Input for OHCHR report on the application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies

Introduction

Today, digital technologies are central to business and innovation. All sectors including governments, academia, civil society and the private sector largely depend on technology to deliver various products and services including in the social, economic and political realm. In their operations, technology companies have innovated various products, services and solutions, some of which pose adverse impacts to human rights. Some of these include artificial intelligence and the internet of things, cloud services, enterprise software solutions, facial recognition systems, geo-location tools, social media platforms, search engines, telecommunications and network infrastructure, wearables and fitness trackers. The digital age presents new challenges and ways of working that necessitate a review of how the United Nations Guiding Principles on Business and Human Rights (UNGPs) can be achieved in the technology sector.

Emerging Trends

Increasingly, states have become purchasers of digital technologies from technology companies to facilitate the implementation of various national programmes which present previously unforeseen risks to privacy. Some of the commonly implemented national programmes posing threats to individual privacy include mass surveillance programmes, national digital identification systems, voter registration using digital biometric systems, mandatory SIM card registration, smart cities programmes, and national video surveillance (CCTV) programmes integrating facial recognition systems.

Furthermore, digital technologies have fallen prey to legal retrogressive measures undertaken by states to physically and digitally monitor and track citizens and their activities. For instance, across Africa, countries have enacted legislation which compel telecommunications service providers to embed capability within their systems to facilitate the interception of communications by state security agencies, and the state acquisition of software and hardware equipment to facilitate surveillance and interception. In addition, some states have taken advantage of the internet and social media platforms to carry out cyber attacks, disseminate propaganda and disinformation, and censor online content. Moreover, many African governments have adopted laws limiting anonymity and the use of encryption.

Moreover, some governments continue to apply undue pressure on technology companies including social media platforms to provide personal information, take down content, and shut down the internet. Others have adopted repressive legislation to control the spread of information on social media, or to regulate internet intermediaries by placing undue liability on them for content on their platforms. During the COVID-19 pandemic, states developed various contact tracing systems and applications without adequate legal frameworks, or an assessment of the human rights impact of the applications. Also, state

responses to hold companies accountable remain ad hoc, fragmented and not aligned with international standards.

Across the continent, social media, online search, fintech and advertising companies have adopted business models that are based on surveillance capitalism and thus continue to threaten the privacy of users, in some cases without users' explicit knowledge or consent. Further, social media platforms have also contributed to the spread of harmful content online, which companies have failed to take effective measures to address. Also, social media content policies do not always adopt definitions of content that are rights-respecting, and their practices around content moderation are problematic. Content is often moderated using automated systems which lack local context, are discriminatory and embed bias. Moreover, some platforms' practices around content takedowns remain inaccessible, their content policies are not uniformly applied, and redress mechanisms do not always apply the rules of natural justice. In addition, some companies have continued to sell surveillance software and hardware to autocratic governments in the continent, which are subsequently used by state security agencies against human rights activists, government critics, and opposition leaders, which further exacerbates risks to human rights.

The total sum of the government measures coupled with the pressure imposed on tech sector players is continent-wide trade of privacy for business continuity by technology companies. This is commonly seen in state surveillance through electronic technologies, including interception of communications, hacking of information of target persons especially political dissidents, activists and human rights defenders. The tech sector has, however, not done enough to ensure that individual privacy is guaranteed for their customers. In addition, telecom operators are yet to implement their obligations and put in place measures to prioritize the needs of persons with disabilities in the continent. Some telecommunication companies have been found to share with state agencies individuals' private information without their consent. In other cases, companies do not conduct risk assessments before giving out their clients' information. Further, the accountability and transparency of the technology sector has not been visibly evident.

In a continent where strong privacy laws remain scanty, the increased usage of online platforms and social media in the absence of adequate safeguards and oversight over companies remains a critical risk for privacy rights. The enjoyment of human rights and freedoms, especially freedom of expression and access to information, association, assembly and movement have sharply declined. This is because the failure of tech companies to assure clients of their privacy has overly exposed them to threats of potential arrests, detention, prosection, torture and threats to their family members. As a result, individuals, especially the key targeted persons, have been forced to self-censor, which limits their enjoyment of fundamental human rights and basic freedoms online.

Unfortunately, human rights violations continue to become part of the roles of technology companies despite their corporate responsibility to respect human rights. Indeed technology companies are

supposed to take all measures aimed at avoiding the infringement on human rights by putting in place appropriate human rights policies and, where adverse impacts arise, immediately address them but have not actively played this role. More importantly, states need to promote respect for human rights in the technology sector.

Addressing human rights risks in business models (session one):

We recommend the following:

- Companies should meet the expectations set out in the UNGPs. The commitment to respect human rights should be integrated at all levels in the company hierarchy and embedded across all its functions and processes.
- Companies should take steps to mitigate risks within their existing business models, and continuously innovate new business models that are rights-respecting.
- There is a need for continued research to promote greater understanding of the human rights risks in technology business models in the continent.
- Multistakeholder engagement should be promoted as it is a critical avenue to promote shared understanding of the human rights risks and impacts of technology in Africa.

Human Rights Due Diligence and end-use (session two):

We recommend that companies should do the following:

- Demonstrate understanding of their commitment to respecting human rights in the context of their own operations, activities and business relationships.
- Conduct due diligence to identify, prevent or mitigate risks of harmful impact on their business.
- Demonstrate acting with due diligence and take reasonable steps to effectively avoid harm.
- Companies should conduct human rights impact assessments and audits of their practices on a regular basis.
- Ensure due diligence is conducted from the project design and development phase of new products, services and solutions, and thereafter periodically through the lifecycle including promotion, deployment, sale and use.
- Assess and monitor the effectiveness of their responses to human rights risks, with results of such assessments providing information for decision-making.
- Pay attention to the risks posed to vulnerable and marginalized groups e.g. children, ethnic minorities, indigenous communities, women, sexual minorities,persons with disabilities, women and human rights defenders.

- Review their state clients' human rights records and ensure they do not develop, sell or offer them technology products, services or solutions that contribute to or result in adverse human rights impacts.

Accountability and remedy (session three):

We recommend the following:

- Companies, including start-ups, should be transparent and accountable in how they address their human rights impact. More importantly, investors, boards, management and individual technologies play a critical role in promoting respect for human rights and the UNGPs within their business entities.
- Transparency and accountability can be enhanced through periodic reporting to external stakeholders including through public reports.
- Companies should seek to understand the needs of stakeholders who may be potentially affected by their actions. This can be achieved through the creation of platforms for open dialogue, engagement, information sharing and feedback between technology companies and experts including local academia, civil society, human rights defenders, and technologists on the company's actions in the region.
- Increasingly, decisions are being handled by automated systems, in some cases with limited oversight e.g. on content moderation on social media platforms and in complaints handling mechanisms which often fail to provide due process safeguards to users. Companies should therefore implement credible and effective mechanisms to enable reporting and handling of complaints.
- Companies should cease or prevent adverse human rights impacts and put in place effective systems or mechanisms to remedy and mitigate adverse impacts caused by their actions.
- Companies should put in place measures to monitor and promote rights-respecting and responsible business practices and culture. This can include developing rights-respecting policies, and ensure their application is consistent with international human rights standards.

The State's duty to protect, or regulatory and policy responses (session four):

We recommend that states do the following:

- Put in place administrative, policy, legislative, institutions to hold technology companies accountable for human rights violations, provide effective remedies for victims of human rights violations related to technology, require companies to conduct due diligence, and proper safeguards to protect the public from harm.

- Stop the development of laws that restrict digital rights, including freedom of expression and privacy beyond the threshold specified under international human rights law. More specifically, the laws should, at all times, meet the three-part test.
- Promote and provide incentives to businesses that adopt rights-respecting business models and ventures.
- Develop laws, policies, regulations, standards, guidance, including at the regional level to embed and ensure responsible business practices by technology companies and greater respect for human rights in the digital context.
- Promote education of the public, civil society and regulators on how to promote responsible business practices and technologies.
- Take measures to promote the use and adoption of digital technologies, and at the same time put in place measures to address the growing digital divide in the continent, including by removing barriers to internet access and digital technologies.
- Create an enabling environment to promote responsible business practices.

About CIPESA

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) works to enable African stakeholders to use ICT to improve governance and livelihoods. CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFiD, which cited the lack of easy, affordable and timely access to information about ICT related issues and processes as a key barrier to effective and inclusive ICT policy making in Africa. As such, our work responds to shortage of information, resources and actors consistently working at the nexus of technology, human rights and society.