United Nations High Commissioner for Human Rights: Right to Privacy in the Digital Age Consultation

GLOBAL PARTNERS DIGITAL

Global Partners Digital submission
May 2021

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to respond to the Office of the United Nations 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.

Global Partners Digital is actively working on artificial intelligence (AI) issues from a human rights perspective. There is a pressing need to further examine AI technologies, including the benefits and risks they pose to the enjoyment of human rights, and scrutinise trends in the adoption of laws, policies and practices by states and companies. In this contribution, we respond to the key questions posed in the call for input where we hope that, as a result of our experience and ongoing work on the issues raised, we are able to provide useful insight and perspectives. We have also provided a set of recommendations for states and companies at the end of this submission.

Consultation Questions

1. Specific impacts on the enjoyment of the right to privacy

We have seen the rapid development and increasing use of AI, particularly automated decision-making and machine learning, by both public and private actors in recent years. This trend is driven by the potential economic and societal benefits of AI technologies across a broad range of sectors. AI systems and applications may provide opportunities for the enjoyment of human rights, but also create risks, depending on the manner in which they are developed and deployed. As such, examining the human rights impacts of AI requires a careful consideration of the specific context, safeguards and objectives of AI applications.

It is widely acknowledged that AI may provide specific benefits for human rights, including the right to privacy.[1] For example, AI may be used to protect the confidentiality of data from unauthorised access by cybercriminals - detecting cybersecurity threats and swifty enacting automated responses when necessary to avoid data breaches.[2] Certain AI systems could 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 right to health. For example, AI systems may provide much needed support to healthcare systems (such as triage and treatment delivery) benefiting public health through increased efficiency and resource allocation, as well as in protecting personal medical information.

However, the international community is currently grappling with the many risks that AI poses to the enjoyment of human rights. The development and deployment of AI systems and applications by public and private actors presents unique challenges for the right to privacy. This is primarily because AI applications rely on the collection and processing of massive amounts of data - 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 identify or monitor individuals who wish to remain anonymous. AI systems employed for surveillance purposes, including mass biometric surveillance in public spaces, are especially concerning due to their potentially disproportionate impact on individuals' right to privacy and other associated rights.

AI may also pose risks to the enjoyment of a number of other rights, particularly those which are closely linked with the right to privacy. For example, the right to privacy is often considered a gateway for freedom of expression as it enables individuals to communicate privately and fully express themselves without potential repercussions. AI systems which identify and monitor individuals may produce a chilling effect for freedom of expression and encourage individuals to engage in self-censorship. Moreover, AI systems may have discriminatory impacts that pose risks to individuals rights to equality and non-discrimination. AI decision-making is based on existing datasets, which, even if permissible obtained, are often biased or flawed. The outputs of AI systems may therefore allow for historical patterns of discrimination to continue, chiefly against marginalised groups. This is particularly concerning for AI systems used in law enforcement or national security purposes.

2. Legislative and regulatory frameworks

While AI may pose risks to the enjoyment of human rights, the 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 rights to privacy, non-discrimination and effective remedy, apply to many of the challenges posed by these technologies. For example, Article 2 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

[1] United Nations General Assembly, "The right to privacy in the digital age" resolution adopted December 2020, A/RES/75/176.
[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, Scient & Technology 169 (2019).

from AI. The UN 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 data protection and non-discrimination laws, that apply to the development and use of AI. At the regional level, the EU's General Data Protection Regulation (GDPR), for example, establishes restrictions on the processing of personal data and accountability mechanisms for violations. Article 22 limits the circumstances where entities can make solely automated decisions, including those based on profiling, which produce legal or similarly significant effects on an individual.

These frameworks present obligations and human rights protections which apply to the use of AI, 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 difficult to assess or assign responsibility and rectify specific human rights concerns. As a result, states are now developing new AI-specific frameworks to address these concerns. The European Commission recently published its proposal for a Regulation on artificial intelligence (known as the Artificial Intelligence Act), which seeks to regulate AI systems according to risk—prohibiting those posing an "unacceptable" risk, imposing obligations and duties on those that are considered "high-risk", and transparency requirements on certain systems. The Council of Europe is also working to develop a legal framework to regulate AI through its Ad hoc Committee on Artificial Intelligence. UNESCO is working to adopt a Recommendation on the Ethics of AI by the end of the year. Despite its non-binding nature, this Recommendation may be influential if translated into national policy or if used to inform other ongoing efforts to develop binding frameworks.

But civil society has been critical of many aspects of these proposals, arguing that they do not go far enough to safeguard human rights and are not informed by a holistic understanding of AI and existing frameworks. Many groups have called on the EU to go further in its proposed prohibitions, advocating for a ban on the use of facial recognition and social scoring by both private and public actors.[3] Concerns have also been raised that the proposal does not address AI systems that are not considered "high-risk" but may still pose risks to human rights, for example, by imposing additional obligations on providers to conduct mandating impact assessments and mitigate identified risks. The UNESCO draft Recommendation has been criticised by stakeholders as well, who argue that the development of an alternative "ethical" approach to AI may suggest that the international human rights framework is inappropriate or unsufficient, or that it may encourage public and private actors to avoid their obligations and responsibilities under international human rights law.

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 must ensure useful and meaningful transparency in the development and deployment of AI

[3] EDRi, "EU's AI proposal must go further to prevent surveillance and discrimination" (2021), available at: eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination

technologies, suitable for audiences including users and regulatory bodies. Furthermore, any framework must not simply provide a basis for remedy, but ensure effective remedies from both the public and private sector 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 applications in circumstances where risks to human rights cannot be sufficiently mitigated, for example where they are exploitative of certain vulnerable groups such as children or persons with certain disabilities, causing harm.

3. Other safeguards and measures

In addition to these existing and proposed legal frameworks, private actors are actively involved in the development of self-governance approaches to AI. Major players in the industry have established corporate frameworks on AI, both as individual companies and through initiatives such as the Partnership on AI to Benefit People and Society.[4] But these self-regulatory approaches by business enterprises often fail to satisfy obligations set out under the "Respect" Pillar of the UNGPs which outlines how companies should implement the framework and take action to prevent and mitigate adverse impacts on human rights as a result of their products or services.

Self-governance approaches by business enterprises are primarily undertaken by larger companies, whereas small or medium sized companies, despite having the same responsibilities to respect human rights, may have fewer opportunities or resources to effectively develop or implement rights-respecting approaches to AI. Moreover, even well intentioned corporations tend to pursue the issue from a purely ethics-based perspective, which would not represent a sufficient policy commitment to meet their responsibility to respect human rights under Principle 16 of the UNGPs.

Self-governance approaches by businesses have also been criticised for failing to adequately identify and address the risks AI may pose to human rights, particularly the right to privacy. Under Principles 17 and 21 of the UNGPs, business enterprises are obliged to undertake human rights due diligence efforts to identify, prevent, mitigate and account for how they address their impacts on human rights, including through human rights impact assessments. While some companies have conducted human rights impact assessments with respect to certain applications of AI, it is uncommon for businesses to ensure that the findings of these assessments are fully integrated into practice.[5]

Human rights due diligence in the context of the development and use of AI by both state and private actors requires that relevant processes be developed to actually enable the remediation of any adverse impacts on human rights. Companies must commit themselves to adopting human rights due diligence processes for AI applications which assess their actual and potential human rights impacts, and integrating these findings through mitigation efforts and remedial actions.

---

[4] For example, 'Microsoft AI Principles' and 'Artificial Intelligence at Google: Our Principles'. See also, The Partnership on Artificial Intelligence to Benefit People and Society, available at: https://www.partnershiponai.org

[5] Lorna McGrgor and Vivian Ng, "Google's New Principles on AI Need to be Better at Protecting Human Rights" *The Conversation* (June 2018), available at: https://theconversation.com/googles-new-principles-on-ai-need-to-be-better-at-protecting-human-rights-98035

Best practice demands that impact assessments are undertaken throughout the lifecycle of an AI system, and complemented by audits and ongoing review even in the absence of legislative requirements. Assessments should be carried out with independent oversight as well, including relevant human rights and technical expertise.

Recommendations

While the recommendations below are directed towards states and companies, we recognise the important role of other stakeholders in promoting a rights-respecting approach to AI, including civil society, the technical community, and academia.

Recommendations for states:

Recommendation: 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 human rights law, principles and standards.

Recommendation: 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.

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

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

Recommendation: States should mandate that companies undertake human rights impact assessments for AI technologies which specifically consider impacts on the right to privacy. Mandatory impact assessments should also extend to the development, public procurement and deployment of any AI technologies by public sector agencies.

Recommendation: 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.

Recommendation: 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.

Recommendation: States should ensure that legal frameworks provide effective remedies from both the public and private sector when human rights are adversely impacted by AI technologies. Red lines, or prohibitions on certain AI systems, should also be established to restrict the use or deployment of AI applications where risks to human rights cannot be sufficiently mitigated.

<u>Recommendations for companies</u>:

Recommendation: Companies of all sizes should be encouraged to develop policies which explicitly acknowledge their responsibilities to respect human rights in the context of AI, as opposed to simply taking an ethics based approach.

Recommendation: Companies 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.

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

Recommendation: Companies 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. The development, implementation and oversight of self-governance approaches should involve all relevant stakeholders, including those mostly likely to be adversely affected by AI technologies.