Call for input to the High Commissioner's report on "the right to privacy in the digital age"

Global Partners Digital submission
June 2022

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights. We work with a consortium of civil society organisations from around the world engaged in advocacy work on issues relating to emerging technologies, particularly artificial intelligence (AI). This submission has been prepared in collaboration with Derechos Digitales, Transparência Brasil, Paradigm Initiative Nigeria (PIN), the Nigeria Network of NGOs (NNNGO) and Fundación Karisma.

Introduction

We welcome the opportunity to respond to the Office of the High Commissioner for Human Rights' call for input to inform the development of the upcoming thematic report on the right to privacy in the digital age. There is a pressing need to further examine trends and challenges with regard to the promotion and protection of the right to privacy in the digital age, as well as related human rights principles, safeguards and best practice.

In this joint response, we share insights on a number of the issues set out in the consultation as they relate to artificial intelligence (AI). We draw on our expertise and ongoing engagement on these issues, including through collaboration with civil society organisations who engage with national governments and international forums to advance human rights-respecting approaches to AI.

We also provide a set of recommendations at the end of this submission.

Response

Artificial intelligence and the right to privacy: challenges and trends

It is widely acknowledged that AI may provide specific benefits for human rights, including the right to privacy.[1] AI may be used, for example, to protect the confidentiality of data from unauthorised access by criminals - detecting cybersecurity threats and swifty enacting automated responses when necessary to avoid data breaches.[2] Certain AI systems may therefore help protect individuals' right to privacy by ensuring that they retain control over their personal information or communications. AI may also have positive impacts on a range of other rights, such as the rights to health and education.

However, the development and deployment of AI systems by public, private and other non-governmental actors presents unique challenges for the right to privacy in the digital age. This is because AI systems rely on the collection and processing of massive amounts of data - including potentially sensitive or personal data - that is often obtained through devices, online services, or even in public places without individuals' knowledge or consent. AI systems may be used to infer private or sensitive information based on available data, including the inference of sensitive health information.

AI systems may be used to identify or monitor individuals who wish to remain anonymous or who could see their security threatened by their identification. AI systems employed for surveillance purposes, including mass biometric surveillance in public spaces or in migratory contexts, among others, are especially concerning due to their potentially disproportionate impact on individuals' right to privacy.

AI may pose risks to the enjoyment of a number of other human rights, particularly those which are closely linked with the right to privacy. The right to privacy is often considered a gateway for the exercise of the right to freedom of expression as it enables individuals to communicate privately and fully express themselves without adverse repercussions. AI systems that identify and monitor individuals may produce a chilling effect for freedom of expression and encourage individuals to engage in self-censorship, as well as deterring peaceful assembly and association.

---

[1] United Nations Human Rights Council, "The right to privacy in the digital age" resolution adopted 7 October 2021, A/HRC/RES/48/4.

[2] *See,* Brandon W. Jackson "Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense", 21 Minnesota Journal of Law, Science & Technology 169 (2019).

Moreover, AI systems can have discriminatory impacts that endanger individuals' rights to equality and non-discrimination. AI decision-making is based on existing datasets, which, even if permissible obtained, are often biassed or flawed. The outputs of AI systems may therefore exacerbate historical patterns of discrimination, chiefly against marginalised groups. This is particularly concerning when AI systems are used in law enforcement, national security or criminal justice purposes.

Applicable frameworks

While AI may pose risks to the enjoyment of human rights, existing international and regional human rights frameworks are already applicable to the development and use of AI. The specific provisions and rights guaranteed under these frameworks, such as the right to privacy, equality and non-discrimination and effective remedy, apply to many of the challenges posed by these technologies.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family home or correspondence, nor to unlawful attacks on his honour and reputation. Article 2(3) of the ICCPR provides that any person whose rights or freedoms are violated shall have the right to an effective remedy, which would extend to violations that stem from AI. These rights apply to everyone as the right to equality and non-discrimination is protected by various provisions of the ICCPR, including Articles 2(1), 3 and 26. The United Nations Guiding Principles on Business and Human Rights (UNGPs) further clarify the role of the state and the responsibilities of the private sector when it comes to businesses' impacts on human rights. There are also issue-specific frameworks, such as those relating to data protection and non-discrimination, which apply to the development and use of AI.

These frameworks set out obligations and human rights protections which apply to the use of AI and the right to privacy, but they do not always account for the intricate features and unique challenges posed by these technologies. AI systems are complex and may pose challenges for humans when it comes to identifying and understanding the reasoning behind a particular outcome, particularly when decisions are made through reinforced learning. It is therefore more difficult to assess or assign responsibility and rectify specific human rights concerns. The risks which stem from this opaqueness and lack of transparency of AI systems are compounded by their ubiquity. Individuals may be unaware that they are either interacting with an AI system or being impacted by its deployment. This makes it extremely difficult for individuals to challenge violations of privacy and discriminatory impacts or seek effective remedies.

Legislative and regulatory developments

States are actively working to address many of these unique challenges through the modification of existing frameworks or the development of new AI-specific frameworks or instruments. The European Commission is currently developing a Regulation on artificial intelligence (known as the Artificial Intelligence Act), which seeks to regulate AI systems according to risk — including the prohibition of those posing an unacceptable risk. The Council of Europe is simultaneously working to develop a separate legal framework to regulate AI. There has also been a proliferation of non-binding frameworks, instruments and guidelines on AI in recent years such as UNESCO's Recommendation on the Ethics of AI and the OECD's Principles on Artificial Intelligence. These are complemented by efforts at the national level to develop National AI Strategies and either modify or adopt data protection frameworks that apply to AI.

We and many other civil society organisations have concerns over these developments, including for binding and non-binding instruments. We maintain that they do not go far enough to safeguard human rights, are not informed by a holistic understanding of AI and existing frameworks, and do not adequately consider the perspectives or involvement of relevant stakeholders, particularly those from the global south and the civil sector. There are concerns that this may result in the development of frameworks that are not adequate for specific regions or do not sufficiently mitigate risks to human rights. This is compounded by concerns relating to the inadequacy of existing data protection frameworks in the context of AI and the inability of the state to provide effective and meaningful oversight.

There are specific concerns, for example, that the EU is not going far enough in its proposed prohibitions on certain AI systems, with civil society advocating for a ban on the use of facial recognition and social scoring by both private and public actors.[3] These perspectives have been similarly expressed by the UN High Commissioner for Human Rights, who has called for a moratorium on the use of facial recognition technology in the context of peaceful protest until states meet certain conditions including human rights due diligence before deployment.[4] Civil society organisations have voiced concerns over the Council of Europe's ongoing efforts to develop a new legal framework on AI due to its potential exclusion of AI systems for national security purposes and dual use systems.[5] The UNESCO

[3] EDRi, "EU's AI proposal must go further to prevent surveillance and discrimination", 21 April 2021, https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination/

[4] Office of the United Nations High Commissioner for Human Rights, "New technologies must serve, not hinder, right to peaceful protests, Bachlete tells States", Press Release, 25 June 2020.

[5] Joint Civil Society Statement ahead of the Inaugural Meeting of the Committee on Artificial Intelligence (CAI) at the Council of Europe, 4 April 2022, https://algorithmwatch.org/en/joint-statement-council-of-europe-negotiations/

Recommendation on the Ethics of AI has been criticised by some stakeholders who argue that the development of an alternative "ethical" approach to AI may imply that the international human rights framework is inappropriate or insufficient, without first considering how it applies and identifying where further clarification is needed.

Safeguards, best practice and other considerations

There is therefore a clear need for the international community to further consider the applicability of relevant legal frameworks and address any gaps when it comes to the human rights impacts of AI. Frameworks should require, where appropriate, meaningful consent to individuals whose data is used in AI technologies, including the ability to withhold consent. They should impose meaningful safeguards on the type of data that may be processed, inferred or further used by third parties.

Frameworks must ensure useful and meaningful transparency in the development and deployment of AI technologies, suitable for audiences including users and regulatory bodies. There should be provisions that promote the explainability of decision-making processes to ensure they are less opaque. Frameworks must not simply provide a basis for remedy, but ensure effective remedies from public, private and other non-governmental actors when human rights are adversely impacted by AI.

Red lines, or prohibitions on certain AI systems should also be established to restrict the use of AI systems in circumstances where risks to human rights, including the right to privacy, cannot be sufficiently mitigated. This should include, for example, AI systems that are exploitative of certain vulnerable groups such as children or persons with disabilities, causing harm. It is imperative that these frameworks, and any bans or moratoriums, be developed through multistakeholder approaches that involve all relevant actors.

There is some evidence of best practice and positive developments taking place at the international, regional and national levels. There have been notable efforts to better understand AI and fully recognise the need to protect individuals' rights to privacy in the digital age. In addition to the work being carried out by the Office of the High Commissioner for Human Rights, the African Commission on Human and Peoples' Rights has called for the need to undertake a study of human and people's rights and artificial intelligence, robotics and other new and emerging technologies in Africa.[6] Countries in Latin America, including Argentina, Mexico and Uruguay, have recently adopted the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal

[6] African Commission on Human and Peoples' Rights (Commission), 473 Resolution on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa - ACHPR/Res. 473 (EXT.OS/ XXXI) 2021.

Data. These developments highlight the ability of states to better safeguard the right to privacy in response to increasing levels of automatic processing of personal data by the public and private sectors.

We have also seen major players in the industry developing corporate frameworks on AI and carrying out due diligence processes, both as individual companies and through initiatives such as the Partnership on AI to Benefit People and Society.[7] These are welcome developments, but they should be matched by more widespread and systematic efforts to undertake human rights impact assessments that adequately assess the actual and potential impacts on the right to privacy throughout the life cycle of the AI system. Such efforts should be complemented by processes which assess whether business models themselves may create risks to human rights.

States, companies and other non-governmental actors must ensure that due diligence efforts are complemented by meaningful oversight and transparency, which should include those with expertise in technical and human rights issues. The development and implementation of these approaches should involve all relevant stakeholders, particularly those in the global South and those most likely to be adversely impacted by AI.

Recommendations

Recommendations for states

States should acknowledge their obligations to respect, protect and promote the right to privacy in the context of AI. This extends to the development, deployment and use of AI systems, which must be consistent and compliant with existing international and regional human rights laws and standards.

States should develop, implement and effectively enforce data protection legislation as an essential prerequisite for the protection of the right to privacy in the context of AI, whilst also recognising that these frameworks do not mitigate against all potential interferences or challenges which stem from the development or use of AI.

[7] For example, 'Microsoft AI Principles' and 'Artificial Intelligence at Google: Our Principles'. *See also,* The Partnership on Artificial Intelligence to Benefit People and Society.

States should consider existing frameworks applicable to AI, and use these as a starting point to guide the development of any additional frameworks which seek to address the unique challenges posed by AI.

States should ensure an open, inclusive and transparent approach during the development of legal and regulatory frameworks on AI to address political, socioeconomic and regional inequalities, engaging all relevant stakeholders.

States should undertake impact assessments for the development, public procurement and deployment of AI technologies which specifically consider the right to privacy. This should involve some degree of participation by multiple stakeholders including civil society.

States should mandate companies and other non-governmental actors to undertake human rights impact assessments for AI technologies which specifically consider impacts on the right to privacy.

States should ensure that legal frameworks require, where appropriate, meaningful consent to individuals whose data is used in AI technologies, including the ability to withhold consent. They must also ensure useful and meaningful transparency in the development and deployment of AI technologies, suitable for users and regulatory bodies.

States should ensure that datasets used by AI systems in different sectors - from policing, criminal justice and migration to employment, health and education - do not result in discriminatory outcomes.

States should ensure that AI systems which interfere with the right to privacy are only permitted when the interference is provided by law, pursues a legitimate aim recognised under international human rights law, is proportionate and is no more than what is necessary to achieve the legitimate aim.

States should ensure that legal frameworks provide effective remedies from public, private and other non-governmental actors when human rights are adversely impacted by AI technologies.

States should establish prohibitions on certain AI systems, to restrict the use or deployment where risks to human rights, including the right to privacy, cannot be sufficiently mitigated.

Recommendations for companies

Companies and other non-governmental actors should engage in human rights due diligence efforts in the context of AI design, development and deployment which identify, prevent, mitigate and account for how they address their impacts on human rights. Privacy-specific efforts should also be encouraged to mitigate against the particular risks AI may pose to the enjoyment of this right, even when not mandated by regional or national frameworks.

Companies and other non-governmental actors should undertake human rights impact assessments and ensure that the findings of these assessments are fully integrated into practice through mitigation efforts and remedial actions. These findings should be made publicly available when appropriate and on a periodic basis to promote transparency.

Companies and other non-governmental actors should ensure that due diligence efforts are complemented by meaningful accountability and independent oversight which should include those with expertise in technical and human rights issues, particularly academia and civil society. The development, implementation and oversight of these approaches should involve all relevant stakeholders, including those in the global South and those most likely to be adversely impacted by AI systems.