trust, promoting innovation, and realising the full potential of AI technologies for the benefit of all. Key implications are as follows:

Need for balanced and context-specific AI governance:



The diversity among DCO Member States, ranging from those in the early stages of AI adoption to those with more advanced AI frameworks, necessitates flexible and culturally sensitive approaches to AI governance. There is no one-size-fits-all solution, and strategies should be tailored to the specific needs and challenges of each nation while adhering to internationally accepted human rights standards.³

Collaboration as a cornerstone of responsible AI:



The report stresses the importance of fostering collaboration between AI policymakers, human rights experts, industry leaders, and civil society. This multi-stakeholder approach is essential for developing AI systems that are not only innovative but also ethical, inclusive, and beneficial to society as a whole. By working together, stakeholders can ensure that human rights considerations are integrated into every stage of AI development, from design to deployment.

Opportunity for human rights-based responsible AI governance frameworks:



By adapting international AI principles to regional and domestic contexts, the DCO can develop a unique approach to AI governance that reflects the diverse cultural perspectives of its Member States.⁴

The report's findings highlight the urgent need to adopt balanced and comprehensive AI governance frameworks in the DCO Member States. The implications extend beyond technological advancement, emphasising the need to create AI systems that are deeply rooted in human rights principles and cultural values. By following the report's recommendations, DCO Member States can benefit from the transformative power of AI while safeguarding the fundamental rights and freedoms of their citizens, potentially setting a new global benchmark for responsible AI development.

02

INTRODUCTION

2.1 PURPOSE AND SCOPE OF THE REPORT

Since the adoption of the Riyadh AI Call for Action Declaration⁵ (RAICA), the DCO has been actively working to support its Member States with their efforts and plans to adopt and govern AI in a responsible and human rights-centric way.

As part of these efforts, the DCO presents this report, which conducts a comprehensive analysis of the intersection between AI technologies and human rights to identify potential risks, challenges, and opportunities arising from the development and deployment of AI systems, with a specific focus on their impact on fundamental human rights.

The scope of this report includes examining issues such as algorithmic bias, discrimination, privacy infringements, impacts on freedom of expression, and threats to other globally accepted human rights – all identified as priorities by the DCO Member States. The report has also considered the different stages of AI within its lifecycle, from development to deployment. This approach allows the identification of specific stages where human rights risks are most likely to emerge, aiming to identify best practices and potential gaps in current governance approaches.

Another area of focus is the evaluation of existing AI governance strategies, frameworks, policies, and regulations within the DCO Member States through a human rights lens. This assessment highlights both challenges and opportunities in the design and adoption of responsible AI specific to these regions.

Overall, the findings presented in this report aim to inform policymakers, industry leaders, AI developers and deployers, and civil society organisations, enabling them to make informed decisions that balance technological advancement with the protection of fundamental human rights.



2.2 IMPORTANCE OF HUMAN RIGHTS IN THE AI SPHERE

Human rights are fundamental rights and freedoms that belong to every person simply because they are human. These rights are universal, meaning they apply to everyone, regardless of race, gender, nationality, ethnicity, language, religion, or any other status.⁶



Figure 1. List of the 30 Human Rights

Since the adoption of the Universal Declaration of Human Rights (UDHR) by the UN General Assembly in 1948,⁷ work around human rights has expanded and reached almost every country across the world. Following the signature of the UDHR, many other milestones have taken place, such as the adoption of the European Convention on Human Rights (ECHR)⁸ in 1950, the International Covenant on Civil and Political Rights (ICCPR),⁹ and the International Covenant on Economic, Social and Cultural Rights (ICESCR),¹⁰ both adopted in 1966, further elaborating on the rights outlined in the UDHR. The Cairo Declaration of Human Rights in Islam,¹¹ adopted by Member States to the Organisation of Islamic Cooperation (OIC) in 1990 and later revised in 2020, was fundamental in the Islamic world as it provided an alternative framework based on Shari'a law.

The intersection of human rights and AI has become increasingly prominent as the technology has gained momentum, particularly in recent years with the advent of publicly available generative AI programmes such as ChatGPT, Claude, and Microsoft Copilot, among others. Launched in 2022 and 2023, these products have been revolutionising many people's daily lives. While numerous opportunities and use cases have emerged, so have the risks if the technology does not develop in a human-centric manner. AI systems can pose significant threats to human rights if not properly designed and regulated, including potential violations of privacy through mass surveillance, perpetuation or amplification of biases leading to discrimination, manipulation of public opinion affecting democratic processes, and automation-driven job displacement impacting economic rights. Significant human rights threats also

lie in the everyday uses of social media, which are heavily powered by AI systems. Exacerbating biases, propaganda and misinformation, and anonymous, unfiltered hate speech are only some of the risks governing social media with the aid of AI systems, which are not trained to battle these behaviours.

Balancing free speech and protective regulations in the context of AI and digital platforms presents significant challenges for policymakers and tech companies alike. On one hand, the open nature of these platforms has democratised information sharing and given voice to diverse perspectives, fostering innovation and public discourse. However, this same openness has also enabled the rapid spread of misinformation, hate speech, and harmful content, potentially undermining social cohesion and individual rights.

The integration of AI into content moderation further complicates this balance.¹² While AI can efficiently process vast amounts of data and identify potentially harmful content, it often lacks the nuanced understanding required to distinguish between legitimate free speech and genuinely harmful material. Overzealous content removal risks stifling legitimate expression, while insufficient moderation may fail to protect vulnerable users. Moreover, the global nature of digital platforms means that navigating varying cultural norms and legal frameworks across different jurisdictions adds another layer of complexity to this delicate balancing act.

As AI continues to evolve, finding the right equilibrium between protecting free speech and implementing necessary safeguards remains a critical challenge for the digital age.

The power and reach of AI technologies make it imperative that their development is guided by human rights principles to prevent such negative outcomes. Recognising this fundamental shift in technological capabilities, many international organisations and countries have acknowledged the need to harness AI's potential, ensure inclusivity, and actively manage and mitigate risks. Nevertheless, it's important to mention that AI has many significant potential benefits for society. The UN High Commissioner for Human Rights, Volker Türk, has recognised the added value and advantages that AI can bring to human rights, such as improving strategic foresight and forecasting, democratising access to knowledge, and accelerating scientific progress that can help address challenges like the climate crisis.¹³ When developed responsibly, AI can enhance access to information and education, improve healthcare outcomes, aid in environmental protection efforts, and strengthen the rule of law through more efficient and fair judicial systems. AI tools can also be leveraged to monitor human rights violations, predict and prevent conflicts, and assist humanitarian efforts.

The dual nature of AI's impact on human rights underscores the importance of integrating human rights considerations into every stage of AI development and deployment. This integration ensures that AI technologies are innovative but also ethical, inclusive, and beneficial to society.

International organisations around the world have begun to take action to ensure that a balance is achieved between AI innovation and human rights protection.

For example, as early as 2019, the OECD adopted its Principles on AI. These principles are based on key values, including the importance of AI systems being designed in a way that respects the rule of law, human rights, democratic values, and diversity, and that they should include appropriate safeguards to ensure a fair and just society.¹⁴ These principles were updated in 2024 to better include AI-associated challenges involving privacy, intellectual property rights, safety, and information integrity.¹⁵

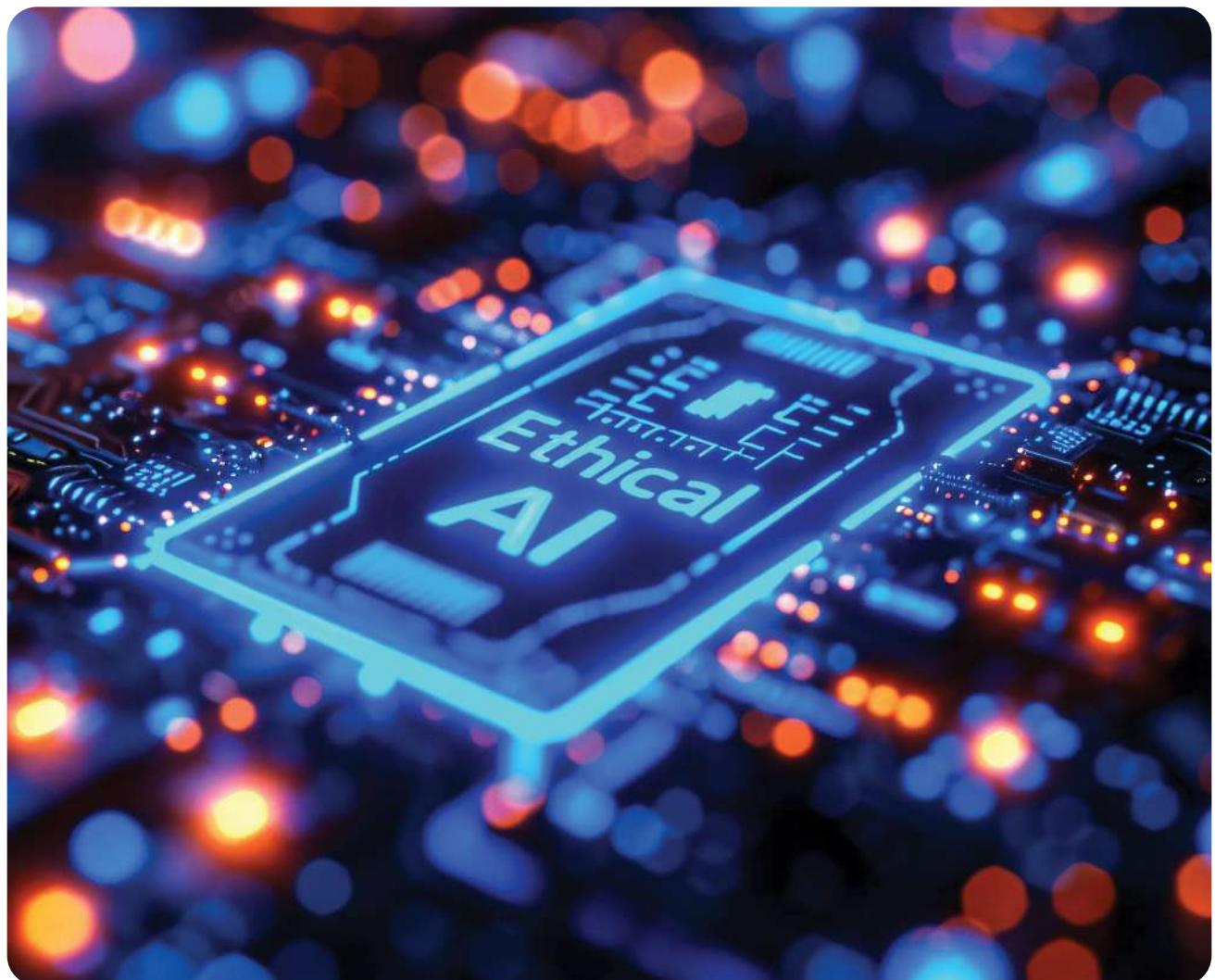
The UN¹⁶ has adopted a similar approach by stating that AI must be grounded in human rights, highlighting the importance of understanding why and which limits should be implemented around AI.¹⁷ This was further reinforced in the recent report Governing AI for Humanity, launched in September 2024 by the multi-stakeholder High-level Advisory Body on Artificial Intelligence.¹⁸ This report recommends

specific action within the UN and calls on UN Members States for action. The drafters' intention was for it to be based on a comprehensive vision for an equitable and effective global AI governance regime, with careful thought on the implementation steps. The recommendations include, among others, (i) the launch of a twice-yearly intergovernmental and multi-stakeholder policy dialogue on AI governance, (ii) an AI standards exchange among representatives from the public and private sectors, and (iii) creating an AI capacity development network to connect capacity development centres making available expertise, compute, and AI training data to key actors. The Advisory Body on Artificial Intelligence was initially proposed in 2020 as part of the United Nations Secretary-General's Roadmap for Digital Cooperation and was formed in October 2023 to undertake analysis and advance recommendations for the international governance of AI.

The World Economic Forum, meanwhile, has created an AI Governance Alliance to support the responsible and ethical development of AI systems and regulations, with a focus on human rights to access information and reduce the digital divide.¹⁹

The Global Privacy Assembly (GPA) is a global forum that brings together privacy regulators and experts to discuss emerging privacy issues, including the use of AI. In 2018, the GPA adopted a Declaration on Ethics and Data Protection in AI, emphasising fairness, transparency, and accountability in AI deployment.²⁰ Since then, it has adopted various resolutions focused on AI governance, including a 2020 resolution on AI accountability that calls for clear accountability measures for AI systems.²¹

The GPA's recent 2023 Resolution on Generative AI²² highlights the growing concerns around the deployment of these systems without adequate pre-deployment assessments. This resolution underscores the need for stronger governance to mitigate risks to privacy and fundamental rights.



The G7 has been at the forefront of discussions on the ethical and responsible development of AI. In 2018, the Canadian and French presidencies of the G7 launched the Global Partnership on AI (GPAI),²³ which fosters international collaboration on AI-related priorities, including research, development, and policy. GPAI focuses on ensuring that AI technologies are developed in alignment with human rights.

More recently, the 2023 G7 summit in Hiroshima marked a significant development in AI policy. The G7 leaders endorsed the Hiroshima AI Process,²⁴ which includes guiding principles applicable to AI actors across the entire AI lifecycle. This framework emphasises generative AI governance and human-centric AI development, reflecting the G7's commitment to managing AI risks while promoting innovation.

The G20, representing the world's major economies, has also played a significant role in shaping global AI policy. The G20 AI Principles,²⁵ endorsed in 2019, draw heavily from the OECD AI Principles²⁶ to emphasise human-centric AI. These principles encourage countries to foster innovation while ensuring ethical standards are met. The G20 has particularly focused on promoting international cooperation and fostering an open, fair, and non-discriminatory digital economy.

At the 2023 G20 summit in New Delhi, leaders reaffirmed their commitment to these principles, calling for AI governance that prioritises transparency, accountability, and human rights protection. The G20 also recognised the importance of leveraging AI to solve global challenges in a responsible and inclusive manner.

More recently, in September 2024, the Council of Europe (CoE), an international organisation with the goal of upholding human rights, democracy, and the rule of law in Europe, published its Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.²⁷ This comprehensive document also recognises the complex relationship between AI and fundamental human rights by highlighting both the potential benefits and risks and listing a series of common principles and rules to govern AI activities. Aligned with other international standards, these principles focus on transparency, accountability, and oversight mechanisms for AI systems and call for measures to prevent discrimination and promote equality. The document requires the establishment of remedies and procedural safeguards for those affected by AI systems and promotes risk assessment and mitigation throughout the AI lifecycle. To ensure ongoing implementation and adaptation, the convention establishes a Conference of the Parties and encourages public consultation and digital literacy initiatives. It also provides mechanisms for international cooperation and information sharing on AI developments. The value of this Framework²⁸ lies in its comprehensive approach to addressing AI's impact on human rights within an internationally agreed-upon framework.

In Asia, both the Asian Development Bank (ADB)²⁹ and the Association of Southeast Asian Nations (ASEAN) have released their own ethical AI frameworks and guidelines for AI governance and ethics, emphasising transparency, fairness, security, and human-centrality.³⁰ Among the DCO Member States, some have adopted national initiatives, which will be discussed further in Section 3.2 of this report.

The African Union's (AU) Continental Artificial Intelligence Strategy,³¹ launched in July 2024, aims to provide a harmonised framework for AI development across the continent. It promotes an inclusive, ethical, and people-centred approach to AI that aligns with Africa's broader developmental aspirations under Agenda 2063.³² The strategy focuses on leveraging AI to accelerate socioeconomic development, addressing key areas such as healthcare, education, agriculture, and governance. The strategy supports African nations in developing their own AI frameworks, ensuring they integrate key ethical principles such as transparency, accountability, fairness, privacy, and minimisation of bias while promoting homegrown solutions to address pressing societal challenges.

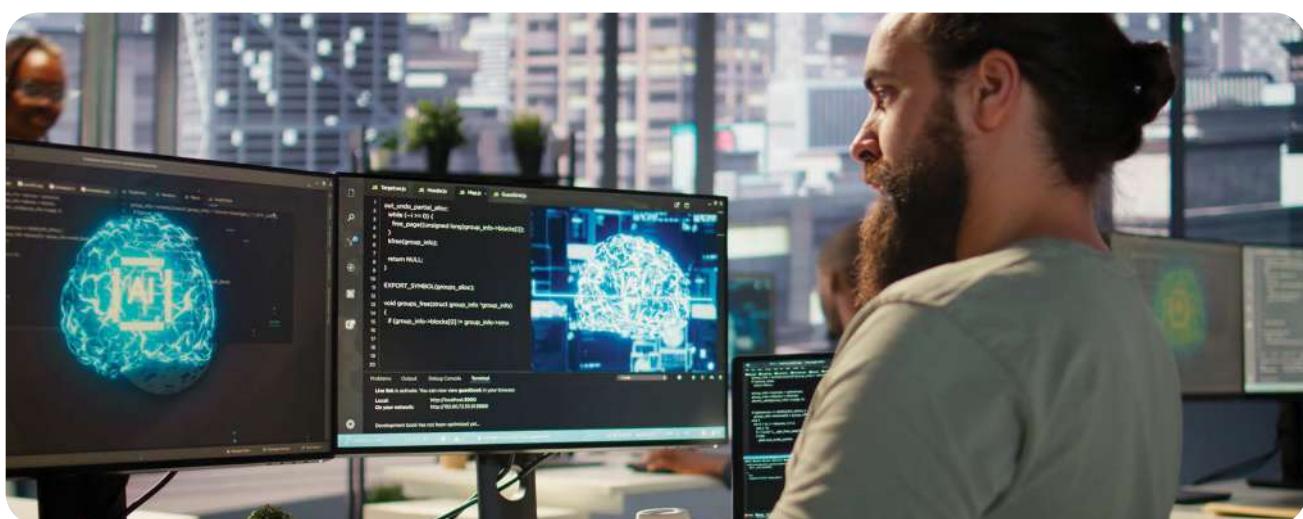
2.3 RESPONSIBLE AI VS. ETHICAL AI – THE RELEVANCE OF INCORPORATING HUMAN RIGHTS IN THE AI CONCEPT

Although there is no universally recognised definition of ethical AI or responsible AI, many organisations have worked to identify the main characteristics of what these concepts represent.

The current literature suggests ethical AI and responsible AI have distinct focuses, although, in practice, these terms are often used synonymously. **In simple terms, ethical AI focuses on moral imperatives, while responsible AI concentrates on practical implementation.** Ethical AI aligns AI systems with moral and societal values, emphasising fairness, transparency, accountability, and human rights.³³ Conversely, responsible AI addresses the practical aspects of AI development and deployment. It ensures AI systems are safe, reliable, and compliant with legal and ethical standards.³⁴ Responsible AI emphasises transparency in processes, accountability for outcomes, minimising biases, ensuring privacy, and building stakeholder trust.³⁵

Among the DCO Member States, several have included definitions of ethical and responsible AI in their current AI policy frameworks, generally staying close to the definitions discussed above. For example, Jordan states that ethical AI refers to AI systems designed and deployed in a manner that aligns with ethical principles, ensuring fairness, transparency, and accountability.³⁶ Oman follows a similar approach, highlighting that ethical AI focuses on fairness, transparency, accountability, and respect for human values. Oman aims to create AI systems that make decisions respecting everyone's rights and follow moral guidelines. The country also mentions responsible AI, aspiring to create safe, reliable, and morally sound AI systems. It aims to consider the broader societal impact of AI and align these technologies with stakeholder values, legal standards, and ethical principles.³⁷ The Kingdom of Saudi Arabia defines AI ethics as a set of values, principles, and techniques to guide moral conduct in developing and using AI technologies.³⁸

Outside the DCO, we can also find examples of countries defining ethical AI and its implementation. For example, the UK launched its Ethics, Transparency and Accountability Framework for Automated Decision-Making.³⁹ This framework was developed based on the Data Ethics Framework⁴⁰ and other relevant documents that set the basis for the responsible use of data. AI ethics is defined as a set of values, principles, and techniques that employ widely accepted standards to guide moral conduct in the development and use of AI systems.⁴¹ The goal is to mitigate the potential harms caused by AI, such as misuse and negative impact. Singapore has taken a more practical approach by establishing a framework that consists of 11 AI ethics principles aligned with international frameworks. These principles set the basis for the AI Verify tool,⁴² which is a testing framework and software toolkit that helps organisations validate the performance of their AI systems against these ethical principles through standardised tests.



03

HUMAN RIGHTS AND AI: AN OVERVIEW

3.1 KEY HUMAN RIGHTS WITHIN THE AI ECOSYSTEM

As universal and inalienable principles, human rights cover a wide range of freedoms and entitlements that are fundamental to human dignity and wellbeing. These rights range from civil, political, economic, and social aspects to cultural topics of human life. While all human rights are interconnected and equally important, the rapid advancement of AI technology requires a focused examination of specific rights that are particularly vulnerable to or impacted by AI systems.

On a global scale, the growing use of AI in domains like healthcare, criminal justice, education, and employment has raised concerns about its effects on the right to equality, non-discrimination, privacy, freedom of expression, and due process, among others. AI-powered decision-making systems have the potential to perpetuate and amplify biases, undermine transparency and accountability, and infringe on individual autonomy if not designed and deployed with rigorous human rights safeguards. Understanding these concepts is fundamental to harnessing the positive potential that AI can have while mitigating its risks and ensuring it serves to enhance human dignity and fundamental freedoms.

According to the interviews of AI stakeholders (citizens, non-government/civil society organisations, private-sector players, and government officials) conducted during the AI & Human Rights roundtables held in Riyadh (11 September 2024) and Singapore (30 October 2024), the most relevant human rights regarding AI are the right to privacy, non-discrimination, and freedom of opinion and expression. These are followed by the right to work, the right to education, the right to health, the right to a healthy environment and the right to leisure, among others.

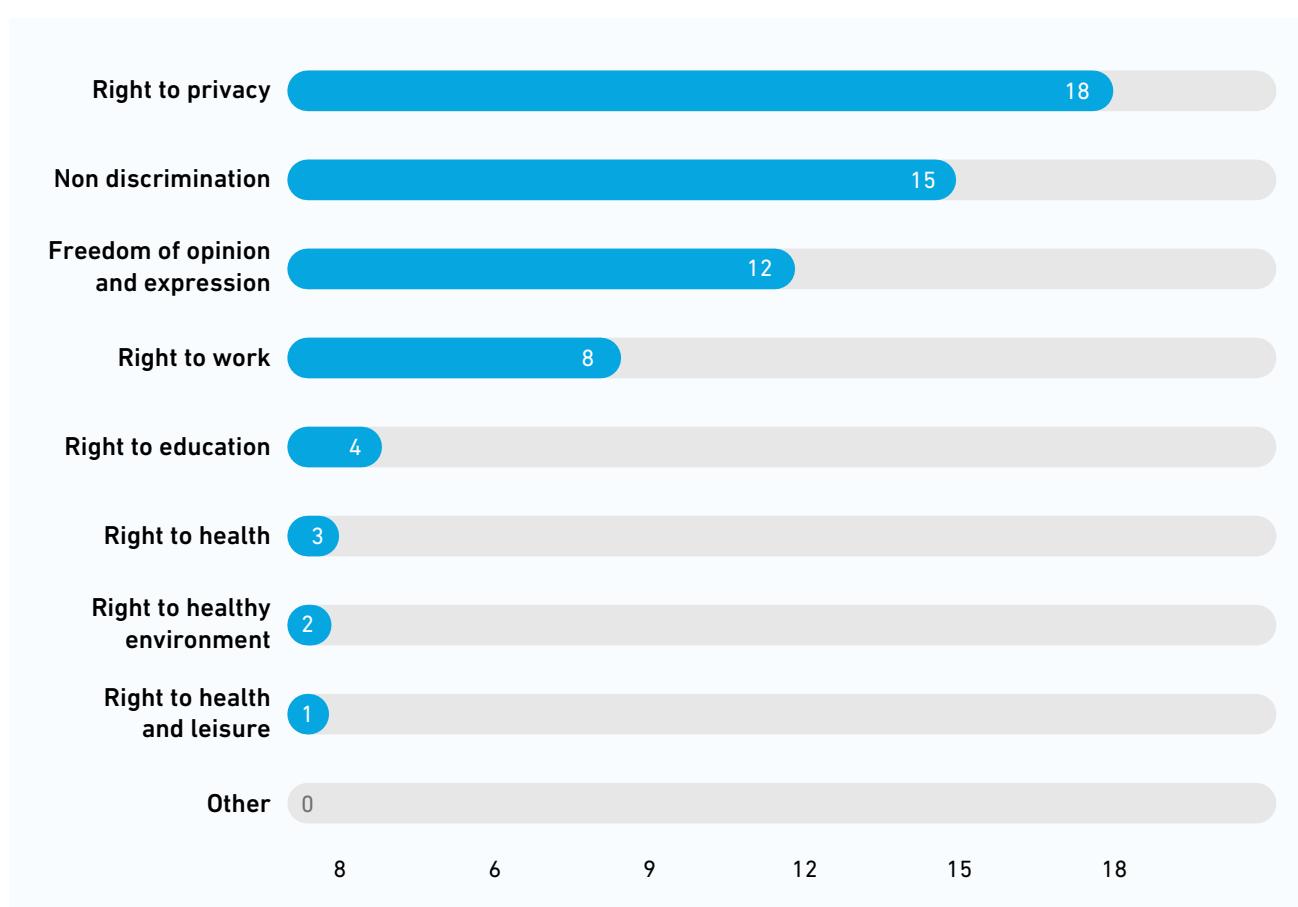


Figure 3. Interview results from the roundtable held in Riyadh showing the key human rights affecting the development of AI.

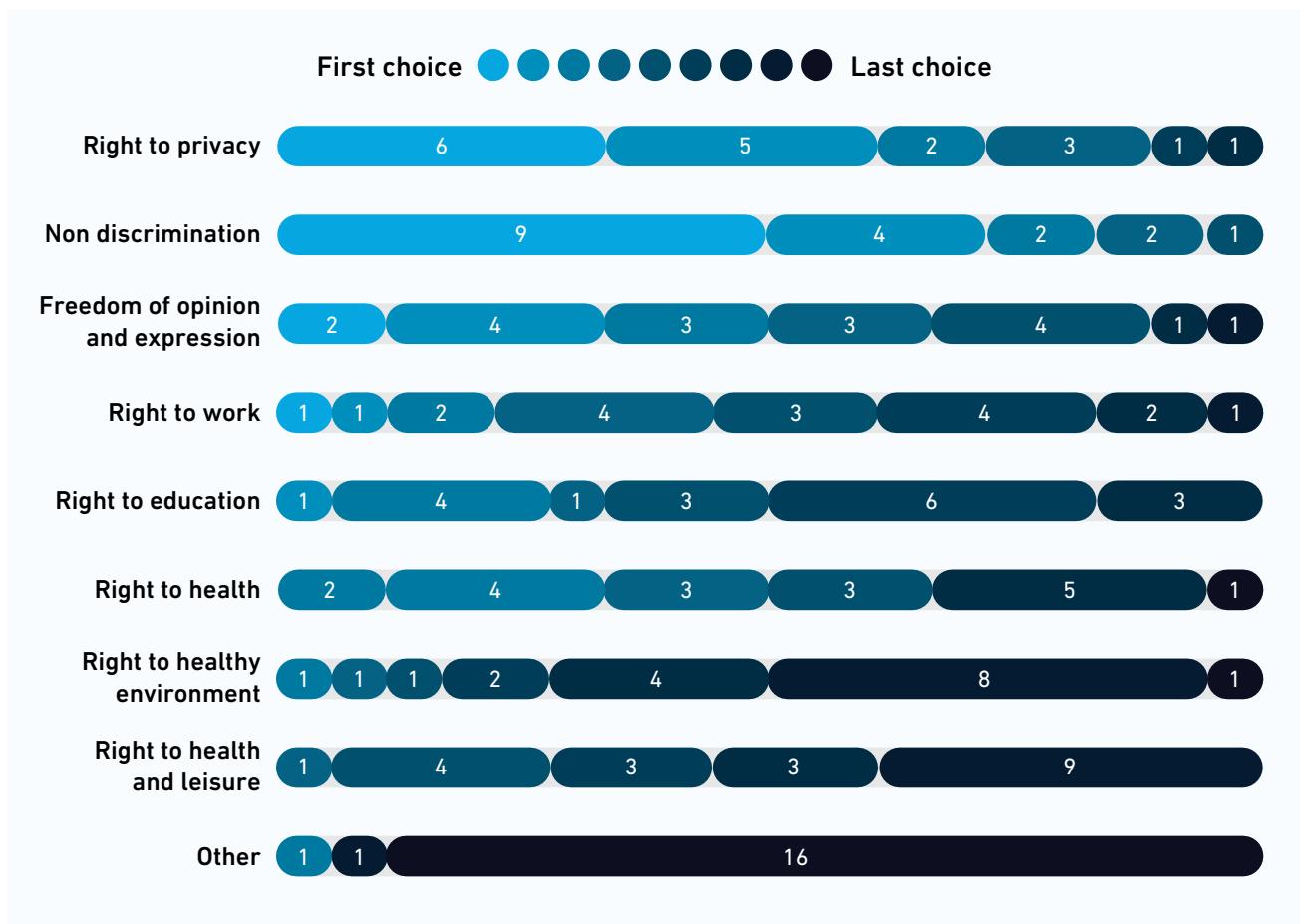


Figure 4. Interview results from the roundtable held in Singapore showing the key human rights affecting the development of AI.

Source: In-person interviews conducted by Access Partnership on 11 September 2024 and 30 October, covering 21 respondents and 18 respondents, respectively, who attended the DCO AI & HRs Roundtable organised on the margins of the GAIN Summit in Riyadh and the margins of the Switch event in Singapore. Respondents include policymakers, regulators, industry players, and non-government/civil society organisations.

3.1.1 Right to Privacy

The right to privacy is a fundamental human right that encompasses various aspects of personal life, including privacy of communications, physical privacy, psychological privacy, surveillance, associational privacy, and informational privacy. An important aspect of this concept is “data protection”, which is the legal and practical measures designed to implement and enforce privacy rights in the context of data processing. AI technologies, especially those involving data collection and surveillance, can infringe on individuals’ privacy.

Concerns around privacy began to rise with the advent of digital technology and the increasing use of computers and the internet. Corporate data breaches have hit the front pages of newspapers globally, making this topic a priority for many regulators around the world.⁴³ Large scandals involving the leak of confidential information and the misuse of personal data to influence political campaigns or to scam users and commit theft show how important data protection and the right to privacy are in the modern world. Although data protection comes as one of the first concerns when talking about privacy risks, AI has introduced complex challenges to various dimensions of privacy beyond data.

In terms of **physical privacy**, AI-powered **surveillance systems**,⁴⁴ often combined with facial recognition technology, have a significant impact on the privacy of one’s physical movements and presence.⁴⁵ Such systems can track individuals’ whereabouts in public and private spaces, often without explicit consent. With sensors and biometric data collection in devices like wearables and smart home devices, there is an increased potential for monitoring and profiling based on

daily habits and routines.⁴⁶ This invasion extends to AI-driven drones and autonomous vehicles capable of capturing footage in real-time, while location tracking in various apps creates detailed records of personal and locational history. This is also known as **spatial privacy** under threat in the context of smart city technologies, which deploy AI to monitor public areas, as well as private environments, through automated home and workplace systems. These technologies observe and interpret patterns in movement and interaction within both public and private spaces, leading to highly detailed location-based profiles, which, when combined with data from other sources, enable a near-complete view of a person's spatial and situational presence.⁴⁷

Another concept to explore within privacy is **decisional privacy**, the right to make autonomous personal decisions. It is threatened by AI systems that influence or make decisions impacting one's life choices. AI-driven algorithms increasingly affect access to essential opportunities, like loans, job offers, and educational resources, often relying on data-driven predictions. The extensive personalisation capabilities of AI, although intended to improve user experience, can inadvertently restrict exposure to diverse perspectives, creating "filter bubbles" that limit users' understanding of alternative viewpoints. This extends to health-related AI applications that make or recommend important health decisions, as well as the influence AI-based advertising has on consumer choices, subtly guiding purchasing behaviours and personal preferences.

On the dimension of **mental and psychological privacy**, AI tools analyse emotional states and mental health indicators through observed behaviour and digital interactions, which can intrude into deeply personal aspects of individual well-being. For example, sentiment analysis across emails and social media offers insight into emotional conditions and trends, sometimes revealing more than users intend to share. Emerging technologies, such as brain-computer interfaces, present an even more direct challenge to psychological privacy as they capture and potentially interpret neural data, leading to advanced psychological profiling based on one's online behaviour. In turn, AI-powered personalisation can interfere with cognitive autonomy by presenting content tailored to influence thoughts and behaviours in subtle, often unnoticeable ways.

Associational privacy is affected as AI systems analyse social networks to uncover relationships, affiliations, and communication patterns. By mapping personal and professional connections, AI systems can reveal sensitive information about group memberships and associations, potentially impacting the freedoms of association, particularly when **surveillance** is used to track group activities or other collective environments.

Finally, we have **data privacy**, a concept that stands out as a crucial and overarching aspect, functioning as a connective thread with all other privacy domains. It forms the essential foundation of the personal information cycle. As such, data privacy becomes the pivotal point that can either safeguard or jeopardise the integrity of physical, decisional, psychological, associational, behavioural, and spatial privacy realms. This central role of data privacy underscores its significance in the broader landscape of privacy concerns, acting as both a potential shield and a vulnerability point for other privacy dimensions, which is present and addressed in several data protection regimens that are necessary foundations for the development of other policies related to the responsible use of AI. As all human activities increasingly leave traces of personal data in each digital interaction, the protection of privacy and possible use of this data, among other elements, has been a public policy concern for over a decade, with many nations adopting modern regulatory frameworks to answer to the challenges of personal data being collected and used every second over the internet; for instance, the EU's General Data Protection Regime (GDPR) is often the most quoted example of such regimen.

Adopting personal data protection regimens is recommended as a necessary foundation for the development of other policies related to the responsible use of AI. Concerns around personal data protection increase within the context of AI. Consequently, the existence of a robust regimen at the domestic level can be used as a proxy for the awareness and level of advancement of each nation's

regulatory framework for AI-related concerns. Within the DCO Member States, 12 out of 16 have adopted a data protection law and, as such, could be deemed to have a certain level of foundational readiness in their framework regarding AI use. This is because the protection of personal data entails several human rights and, typically, countries with a data protection regime that was developed to acknowledge the challenges of the digitalisation of human activities are likely already considering issues that are reflected in AI principles. For the rest of the DCO Member States, it must be noted that Bangladesh is currently working on a draft Personal Data Protection Act, while Pakistan's Prevention of Electronic Crimes Act 2016 (PECA) serves as the current primary legislation on data protection.

Furthermore, the existence of the Data Protection Authority is a healthy indicator for countries that are addressing these fundamental rights. Among DCO Member States, 12 have data protection laws implemented and nine have specific authorities working on data protection issues, ensuring that this right is respected, as summarised below.

Country	Data Protection Law	Data Protection Authority
 Bahrain	Personal Data Protection Law (PDPL) ⁴⁸	Personal Data Protection Authority ⁴⁹
 Cyprus	Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR) ⁵⁰	Office of the Commissioner for Personal Data Protection ⁵¹
 Ghana	The Data Protection Act 2012 ⁵²	Data Protection Commission ⁵³
 Greece	Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR) ⁵⁴	Hellenic Data Protection Authority (HDPA) ⁵⁵
 Jordan	Data Protection Law ⁵⁶	
 Kuwait	Decision No. 42 of 2021 on Data Privacy Protection Regulation ("Data Protection Regulation") ⁵⁷	
 Morocco	Law No. 09-08 on the Protection of Individuals regarding the Processing of Personal Data ⁵⁸	The National Commission for the Control of Personal Data Protection (CNDP) ⁵⁹
 Nigeria	Nigeria Data Protection Regulation (NDPR) ⁶⁰	Nigeria Data Protection Commission ⁶¹
 Oman	Personal Data Protection Law ⁶² (PDPL) 2022 Executive Regulations of the Law ⁶³ 2024	
 Qatar	Law No. 13 of 2016 Concerning Personal Data Protection ⁶⁴	National Cyber Governance and Assurance Affairs ⁶⁵
 Rwanda	Law No 058/2021 of 13/10/2021 relating to the protection of personal data and privacy ⁶⁶	Rwanda's Data Protection & Privacy Office ⁶⁷
 Saudi Arabia	Saudi Arabia's Personal Data Protection Law (PDPL) ⁶⁸	Saudi Authority for Data and Artificial Intelligence ("SDAIA") ⁶⁹

Table 1. Data Protection and National Authorities per country

Source: Access Partnership research

Dedicated data protection authorities (DPAs) provide specialised expertise, focused oversight, and independent enforcement of data protection regulations, ensuring a consistent approach across sectors. Their independence enhances public trust and allows for impartial decision-making. DPAs also play a crucial role in raising public awareness and adapting to emerging challenges in the rapidly evolving digital landscape.

Countries that recognise the importance of protecting privacy have taken measures in this regard, as can be seen in several DCO Member States. For example, Ghana, in its National Artificial Intelligence Strategy,⁷⁰ established objectives to facilitate data access and governance by implementing and enforcing data sharing and governance policies, clarifying data privacy agreements, and disseminating guidance on ethical AI practices.

Jordan's principles under the National Charter of Ethics for Artificial Intelligence⁷¹ include privacy and data protection. The principles emphasise adherence to laws and best practices in data management, including collection, processing, storage, and deletion. The focus is on preserving privacy and confidentiality and respecting intellectual property rights. Jordan also prohibits unauthorised surveillance or tracking of individuals and stresses the importance of data quality, validity, and integrity.

Jordan's principles advocate for strong data governance, accountability for privacy violations, and obtaining informed consent for data use. Additionally, they forbid illegal data acquisition, misuse of data for undeclared purposes, and exploitation of AI outputs to harm individuals. The national charter is aligned with the local Data Protection Law,⁷² which has significant implications for AI development and deployment in the country, some of which are highlighted below:

Consent and transparency:



AI systems that process personal data will need to obtain explicit consent from individuals. This means AI developers must ensure transparency about how data is collected, used, and stored.

Data minimisation:



The law emphasises the principle of data minimisation, requiring AI systems to only collect data that is necessary for their specific purpose. This could limit the amount of data AI systems can access, potentially affecting their performance.

Sensitive data:



Special provisions for sensitive personal data mean that AI systems handling such data will need to implement additional safeguards. This includes data related to health, biometric information, and other sensitive categories.

Accountability and compliance:



Organisations using AI will need to ensure compliance with the new regulations, which may involve updating their data processing practices and implementing robust data protection measures.

Bahrain follows a very similar approach to Jordan under its Law No. (30) of 2018 with respect to Personal Data Protection.⁷³ It mandates proper consent or legal basis for data collection and processing, with stricter rules for sensitive data (health information, biometrics, etc). The law emphasises data quality, relevance, and purpose limitation while granting data subjects various rights, including access and rectification. It addresses automated decision-making, allowing for human intervention in certain cases.

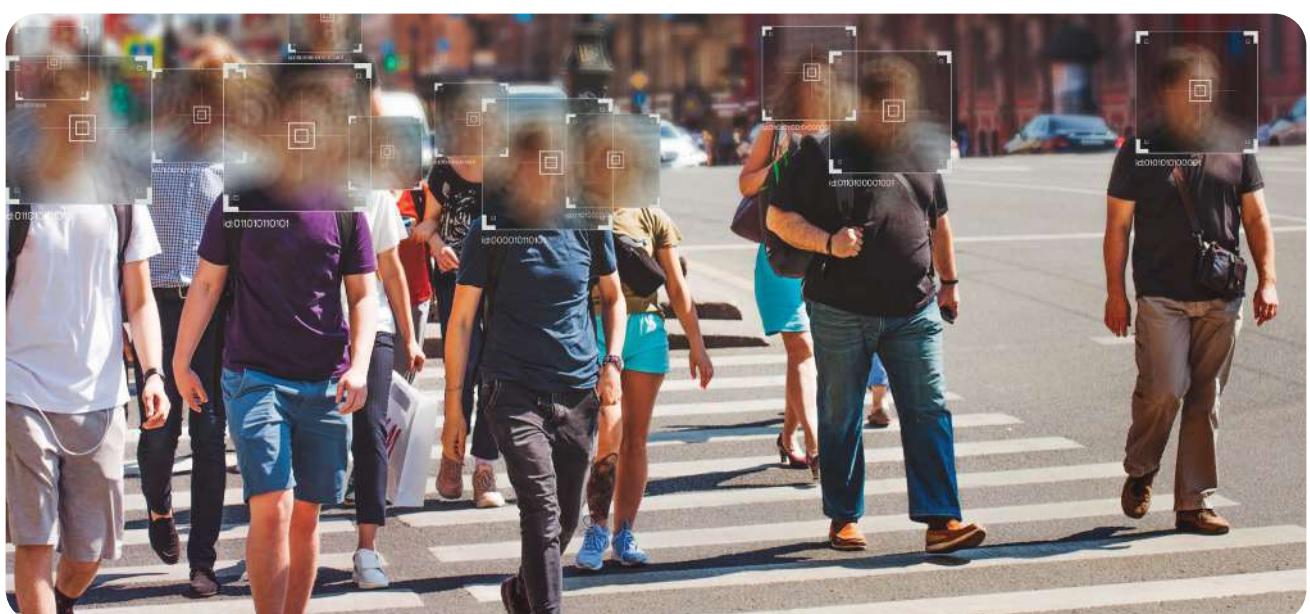
The law puts checks on cross-border data transfers, requires robust security measures, and may necessitate prior authorisation for certain data types, like biometrics. It also imposes accountability obligations on data controllers. These provisions collectively ensure that AI systems in Bahrain must be designed and operated with a strong emphasis on data protection, user rights, and privacy, potentially affecting their development, deployment, and operational processes.

Other DCO Member States have developed similar laws. Examples include Saudi Arabia's Personal Data Protection Law (PDPL),⁷⁴ Qatar's Personal Data Privacy Protection Law (PDPPL),⁷⁵ and Oman's Personal Data Protection Law (PDPL).⁷⁶ All of these have similar provisions to those of Bahrain and Jordan's regulations requiring AI developers to maintain transparency about how data is used and ensure accountability for any misuse. This includes providing clear information about AI decision-making processes and ensuring that AI systems are explainable.

DCO Member States that belong to the European Union, such as Greece and Cyprus, must adhere to and enforce the rules under the General Data Protection Regulation (GDPR).⁷⁷ This regulation sets high standards for data protection rules and is seen as the gold standard regulatory model.

Several DCO Member States are still in the process of developing comprehensive data protection laws and authoritative bodies dedicated to safeguarding citizens' privacy rights. This gap, coupled with rapid digitalisation, exposes individuals and businesses to significant risks. Without formal mechanisms to enforce data security standards or respond effectively to cyber threats, these economies are increasingly vulnerable to privacy breaches and data misuse.

Even for those countries that do have regulations, there could be concerns about the lack of transparency regarding what data is collected by various actors and how it is used, which can lead to misuse and privacy violations. Consequently, the next challenge for countries that do have a well-developed framework is to ensure transparency in the use and collection of data. The other major challenge for countries with specific data protection frameworks is to correctly educate their authorities to ensure the correct enforcement of their regulations.



3.1.2 Right to non-discrimination

Non-discrimination relates to non-biased algorithms, as AI systems can perpetuate or even exacerbate biases if not properly designed and monitored. It is essential to ensure that AI algorithms do not discriminate based on race, gender, or other personal characteristics.

This topic is constantly raised by international organisations, academics, and civil societies as it represents one of the major areas of concern for society. The use of AI in sensitive areas, such as employment, health, finance, and criminal justice, needs to be carefully monitored to prevent discriminatory outcomes because, without proper oversight, AI can reinforce and perpetuate existing social inequalities. For example, on the employment front, AI in hiring processes raises questions about fairness and discrimination. This is an area of great impact for all, and addressing discrimination in this field would increase fairness and employment opportunities for minorities, candidates coming from lower income classes, and other discriminated categories.

Two cases of AI violation of the non-discrimination right are (i) the Robodebt scandal in Australia and (ii) the Dutch childcare benefit scandal. The Robodebt scandal involved an unlawful AI-automated debt recovery system used by the government from 2016 to 2019. The system incorrectly calculated debts owed by welfare recipients.⁷⁸ This led to many people receiving false debt notices, causing significant financial and emotional distress (even suicides). The scheme was ruled illegal in 2019.⁷⁹

Similarly, the Dutch childcare benefit scandal⁸⁰ involved an algorithmic system used by the Dutch tax authorities to detect welfare fraud. Introduced in 2013, the system used data on nationality and ethnicity as risk factors, leading to racial profiling and disproportionately targeting ethnic minorities. Thousands of families, mostly from low-income backgrounds, were falsely accused of fraud, resulting in severe financial and emotional distress. The scandal came to light in 2019, leading to the resignation of the Dutch government in January 2021. A Dutch court ruled that the system breached human rights laws, emphasising the need for transparency and accountability in the use of AI.⁸¹

Within the current legal framework of many countries globally, including the DCO Member States, only a few countries have developed specific policies to reduce discrimination in the development and application of AI systems and algorithms. There are more generic references to transparency in policies and strategies, but the absence of robust legal protections increases the risk of AI being used in ways that exacerbate existing inequalities, whether intentional or not. Although this is one of the more complex challenges posed by AI, some interesting approaches have been followed around the world to reduce the impact. For example, the UK launched a Fairness Innovation Challenge, a government initiative offering up to GBP 400,000 in funding for innovative solutions tackling bias and discrimination in AI systems. The project had a big focus on healthcare and other real-world use cases.⁸² From a policy angle, the White House Office of Science and Technology Policy in the US proposed the Blueprint for an AI Bill of Rights, which includes principles to guide the design and use of AI systems, including protections against algorithmic discrimination.⁸³ Another example of non-discrimination inclusion can be found in the National Charter of Ethics for Artificial Intelligence⁸⁴ of Jordan. This document describes a series of principles⁸⁵ for the responsible use of AI technologies, among which include inclusiveness and justice. These principles emphasise the importance of respecting, protecting, and promoting diversity, inclusion, and impartiality throughout all stages of AI technology development and use. It recognises that bias in AI systems can result from incomplete or deficient datasets, as well as from the cognitive or real-world biases of individuals designing and training these systems. The goal is to promote economic, social, and digital justice by eliminating unfair discrimination and unequal opportunities. This involves ensuring AI technologies are fair and unbiased, use diverse and comprehensive datasets, avoid the perpetuation of negative stereotypes or exclusionary practices, and make AI technologies accessible to all, including marginalised groups and people with disabilities.

Bahrain has also adopted some concrete measures to reduce this risk, imposing a fine of up to BHD 2,000 for anyone misusing AI for discrimination or in violation of its intended purposes.⁸⁶ Other countries

refer to non-discrimination as a key principle within their national frameworks without expanding on what this means in practice or how it should be protected. A table summarising all DCO frameworks and AI references can be found in section 3.3.

Governments must prioritise transparency in AI development and provide clear guidelines to prevent discrimination. These guidelines should target software engineers, programmers, AI enthusiasts, and anyone involved in building or applying AI-related technology. Concurrently, public sector officials and policymakers need to deepen their understanding of AI sectors to craft effective regulations that balance innovation with responsible development. This approach will help avoid unnecessary delays or barriers while ensuring responsible AI implementation.

3.1.3 Freedom of opinion and expression

Freedom of opinion and expression concerns data moderation, content, misinformation, and fake news. AI can impact freedom of expression through content moderation and censorship; for example, on social media platforms. Balancing protective regulations against free speech is the main challenge under this topic.

This is one of the most complex rights identified in the research, as it can be seen as one of the most difficult trade-offs to achieve. This applies to both the public sector, which can be criticised for restricting freedom of speech to protect society, and online platforms that struggle with ensuring freedom of expression and ideas while reducing the dissemination of fake news and illegal content. Moreover, increasing concerns have been raised about misleading algorithms and opaque formulas exacerbating biases and hate speech that target certain individuals and minority groups, with the result of increasing social tensions and unrest.

Examples of violations of this right include receiving propaganda and manipulation by various political actors to generate specific political results. Since 2023, more than 1,110 AI-generated news and information websites have been tracked, operating with little to no human oversight.⁸⁷ In May 2023, there were only 49.⁸⁸ According to Brewster, a researcher at NewsGuard who conducted the investigation, these sites work in two ways.⁸⁹ Some stories are created manually by people who are consulting with chatbots throughout drafting the article. Otherwise, the process can be automatic, with AI systems searching for articles that contain certain keywords and feeding those stories into a large language model that rewrites them to seem original and avoid plagiarism.

AI systems are now central to the content moderation strategies used by both governments and online platforms. While these systems can efficiently manage the vast flow of information online, they



also amplify inherent biases and exacerbate social divides. By prioritising or de-prioritising certain content types or topics, algorithms often reinforce existing biases, leading to the disproportionate targeting of specific viewpoints or demographic groups. This algorithmic targeting can influence public opinion by over-exposing certain individuals or groups to content that may contain misinformation or inflammatory rhetoric. As such, these algorithms can inadvertently contribute to social polarisation, bias reinforcement, and the spread of hate speech.

Protecting freedom of speech requires ongoing dialogue, careful consideration of diverse perspectives, and a commitment to upholding individual rights and collective wellbeing. The challenge lies in finding an appropriate balance that preserves the core values of free speech while addressing legitimate societal concerns. Transparency, proportionality, and a detailed legal framework are some of the foundations upon which protection of the freedom of expression should be based while regulating AI uses.

Among DCO Member States, although the concept might be included in their legal frameworks, there are opportunities to improve practical implications by offering concrete references on how to ensure fair implementation of freedom of speech concerning digital technologies. Around the world, concerns have been raised that laws aimed at ensuring the safety of the internet have, in some cases, overstepped and impinged on this right, creating new tools for censorship. Addressing these concerns, Nigeria debated the Digital Rights and Freedom Bill,⁹⁰ which was designed to protect the rights of Nigerians in the digital space by addressing issues such as privacy, surveillance, and censorship. It was intended to promote human rights online, but since 2019, the bill has remained under discussion and has not been approved or updated.

Balancing free speech and protective regulations on AI-powered digital platforms is a complex challenge for policymakers and tech companies. While these platforms democratise information and amplify diverse voices, they also accelerate the spread of misinformation, hate speech, and harmful content, potentially disrupting social cohesion and infringing on individual rights. AI-driven content moderation, although efficient in processing large data volumes, often struggles to distinguish between free expression and genuinely harmful material. This can lead to either excessive censorship or insufficient protection, further complicated by the global nature of digital platforms and varying cultural and legal norms. As AI evolves, achieving an effective balance between safeguarding free speech and ensuring necessary protections remains a challenge and a priority.

3.1.4 Right to Work

Everyone has the right to work, as well as the right to choose employment, just working conditions, and protection from unemployment. There is considerable concern about the potential substitution effects of AI in labour markets. The right to work is intricately linked to economic security and personal fulfilment. As AI continues to evolve, its impact on the labour market generates benefits but also raises concerns about job displacement and the potential erosion of this right.

AI can enhance job opportunities and working conditions in several ways, as it often automates repetitive or dangerous tasks, potentially improving workplace safety and allowing workers to focus on the more engaging, creative aspects of their jobs. AI-powered tools can increase productivity and efficiency, which may lead to economic growth and new job creation in emerging fields. On the other hand, the negative effect that AI could have would be to abolish several job categories or positions as it automates processes. Therefore, boundaries and long-term thinking are imperative in the development of AI systems to maintain the importance of human factors in employment and find resourceful ways to generate new positions in replacement of those that cease to exist.

An example of the negative impact of AI on employment is the lawsuit in August 2023 against the tutoring company iTutor Group.⁹¹ This ended in a settlement, where iTutor Group agreed to pay USD 365,000 to the US Equal Employment Opportunity Commission (EEOC). The federal agency claimed that the company used AI-powered recruiting software that automatically rejected female applicants aged

55 and older and male applicants aged 60 and older. This resulted in the automatic rejection of more than 200 qualified applicants by the software.

The right to work is intricately linked to economic security and personal fulfilment. As AI continues to evolve, its impact on the labour market generates benefits but also raises concerns about job displacement and the potential erosion of this right.

However, if the people in charge of automated tasks are not trained and prepared to move to new areas of work or responsibilities, this could disproportionately displace workers. Industries such as manufacturing, logistics, and certain service sectors face a higher risk of job losses as AI systems and robots become more capable of performing tasks traditionally done by humans. Positions like data analysts/scientists, project managers, administrative assistants, and secretaries are expected to be highly impacted by AI uses and development, according to the World Economic Forum Report on Future of Jobs 2024.⁹² Governments, with the support of the private sector, should prepare society and support their continuous learning and skill development, including through AI-driven educational platforms, helping workers adapt to changing job markets. Otherwise, AI could create a skills gap where the workforce struggles to keep pace with evolving technological demands.

AI can also democratise access to work by enabling remote work opportunities, assisting people with disabilities through adaptive technologies, and providing personalised job matching services. The integration of AI in hiring processes raises questions about fairness and discrimination. While AI can potentially reduce human bias in recruitment, poorly designed algorithms might perpetuate or even amplify existing biases, affecting equal access to job opportunities.

In navigating these challenges, the goal is to use AI's potential to improve the quality and accessibility of work while mitigating its disruptive effects on employment. In this regard, governments within the DCO Member States have already taken several measures to address the risk while fostering the benefits of AI. Most countries that have regulations, policies, or frameworks on AI have references to the importance of protecting employment access and using AI to create new job opportunities.

Pakistan's (draft) National AI Policy⁹³ mentions among its objectives offering higher education scholarships, improving opportunities for job training for applied skills, developing new skilled human capital, and upskilling the existing workforce.

Cyprus' National AI Strategy⁹⁴ emphasises the need for ongoing education and skill development within the existing workforce. Customised training programmes and the exploration of Massive Open Online Courses (MOOCs) in AI are being considered as accessible learning tools. The Cyprus Human Resource Authority (AnAD)⁹⁵ aims to play a crucial role by providing information and incentives to employers who invest in upgrading their employees' digital and AI skills. This collaborative effort aims to ensure a future-proof workforce with the necessary competencies to thrive in the digital age.

Ghana's National Artificial Intelligence Strategy⁹⁶ includes a section to empower youth for AI jobs by facilitating remote jobs or internships in AI and promoting continuous training for students and professionals.

The right to work and the ways to address this human right are directly connected with the right to education described below, as it reinforces the importance of providing fit-for-purpose training and courses to ensure the workforce is prepared to deal with new market dynamics and changes.

3.1.5 Right to Education

AI's integration into national education programmes is crucial, with a focus on enhancing access to personalised learning experiences and educational resources. However, this integration raises concerns about digital divides and underscores the need for AI literacy.

AI education and AI literacy are two related but distinct concepts in the field of artificial intelligence and education. AI education refers to the process of integrating and applying AI technologies within educational settings to enhance teaching and learning experiences.⁹⁷ Examples include grammar-checking software, plagiarism detection tools, and AI-powered assistants for personalised study support. AI literacy, on the other hand, is the ability to understand, use, monitor, and critically reflect on AI applications.⁹⁸ It encompasses the knowledge and skills that enable individuals to recognise, grasp, use, and critically assess AI technologies and their impacts.

While AI education is about implementing AI in educational contexts, AI literacy is about developing the skills to interact with and evaluate AI systems effectively. AI literacy is essential for students, educators, and the general public to navigate the increasing presence of AI in various aspects of life.

AI can tailor educational content and address individual students' needs, ensuring that each learner receives the optimal level of support. AI-powered tutoring systems can provide personalised guidance, answer questions, and offer feedback, helping students to understand complex concepts more effectively. AI can help to make education more accessible to students with disabilities by providing tools and accommodations that cater to their specific needs. AI-powered language learning apps and platforms can provide immersive and engaging experiences that help students acquire new languages more quickly.



While there are significant opportunities for improvement in the educational field, the digital divide could negatively affect the outcomes of AI implementation. Access to technology and internet connectivity are essential for benefiting from AI-powered learning resources. In countries where internet penetration remains low or where students do not have access to computers or the internet, it will be extremely difficult for students to have access to these new sources of education. Furthermore, AI algorithms can perpetuate biases present in the data they are trained on. This could lead to discriminatory outcomes in education, such as biased assessments or recommendations.

Many DCO Member States have paid substantial attention to this human right concerning AI. Ghana's National Artificial Intelligence Strategy⁹⁹ aims to (i) expand AI education and training by conducting annual skills gap assessments, (ii) launch the AI Ready Ghana programme, (iii) expand AI education courses, and (iv) promote training for teachers. Furthermore, the government has invested in AI research centres and initiatives, particularly through AI programmes at universities like the University of Ghana and Kwame Nkrumah University of Science and Technology (KNUST).¹⁰⁰

Nigeria's Federal Ministry of Communications, Innovation, and Digital Economy (FMCIDE) has conducted various workshops and educational initiatives¹⁰¹ aimed at upskilling Nigerian researchers and practitioners in AI technologies. Rwanda,¹⁰² Morocco,¹⁰³ Jordan,¹⁰⁴ Bahrain,¹⁰⁵ and other governments have also announced partnerships and initiatives with local universities and schools to develop courses and training on AI.

There is a growing focus on addressing the ethical implications of AI. Workshops on UNESCO's Recommendation on the Ethics of AI and the intersection of AI and human rights are prominent topics of discussion. This reflects an increasing awareness of the need to balance technological advancement with ethical considerations and human rights protection. Notably, many initiatives focus on improving and protecting human rights, particularly in areas such as health, sustainability, privacy, and education, demonstrating AI's potential to contribute to pressing social and environmental issues.

Another significant trend is collaboration with international organisations and institutions from other countries, including GIZ FAIR Forward, UNESCO, EU, UNIDO, and the World Bank. However, there appears to be less cooperation among DCO countries or within their own geographical clusters.

3.1.6 Right to Health

AI in healthcare can improve diagnostics and treatment but must be used ethically to ensure equitable access and avoid harm. AI-powered algorithms can analyse vast amounts of medical data to improve disease diagnosis and detection. This can lead to earlier interventions and more effective treatments. Additionally, AI can assist in developing new drugs and therapies by identifying potential targets and accelerating the drug discovery process. AI-enabled medical devices can also provide real-time monitoring and personalised care, helping patients to manage chronic conditions more effectively.

AI technologies offer promising healthcare innovations, but they also present significant ethical challenges that require careful examination. The key concerns include:



Unequal Access:

Without deliberate intervention, AI-powered healthcare services may deepen existing health disparities, preventing vulnerable populations from benefiting from advanced medical technologies.



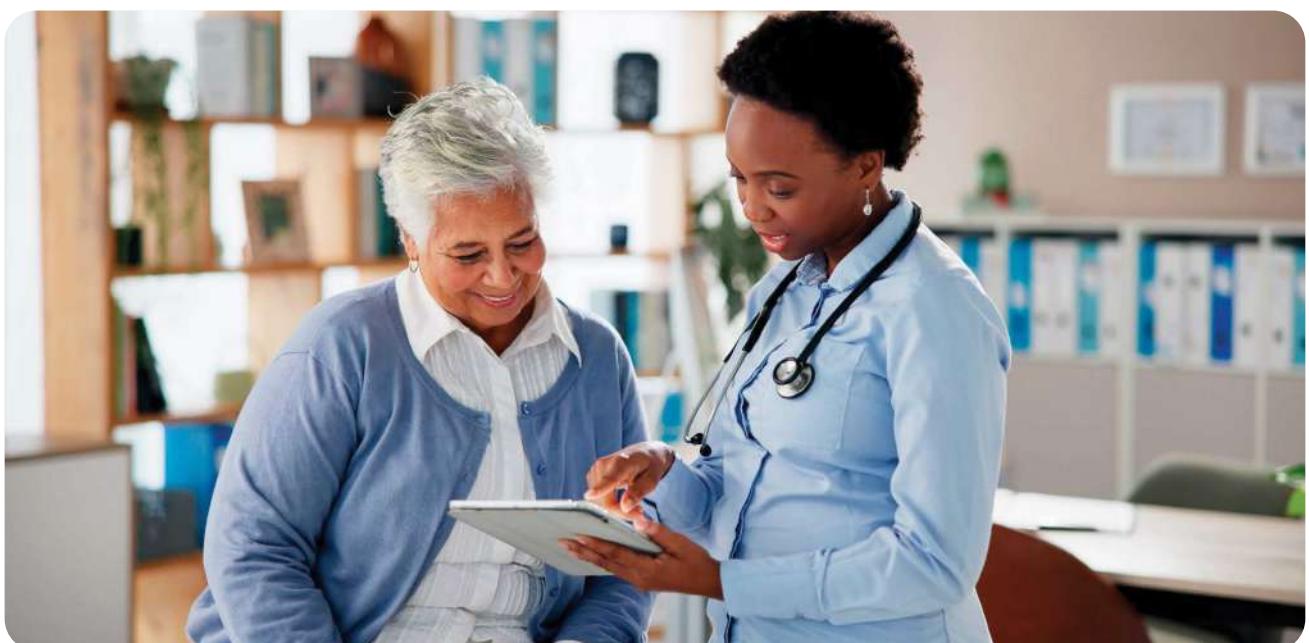
Algorithmic Bias:

AI systems can perpetuate discrimination if trained on biased datasets. This may result in inaccurate diagnoses or treatment recommendations that disproportionately harm certain demographic groups.



System Reliability:

The potential for errors, misinformation, or technical malfunctions in AI healthcare applications poses serious risks to patient safety. Comprehensive safety protocols and rigorous oversight mechanisms are essential to mitigate these risks.



These challenges underscore the need for proactive, ethical approaches to integrating AI into healthcare, ensuring that technological advancement does not compromise patient welfare or medical equity.

A relevant case regarding the repercussions of AI use in healthcare is a lawsuit filed in 2023 before the US District Court for the District of Minnesota.¹⁰⁶ It accused UnitedHealthcare of utilising the nH Predict algorithm to make healthcare determinations. The plaintiffs claimed that the use of this algorithm led to the premature and bad-faith denial of payment for healthcare services. The plaintiffs, insured by UnitedHealthcare, were allegedly forced to personally pay for medically necessary care. The lawsuit alleges that the nH Predict algorithm developed by NaviHealth systematically denied elderly patients' claims for extended care. This case has not yet reached a decision.

There are some examples of sector-specific initiatives led by public sector authorities in DCO Member States, but there is a big opportunity for improvement here as those examples are largely supported by academia and the private sector. For example, there are several start-ups in DCO Member States working on health initiatives driven by AI solutions. In Qatar, AI is being integrated into the healthcare sector through partnerships that aim to improve patient care and streamline medical processes.¹⁰⁷ Companies like Avey, founded in 2017, focus on AI-driven healthcare solutions, providing mobile apps for ordering healthcare products and communicating with healthcare providers.¹⁰⁸ In Ghana, Chestify AI Labs aims to transform healthcare by connecting radiologists and medical practitioners to healthcare facilities. It uses AI to facilitate faster annotations and report writing for biomedical images.¹⁰⁹

Governments can do much to support initiatives at the intersection of AI and health. This is especially important in countries where resources are scarce and health problems are among society's top priorities.



3.1.7 Right to a Healthy Environment

AI can be used to measure, analyse, and reduce emissions and climate effects, optimise the management and consumption of natural resources, and foster environmental sustainability. On the other hand, there are concerns about carbon emissions from AI.

AI can provide valuable insights into climate change, pollution levels, and resource consumption by collecting and analysing vast amounts of environmental data. For example, AI-powered sensors can monitor air and water quality, detect changes in biodiversity, and track deforestation rates. Several projects are running powered by these technologies. One example is the IKI Project¹¹⁰ in Africa, which uses AI technology to help predict weather patterns, enabling communities and authorities to better adapt to climate change and mitigate its impact.¹¹¹ There is also Space Intelligence,¹¹² a company based in Scotland that leverages AI and satellite monitoring to map the impact of deforestation on the climate crisis, covering more than 30 countries.¹¹³ This data can be used to identify environmental hotspots, assess the effectiveness of conservation efforts, and inform policy decisions.

At the same time, the training and operation of AI models can be energy-intensive, potentially contributing to increased carbon emissions. Microsoft, (ChatGPT, OpenAI, etc.) announced in its Environmental Sustainability Report 2024¹¹⁴ that its CO₂ emissions had risen nearly 30% since 2020 due to data centre expansion. By contrast, Google's GHG emissions in 2023 were almost 50% higher compared to the 2019 numbers, largely due to its data centres, as mentioned in its Environmental Report 2024.¹¹⁵

Another aspect of the environmental chain is the impact of electricity users to create related components, such as AI chips, which represent 1.5% of electricity use over the next five years. This represents an important part of the world's energy supply.¹¹⁶ Additionally, a recent study conducted by Cornell University scientists found that training Large Language Models (LLMs) like GPT-3 consumed an amount of electricity equivalent to 500 metric tons of carbon, which amounts to 1.1 million pounds of carbon dioxide (CO₂).¹¹⁷ For reference, a typical coal-fuelled power plant working continuously for 24 hours burns about 2.7 million pounds of coal.

While AI offers significant potential for environmental monitoring and decision-making, several challenges may impede its effective implementation. Poor data quality and availability can reinforce inherent biases (such as developing countries or those from certain regions performing worse than richer countries in terms of a metric due to their geographical positions or economic history), which can lead to incorrect environmental assessments and misguided policy decisions. Ethical concerns, particularly regarding privacy, arise when collecting and analysing vast amounts of environmental information. Additionally, the technological limitations of certain AI tools due to their lack of maturity may restrict their reliability and applicability. These challenges underscore the need for careful consideration and robust safeguards when deploying AI for environmental purposes, ensuring that the benefits of AI-driven insights are not undermined by data inaccuracies, ethical breaches, or technological shortcomings.

An interesting example from the DCO Member States comes from Jordan, where AI policies explicitly address the link between AI and a healthy environment. Jordan's National Charter of Ethics for AI¹¹⁸ refers to the principle of preserving a good environment for future generations and protecting the components of human life and the environment. Natural resources used during the development and use of AI technologies must be protected by ensuring the energy efficiency of AI technologies, which reduces their carbon impact on the environment and limits climate change.¹¹⁹

There are also examples of specific practical initiatives in DCO Member States at the intersection of AI and the environment; for example, projects focused on smart cities¹²⁰ to reduce carbon emissions or start-ups using AI to detect pests in their agricultural crops and reduce the use of chemical pesticides.¹²¹ However, to date, it is hard to find examples where these initiatives have received significant financial or non-financial support from the public sector.

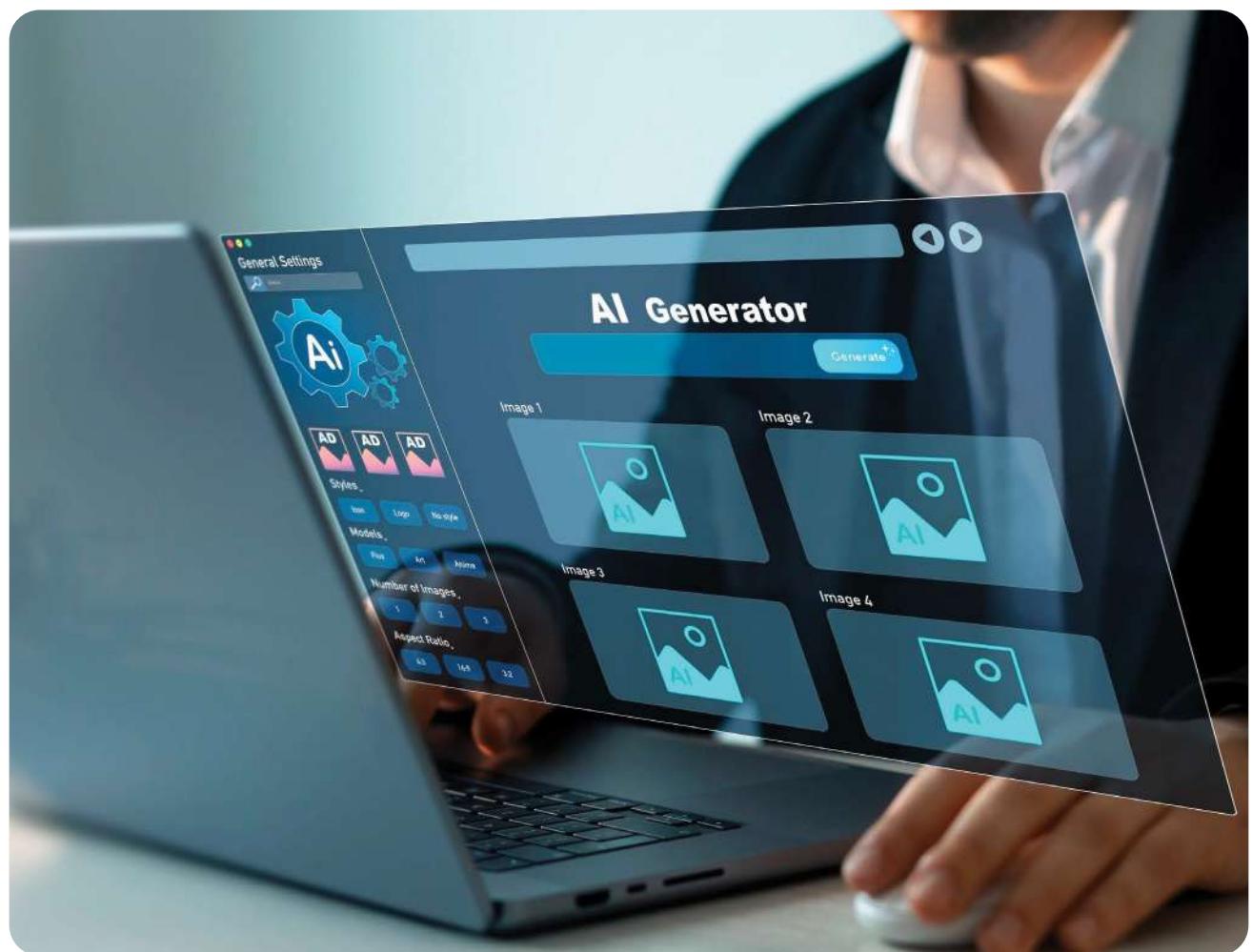
Governments and businesses in DCO Member States should collaborate to develop policies and initiatives that promote the responsible use of AI for environmental protection and mitigate the environmental impacts of AI. For example, governments could offer financial incentives or incubator support to start-ups working on AI solutions in the climate action space.

3.1.8 Right to Participate in Cultural Life

The right to take part in cultural life guarantees the right of everyone to access, participate in, and enjoy culture, cultural heritage, and cultural expressions.¹²² AI technologies have the potential to both enhance and hinder cultural participation, creating a complex landscape of opportunities and challenges. It could enhance access by improving recommendation systems and content discovery but may also create filter bubbles that limit exposure to diverse cultural expressions.

Concerning the creation and support of culture, AI is opening new avenues for artistic expression. Artists and creators are using AI tools to push the boundaries of their craft, leading to innovative forms of art, music, and literature. However, the line between human and machine-generated content is becoming increasingly blurred, challenging traditional notions of cultural production. Moreover, AI-generated art is triggering further concerns regarding ownership and the possibility of reducing creativity as a way of self-expression.

One of the consequences of violation of the right to participate in cultural life is the misrepresentation of artistic content copyrights. In practice, AI-generated art could be presented as tech-generated, whereas it may be the exact or very similar work of an actual artist that the AI system has used as a sample or inspiration for its "creation". There is currently an ongoing lawsuit being brought against two AI start-ups over alleged copyright violations.¹²³ Firms including Sony



Music, Universal Music Group, and Warner Records allege that Suno and Udio have committed copyright infringement by using their copyrighted music to generate similar work. They are demanding a compensation of USD 150,000 per work. These lawsuits follow a wave of lawsuits from authors, news organisations, and other groups that are challenging the rights of AI firms to use their work.

AI can also play a role in preserving cultural heritage. Advanced image recognition and data processing capabilities can aid in digitising, cataloguing, and preserving cultural artefacts at an unprecedented scale. For instance, Google Arts & Culture has partnered with museums globally to digitise and annotate thousands of artworks, providing detailed descriptions and analyses.¹²⁴ The Louvre Museum employed 3D modelling to create virtual tours of its exhibits, allowing global audiences to explore cultural treasures remotely.¹²⁵ In Timbuktu, Mali, AI-based imaging techniques are used to restore murals in historic mosques by analysing faded pigments and reconstructing missing elements.¹²⁶ However, there's a risk that biases in data collection and curation could lead to the underrepresentation or misrepresentation of certain cultural elements, particularly those from marginalised or underrepresented communities.

The deployment of AI systems trained on cultural data raises concerns about perpetuating or amplifying existing biases and stereotypes in cultural representation. These "cultural algorithms" could shape perceptions and narratives about different cultures in ways that may not accurately reflect their richness and diversity.

Regarding this specific right, there are limited examples from the DCO Member States to protect and enhance their cultural patrimony using AI. There are references to the protection of cultural norms in a broad sense, such as Qatar's National AI Strategy,¹²⁷ which proposes the development of an AI Ethics and Governance framework that should be consistent with Qatari social, cultural, and religious norms, as well as international guidelines.

The Saudi Arabia Data & AI Authority (SDAIA) AI Ethics Principles¹²⁸ reinforce the idea of building AI systems based on fundamental human rights and cultural values. SDAIA urges the designers of AI models to define how their AI system will align with fundamental human rights and KSA's cultural values while designing, building, and testing the technology. Furthermore, after the deployment of the AI system, the principles advocate for the AI System Owner to ensure that continuous assessment of the human, social, and cultural impact of AI technologies is conducted. On top of these principles, SDAIA has launched an AI Ethics Assessment tool¹²⁹ to enable controllers¹³⁰ to conduct a comprehensive and systematic analysis of the extent of their compliance with ethical standards in the development and application of AI technologies. This assessment is built considering the cultural values that KSA embraces to generate a beneficial impact on society.

In this section, we have analysed national policies and efforts to bridge the gap between the potential of AI and its responsible integration into society. However, this work cannot be done unilaterally, as the intrinsic characteristics of AI and its rapid evolution make it a worldwide issue where international cooperation is fundamental. This is why it is crucial to consider existing international frameworks and standards that address both Human Rights and AI. These frameworks serve as a foundation for developing ethical guidelines and practices that align AI deployment with the broader objectives of safeguarding human rights and promoting environmental sustainability. By examining these international principles in the next section, we can better understand how to implement AI in a manner that not only drives innovation and economic growth but also ensures that human rights and environmental goals are upheld in the digital age.

3.2 INTERNATIONAL FRAMEWORKS AND STANDARDS ADDRESSING HUMAN RIGHTS AND AI

The global consensus on ethical and responsible AI use has led to the adoption of universal guiding principles by international bodies, summarised in the table below. Some commonality is apparent, particularly when considering these principles:



Organisation	Principles
ASEAN Guide on AI Governance and Ethics¹³¹	The principles include transparency and explainability, fairness and equity, security and safety, human-centricity, privacy and data governance, accountability and integrity, and robustness and reliability.
African Union (AU) Continental AI Strategy¹³²	The principles include human-centricity, transparency, accountability, fairness, human rights, privacy, equitable access, and minimisation of bias, discrimination, and societal harms.
G-20 AI Principles¹³³	The principles include human rights protection, transparency, explainability, fairness, accountability, regulation, safety, appropriate human oversight, ethics, biases, privacy, and data protection.
OECD AI Principles¹³⁴	The principles include inclusive growth, sustainable development and well-being; human rights and democratic values, including fairness and privacy; transparency and explainability; robustness, security and safety; and accountability.
United Nations Principles for the Ethical Use of Artificial Intelligence¹³⁵	The principles include do not harm; defined purpose, necessity, and proportionality; safety and security; fairness and non-discrimination; sustainability; the right to privacy, data protection, and data governance; human autonomy and oversight; transparency and explainability; responsibility and accountability; and inclusion and participation.
Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law¹³⁶	The principles established are as follows: human dignity and individual autonomy, equality and non-discrimination, respect for privacy and personal data protection, transparency and oversight, accountability and responsibility, and reliability and safe innovation.
European Union (EU) AI Act¹³⁷	The principles highlighted are safety, transparency, accountability, and non-discrimination. They consist of a risk-based approach to categorise AI systems, ensuring safety and transparency for high-risk sectors like healthcare. The Act provides robust compliance standards while fostering innovation.
G7 Hiroshima AI Process¹³⁸	The principles established are human-centric AI, transparency, accountability, and security. It focuses on generative AI governance, emphasising transparency and accountability in AI systems.
United Nations (UN) Roadmap for Digital Cooperation¹³⁹	Calls for global AI governance based on building capacity, especially in developing nations, focusing on the principles of "do no harm", transparency, safety, accountability, and inclusion.
UNESCO Recommendation on the Ethics of Artificial Intelligence¹⁴⁰	Promotes ethical AI use aligned with human rights and sustainability goals, aiming for inclusive, transparent, and accountable AI development. The principles underlined are human dignity, inclusion, environmental sustainability, and transparency.

Organisation	Principles
Global Privacy Assembly (GPA) Declaration on Ethics and Data Protection in AI¹⁴¹	The principles established are privacy, fairness, accountability, transparency, and human rights. This declaration promotes fairness and accountability, calling for stricter governance to mitigate risks to privacy and fundamental rights.
United Nations Global Digital Compact¹⁴²	Focuses on leveraging AI to support the Sustainable Development Goals (SDGs), promoting inclusive, human-centric AI governance at a global scale. This document manifests digital inclusion, security, transparency, equity, and human-centricity.
Council of Europe (COE) Convention 108+¹⁴³	The COE promotes AI frameworks that protect human rights and privacy. Convention 108+ extends data protection to AI, and the Ad Hoc Committee on AI (CAHAI) explores legal frameworks for ethical AI use, particularly regarding facial recognition. It concentrates on the principles of human rights, democracy, the rule of law, transparency, and data privacy.
European Commission Ethical Guidelines for Trustworthy AI¹⁴⁴	Emphasis on lawful, ethical AI development, providing a foundation for ongoing regulations, such as the AI Act. The Guidelines support both the private and public sectors in aligning with fundamental rights. They highlight the principles of human agency, technical robustness, transparency, and non-discrimination.

Table 2. International Principles for AI

Source: Access Partnership research. Please note that this is not an exhaustive list.

As highlighted above, most international organisations, institutions, and bodies, due to their legal mandate and capabilities, have taken a high-level path of soft regulation towards AI governance, with members responsible for determining the specific regimes to be implemented in their countries. These developments can also serve as points of comparison in the respective regions. This approach provides a set of guiding parameters to evaluate and decide on the required elements and measures that should be in place to maximise the benefits of AI while minimising the risks. This considers the fact that a one-size-fits-all policy is unlikely to be effective, especially when you look at particular points along the AI lifecycle and the growing number of AI use cases. Likewise, this approach can be useful when there is a debate as to which human rights take priority.¹⁴⁵

The first binding international treaty on AI: EU, UK, US signatories



The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, published in September 2024, is the first binding international treaty signed by EU, UK, and US. It aims to ensure AI system lifecycles align with human rights, democracy, and the rule of law while fostering technological progress. Its objective is to ensure that activities within the lifecycle of AI systems are fully consistent with human rights, democracy, and the rule of law while being conducive to technological progress and innovation. **This concerns public authorities' use of AI systems, as well as private entities acting on their behalf.** The framework recommends mechanisms to ensure its objectives are met including (i) establishing information systems to provide transparency on AI uses, (ii) establishing an effective complaint-handling mechanism under the suitable authorities, (iii) providing effective procedural guarantees, safeguards, and rights to affected persons in connection with the application of an AI system where it significantly impacts upon the enjoyment of human rights and fundamental freedoms, and (iv) mandating disclosure of AI involvement in interactions.

The international frameworks referred to in Table 2 describe guiding principles and recommendations (soft law) that would need to be adopted at the domestic level to become enforceable (hard law). However, to date, except for the EU, there has not been significant progress regarding enforcement measures.

The EU AI Act represents a comprehensive regulatory framework applicable to all EU members. It classifies AI risks and prohibits applications that pose unacceptable threats to human rights, such as systems involving biometric data misuse or privacy violations. Typical categories of unacceptable risk are systems that entail the following:

Issue	Example	Related Human Rights
 Cognitive behavioural manipulation	Voice-activated toys that encourage dangerous behaviour in children	Freedom
 Social scoring	Classifying people based on behaviour, socioeconomic status, or personal characteristics	Non-discrimination, equal access to law and justice
 Biometric identification	Categorisation of people	Privacy and data protection
 Real-time and remote biometric identification systems	Bias or discriminatory facial recognition	Privacy and data protection

Table 3. Unacceptable threats to human rights under the EU AI Act

Source: Access Partnership research.

Beyond the EU and US, through the US Executive Order on AI,¹⁴⁶ China stands out as the only other nation to adopt prescriptive AI regulations with non-compliance consequences and specific prohibitions. The Deep Synthesis Provisions,¹⁴⁷ enacted by China in 2023, address risks associated with deepfakes by imposing responsibilities on deep synthesis service providers regarding data security, personal information protection, transparency, content management, and technical security.

To effectively address AI risks and determine which can be managed versus those requiring outright suppression, international articulation and cooperation are essential. This collaborative approach allows for the implementation of minimum principles guided by globally recognised human rights frameworks while enabling nations to adopt tailored domestic measures that align with these universal parameters.

Based on the identified international principles and existing instruments for the responsible use of AI, the next section delves into the specific regulatory landscapes of the DCO Member States, identifying how these international principles manifest within diverse national frameworks. It is important to recognise that each Member State's approach to AI governance reflects its unique sociopolitical context and technological readiness. However, they are bound together by a shared commitment to ethical AI practices and the protection of human rights.

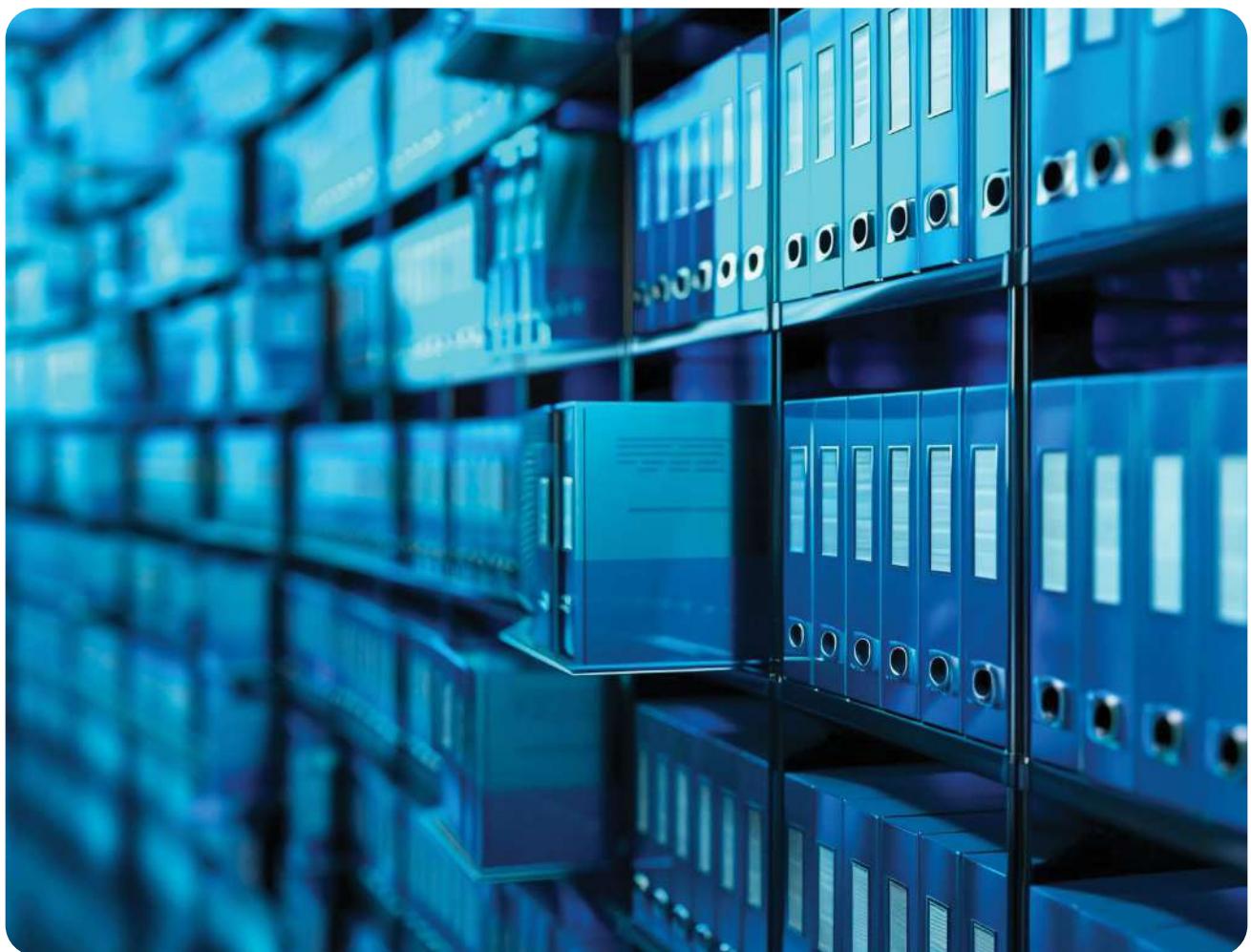
3.3 DCO MEMBER STATES' REGULATORY LANDSCAPE

By exploring how international principles for the responsible use of AI are implemented within various national frameworks, we can discern the unique approaches of each DCO Member State. This section will highlight the specific regulatory measures that DCO Member States adopt, offering insights into their readiness and commitment to responsible AI governance.

Establishing a national AI framework is imperative for countries to foster innovation while ensuring ethical standards and public safety. Such frameworks provide clear guidelines for developing, deploying, and regulating AI technologies, thus addressing potential risks like privacy violations, bias, and security threats.

Moreover, a national AI framework can promote transparency and accountability, encouraging public trust in AI systems. By defining public policy objectives and governance structures, countries can harmonise efforts between public and private sectors, optimise resource allocation, and create a supportive environment for technological advancements. Ultimately, a well-defined AI framework can help nations navigate the complexities of AI, mitigate human rights challenges, and leverage the technology's full potential for economic and societal benefits.

Across nations developing AI governance frameworks and national strategies, a common priority is protecting humans from potential risks associated with AI use and AI-generated decisions. Ethical and responsible AI deployment has emerged as a critical public policy concern for governments worldwide. Naturally, as the DCO Member States are diverse and present different levels of advancement in adopting digital policies and enabling regulations, the specific policies or instruments regarding the protection of human rights in the context of AI use also differ.



Country	Instrument	Relevant Principles
 Bahrain	Standalone law for artificial intelligence (AI) ¹⁴⁸ Bahrain AI Procurement Guidelines ¹⁴⁹	Privacy, personal freedoms, social values and traditions, non-discrimination, transparency, accountability, and liability regarding ethical concerns.
 Bangladesh	Draft National AI Policy 2024 ¹⁵⁰	Social equity, equality, and fairness; transparency and accountability; safety, security, and robustness; sustainability; partnership and collaboration; human-centred AI.
 Cyprus	National AI strategy ¹⁵¹	Not listed. However, it should be noted that the EU AI Act is directly applicable in Cyprus as a Member State.
 Ghana	National Artificial Intelligence Strategy ¹⁵² 2023—2033	Follows OECD and UNESCO principles. The strategy acknowledges the potential risks AI poses to security, safety, privacy, and human rights. It emphasises the importance of ensuring a responsible, inclusive, and sustainable AI ecosystem to mitigate these risks.
 Greece	Law N.4961/2022 ¹⁵³ "Emerging IT and communications technologies, strengthening of digital governance and other provisions" Law Draft National Strategy for AI ¹⁵⁴	It should be noted that the EU AI Act is directly applicable in Greece as a Member State.
 Jordan	AI Strategy and Implementation Roadmap (2023-2027) ¹⁵⁵	The deployment of AI will be done by "finding a common ethical base" based on "human and religious values and the customs and traditions of society".
 Nigeria	National Artificial Intelligence Strategy ¹⁵⁶	The strategy proposes the development of national AI ethical principles that reflect fairness, transparency, accountability, privacy, and human well-being.
 Oman	National programme for AI and advanced technologies ¹⁵⁷ Policy for the use of AI systems ¹⁵⁸	Ethical, fair, and safe use of AI applications. Inclusiveness, accountability, fairness, transparency, and security.
 Pakistan	Draft National AI Policy ¹⁵⁹	No specific principles are listed. Promoting the responsible use of AI is part of the objectives.
 Qatar	Qatar's National AI Strategy ¹⁶⁰ Guidelines for Secure Adoption and Usage of 2024 Version 1.0 Artificial Intelligence ¹⁶¹	Qatari social, cultural, and religious norms. International guidelines, including explainability and interpretability. Ethical Principles.
 Rwanda	National Artificial Intelligence Policy for Rwanda ¹⁶²	The strategy emphasises the importance of ethical principles and precautions to mitigate the risks associated with AI, ensuring that the technology benefits citizens and does not cause harm.
 Saudi Arabia	National Strategy for Data & AI ¹⁶³ Generative AI Guidelines (1 & 2) AI Ethics Principles ¹⁶⁴	Fairness, reliability and safety; transparency and interpretability; accountability and responsibility; privacy and security.

Table 4. Policies and Laws Related to AI in DCO Member States

*Discussion on AI national strategy is ongoing.

Source: Access Partnership research

As Table 4 demonstrates, most of the DCO Member States have already adopted or are in the process of adopting some form of AI framework. Meanwhile, some have yet to advance in discussing and defining a national instrument for AI public policy.¹⁶⁵ This highlights the big opportunity for the DCO Member States to advance in readiness regarding AI use, which starts with the adoption of an instrument to define and articulate public policy objectives, as well as defining the elements to address the human rights challenges that will come with AI use, regardless of it being a national public policy or not, as the market is already advancing to make AI available in all industries and services.

Integration of human rights principles in AI strategies

Integrating human rights principles into AI strategies and regulatory frameworks is essential for fostering responsible innovation and protecting individual freedoms in the digital age. This approach serves multiple critical purposes:

- 1** It establishes a strong ethical foundation for AI development and deployment, helping to prevent potential abuses and ensure that these powerful technologies respect human dignity.
- 2** In jurisdictions where AI governance is still emerging, incorporating human rights considerations from the outset creates a stable basis for more detailed regulations, ensuring that subsequent developments remain aligned with these fundamental principles.
- 3** By prioritising human rights in AI governance, governments can effectively encourage private sector actors to adopt rights-respecting approaches in their own AI initiatives, creating a positive ripple effect throughout the entire AI ecosystem.
- 4** Lastly, this human rights-centric approach provides a flexible yet robust framework that can adapt to the rapid evolution of AI technologies, ensuring that governance mechanisms remain relevant and effective in protecting individual rights and freedoms as the field advances.



Most DCO Member States have published their AI strategies. Below are some examples where national strategies include specific references to human rights:

Ghana:



Ghana published the National Artificial Intelligence Strategy 2023-2033 in October 2022. One of its highlighted objectives was to disseminate local and international guidelines on trustworthy, safe, secure, and ethical AI practices to AI developers and adopters. References to the compliance with OECD, UNESCO, and other organisations and efforts have also been included.

Jordan:



In mid-2022, the cabinet of Jordan's Ministry of Digital Economy and Entrepreneurship approved the National Charter of Ethics for Artificial Intelligence.¹⁶⁶ The charter called for Jordan to develop a national strategy and regulatory regime for the deployment of AI technology. The deployment of AI will be done by "finding a common ethical base" based on "human and religious values, and the customs and traditions of society". The charter contains several ethical principles for AI, including accountability, transparency, and respect for individual privacy.¹⁶⁷

Nigeria:



The Nigerian strategy emphasises a human-centred approach and highlights the importance of human rights in two ways:

- Human-Centric Design: The strategy prioritises the well-being and values of stakeholders in the design and implementation of AI technologies. It aims to ensure that AI enhances human capabilities, autonomy, and dignity, rather than undermining human agency.
- Protection of Human Rights: One of the objectives is to develop a legal framework that promotes responsible AI development and protects human rights and privacy. This involves conducting foresight studies to understand AI's potential societal disruptions and implementing legislative reforms to address emerging legal and ethical challenges.

Oman:



The "Integrated National Action Plan" programme is a key part of Oman's Vision 2040¹⁶⁸ and aims to support the strategic direction towards AI and advanced technologies. One of the four main pillars of this programme is "Governance of AI applications and advanced technologies through a human-centred vision". Under this governance pillar, the document mentions:

- Focusing on the "ethical, fair, and safe use of AI applications".
- "Managing ethical issues by laying the foundations that consider human aspects, community privacy, governance of data collection processes, and the development of safe AI algorithms".

The document emphasises a "human-centred vision" for AI governance.



Rwanda:

Rwanda's AI Strategy emphasises the importance of ethical principles and precautions to mitigate the risks associated with AI, ensuring that the technology benefits citizens and does not cause harm. As such, it highlights the need for:

- Practical AI Ethics Guidelines: These guidelines are designed to be widely diffused and operationalised across both the private and public sectors. They were included in the National AI Policy published in 2022. They set guidelines and objectives for the Rwandan ICT Ministry (MINICT) and Telecommunications Regulator (RURA) to implement. These include (i) the addition of AI ethics in their mandates, (ii) initiating regulatory sandboxes, and (iii) promoting and updating Rwanda's Guidelines on the Ethical Development and Implementation of Artificial.
- Regular Updates and Consultation: The guidelines will be updated every three years based on feedback from an annual consultation forum that includes industry and societal stakeholders.
- Promoting ethical AI Development: There are specific actions to promote and advertise these ethical guidelines, integrate them into government functions, and develop sector-specific guidelines.



Saudi Arabia:

The report on AI Ethics Principles¹⁶⁹ states that the principles are aligned with Saudi Arabia's commitment to human rights and cultural values. It emphasises that AI systems should respect fundamental human rights and not deceive or impair people's freedom of choice. There are multiple references to assessing AI systems' impact on human rights throughout the development lifecycle.



Greece and Cyprus:

With the recent signature of the European Council's Framework Convention, Cyprus and Greece will be bound to an AI governance approach based on the protection of human rights.

3.4 GLOBAL DISCOURSE ON AI AND HUMAN RIGHTS AND THE DCO MEMBER STATES

The global discourse on AI and human rights has evolved from theoretical discussions to urgent policy imperatives. Internationally, there is growing recognition that AI technologies pose unprecedented challenges to fundamental human rights, as presented earlier in the report; specifically, those concerning privacy, non-discrimination, and individual autonomy. Key multilateral forums, like the United Nations, OECD, and European Union, are increasingly focusing on developing comprehensive frameworks that balance technological innovation with robust human rights protections.

The DCO membership encompasses a diverse array of countries with vastly different AI landscapes. While some Member States have implemented sophisticated regulations, established dedicated AI regulators, built robust networks, and instituted academic programmes to address AI challenges, others are in the process of building their basic frameworks. Consequently, discussions about future regulations must be tailored to each state's specific status. For countries without existing data protection or AI regulations, the initiation of discussions is a positive step. Implementing data protection rules is a crucial milestone for any nation aiming to develop a robust AI framework, as privacy and data protection represent some of the most significant risks to society. The absence of safeguards against data misuse poses one of the most pressing challenges a government can face.

In Gambia, for example, in the absence of a comprehensive data protection law, the Information Act¹⁷⁰ governs some aspects of data processing and retention. It does so only within the context of information and communication services. The Public Utilities Regulatory Authority (PURPA)¹⁷¹ issued a Draft Data Protection and Privacy Policy Strategy¹⁷² in 2019 that still needs to attain legal status.

Pakistan and Bangladesh demonstrate progress in this area. Pakistan's National AI Policy draft,¹⁷³ released in November 2023, aims to raise public awareness of AI, develop the existing workforce, invest in R&D, and establish regulatory frameworks and ethical practices. Similarly, Bangladesh's draft National AI Policy 2024¹⁷⁴ outlines objectives, AI principles, implementation approaches, key development sectors, challenges, and mitigation strategies. Both countries emphasise principles such as social equity, transparency, accountability, security, sustainability, and human-centred AI in their draft policies.



A promising trend among these countries is the cross-collaboration between ICT departments and relevant ministries, industry, academia, and civil society to establish institutional frameworks for AI policy implementation. This practice should be extended and replicated, with particular emphasis on including human rights and justice authorities, which are often overlooked in favour of finance or labour ministries.

Countries with more robust legal frameworks, including concrete data protection rules and AI strategies, are beginning to establish National Artificial Intelligence authorities, such as SDAIA (Saudi Data and AI Authority) in Saudi Arabia. These bodies are tasked with organising, developing, and monitoring domestic AI-related activities, with a primary focus on creating and enforcing regulatory frameworks. The establishment of such institutions correlates strongly with investments in education, policy development, and framework creation, typically observed in countries with more advanced AI ecosystems. At the international level, recommendations have been published to set criteria for building ethical and responsible AI systems and to assess and mitigate risks. Looking ahead, the AI landscape is expected to evolve further, with more refined definitions of the AI ecosystem and clarification of different actors' responsibilities.

As countries continue to release guidelines and regulations – those described throughout section 3 – on AI system development and usage, more precise delineations of responsibility can be expected, particularly concerning the protection of specific human rights. This could lead to greater involvement of authorities beyond ICT or AI/Data Protection ministries. Additionally, forthcoming court cases linking liability to different roles in the AI value chain are expected to provide valuable insights into the evolving regulatory landscape. Global cooperation will be essential to ensure consistency and effectiveness in addressing the challenges and maximising the benefits of AI technologies.

04

CONCLUSIONS AND RECOMMENDATIONS

4.1 CONCLUSIONS

This report examined the evolving landscape of AI and its implications for human rights globally and across DCO Member States. A consistent finding across the Member States is the recognition that AI technologies, while holding immense potential for economic growth and societal benefit, also present inherent risks to human rights if not developed ethically and deployed responsibly.

The research also revealed a diverse array of approaches to AI governance, discussing the differences between soft governance and prescriptive approaches, reflecting not only the varied levels of technological advancement but also the regulatory maturity and cultural contexts within the DCO. Expectedly, as the adoption of AI and its regulation depends on the underlying economic, political, social and cultural factors of a country, AI 'readiness' varies across DCO Member States.

In terms of human rights-focused AI risks, privacy stands at the forefront of these concerns, defined as a multifaceted concept extending far beyond traditional data protection. The research highlights how AI's capacity to aggregate and interpret seemingly disparate information creates unprecedented challenges for personal autonomy. From physical surveillance to the subtle manipulation of behavioural patterns, AI technologies can potentially compromise the intricate layers of human privacy – decisional, psychological, associational, and spatial.

Equally critical is the imperative to address algorithmic bias, which threatens to perpetuate and potentially amplify existing social inequalities. The absence of robust legal mechanisms to ensure fairness in AI systems represents a significant governance gap. This challenge demands not just technical solutions but a fundamental reimagining of how technological systems are conceptualised, developed, and deployed.

The right to work and education emerges as another crucial domain where AI's impact is profound and potentially transformative in people's day-to-day lives. While AI presents opportunities for job creation and enhanced learning experiences, it simultaneously poses risks of workforce displacement and educational inequality. The report emphasises the need for proactive strategies that prioritise skills development, lifelong learning, and equitable access to AI-powered educational resources.

Where AI or related authorities demonstrate proactivity regarding technological developments, there was little evidence of collaboration between human rights stakeholders (academics, activists, journalists, judges, professors, civil society, etc.) and AI policymakers. Fostering cooperation between these groups, whether through government and non-government partnerships, public campaigns, or oœcial work, could help to incorporate human rights principles into AI governance frameworks, promote transparency and accountability, strengthen public awareness and engagement, and facilitate multistakeholder problem-solving. By fostering public-private partnerships, investing in continuous education, and creating inclusive policy development processes, DCO Member States can develop AI governance frameworks that are both innovative and fundamentally human-centric.

The path forward requires more than technological expertise – it demands a holistic commitment to human rights principles. This means creating governance structures that are not just reactive but anticipatory, not just regulatory but fundamentally ethical. As AI continues to evolve, the approach must be dynamic, adaptive, and unwavering in its commitment to preserving human dignity.

By embracing this integrated, forward-looking approach, DCO Member States can transform the potential challenges of AI into opportunities for enhanced human capabilities, societal progress, and collective well-being.

Success in protecting human rights in the AI era requires sustained commitment, adequate resources, and concrete action from all stakeholders. By implementing these recommendations within a clear timeline and with appropriate accountability measures, nations can work towards ensuring that AI technologies serve to enhance, rather than diminish, human dignity and fundamental rights.

4.2 POLICY RECOMMENDATIONS

The recommendations provided below are framed based on the analysis of human rights-based approaches to responsible AI governance in the DCO Member States. However, the suggested actions described below are equally applicable to other states concerned with this subject and dependent on the respective context and government objectives in those countries. As described in this report, the appropriate policy and regulatory response is a spectrum and there is no 'one-size-fits-all' approach.

4.2.1 Recommendations for Governments and Policymakers

Strategic Implementation Framework

1. Establish clear ethical principles and definitions through a multi-stakeholder approach to be embedded in national regulations and policies

The foundation of effective human rights protection in AI systems begins with precise and universally understood definitions and principles. Nations must prioritise the development of clear, rights-centred principles and key AI concepts within their legal and policy frameworks. These concepts should explicitly address how AI intersects with fundamental human rights, including privacy, dignity, autonomy, and non-discrimination.

For instance, when defining algorithmic transparency, the definition should encompass not only technical aspects but also the right of individuals to understand how AI systems affect their fundamental rights. Similarly, data privacy definitions should extend beyond basic data protection to address the full spectrum of privacy rights, including physical, mental, and associational privacy in the context of AI systems.

The development of these definitions should involve human rights experts, civil society organisations, and affected communities, ensuring that technical concepts are grounded in human rights principles and aligned with internal best practices to allow for wider regulatory and policy harmonisation. This participatory approach helps create definitions that protect vulnerable populations and address the potential discriminatory impacts of AI systems.



2. Harmonise AI governance for consistent rights protection

Creating compatible AI governance frameworks across DCO Member States requires a careful balance between standardisation and local context. The focus should be on establishing common human rights safeguards while respecting diverse cultural and social contexts. This harmonisation effort should prioritise:

- The development of shared human rights impact assessment methodologies that can be applied across jurisdictions. These assessments should examine how AI systems affect various rights, from freedom of expression to economic and social rights.
- The creation of cross-border remediation mechanisms for individuals whose rights have been violated by AI systems. This includes establishing clear paths for redress and ensuring that human rights protections remain consistent as AI systems operate across national boundaries.
- The implementation of joint monitoring systems to track how AI deployments affect human rights across different contexts and populations. This monitoring should inform ongoing policy development and adjustment.

3. Develop comprehensive rights-based policy frameworks

Transversal policies for AI must extend beyond technical considerations to embed human rights protection throughout the AI lifecycle. This requires integrating human rights considerations into every aspect of AI governance, from research and development to deployment and monitoring.

The national policy frameworks should address how AI intersects with existing human rights legislation and international human rights law. This includes developing specific guidelines for high-risk AI applications that could significantly impact human rights, such as AI systems used in criminal justice, healthcare, or social services.

Furthermore, policies should establish clear accountability mechanisms for human rights violations caused by AI systems. This includes defining responsibility among different stakeholders, from developers (engineers and technicians in charge of developing the AI systems) to general users, and ensuring that affected individuals have access to effective remedies.

Implementation guidelines should detail specific steps that organisations must take to protect human rights when developing or deploying AI systems. These guidelines should address issues such as:



The right to human review of significant AI decisions affecting individual rights and freedoms.



Mechanisms for identifying and mitigating discriminatory bias in AI systems.



Requirements for meaningful transparency about AI capabilities and limitations.



Protocols for protecting privacy and personal data throughout the AI lifecycle.

The success of these policies depends on regular evaluation and updates to address emerging human rights challenges as AI technology evolves. This requires establishing an ongoing dialogue between technical experts, human rights advocates, and affected communities to ensure that governance frameworks remain effective in protecting human rights in an evolving technological landscape.

These comprehensive recommendations provide a foundation for ensuring that AI development and deployment consistently uphold and promote human rights across all DCO Member States while fostering innovation and cross-border collaboration in a rights-respecting manner.

4. Establishing Foundational Governance Structures

National AI Oversight Bodies

Countries should establish dedicated AI governance bodies with explicit human rights mandates. For example, a National AI Ethics and Rights Council could be created with representation from human rights organisations, technical experts, and civil society. This council would be responsible for reviewing high-risk AI applications and ensuring human rights impact assessments are conducted before deployment.

Approaching the implementation of such a body, authorities should consider:

- Creating a legislative framework defining the council's authority and composition.
- Establishing mandatory human rights impact assessments for AI systems in critical sectors.
- Developing clear enforcement mechanisms, with penalties for non-compliance.
- Instituting regular auditing processes with public reporting requirements.

Building Human Rights Capacity – Educational Framework Development and Public Awareness

The foundation of effective human rights protection in AI systems begins with comprehensive education and capacity building across all sectors of society. A robust educational framework must be established that goes beyond basic AI literacy to deeply integrate human rights principles into all aspects of AI development and deployment.

For government officials, specialised training programmes should be developed that focus on conducting thorough human rights impact assessments of AI systems. These programmes must include practical case studies and hands-on experience in evaluating AI systems through a human rights lens. Officials should learn to identify potential human rights violations in AI applications, understand the implications of algorithmic bias, and develop strategies for protecting vulnerable populations.

Technical education programmes in universities and vocational institutions must incorporate mandatory courses on AI ethics and human rights. These courses should cover not only theoretical frameworks but also practical applications, teaching future AI practitioners how their technical decisions impact human rights. Students should learn to implement privacy-preserving techniques, develop bias-mitigation strategies, and design systems that protect user autonomy and dignity.

Public awareness campaigns should be designed through collaboration between public authorities, regulators, and civil society to educate citizens about their rights in an AI-driven world. These campaigns must go beyond simple information dissemination to actively engage communities in discussions about AI's impact on their daily lives. Citizens should understand their rights regarding automated decision-making, data privacy, and algorithmic transparency.

4.2.2 Recommendations for industry stakeholders

Industry Engagement and Accountability

Private sector participation in human rights protection requires a comprehensive approach that combines regulatory requirements with positive incentives. Companies developing AI systems must establish internal human rights review boards with the authority to influence product development decisions. These boards should include external human rights experts and representatives from affected communities.

Industry-specific guidelines, made in collaboration with trade associations, should be developed that address the unique human rights challenges in different sectors. For example, guidelines for healthcare AI systems must prioritise patient autonomy and privacy, while those for AI in criminal justice must ensure due process and non-discrimination. These guidelines should include specific technical requirements and implementation strategies.

Entities involved in developing high-risk AI systems must implement continuous human rights monitoring and regular public reporting. These reports should detail potential human rights impacts, mitigation strategies, and outcomes of human rights assessments. These entities should also establish clear mechanisms for stakeholder feedback and grievance resolution.

To encourage excellence in human rights preservation, incentive programmes should be established. These could include tax benefits, preferential government contracting, or public recognition for companies that demonstrate exceptional commitment to human rights in AI development. However, these incentives must be coupled with rigorous verification processes to prevent superficial compliance.



Technical Implementation and Oversight

1

Rights-Preserving Technical Standards

Technical requirements for AI systems must be developed with human rights protection as a core principle, rather than an afterthought. Explainability requirements should be tailored to the potential human rights impact of the system, with stricter standards for systems affecting fundamental rights, such as liberty, privacy, or access to essential services.

Privacy-preserving technical standards should address not only data protection but also the broader right to privacy in all its dimensions. This includes protection against surveillance, respect for personal autonomy, and safeguards against indirect privacy violations through data inference and aggregation.

Certification processes for AI systems in sensitive domains must include rigorous human rights testing. This testing should examine both the intended and unintended consequences of system deployment, with particular attention to impacts on marginalised communities. Certification should be an ongoing process, rather than a one-time approval, with regular reassessment as systems evolve and contexts change.

2

Monitoring and Enforcement

Effective oversight requires the development of sophisticated monitoring systems that can track both the quantitative and qualitative impacts of AI systems on human rights. This would include establishing regular auditing procedures (conducted either by internal auditors or specialised auditing consulting firms) to examine AI deployments for technical compliance and real-world human rights impacts, ensuring audit results are made publicly available to promote transparency and accountability. These audits should be adapted to expand the scope and depth of monitoring, moving beyond just technical compliance checks to thoroughly evaluate the actual, on-the-ground effects of AI systems on human rights, incorporating both quantitative metrics and qualitative assessments, and involving diverse stakeholders, including human rights experts and affected communities, in the monitoring and auditing processes.

These auditing processes must be established for both public and private sector AI deployments. These audits should examine not only technical compliance but also real-world impacts on human rights. Audit results should be publicly available to ensure transparency and accountability.

Enforcement mechanisms must include meaningful penalties for human rights violations, scaled according to the severity and scope of the violation. These penalties should be accompanied by requirements for remediation and system improvement. A structured process should be established for affected individuals and communities to seek redress for human rights violations.

The effectiveness of these measures should be regularly evaluated and updated based on emerging challenges and lessons learned. This requires establishing feedback loops between technical implementers, human rights experts, affected communities, and oversight bodies. Regular multi-stakeholder dialogues should be held to discuss evolving challenges and develop new protection strategies.

Through this comprehensive approach to building human rights capacity, organisations can work towards ensuring that AI development and deployment consistently uphold human dignity and fundamental rights while fostering innovation and technological progress.

05

ANNEX 1 METHODOLOGY

5.1 RESEARCH APPROACH AND DESIGN

This report made use of a qualitative and comparative research approach to examine AI governance frameworks globally and across the DCO Member States. The primary objective was to assess how these countries address the ethical implications of AI and its impact on human rights.

Multiple data collection methods were used, including comprehensive desk research, expert consultations, and interviews. The research incorporates global, regional, and national benchmarking to assess alignment with international norms. The comparative analysis enables the identification of best practices and challenges in AI governance, while expert input validates findings and ensures alignment with current developments. This multifaceted approach provides a nuanced understanding of how national contexts influence AI policymaking and implementation across Member States.

The research design was structured as follows:

Qualitative Research:



The study was grounded in qualitative methodologies, allowing for an in-depth exploration of the complex relationships between AI technologies, ethical considerations, and human rights. By focusing on the policies, legal frameworks, and AI strategies of the DCO Member States, the study provided a nuanced understanding of how these elements intersect.

Comparative Analysis:



A key aspect of the research design was the comparative analysis across the Member States. This approach allowed the identification of best practices, as well as the gaps and challenges that different countries face in AI governance. The comparative analysis facilitated a detailed understanding of how different national contexts influence AI policymaking and implementation.

Expert Consultation:



The research was enriched by consultations with experts in AI ethics and policymakers. These consultations provided critical insights that validated the findings and ensured that the analysis was aligned with the latest developments in AI governance.

Global, Regional, and National Benchmarking:



The study incorporated comparative analysis against global standards (e.g., OECD AI Principles), regional frameworks (e.g., African Union Continental AI Strategy), and national initiatives. The objective of this was to assess the alignment of the DCO Member States with international norms and identify areas for improvement.

5.2 DATA COLLECTION METHODS

Data for the study was collected through multiple methods, ensuring a comprehensive and robust analysis of AI governance frameworks:

1. Desk Research:

- Literature Review: A systematic literature review was conducted, focusing on academic publications, AI ethics guidelines, and reports from international organisations. This review provided the foundational knowledge required to understand the state of AI governance globally and within the DCO Member States.
- Policy and Legal Document Analysis: National AI strategies, legal texts, and policy documents from each Member State were thoroughly analysed. This analysis focused on identifying the legal and regulatory mechanisms in place to govern AI, particularly concerning human rights and ethical considerations.
- Review of Country-Specific AI Policy Developments: An in-depth investigation of AI policy implementations and partnerships in Member States was carried out.

2. Interviews:

- Design and Distribution: Where applicable, interviews were distributed to key stakeholders, including government officials, AI developers, and representatives from civil society organisations. The interviews were designed to capture perceptions of AI governance, challenges in implementation, and potential solutions for enhancing AI ethics frameworks.



06

ANNEX 2 BIBLIOGRAPHY

BIBLIOGRAPHY

- 1 Difference Between Responsible AI & ethical AI | Shaip, <https://www.shaip.com/blog/responsible-ai-vs-ethical-ai/>
- 2 Difference Between Responsible AI & ethical AI | Shaip, <https://www.shaip.com/blog/responsible-ai-vs-ethical-ai/>; Constantinescu, M., Voinea, C., Uszkai, R. et al. Understanding responsibility in Responsible AI, <https://doi.org/10.1007/s10676-021-09616-9>. Dianoetic virtues and the hard problem of context. Ethics Inf Technol 23, 803–814 (2021).
- 3 Please see section 3.2 for a detailed list of such standards.
- 4 The DCO Secretariat is currently working on a model framework, grounded in both international standards and local values, to support its Member States in navigating the complex intersection of AI and human rights.
- 5 The Riyadh AI Call for Action Declaration (RAICA), <https://dco.org/wp-content/uploads/2024/06/Riyadh-AI-Call-for-Action-RAICA-Declaration.pdf#:~:text=The%20Riyadh%20AI%20Call%20for%20Action%20Declaration%20advances,policy%20and%20bring%20efficiency%20into%20the%20ecosystem.>
- 6 Universal Declaration of Human Rights (UDHR), <https://www.standup4humanrights.org/en/declaration.html>
- 7 Universal Declaration of Human Rights (UDHR), <https://www.standup4humanrights.org/en/declaration.html>
- 8 Reference texts - The European Convention on Human Rights (coe.int), <https://www.coe.int/en/web/human-rights-convention/reference-texts>
- 9 International Covenant on Civil and Political Rights | OHCHR, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- 10 International Covenant on Economic, Social and Cultural Rights | OHCHR, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>
- 11 The Cairo Declaration, https://www.oic-oci.org/upload/pages/conventions/en/CDHRI_2021_ENG.pdf
- 12 Use of AI in online content moderation – Cambridge Consultants, <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/cambridge-consultants-ai-content-moderation.pdf?v=324081>
- 13 Speech delivered at Stanford University, USA, February 2024, <https://www.ohchr.org/en/statements-and-speeches/2024/02/human-rights-must-be-core-generative-ai-technologies-says-turk>
- 14 AI principles | OECD, <https://www.oecd.org/en/topics/sub-issues/ai-principles.html#:~:text=The%20OECD%20AI%20Principles%20are%20the%20first%20intergovernmental,AI%20that%20respects%20human%20rights%20and%20democratic%20values.>
- 15 2024 OECD Ministerial Council Meeting (MCM) has adopted revisions to the landmark OECD Principles on Artificial Intelligence (AI), <https://www.oecd.org/en/about/news/press-releases/2024/05/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html>
- 16 The UN has endorsed the Principles for the Ethical Use of Artificial Intelligence in the United Nations System, https://unseb.org/sites/default/files/2023-03/CEB_2022_2_Add.1%20%28AI%20ethics%20principles%29.pdf developed through the High-level Committee on Programmes (HLCP). Furthermore, the UN work on AI
- 17 Artificial intelligence must be grounded in human rights, says High Commissioner | OHCHR, <https://www.ohchr.org/en/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner>
- 18 Governing AI for humanity (un.org), https://www.un.org/sites/un2.un.org/files/governing_ai_for_humaniy_final_report_en.pdf
- 19 AI Governance Alliance Calls for Inclusive Access to Advanced Artificial Intelligence > Press releases | World Economic Forum (weforum.org), <https://www.weforum.org/press/2024/01/ai-governance-alliance-calls-for-inclusive-access-to-advanced-artificial-intelligence/>
- 20 Global Privacy Assembly (2018) Declaration on Ethics and Data Protection in Artificial Intelligence, https://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
- 21 Global Privacy Assembly (2020) Working Group on Ethics and Data Protection in Artificial Intelligence, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2e-Day-3-3_2f-v1_0-Ethics-and-Data-Protection-in-AI-Working-Group-Report-Final-postconf.pdf
- 22 Global Privacy Assembly (2023) Resolution on Generative Artificial Intelligence Systems, <https://globalprivacyassembly.org/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf>
- 23 Global Partnership on Artificial Intelligence (n.d.) Responsible AI, <https://gpai.ai/projects/responsible-ai>
- 24 European Commission (2023) G7 Leaders' Statement on the Hiroshima AI Process, <https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process>
- 25 OECD (2019) G20 AI Principles, <https://oecd.ai/en/wonk/documents/g20-ai-principles>
- 26 OECD (2019) AI Principles, <https://accesspartnershipuk.sharepoint.com/sites/GlobalGovernmentAdvisory/Shared%20Documents/2.%20Client%20Projects/DCO/AI%20Global%20report%20&%20HHRR%20report/Draft%20Reports/Sent%20to%20client/www.oecd.org/en/topics/sub-issues/ai-principles.html>

- 27 The Framework Convention on Artificial Intelligence - Artificial Intelligence, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- 28 The Framework Convention on Artificial Intelligence - Artificial Intelligence, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- 29 Harnessing AI to Address Asia and the Pacific's Development Needs | Asian Development Bank (adb.org), <https://www.adb.org/news/videos/harnessing-ai-address-asia-and-pacific-s-development-needs>
- 30 ASEAN Guide on AI Governance and Ethics, https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf
- 31 African Union (2024) Continental Artificial Intelligence Strategy, <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>
- 32 African Union (2013) Agenda 2063: The Africa We Want, https://au.int/Agenda2063/popular_version
- 33 Difference Between Responsible AI & ethical AI | Shaip, <https://www.shaip.com/blog/responsible-ai-vs-ethical-ai/>
- 34 Difference Between Responsible AI & ethical AI | Shaip, <https://www.shaip.com/blog/responsible-ai-vs-ethical-ai/>; Constantinescu, M., Voinea, C., Uszkai, R. et al. Understanding responsibility in Responsible AI, <https://doi.org/10.1007/s10676-021-09616-9>. Dianoetic virtues and the hard problem of context. Ethics Inf Technol 23, 803–814 (2021).
- 35 Constantinescu, M., Voinea, C., Uszkai, R. et al. Understanding responsibility in Responsible AI, <https://doi.org/10.1007/s10676-021-09616-9>. Dianoetic virtues and the hard problem of context. Ethics Inf Technol 23, 803–814 (2021).
- 36 AI Strategy and Implementation Roadmap, https://www.modee.gov.jo/NewsDetails/%D8%A7%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A9_%D8%AA%D9%82%D8%B1%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9_%D8%A7%D9%84%D8%A3%D8%B1%D8%AF%D9%86%D9%8A%D8%A9_%D9%84%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B9%D9%8A_%D9%88%D8%A7%D9%84%D8%AE%D8%B7%D8%A9_%D8%A7%D9%84%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A%D8%A9_20232027
- 37 Oman Policy for the Use of AI Systems, <https://opendata.om/wp-content/uploads/2021/07/2021-06-AI-Policy.pdf> and Ministry of Transport, Communications and Information Technology, <https://www.ita.gov.om/itaportal/Pages/Page.aspx?NID=292589&PID=1342792>
- 38 AI Ethics Report EN (sdaia.gov.sa), <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- 39 Ethics, Transparency and Accountability Framework for Automated Decision-Making - GOV.UK, <https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making>
- 40 Data Ethics Framework, <https://www.gov.uk/government/publications/data-ethics-framework>
- 41 UK Government Guidance; Understanding artificial intelligence ethics and safety, <https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety>
- 42 NAIS 2.0 Singapore National AI Strategt, <https://file.go.gov.sg/nais2023.pdf>
- 43 Examples of data breaches: **Yahoo** (2013): This breach affected all 3 billion of its user accounts. The attackers accessed account information, including security questions and answers, but not plaintext passwords or payment data, <https://www.ft.com/content/9412c2b0-a87c-11e7-93c5-648314d2c72c>. **Equifax** (2017): One of the largest credit reporting agencies in the U.S. was breached, exposing the personal information of approximately 147 million consumers. [This included Social Security numbers, birth dates, and addresses, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html](https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html). **Marriott** (2018): The personal information of around 500 million guests was compromised. The breach affected the hotel giant's Starwood brand and included names, addresses, phone numbers, and passport numbers, <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>.
- 44 AI Facial Recognition Surveillance in the UK | TechPolicy.Press, <https://www.techpolicy.press/ai-facial-recognition-surveillance-in-the-uk/>
- 45 7 Biggest Privacy Concerns Around Facial Recognition Technology | LibertiesEU | [liberties.eu, Edge Face Recognition and Privacy. Is there cause for concern?, https://liberties.eu/en/stories/facial-recognition-privacy-concerns/44518](https://liberties.eu/en/stories/facial-recognition-privacy-concerns/44518)
- 46 Facial Recognition: Balancing Tech & Privacy in A New Era | OLOID, <https://www.oloid.ai/blog/facial-recognition-and-data-privacy/>
- 47 Facial Recognition: Balancing Tech & Privacy in A New Era | OLOID, Facial Recognition in the US: Privacy Concerns and Legal Developments, <https://www.oloid.ai/blog/facial-recognition-and-data-privacy/>
- 48 Personal Data Protection Law (PDPL), <http://www.pdp.gov.bh/en/regulations.html>
- 49 Personal Data Protection Authority, <http://www.pdp.gov.bh/en/index.html>
- 50 Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 51 https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument

- 52 Data Protection Act 2012, <https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf>
- 53 Data Protection Commission – Welcome to Data Protection Commission – page under construction, <https://dataprotection.org.gh/>
- 54 Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 55 Hellenic Data Protection Authority (HDPA), <https://www.dpa.gr/>
- 56 Data Protection Law, https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf
- 57 Decision No. 42 of 2021 on Data Privacy Protection Regulation ("Data Protection Regulation"), <https://www.citra.gov.kw/sites/en/LegalReferences/Resolution-No-42-On-Data-Privacy-Protection-Regulation.pdf>
- 58 Law No. 09-08 on the Protection of Individuals regarding the Processing of Personal Data, <http://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf>
- 59 The National Commission for the Control of Personal Data Protection (CNDP), <https://www.cndp.ma/>
- 60 Nigeria Data Protection Regulation (NDPR), <https://nidta.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf>
- 61 Nigeria Data Protection Commission, <https://ndpc.ng/>
- 62 Royal Decree 6/2022 Promulgating the Personal Data Protection Law – Decree, <https://decree.om/2022/rd20220006/>
- 63 Ministry of Transport, Communications and Information Technology, https://www.mtcit.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=10153
- 64 Law No. 13 of 2016 Concerning Personal Data Protection, <https://cyrilla.org/api/files/1589439522841z89bw82q9cc.pdf>
- 65 National Cyber Governance and Assurance Affairs, <http://assurance.ncsa.gov.qa/en/privacy>
- 66 04.Law_relating_to_the_protection_of_personal_data_and_privacy.pdf, https://www.rfl.rw/docs/kifclaws/04_Law_relating_to_the_protection_of_personal_data_and_privacy.pdf
- 67 Rwanda's Data Protection & Privacy Office, <https://dpo.gov.rw/>
- 68 Saudi Arabia's Personal Data Protection Law (PDPL), [https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal Data English V2-23April2023- Reviewed-.pdf](https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-Reviewed-.pdf)
- 69 Saudi Authority for Data and Artificial Intelligence ("SDAIA"), <https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx>
- 70 National Artificial Intelligence Strategy, <https://drive.google.com/file/d/1BBOCB6r6qERMt0lzpGCfI2yS0aaMTd/view?usp=sharing>
- 71 National Charter of Ethics for Artificial Intelligence, https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/sanadapp/%D8%A7%D9%84%D9%85%D9%8A%D8%AB%D8%A7%D9%82%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A7%D8%AA%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.pdf
- 72 Data Protection Law, https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf
- 73 Bahrain Business Laws | Personal Data Protection Law, <https://bahrainbusinesslaws.com/laws/Personal-Data-Protection-Law>
- 74 Microsoft Word - Personal Data English V2-23April2023- Reviewed-.docx (sdaia.gov.sa), [https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal Data English V2-23April2023- Reviewed-.pdf](https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-Reviewed-.pdf)
- 75 Law No.13 of 2016 (ncsa.gov.qa), <https://assurance.ncsa.gov.qa/sites/default/files/library/2020-11/Law%20No.%2813%29%20of%202016%20on%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf>
- 76 News Article on data protection law, <https://www.addleshawgoddard.com/en/insights/insights-briefings/2022/data-protection/oman-data-protection-law-2022/>; New Omani Personal Data Protection Law Comes into Force - (OMAN) | GCC Board Directors Institute (gccbdi.org), <https://gccbdi.org/legal-updates/new-omani-personal-data-protection-law-comes-force-oman>
- 77 Regulation (EU) 2016/679 on the General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 78 How to avoid algorithmic decision-making mistakes: lessons from the Robodebt debacle, <https://stories.uq.edu.au/momentum-magazine/robodebt-algorithmic-decision-making-mistakes/index.html>
- 79 Robodebt: Illegal Australian welfare hunt drove people to despair - BBC News, <https://www.bbc.co.uk/news/world-australia-66130105>
- 80 Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms - Amnesty International, <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/>; Tax office algorithm led to racial profiling: Amnesty International - DutchNews.nl, <https://www.dutchnews.nl/2021/10/tax-office-algorithm-led-to-racial-profiling-amnesty-international/>
- 81 Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms - Amnesty International, <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/>; Tax office algorithm led to racial profiling: Amnesty International - DutchNews.nl, <https://www.dutchnews.nl/2021/10/tax-office-algorithm-led-to-racial-profiling-amnesty-international/>

- 82 New innovation challenge launched to tackle bias in AI systems - GOV.UK, <https://www.gov.uk/government/news/new-innovation-challenge-launched-to-tackle-bias-in-ai-systems>
- 83 Blueprint for an AI Bill of Rights, <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>
 "To be noticed that on January 20, 2025, President Donald Trump revoked Executive Order 14110, and issued a new executive order on January 23, 2025, titled "Removing Barriers to American Leadership in Artificial Intelligence." This new directive emphasizes enhancing America's global AI dominance by eliminating what it describes as "harmful" regulations imposed by the Biden administration. The Trump order directs federal agencies to review and potentially rescind policies inconsistent with its goals of fostering innovation and reducing government control over AI development. Since these documents were published after the date of finalization of this report, this information is added as complementary information."
- 84 National Charter of Ethics for Artificial Intelligence, [https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/sanadapp/%D8%A7%D9%84%D9%85%D9%8A%D8%AB%D8%A7%D9%82%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A7%D8%AA%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.pdf.](https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/sanadapp/%D8%A7%D9%84%D9%85%D9%8A%D8%AB%D8%A7%D9%82%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A7%D8%AA%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.pdf)
- 85 The Jordanian National Charter of Ethics for AI - Legal Note Nov 1 2022.pdf (karajahlaw.com), https://www.karajahlaw.com/sites/default/files/2022-11/The_Jordanian_National_Charter_of_Ethics_for_AI_-_Legal_Note_Nov_1_2022.pdf
- 86 Bahrain Pioneers AI Regulation with New Standalone Law - HyScaler, <https://hyscaler.com/insights/bahrain-pioneers-ai-regulation/>
- 87 NewsGuard "Tracking AI-enabled Misinformation: 1,110 'Unreliable AI-Generated News' Websites (and Counting), Plus the Top False Narratives Generated by Artificial Intelligence Tools", <https://www.newsguardtech.com/special-reports/ai-tracking-center/>, October 2024.
- 88 P. Verma "The rise of AI fake news is creating a 'misinformation superspreader'", <https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation/>, December 2023.
- 89 P. Verma "The rise of AI fake news is creating a 'misinformation superspreader'", <https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation/>, December 2023.
- 90 Digital Rights and Freedom Bill, <https://www.vanguardngr.com/2024/04/nhrc-others-urge-fg-to-pass-digital-rights-freedom-bill/#:~:text=Related%20News&text=Vanguard%20reports%20that%20the%20Digital,Internet%20as%20a%20fundamental%20right.>
- 91 T. Olavsrud, "12 famous AI disasters", <https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html>, October 2024.
- 92 World Economic Forum Report on Future of Jobs 2024, https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf
- 93 National AI Policy, <https://moitt.gov.pk/Detail/ZTM4Nml3MDAtZmM0OC00MzJlLThhODAtMWVhNWE4MmJmMDU5>
- 94 National AI strategy, https://knowledge4policy.ec.europa.eu/sites/default/files/cyprus_ai_strategy.pdf
- 95 Cyprus Human Resource Authority (AnAD), <https://www.anad.org.cy/>
- 96 National Artificial Intelligence Strategy, <https://drive.google.com/file/d/1BB0CB6r6qERMt0lzpzGC-fl2yS0aaMTd/view?usp=sharing>
- 97 AI in Education Definition and Meaning | Top Hat: AI_Literacy_Taxonomy.pdf, https://era.library.ualberta.ca/items/a5437b82-eac3-4859-81cf-98e8e3d37c24/view/f41f0931-f25f-4730-bf62-9469094a4092/AI_Literacy_Taxonomy.pdf
- 98 What is AI Literacy? | Data Literacy, <https://dataliteracy.com/what-is-ai-literacy/>
- 99 National Artificial Intelligence Strategy, <https://drive.google.com/file/d/1BB0CB6r6qERMt0lzpzGC-fl2yS0aaMTd/view?usp=sharing>
- 100 Kwame Nkrumah University of Science & Technology, <https://www.knust.edu.gh/search/node?keys=Artificial+intelligence>
- 101 FMCIDE, <https://fmcide.gov.ng/initiative/nais/>
- 102 Carnegie Mellon University (CMU) and the Mastercard Foundation, in collaboration with the Government of Rwanda, <https://mastercardfdn.org/carnegie-mellon-university-and-mastercard-foundation-partner-to-drive-youth-led-digital-transformation-in-africa/> announced a transformational investment in higher education and innovation in Africa to catalyse opportunities for 10,000 young people from economically disadvantaged communities—particularly young women, young people with disabilities, and forcibly displaced young people—and to drive inclusive development.
- 103 Morocco announced the establishment of two schools for artificial intelligence, <http://Morocco announced the establishment of two schools for artificial intelligence>
- 104 Faculty at King Abdullah II School of Information Technology, part of the University of Jordan, established the first Department of Artificial Intelligence in the country. The faculty members here are leading research and education in AI, <https://www.jordantimes.com/news/local/jordan-excel-s-ai-achieves-advanced-places-international-ranking-%E2%80%93oecials>

- 105 Bahrain Polytechnic has launched the Artificial Intelligence Academy, https://bahrain.bh/wps/portal/ar/BNP/HomeNationalPortal/ContentDetailsPage/!ut/p/z0/nc4xT8MwEAXgv3IMGZHdByUio1IJUGkKD1UjnOyb7W0aeOW-DfE5gQ3djnZ6ePgHEWijWJ7i6UDth7xRxXZ0fy3L6Z2U1fxqL9eb56L2XIkI4tcvOgoHoT6XSofq7ksVuV0Mp7M8lWVf6_Q7nBQt0KZwAk_kljX3G2RM6nrcEyQHMKe2DahzWStXdTEBB4t9f7H0mcy4nBiAyl0ZlzsHPkGilmX-r-Gc-j_DNCQpaQ92HDCyC1ygl04RsbPc5Duuh0ccMDGN8BW4x2GISExnHwwRL2otsv3i7V5uIL7LKaYg!!/ in collaboration with Tamkeen and Microsoft. It is the first of its kind in the Middle East and represents an educational platform that provides integrated and specialised programmes aimed at enhancing innovation and creativity capabilities in the field of artificial intelligence.
- 106 I. Lopez, "UnitedHealthcare Accused of AI Use to Wrongfully Deny Claims (1)", <https://news.bloomberglaw.com/health-law-and-business/unitedhealthcare-accused-of-using-ai-to-wrongfully-deney-claims> November 2023.
- 107 WEF article: AI is being integrated into the healthcare sector through partnerships that aim to improve patient care and streamline medical processes, <https://www.weforum.org/agenda/2024/01/public-private-partnerships-ai-reskilling/>
- 108 Avey, https://www.bing.com/aclick?ld=e8ICIVLRqzHhTDxt0mNPUDDVUCUy0m44xC6WmcYn4BTa_8ga4ubb765GKN0wl_-fa0qDchXPpc61wlfBVvfTpdmckN3k9aL5hKSNmDoYxnU_kFQICMRkfud2HGRsYAHnyj2QT6cImZQFJ10psWDbeg-0hLjswSJ4IfRUHufiN6rLQYE5&u=aHR0cHMlM2ElMmYlMmZib29taS5jb20lMmZjb250ZW50JTJmcmVwb3J0JTJmZ2FydG5lc1mbGV4LXJlcG9ydC1ob3ctdG8tcGlzb3QtZ2VuZXJhdGI2ZS1haSuYZiUzZhV0bV9zb3VY2UIM2RiaW5nJTI2dXRtx21lZG1bSuZzhBhaWRzZWFnY2gIMjZhZf9wbGF0Zm9ybV9pZCuZDQ5NDE5MjE0Mi0xMj95MDQ2NTE0MDQ0MjMwLtc4MDY1NTM2NjExOTU1JTI2dXRtx2NhbxBhaWduJTNKRU1FQSUYNTlwLSuyNTlwR5HJT1MjAtJTI1MjBTZWFnY2gIMjUyMC0lMjUyME5vbi1CcmFuZCuYNTlwLSuyNTlwQm9vbWkIMjUyMEFJJT2dXRtX2tlexdvcmlM2RhcnRpZmljaWFsJTI1MjBpbnRlbGxpZ2VuY2UIMjUyMGljJTI1MjBidXNpbmVzcyUyNI9idCUzzDc4MDY1NTM2NjExOTU1JTI2X2JrJTNkYXJ0aWZpY2lhbcUyNTlwA50ZWxsawdIbmNIJTI1MjBpbjUyNTlwYnVzaW5l3MIMjZfYm0lM2RwJTI2X2JuJTNkbyUyNI9iZyUzZDeyNDkwNDY1MTQwNDQyMzAlMjZtc2Ns2lkJTNkMtgyZwvIMTM3NmE1MTRm0GjiY2M4OGI4ZDBiZTExMzl&rlid=18eee1376a514f8bbcc88b8d0be1132
- 109 Chestify AI Labs, <https://www.chestifyai.com/about.html>
- 110 IKI Project, <https://eecentre.org/2019/05/01/iki-project>
- 111 World Economic Forum, "9 ways AI is helping tackle climate change", February 2024, <https://www.weforum.org/stories/2024/02/ai-combat-climate-change/>
- 112 Space Intelligence, <https://www.space-intelligence.com>
- 113 World Economic Forum, "9 ways AI is helping tackle climate change", February 2024, <https://www.weforum.org/stories/2024/02/ai-combat-climate-change/>
- 114 Environmental Sustainability Report 2024, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1lMjE>
- 115 Environmental Report 2024, <https://www.gstatic.com/gumdrop/sustainability/google-2024-environmental-report.pdf>
- 116 A. Shah "Generative AI to Account for 1.5% of World's Power Consumption by 2029" <https://www.hpcwire.com/2024/07/08/generative-ai-to-account-for-1-5-of-worlds-power-consumption-by-2029/>, July 2024.
- 117 D. Patterson, J. Gonzalez, Q. Le ET al. "Carbon Emissions and Large Neural Network Training", April 2021.
- 118 The Jordanian National Charter of Ethics for AI - Legal Note Nov 1 2022.pdf (karajahlaw.com), https://www.karajahlaw.com/sites/default/files/2022-11/The_Jordanian_National_Charter_of_Ethics_for_AI_-_Legal_Note_Nov_1_2022.pdf
- 119 National Charter of Ethics for Artificial Intelligence, https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/sanadapp/%D8%A7%D9%84%D9%85%D9%8A%D8%A%D8%A7%D9%82_%D8%A7%D9%84%D9%88%D8%D8%D9%86%D9%8A_%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A7%D8%AA_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%BD%D9%86%D8%A7%D8%BD%D9%8A.pdf
- 120 NEOM, Saudi Arabia's megacity project, is leveraging AI to address various environmental challenges, <https://www.neom.com/en-us/our-business/sectors/energy>
- 121 Palmear – Using AI and acoustics to detect pests in agriculture, <https://www.palmear.ai/>
- 122 Art. 24 and 27 of the Universal Declaration of Human Rights, <https://www.ohchr.org/en/press-releases/2018/12/universal-declaration-human-rights-70-30-articles-30-articles-article-24>
- 123 N. Sherman, "World's biggest music labels sue over AI copyright", <https://www.bbc.co.uk/news/articles/ckr8yelvo> June 2024.
- 124 Google Arts & Culture, <https://artsandculture.google.com/>
- 125 Impact of AI on Cultural Heritage Preservation - Christos Chiotis Personal Blog, <https://chiotis.eu/impact-of-ai-on-cultural-heritage-preservation.html>
- 126 AI and African Cultural and Heritage Preservation – Convergence, <https://convergenceai.io/ai-and-african-cultural-and-heritage-preservation/>

- 127 Qatar's National AI Strategy, https://www.mcit.gov.qa/wp-content/uploads/sites/4/2025/02/national_artificial_intelligence_strategy_for_qatar_2019_en.pdf?csrt=9376201623329387066
- 128 AI Ethics Report EN (sdaia.gov.sa), <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- 129 AI Ethics Self-Assessment (sdaia.gov.sa), https://dgp.sdaia.gov.sa/wps/portal/pdp/services/servicesdetails/AIEthicsAssessment!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfjo8zijQJdHA2dTAWNA4zC3AzMHC0CQ8L8A41MzMz0g1Pz9L30o_ArAppiVOTr7JuH1WQWJKhm5mXlq8f4ejpWpKRmVzsWFycWlycm5pXoI-Q7R40ANZK2lw!/
- 130 "Any public entity, natural person or private legal person that specifies the purposes and manner of processing personal data, whether the data is processed by that controller or by the Processor." The Rules Governing the National Register of Controllers Within the Kingdom, <https://sdaia.gov.sa/Documents/TheRulesGoverningTheNationalRegisterOfControllersWithinTheKingdomPublicEN.pdf>
- 131 ASEAN Guide on AI Governance and Ethics, https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf
- 132 African Union (AU) Continental AI Strategy, <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>
- 133 G-20 AI Principles (G20 New Delhi Leaders' Declaration), <https://www.caidp.org/resources/g20/#:~:text=The%20G20%20guidelines%20call%20for,and%20internationally%20recognized%20labor%20rights.>
- 134 OECD AI Principles, <https://oecd.ai/en/ai-principles>.
- 135 United Nations Principles for the Ethical Use of Artificial Intelligence, <https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system#:~:text=It%20is%20intended%20to%20be,data%20governance%3B%20human%20autonomy-%20and>
- 136 Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- 137 European Union (EU) AI Act, <https://artificialintelligenceact.eu/ai-act-explorer/>
- 138 G7 Hiroshima AI Process, <https://www.soumu.go.jp/hiroshimaiprocess/en/documents.html>
- 139 United Nations (UN) Roadmap for Digital Cooperation, <https://www.un.org/en/content/digital-cooperation-roadmap/>
- 140 UNESCO Recommendation on the Ethics of Artificial Intelligence, <https://www.unesco.org/en/articles/unescos-recommendation-ethics-artificial-intelligence-key-facts?hub=32618>
- 141 Global Privacy Assembly (GPA) Declaration on Ethics and Data Protection in AI, https://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
- 142 United Nations Global Digital Compact, <https://www.un.org/techenvoy/global-digital-compact>
- 143 Council of Europe (COE) Convention 108+, <https://www.coe.int/en/web/data-protection/convention108-and-protocol>
- 144 European Commission Ethical Guidelines for Trustworthy AI, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- 145 For instance, the right to individual privacy can clash with the right to security and health in the case of accessing health data to determine the origin or control of a pandemic, or to prevent security threats.
- 146 FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence | The American Presidency Project, <https://www.presidency.ucsb.edu/documents/fact-sheet-president-biden-issues-executive-order-safe-secure-and-trustworthy-artificial>
- 147 Provisions on the Administration of Deep Synthesis Internet Information Services, <https://www.chinalawtranslate.com/en/deep-synthesis/>
- 148 Full text of this document has not been found online.
- 149 Bahrain AI Procurement Guidelines, <https://www.bahrain.bh/wps/wcm/connect/50050309-efa0-4302-9a5f-6549a6c1fe38/Bahrain+AI+Procurement+guidelines.pdf?MOD=AJPERES&CVID=o8QbKtN>
- 150 Draft National AI Policy 2024, <https://www.bahrain.bh/wps/wcm/connect/50050309-efa0-4302-9a5f-6549a6c1fe38/Bahrain+AI+Procurement+guidelines.pdf?MOD=AJPERES&CVID=o8QbKtN>
- 151 National AI strategy, https://knowledge4policy.ec.europa.eu/sites/default/files/cyprus_ai_strategy.pdf
- 152 National Artificial Intelligence Strategy, <https://drive.google.com/file/d/1BB0CB6r6qERMt0lzpzGC-fl2yS0aaMTd/view?usp=sharing>
- 153 Law N.4961/2022, <https://www.taxheaven.gr/law/4961/2022>
- 154 National Strategy for AI, https://digitalstrategy.gov.gr/project/ethniki_stratigiki_texnitis_noimosinisi
- 155 AI Strategy and Implementation Roadmap (2023-2027), https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/40435648.pdf
- 156 National Artificial Intelligence Strategy, https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf
- 157 Ministry of Transport, Communications and Information Technology, <https://www.ita.gov.om/itaportal/Pages/Page.aspx?NID=292589&PID=1342792>
- 158 Policy for the use of AI systems, <https://opendata.om/wp-content/uploads/2021/07/2021-06-AI-Policy.pdf>

- 159 National AI Policy, <https://moitt.gov.pk/Detail/ZTM4Nml3MDAtZmM00C00MzJlLThhODAtMWVhNWE4MmJmJmDU5>
- 160 Qatar's National AI Strategy, https://www.mcit.gov.qa/wp-content/uploads/sites/4/2025/02/national_artificial_intelligence_strategy_for_qatar_2019_en.pdf?csrt=9376201623329387066
- 161 Guidelines for Secure Adoption and Usage of 2024 Version 1.0 Artificial Intelligence, https://assurance.ncsa.gov.qa/sites/default/files/publications/policy/2024/CSSP_Guidelines_for_Secure_Usage_and_Adoption_of_Artificial_intelligence-Eng-v1.0.pdf
- 162 National Artificial Intelligence Policy for Rwanda, https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_national_Artificial_intelligence_Policy.pdf
- 163 National Strategy for Data & AI, <https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx>
- 164 AI Ethics Principles, <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- 165 Although Greece falls under the EU AI Act, the country has not enacted a national strategy yet, as it is still under discussion as a draft version.
- 166 Draft National Code of Ethics for Artificial Intelligence of Jordan
- 167 The Jordanian National Charter of Ethics for AI - Legal Note Nov 1 2022.pdf (karajahlaw.com), https://www.karajahlaw.com/sites/default/files/2022-11/The_Jordanian_National_Charter_of_Ethics_for_AI_-_Legal_Note_Nov_1_2022.pdf
- 168 Oman Vision 2040, <https://www.oman2040.om/vision?lang=en>
- 169 AI Ethics Report EN (sdaia.gov.sa), <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- 170 Information Act, <https://pura.gm/wp-content/uploads/2021/02/IC-Info-Comms-Act-2009.pdf>
- 171 Public Utilities Regulatory Authority (PURA), <https://pura.gm/>
- 172 Draft Data Protection and Privacy Policy Strategy in 2019, <https://platform.dataguidance.com/legal-research/public-utilities-regulation-authority-draft-data-protection-and-privacy-policy-and>
- 173 National AI Policy draft, <https://moitt.gov.pk/Detail/ZTMM4NmI3MDAtZmM00C00MzJlLThhODAtMWVhNWE4MmJmJmDU5>
- 174 Feasibility Study of National Centers of Research Innovation and Entrepreneurship in Artificial intelligence and Allied Technologies (NCRIE-AI), <https://www.moitt.gov.pk/SiteImage/Misc/files/National%20AI%20Policy%20Consultation%20Draft%20V1.pdf>



Follow us on

   @dcorg |  www.dco.org

© 2025, The Digital Cooperation Organization, all rights reserved.