The blog is a product of the UN Human Rights B-Tech Project and is part of a series focused on the intersection between human rights and the responsibilities of technology technology companies

Empowering human rights in the State-business nexus: Digital technologies and human rights due diligence.

Sarina Phu, Research & Program Associate, Global Network Initiative

DECEMBER 2021

As an increasing number of States have enacted or are considering legislation mandating the conduct and disclosure of company policies and processes in response to human rights risks presented by emerging technologies, more information and communications technology (ICT) companies are using human rights due diligence (HRDD) processes as part of their commitment to respect human rights. However, ongoing challenges, including confidentiality concerns, hinder the development of best practices around HRDD when it comes to sensitive business decisions that involve States as customers or partners.

A more inclusive approach at the State-business nexus could foster progress in identifying and addressing human rights risks. The B-Tech Project's foundational paper on the State Duty to Protect in the ICT sector highlights a "smart mix" of measures necessary for technology companies to respect human rights, such as through their adherence to relevant laws and implementing transparency measures. In turn, these measures "allow the State to act as a key catalyst to incentivize and drive behavioral change in the very complex and diverse technology sector."

When States are purchasers, end users, or beneficiaries of digital technologies, technology companies may have opportunities to protect users' right to privacy. Equipment vendors are often asked by their telecommunications customers to provide passive lawful interception capabilities because those customers have legal obligations to provide such capabilities to authorized government agencies. Having HRDD processes in place that flag potential sales in high-risk contexts, including by human rights experts within the company, can ensure that human rights impact assessments occur. The company can then apply conditions to the sale of products to government clients, such as contractual provisions, license conditions, or technical limitations. Such an approach can help hardware or software-as-a-service companies generate more leverage and allow for better analysis of how States use new and emerging technologies.

While declining a high-risk sale is an example of responsible company decision making, it does not necessarily prevent a rights violation if another company steps in to provide the same equipment or service, a scenario which signals the need for a more systemic, sector-wide approach to addressing human rights risks. Multistakeholder forums like the Global Network Initiative (GNI), which encourage shared learning between companies across the technology and digital service spectrum and with academics, civil society organizations, and investors, can be particularly helpful for addressing these sector-wide challenges.

Another increasingly common scenario, when States misuse social media services, can force companies to consider priorities related to content moderation, protection of the freedom of expression of users, concerns about legal and regulatory compliance, local staff safety, and the possibility of service restrictions and blockage. Take, for example, the decisions made to suspend former U.S. President Donald Trump's social media accounts for inciting violence, and the case of Brazilian President Jair Messias Bolsonaro, whose content related to medical misinformation surrounding COVID-19 was removed from social media platforms. Companies can strengthen their leverage by working to ensure clarity of approach and consistency of application and using ongoing HRDD to take local contexts into account when they apply content moderation to State officials' social media accounts and posts.

Indeed, the broad principles articulated in human rights law offer a universal framework for designing and implementing content moderation. For instance, UN Human Rights's Rabat Plan of Action emphasizes a high threshold for defining restrictions on freedom of expression, providing guidance on protecting free expression while addressing incitement to hatred. Large companies should use HRDD processes, including developing trusted relationships with local digital rights organizations, to understand and take account of local realities when applying content moderation principles, especially with respect to State actors' use of social media platforms.

Another point to note about the State-company nexus, is that there is often a lack of clarity regarding the types of data that governments have access to, along with a lack of transparency of ongoing impact assessments, including those for data protection. GNI has documented a disturbing trend of government efforts to acquire "direct access" to user data in ways that remove intermediaries' awareness of and opportunities to object to, or provide transparency about, such access. Similar concerns arise in situations where States use their influence to informally pressure ICT companies to hand over data, including through codes of conduct or public-private partnerships. As these public-private partnerships form long-term dependencies, there is often no real ability to assess the impact of that long-term process.

During the COVID-19 pandemic, contact-tracing apps provided some governments with access to citizens' data (such as geolocation, full names, phone numbers), without transparency about how this data would be handled. HRDD and human rights impact assessments should identify, avoid, mitigate, and suggest remedy for, such impacts. In

addition, more authoritative, and risk-based regulations can be implemented to enhance transparency, oversight, and accountability with regard to government uses of technology.

Other measures to protect human rights in public-private partnerships include:

- Requiring that contracts explicitly list the data that the company and government partner has access to and what kinds of processing they are allowed to conduct;
- Applying human rights impact assessments throughout the life cycle of deployment of the partnership; and
- Transparency at the forefront of the procedures, when a partnership is developed.

In conclusion, States looking to apply a "smart-mix" of regulatory measures and policy incentives to protect digital rights should be guided by deliberations involving civil society, affected groups, technology companies and other relevant stakeholders – a "smart-mix" of stakeholders consulted in addition to regulatory measures. Civil society especially can provide expertise and guidance for States and companies navigating the complexities of HRDD legislation. The GNI model is a strong example of the shared learning and impact of stakeholder consultation and engagement. Alongside civil society, states and companies hold responsibilities to ensure that all users enjoy the protection of their human rights, and the benefits of technologies - both current and those that may emerge.

** The Guiding Principles were unanimously endorsed by UN member states in 2011. They have also been affirmed by global and national business organisations, trade unions, civil society organisations and National Human Rights Institutions. This global support, including from business, makes the Guiding Principles the authoritative global framework for preventing and addressing human rights risks involving business, including in the technology sector.*