Human Rights Council Advisory Committee's View
on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies

The work of the Advisory Committee

1. In its 2021 report "*Possible impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights*,"[1] the Advisory Committee (*hereinafter* the Committee) recognizes that technologies should be designed with a sound understanding of the international human rights framework. It recalls the United Nations Guiding Principles on Business and Human Rights (*hereinafter* UNGPs), noting that the whole business ecosystem should abide by the human rights framework.[2]

2. The report reviews the challenges posing potential human rights violations by new technologies. It concludes that the growing importance of private companies in datafication cycles is making their human rights responsibilities greater than ever before.[3] In particular, 1) generous cookie – and data retention policies applied by private sector actors, such as major social media platforms, enabled businesses to collect a vast amount of personal information. Today, private corporations hold more personal information and data about citizens than governments. Business models that rely on user data are not easily reconciled with protecting individuals' right to privacy and minimizing the disclosure of personal data online.[4] 2) Technology-fueled empowerment is likely to continue to be uneven, aggravating existing inequalities and creating new forms of vulnerability and inequality.[5] For example, artificial intelligence decision-making may result in discriminatory outcomes based on biased algorithms even when unintended.

3. Considerable progress has been made in raising the awareness of the private companies of their human rights obligations through UNGPs. However, the Committee stresses that there is still room for improvement where innovative business models are designed.[6] It is necessary to find pragmatic ways to prevent and address human rights harms connected with the development and application of new technologies and their use, as the B-Tech project launched by OHCHR in 2019 suggests.[7] The attempts to integrate the human rights approach into technological development may face pushback when threatening profitability.[8] The competitive pressures can lead to disincentivizing businesses from human rights scrutiny on their business models, while human rights due diligence

[1] A/HRC/47/52
[2] *Ibid.*, para.13.
[3] *Ibid.*, para.56.
[4] *Ibid.*, para.19; If government authorities request access to platforms' data on individual users in breach of the right to privacy and data protection, technology companies should assess the legitimacy of such demands and disclose their processes and practices. The Danish Institute for Human Rights, Tech Giants and Human Rights: Investor Expectations (2021)
[5] A/HRC/47/52, para.23; Inaccessible technologies can be even more problematic for people with disability. Australian Human Rights Commission, Human Rights and Technology Final Report, (March 2021)
[6] *Ibid.*, para.55; Companies use new technologies like IoT or smart mobile devices to enhance productivity at the workplace. But such system can be misused to monitor employees as a form of labor surveillance.
[7] *Ibid.*, para.46.
[8] *Ibid.*, para.57.

is essential. Therefore, governments should encourage and support companies as they strive to meet their responsibilities under UNGPs and facilitate the conduct of human rights due diligence by companies.[9]

4. The report also highlights that private companies should stay updated with the human rights standards on using new technologies and subject their activities to human rights impact assessments. In addition, it is essential to carefully include the voices of all users of new technologies, especially marginalized populations, which are particularly likely to be subjected to new business models.[10]

Preliminary Comments

5. The efforts towards the practical application of UNGPs to the activities of technology companies will benefit from the outcome of the B-Tech findings regarding the four focus areas. However, an integrated approach is essential to guide countries in integrating the future B-Tech guidance within their national polices and to ensure national implementation of sustainable and equitable programs in the tech sector in accordance with this guidance. For example, measures should be preceded and assessed by due diligence and backed up by remedies and accountability.

6. Further, the efforts toward the practical application of the Guiding Principles to the activities of tech companies could potentially leverage the ongoing national activities of development priorities and cycles, planning, implementation, and reporting of the 2030 Agenda. In addition, mapping the linkages of a set of prioritized practical applications of UNGPs in prioritized technologies to the SDGs indicators could help advance momentum, including capacity building and securing funds for the practical application of the UNGPs to the activities of technology companies.

7. Finally, there is an opportunity to maximize the efforts toward the practical application of UNGPs to the activities of technology companies by developing a COVID-19 recovery prioritization matrix for each focus area. This matrix would potentially focus and prioritize national practical applications on those that advance the national COVID-19 recovery and promote the uptake of the UNGPs in the tech industry.

Addressing human rights risks in business models

8. Today, we have witnessed many technology companies' commitment, governmental declaration, and NGO reports emphasizing the need to address human rights risks in new technology business models. But there is a lack of clarity at political, legal, practical, and technical levels about what managing risks means in practice.[11] Moreover, most technology companies are not publicly reporting how their ethics initiatives prevent technologies from violating human rights. Instead,

[9] *Ibid.,* para.69.
[10] *Ibid.,* para.66.
[11] OHCHR B-Tech Report, Applying the UN Guiding Principles on Business and Human Rights to digital technologies: Overview and Scope (November 2019)

public human rights commitments appear little more than a marketing exercise to convince users that their products and platforms respect human rights.

9. First, the lack of transparency and explainability of the technology impedes effective accountability for harms caused by automated decisions, both on governance and an operational level.[12] It is often too complicated for the average user to understand the data processing algorithms of digital services. Second, not acquiring fully informed consent to use personal data threatens the right to privacy and individuals' free and informed decision-making. In addition, private companies' genereous and often unchecked data retention results in an unparalleled wealth of personal data, which will usually be monetized by selling these data to third parties. AI systems collect, analyze, and infer from these massive amounts of private or publicly available data. These data can reveal sensitive personal information like individuals' whereabouts, social networks, personal health, political affiliations, and sexual preferences.[13] Yet, little distinction is made between these sensitive personal data and other data in business practice. Third, when individuals search the internet using online platforms and search engines, AI systems make automated decisions regarding what content internet users see. Suppose AI makes it difficult for users to access diverse political views and perspectives. In that case, it threatens the individual's right to freedom of information and can cause the fragmentation and polarization of public and political opinion.[14] Fourth, AI has also been deployed by online platform companies to prevent the upload of allegedly illegal content or to monitor such content (e.g., child abuse material, hate speech, or other abuse material). But self-regulated AI content filter carries censorial power, which can bypass traditional checks and balances secured by law.[15] The problem could be further complicated by the proliferation of different ethical standards and principles that only offer partial protection from human rights violations or do not meet the standard of international human rights law. The fragmentation of standards and principles is further problematized by the fact that these companies operate in cyberspace, providing services in several countries while only providing for remedies in the originating country of the company.

Human Rights Due Diligence and End-Use

10. To undertake human rights due diligence, many states have introduced mandatory human rights due diligence (mHRDD) regimes though many different variants exist. While imposing the penalty is essential for non-compliance, it should be effective, proportionate, and dissuasive. Monitoring policies need to be updated on an ongoing basis considering the companies' due diligence efforts to mitigate risks. If companies are directly linked to specific human rights harms and fail to take meaningful steps to prevent it, appropriate remedies should be provided in consultation with the affected stakeholders.

[12] Michael Pizzi, et. al., "AI for humanitarian action: Human rights and ethics," International Review of the Red Cross, No.913, (March 2021)
[13] *Ibid.*
[14] The Danish Institute for Human Rights, Tech Giants and Human Rights: Investor Expectations (2021)
[15] Niva Elkin-Koren, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence," Big Data & Society, Vol.7 (July 2020)

11. To conduct effective supply chain and end-use due diligence, it needs to implement the procedure to identify and assess the actual and potential adverse human rights effects of the companies' services, products, supply chains, and business relations.[16] Technology companies encourage their business partners, suppliers, and contractors to observe international human rights standards and comply with their human rights management policy, if available.

12. It is recommended that technology companies 1) set and publicly report on selected indicators covering all its functions, through an annual report on their website or similar, to track and monitor performance related to the application of UNGPs in the tech industry; 2) implement and regularly review policies to prevent and mitigate adverse human rights impacts of their processes, services, and products; 3) promote capacity building through training programs and workshops with internal and external stakeholders, including end-users.

Accountability and remedy

13. The state should ensure access to the whole range of remedies by establishing state-based judicial and non-judicial mechanisms.[17] In addition, states can support non-state-based complaints mechanisms, such as establishing a human rights-related committee or ombudsman within the company. The state should raise public awareness on understanding the interactions between different remedial mechanisms in their design and operations. Special attention should be given to vulnerable groups (such as indigenous people, women, children, older persons, migrant workers, people with disability) and their possible difficulties accessing such mechanisms.

14. The B-Tech project foundational paper highlights that effective judicial mechanisms are always at the core of ensuring access to remedy.[18] While non-judicial mechanisms can play an important role, it depends on strong judicial and law enforcement processes. State-based non-judicial remedies lack legally binding force and primarily rely on the willingness of the authorities concerned. As such accessible, independent, and timely judicial remedies should be at the core of any National Action Plan (NAP). In addition, the state should further increase its implementation by encouraging relevant government institutions to participate in the procedures and standardize the processes.

15. National human rights institutions (NHRIs) can play an important role based on their human rights mandate, competencies, and legal status to strengthen both judicial and non-judicial mechanisms. NHRIs directly offer access to remedy through existing investigative and complaint procedures and can advise victims to use appropriate remedial mechanisms. They can also provide technical assistance to tech companies to set up and run operational-level grievance mechanisms.

[16] OECD Business and Finance Outlook 2021: AI in Business and Finance (2021). For example, establishment of a human rights management system, non-discrimination in employment, guarantee of freedom of association and collective bargaining, prohibition of forced labor, prohibition of child labor, responsible supply chain management, protection of local residents' human rights, and protection of consumer rights are areas to be reviewed.

[17] The Danish Institute for Human Rights, the State duty to protect against business-related Human Rights abuses (2014).

[18] OHCHR B-Tech foundational paper, Access to remedy and the technology sector: basic concepts and principles (2021)

16. Tech companies, particularly those with operations in many different jurisdictions, can encounter challenges engaging meaningfully with stakeholders in practice.[19] The lack of (swift) inter-state cooperation appears as a major source of impunity where the activities of such technology companies cross borders. [20] For example, reinforcement of cooperation between different states for criminal investigations, mutual legal assistance, exchange of information and evidence, and the execution of judgments is essential to ensure effective remedies. Such effective cooperation will benefit from high-level protection by the states of internationally recognized human rights, particularly the right to privacy, data protection, freedom of speech and information, and principles of the democratic rule of law states, such as independent and impartial judicial system.

17. At the same time, companies all too often avoid scrutiny and accountability by operating in cyberspace, accepting only accountability at the original state of business or by even detaching their operations from state jurisdictions. Consequently, victims of human rights violations are frustrated in their efforts to seek remedy or justice. The duty to care and accept accountability where services are offered should be standard duties of tech companies under the UNGPs.

The state's duty to protect, or regulatory and policy responses

18. The regulation of the activities of technology companies is increasingly fragmented with a complex arrangement of laws and standards. Moreover, various ministries, agencies, and bodies specializing in specific domains are engaged in these regulations to comply with the state's duty to protect. In practice, the level of knowledge and awareness of human rights varies across all branches of governmental structures, contributing to potential inconsistencies in how technology companies are regulated. Accordingly, States should maintain a robust policy coherence regarding digital technologies and consolidated NAPs for business and human rights. While having multi-stakeholder initiatives for communication and consultation is essential, it is important to minimize the risks of having many different human rights standards applicable to the tech industry. In this regard, co-regulation is required, which calls for more tech industry participation.[21] Co-regulation shifts the role of government from rule-making and imposing sanctions to providing incentives for implementing regulatory policies and ensuring human rights protections.

19. The state needs to create an environment where technology companies can realistically implement new technology and human rights standards. For example, most small and medium-sized enterprises (SMEs) lack the capacity for human rights management engaged in new tech industries. In this case, even with State policy and regulatory measures in place, companies can benefit from the clear direction on respecting human rights throughout their business activities in practice for their specific part of the technology sector. Therefore, the state needs to provide incentives for companies to introduce human rights management and impose sanctions for non-compliance.

[19] *Ibid.*

[20] Olivier De Schutter, Towards a New Treaty on Business and Human Rights (Cambridge University Press, 2015)

[21] Christopher Marsden, Internet Co-Regulation (Cambridge University Press 2011). Co-regulation denotes various regulatory phenomena that have in common that "the regulatory regime is made up of a complex interaction of general legislation and a self-regulatory body."

20. It is recommended that governments 1) develop or revise national digital strategies, including new and emerging technologies, to guide the practical application of UNGPs to the activities of technology companies; 2) establish an independent statutory entity that promotes safety and protects human rights in the tech industry. [22] This entity would be instrumental in improving the governance needed to strengthen the regulatory environment and execute the national strategies on new and emerging technology.

[22] An example worth recognition is in 2021 Australian Human Rights Commission's report, which has a set of recommendations for establishing an AI Safety Commissioner. *See* Australian Human Rights Commission, Human Rights and Technology Final Report, (March 2021)