**FOC Joint Statement on Artificial Intelligence and Human Rights**

The Freedom Online Coalition (FOC) is a group of 32 countries deeply committed to the promotion and protection of human rights and fundamental freedoms both offline and online. We are committed to working together to support Internet freedom and human rights for individuals worldwide – including the freedoms of expression, association, peaceful assembly, and privacy rights.

The FOC acknowledges that artificial intelligence (AI) systems[1] offer unprecedented opportunities for human development and innovation, with the potential to generate social and economic benefits and help protect and promote human rights and fundamental freedoms. When developed and used in full respect of human rights, AI systems can complement human endeavours across fields such as public and precision health and environmental science to improve people's lives and support the UN Sustainable Development Goals. States play a critical role in promoting these benefits for all.

As is considered with other digital technologies, AI systems can also be developed or used in ways that pose significant risks to human rights, democracy, and the rule of law. The FOC is particularly concerned by the documented and ongoing use of AI systems for repressive and authoritarian purposes, including through remote biometric identification (RBI) such as facial recognition technology,[2] as well as automated content moderation. Some states use these AI systems, often by leveraging private sector tools, to facilitate and/or mandate arbitrary or unlawful surveillance practices, and censorship practices, that are in violation of international human rights law. The application of AI systems towards repressive and authoritarian purposes can further enable and scale human rights violations and abuses.

The use of RBI and automated content moderation, especially when used by states in an unlawful or arbitrary manner, can threaten the enjoyment of human rights, including the right to equal protection of the law without discrimination and privacy rights. In particular, the use of RBI for repressive and authoritarian purposes threatens the enjoyment of the rights to freedom of religion or belief, freedom of association, peaceful assembly, and liberty of movement. Likewise, the use of automated content moderation for repressive and authoritarian purposes further threatens the enjoyment of the right to freedom of expression, including the freedom to seek, receive and impart information of all kinds, and the freedom to hold opinions without interference. This may result in a chilling effect on the right of peaceful assembly and on freedom of expression in online spaces, as well as undermine the integrity of democratic electoral processes.

The use and deployment of AI systems in ways that violate human rights, and particularly for repressive and authoritarian purposes, threatens online and offline democratic and civic spaces,

---

[1] The OECD defines an AI system as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy." OECD Legal Instruments, *Recommendation of the Council on Artificial Intelligence*, May 21, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[2] Remote biometric identification (RBI) relies on biometric information (e.g. facial images, iris scans, gait analysis) and can give governments the ability "to ascertain the identity (1) of multiple people, (2) at a distance, (3) in public space, (4) absent notice and consent, and (5) in a continuous and on-going manner." Laura K. Donohue, "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age." Georgetown Law, 2012. https://scholarship.law.georgetown.edu/facpub/1036/

including political dissent and the important work of journalists and other media workers, human rights defenders, and members of civil society worldwide. This may also further marginalize and oppress persons or groups, such as women and members of ethnic, religious and other minority communities that already face multiple and intersecting forms of discrimination.

As a first step towards the promotion and protection of human rights, states and the private sector should endeavour to promote and increase transparency, traceability, and accountability in the design, development, procurement, and use of AI systems, with appropriate protections for intellectual property. This can help reduce the opacity, inscrutability, and unpredictability of some AI systems and help stakeholders better understand how semi-autonomous AI systems make decisions. The governance, development, and application of AI systems that are grounded in respect for human rights will promote public trust to the benefit of humanity in the long-term.

The FOC reaffirms that states must abide by their obligations under international human rights law to ensure that human rights are fully respected and protected. As also noted in the UN *Guiding Principles on Business and Human Rights*, "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises."[3] We welcome multi-stakeholder attention to this issue in international fora.

**Calls to action:**

To promote respect for human rights, democracy, and the rule of law in the design, development, procurement, and use of AI systems, the FOC calls on states to work towards the following actions in collaboration with the private sector, civil society, academia, and all other relevant stakeholders:

- States should take action to oppose and refrain from the use of AI systems for repressive and authoritarian purposes, including the targeting of or discrimination against persons and communities in vulnerable and marginalized positions and human rights defenders, in violation of international human rights law.

- States should refrain from arbitrary or unlawful interference in the operations of online platforms, including those using AI systems. States have a responsibility to ensure that any measures affecting online platforms, including counter-terrorism and national security legislation, are consistent with international law, including international human rights law. States should refrain from restrictions on the right to freedom of opinion and expression, including in relation to political dissent and the work of journalists, civil society, and human rights defenders, except when such restrictions are in accordance with international law, particularly international human rights law.

- States should promote international multi-stakeholder engagement in the development of relevant norms, rules, and standards for the development, procurement, use, certification, and governance of AI systems that, at a minimum, are consistent with international human rights law. States should welcome input from a broad and geographically representative group of states and stakeholders.

[3] United Nations, *Guiding Principles on Business and Human Rights*, 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

- States need to ensure the design, development and use of AI systems in the public sector is conducted in accordance with their international human rights obligations. States should respect their commitments and ensure that any interference with human rights is consistent with international law.

- States, and any private sector or civil society actors working with them or on their behalf, should protect human rights when procuring, developing and using AI systems in the public sector, through the adoption of processes such as due diligence and impact assessments, that are made transparent wherever possible. These processes should provide an opportunity for all stakeholders, particularly those who face disproportionate negative impacts, to provide input. AI impact assessments should, at a minimum, consider the risks to human rights posed by the use of AI systems, and be continuously evaluated before deployment and throughout the system's lifecycle to account for unintended and/or unforeseen outcomes with respect to human rights. States need to provide an effective remedy against alleged human rights violations.

- States should encourage the private sector to observe principles and practices of responsible business conduct (RBC) in the use of AI systems throughout their operations and supply and value chains, in a consistent manner and across all contexts. By incorporating RBC, companies are better equipped to manage risks, identify and resolve issues proactively, and adapt operations accordingly for long-term success. RBC activities of both states and the private sector should be in line with international frameworks such as the UN *Guiding Principles on Business and Human Rights* and the OECD *Guidelines for Multinational Enterprises*.[4]

- States should consider how domestic legislation, regulation and policies can identify, prevent, and mitigate risks to human rights posed by the design, development and use of AI systems, and take action where appropriate. These may include national AI and data strategies, human rights codes, privacy laws, data protection measures, responsible business practices, and other measures that may protect the interests of persons or groups facing multiple and intersecting forms of discrimination. National measures should take into consideration such guidance provided by human rights treaty bodies and international initiatives, such as human-centered values identified in the OECD *Recommendation of the Council on Artificial Intelligence*,[5] which was also endorsed by the G20 AI Principles.[6] States should promote the meaningful inclusion of persons or groups who can be disproportionately and negatively impacted, as well as civil society and academia, in determining if and how AI systems should be used in different contexts (weighing potential benefits against potential human rights impacts and developing adequate safeguards).

---

[4] OECD, *Guidelines for Multinational Enterprises,* 2011.
http://mneguidelines.oecd.org/guidelines/

[5] OECD, *Recommendation of the Council on Artificial Intelligence*, May 21, 2019.
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[6] "G20 Ministerial Statement on Trade and Digital Economy - Annex, G20 AI Principles," June 9, 2019.
https://www.mofa.go.jp/files/000486596.pdf

- States should promote, and where appropriate, support efforts by the private sector, civil society, and all other relevant stakeholders to increase transparency and accountability related to the use of AI systems, including through approaches that strongly encourage the sharing of information between stakeholders, on topics such as the following:
    - user privacy, including the use of user data to refine AI systems, the sharing of data collected through AI systems with third parties, and if reasonable, how to opt-out of the collection, sharing, or use of user-generated data
    - the automated moderation of user generated content including, but not limited to, the removal, downranking, flagging, and demonetization of content
    - recourse or appeal mechanisms, when content is removed as the result of an automated decision
    - oversight mechanisms, such as human monitoring for potential human rights impacts

- States, as well as the private sector, should work towards increased transparency, which could include providing access to appropriate data and information for the benefit of civil society and academia, while safeguarding privacy and intellectual property, in order to facilitate collaborative and independent research into AI systems and their potential impacts on human rights, such as identifying, preventing, and mitigating bias in the development and use of AI systems.

- States should foster education about AI systems and possible impacts on human rights among the public and stakeholders, including product developers and policy-makers. States should work to promote access to basic knowledge of AI systems for all.