MANUSHYA
#WeAreManushyan ∞ Equal Human Beings

Manushya's Statement on the OECD Due Diligence Guidance for Responsible AI

MANUSHYA
#WeAreManushyan ∞ Equal Human Beings

Manushya's Statement on the OECD Due Diligence Guidance for Responsible AI

Dr Jean Linis-Dinco, Digital Rights Advisor, Manushya Foundation

Manushya Foundation rejects the framing that human rights violations can be classified as risks. Risk-based approach to any technological developments pits human rights side by side with manageable business uncertainties. Manushya Foundation has consistently witnessed how AI harms travel down supply chains and across borders to hit those with the least power the hardest. And oftentimes, in our work, we have seen how the language of risk makes human rights disappear entirely to the point where violations suddenly become probabilities that can be managed, mitigated or even worse, accepted as part of our sacrifice towards a 'better future'.

All these things happen whilst the global AI industry continues to line the pockets of a small class of people whose technological empires were built on the plunder of human creativity and the arts, and whose technologies make possible the creeping global fascism that we are witnessing today. It is from this grassroots reality that we, at Manushya Foundation, approached the guidance and the request for inputs. And it is from this very same position that we must say how the guidance, as it currently stands, is organised around the wrong question. When a framework opens by assuring us that responsible AI (if ever such a thing exists) creates 'competitive advantage' and how trust 'translates into commercial success', we already know everything we need to know about whose interests the guidance is organising its logic for. Such language not only subordinates the question of who is harmed, but also relegates people as 'risks' to manage in exchange for reputation and market access.

The AI industry's energy consumption is growing at a rate that is outpacing every efficiency gain the same industry claims to be making. A single query to a large language model uses approximately 30 times the energy to generate slop as opposed to extracting it from a source. Multiplied across the user bases of BigAI, we are seeing an enormous and rapidly escalating energy demand that is being met, in significant part, by fossil fuel generation, including by the reopening of fossil fuel plants to power data centre expansion. We, as a civilisation, have abandoned our 2030 goals in exchange for a technology that steals water from Indigenous communities. We have a word to fitly describe what happens when more powerful forces arrive and declare the land and resources available for extraction. AI did not invent colonisation; instead, it has given it a new meaning with fancy words such as digital transformation. The colonisers arrived wearing new clothes, pretending to be investors.

The volume of discarded GPUs, TPUs, servers, networking equipment and ancillary hardware being produced by the AI industry's infrastructure expansion is accelerating faster than any responsible disposal infrastructure can handle. And the workers who are doing the processing of the world's electronic waste bear the brunt of sorting them. They exist at the end of a chain of deliberate contractual

fragmentation designed to ensure that no company at the profitable end of the AI value chain ever has to account for what happens at the toxic end.

The AI industry has a labour problem, amongst many others. It is rather insulting for the guidance to participate in that invisibility. The workers who make AI physically and functionally possible are not the engineers in Silicon Valley or Zurich, whose working conditions are unlikely to be featured in any due diligence risk assessment. The AI industry leans heavily on the back of the miners in DRC who extract the cobalt that ends up in the chips that power every AI system, the guidance discusses. The lack of any mention of data labellers in countries like the Philippines is a moral failure. These are the workers earning between 1-3 USD by the hour on obscure platforms processing graphic violence. This work is often done without informed consent, psychological support, sick leave and a complaint mechanism that does not put them at risk of losing their jobs. It is also crucial to bring into the discussion the role of B2B outsourcing companies, the shock absorber of the AI labour violations, that sit between AI tech giants and workers. These companies exist to absorb the reputational and legal risk of the working conditions that the AI industry's economics require but that the AI industry's public commitments cannot accommodate. They provide BigTech companies the plausible deniability to speak publicly about responsible AI development, whilst their subcontractors' workers file labour complaints in Kenyan courts and are terminated for attempting to unionise. Connecting all of them is what the guidance's Note 5 explicitly places outside its scope. It is rather absurd to call it due diligence, if we are excluding cases where harm exists, the worst. Due diligence must step up and be prevented from being weaponised as yet another PR tool.

There is a sentence in the OECD guidance that deserves to be read very carefully.

> **Box 2.12. Deployment in contexts where laws are inconsistent with international standards on RBC**
>
> In contexts where domestic legal requirements may contradict international standards on RBC, enterprises should clearly and widely communicate commitment to respect internationally recognised human rights.
>
> As a preventative measure, this commitment can be clearly communicated and negotiated upfront, prior to deployment. Where the legal context has changed, encourage governments to comply with their human rights obligations, particularly where there are direct links with enterprise's operations. Avoid contributing to the unjust criminalisation of human rights defenders or the use of AI systems to repress peaceful protest. Consider not entering or withdrawing from contexts where human rights cannot be respected.

This box encapsulates the full weight of the framework's response to the question of what happens when the capital gets in bed with the state that uses them to imprison dissidents, disappear activists, surveil ethnic and religious minorities, persecute queer people and crush the political opposition that might otherwise hold them accountable. The BigTech-Military-Industrial complex is the defining human

rights crisis of our time, and it is happening now at full scale in Gaza, Iran and Venezuela, actively supported by commercial participation of companies headquartered in OECD member states. The infrastructure of digital fascism is being built and sold by a global industry whose supply chains run through the same jurisdictions whose governments have committed to the MNE Guidelines and whose companies are the primary audience of this guidance. The guidance's failure to name this explicitly, to trace the accountability chain from the technology provider to the prison cell, and above all to impose anything stronger than the word 'consider' on companies making these decisions is a political accommodation. And we at Manushya strongly believe that it must be challenged. Manushya Foundation works across Southeast Asia, a region that provides some of the world's most instructive and most disturbing case studies in digital authoritarianism. We have seen in Myanmar how Telenor handed over the private data of millions of its customers to a military junta that used that data to hunt down people whose information it had been entrusted to protect. The spyware industry represents the sharpest form of AI-enabled state violence against activists. For instance, it has been documented how companies sell offensive cyber tools to government clients in Indonesia and Thailand to extract communications from activists and to deliver that information to security services. The supply chain of the spyware industry runs through infrastructure and services provided by Big Tech companies.

The increasingly dangerous precedents being set in the United States have prompted other countries around the world to localise AI and other technological development under the banner of 'digital sovereignty'. Whilst commendable on paper, we have seen how this practice is increasingly becoming a tool for states to promote their version of Silicon Valley-style surveillance capitalism, as is the case for the reported social media platform 'W' in Europe, which will require ID verification. The increasing obsession of states to surveil their people, as seen with the repeated resurrection of the ChatControl legislation, amongst many others, is a symbol of a world wherein the distance between democracy and fascism is narrowing as fast as the planet is heating up. Above all, we have to reiterate everything that we have been saying for years. **No amount of voluntary guardrails will protect human rights. What we need is global legislation that will tax big tech billionaires whose empires were built on stolen labour and stolen land and redistribute that wealth to fund binding, enforceable, community-led accountability mechanisms that do not depend on the goodwill of the philanthropies and industry being regulated.** We need laws with teeth. We need them now, laws that do not bend nor get quietly rewritten on the sway of whoever happens to be the sitting president of the 'most powerful country' in the world.