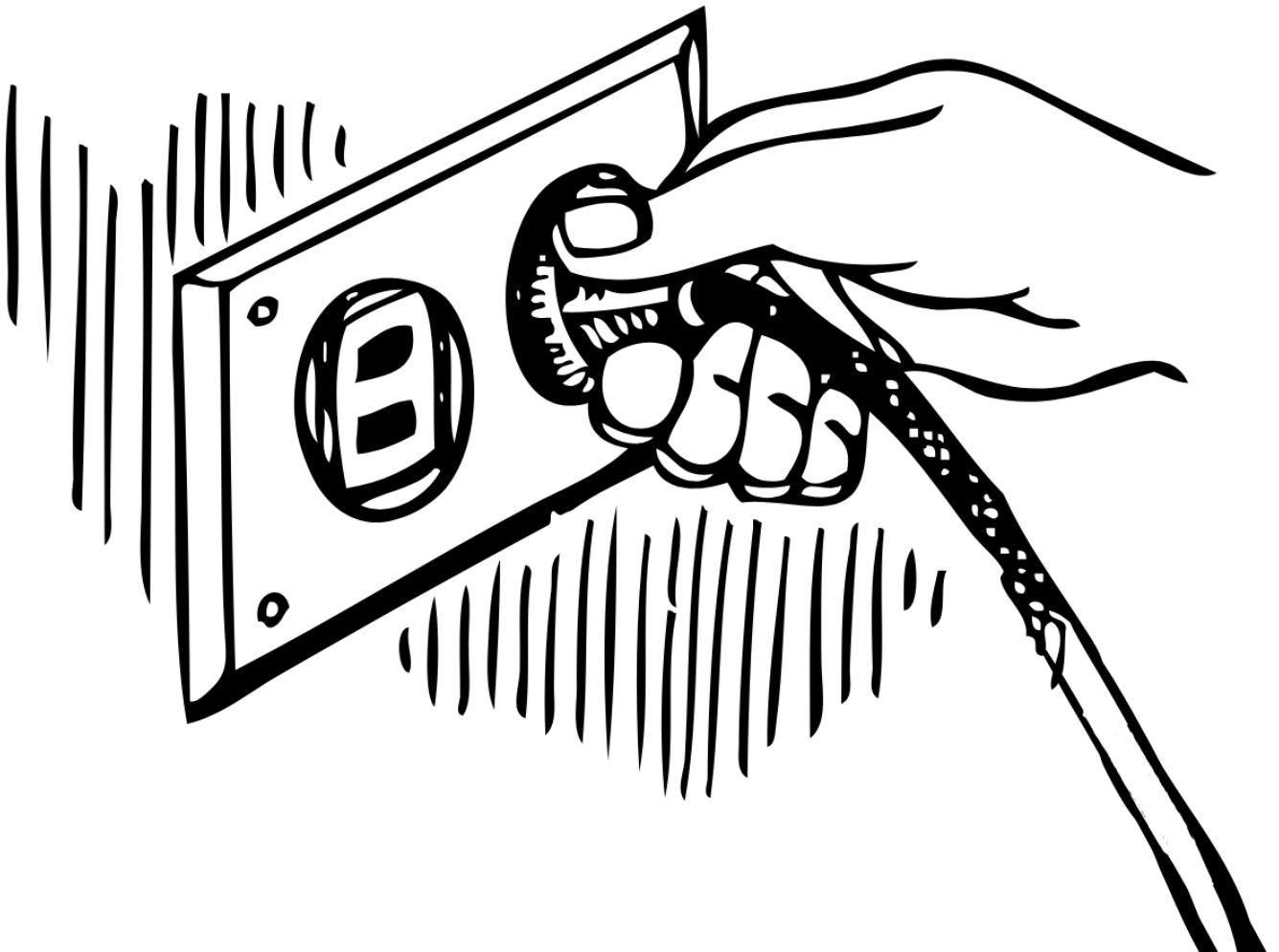


THE HUMAN RIGHTS CRISIS OF BRUTE-FORCE AI

SUBMISSION TO THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION
DATA-CENTRES AND HUMAN RIGHTS INQUIRY
SUBMITTED UNDER SECTION 184 OF THE CONSTITUTION AND
SECTIONS 13, 18 OF THE SAHRC ACT 40 OF 2013
SUBMISSION DATE: 30TH JULY 2026



Submitted by: Data-Centres, Surveillance, Control Working Group - Johannesburg, South Africa

I, on behalf of the Working Group, as well as a member of the drafting team, hereby extend a special thanks to the members of the drafting team, in particular the indefatigable Nicholas H. Tucker (Symanthesist Research Initiative), who was ably supported by his comrade and life partner, Dr. Gabrielle H. Tucker (Decoloniality and Hermeneutics). Dr Shamima Vawda (Social Researcher) has been a consistent contributor and provided substantial input.

Tauriq Jenkins (Human Rights & Digital Justice Researcher), a member of the Working Group, contributed towards the enrichment and finalisation of this document. We are also grateful to members who attended and contributed to the earlier discussions at the first public meeting of the Working Group held in May 2026 and subsequent submission to the Department of Communications and Digital Technologies. Joan Kinyua, a Kenyan digital rights activist and the founding President of the Data Labellers Association of Kenya (DLA), helped to kick us off in the direction where we are heading.

This submission is endorsed by the following organisations: Kensington Palestine Solidarity Group, Save Our Sacred Lands, CSO Tailings Working Group, Owe2 Green Economy, and Palestine Solidarity Alliance.

We thank you all.

In solidarity,

Hassen Lorgat

Social Justice Activist and convenor of CSOs Tailings Working Group

1 Executive Summary

The DSC Working Group (Data-Centres, Surveillance, Control Working Group) welcomes the South African Human Rights Commission's (SAHRC) timely inquiry into the human rights ramifications of hyper-scaled data-centres and rapidly expanding digital infrastructure across South Africa. As independent researchers working at the intersection of artificial intelligence, systems architecture, and legal compliance, our submission advances a crucial technical, social, environmental and constitutional thesis:

The current rush to construct hyper-scaled data-centres in South Africa is driven not by technical necessity but by a business model of extraction. A "circular financing trap" that socialises public resource costs while privatising corporate profits, directly threatening fundamental constitutional rights.

International frontier AI conglomerates led by figures such as Jeff Bezos (Amazon), Mark Zuckerberg (Meta), Elon Musk (xAI, Tesla, SpaceX), and Sam Altman (OpenAI) – to name but a few, wilfully omit truthful declarations attesting to the problematic nature of these hyper-scaled AI factories. Their disregard imposes severe localised human rights burdens by draining municipal power grids, diverting billions of litres of water in a country that is water stressed, as well as the vicious displacement of vulnerable communities, all to sustain corporate hyper-profits. Additionally, when one considers the entire AI value chain, from extraction of rare earth minerals for electronic processing components to the fossil fuels required for power generation, and the exploitation of data-workers and content moderators, its impacts are devastating to social and ecological livelihoods, notwithstanding the lifecycle of AI, from commissioning to decommissioning.

The very same corporations building data centres in South Africa, are named in UN reports as providing cloud and AI technologies that enhance surveillance and data processing in conflict zones. Gaza has become a testing ground for MIC (military industrial complex) armaments manufacturers and Big Tech, with little oversight and no accountability. South Africa cannot advocate for a global ban on autonomous weapons systems while hosting their enabling infrastructure.

A more viable, scientifically grounded alternative exists: distributed, scaled-down data-centre infrastructure that prioritises resource sovereignty, community benefit, environmental sustainability, and agricultural protection over brute-force extraction. It is our contention that through the establishment of regulatory standards that mandate distributed infrastructure, comprehensive human rights impact assessments, and community consent, South Africa can protect both constitutional rights and the environment. We should not be misguided by the tyranny of market forces. We must choose digital infrastructure that is in the service of our people and our planet.

This submission provides:

1. A constitutional analysis linking data-centre impacts to specific Bill of Rights provisions.
2. A technical and economic explanation of why hyper-scaling is a business model, not a technical necessity.
3. A critique of the "circular financing trap" that enables resource extraction.
4. A whole-infrastructure-chain and full lifecycle analysis of AI infrastructure impacts.
5. Seven prioritised policy recommendations for the SAHRC to advance to Parliament and the organs of state.

We thank you for the opportunity to present this framework to the SAHRC's stakeholder engagement process.

2 Introduction & Mandate Alignment

2.1 Why This Submission

The DSC Working Group is a collaborative initiative focused on developing ethical frameworks for human-AI interaction. Our work spans:

- **Philosophical grounding:** Hermeneutics, Ubuntu ethics, decolonial epistemology
- **Technical innovation:** Research into low-power, distributed AI infrastructure
- **Policy engagement:** Formal submission to DCDT on Draft National AI Policy (Notice 3880 of 2026)
- **Extractive industries research:** Investigation into the upstream impacts of AI infrastructure, to properly define it as an extractive data-mining process, as problematic as existent physical mining processes.

2.2 Alignment with SAHRC Mandate

This submission directly supports the SAHRC's constitutional mandate under:

- **Section 184 of the Constitution:** To monitor, assess, investigate and report on the observance of human rights in South Africa, including emerging systemic issues.
- **Sections 13 and 18 of the SAHRC Act 40 of 2013:** To investigate and report on the observance of human rights; to take steps to secure appropriate redress where human rights have been violated.

The rapid expansion of hyper-scaled data-centres represents precisely the type of "emerging systemic issue" that requires the Commission's attention. A technological development with profound implications for constitutional rights, environmental justice, and equitable access.

2.3 Structure of This Submission

This submission is structured as follows:

- **Section 3:** Problem Statement, The human rights crisis of brute-force AI

- **Section 4:** Technical Root Cause, Hyper-scaling as a business model, not a necessity
- **Section 5:** Constitutional & Human Rights Analysis
- **Section 6:** Human Rights Due Diligence & Regulatory Gaps
- **Section 7:** Policy Recommendations
- **Section 8:** Conclusion

3 Problem Statement: The Human Rights Crisis of Brute-Force AI

3.1 The Resource Extraction Model

The massive physical footprint of modern data-centres is not an inevitable technological necessity, but an outcome of market-driven business models that prioritise:

Brute-Force Paradigm	Human Rights Impact
Monolithic, Hyper-Scaled Farms	Centralised infrastructure creates single points of failure and disproportionate strain on local grids
100MW+ Power / Billions of Litres Water	Diverts scarce resources from residential, agricultural, and healthcare needs
Severe Local Human Rights Strain	Water rationing, load-shedding exacerbation, land displacement of vulnerable communities
Profit Before People	Corporate hyper-profits socialise ecological and infrastructure costs onto municipalities

Concrete Example: The proposed Cape Town data-centre (100MW+ electricity, 4.4 billion litres water annually) would consume resources equivalent to serving approximately 200,000 households, during a period of severe water stress and energy grid instability.

The perfect illustration of this extant problem is the River Club development in Cape Town, chosen for Amazon Web Services headquarters, exemplifies this extraction model in its most concentrated form. The site is sacred to the Khoi indigenous peoples as the location of the "First Encounter" between South Africans and Europeans in 1510. A court interdict recognised the threat of irreparable harm to indigenous living heritage, yet development has proceeded, unchecked. Activists call it a heritage and environmental crime in Amazon's name. The site is being book-marked for national heritage status and may become a UNESCO World Heritage site. Paving it over for server farms destroys the material anchors of indigenous memory and identity.

3.2 The Circular Financing Trap

The imposition of failed global strategies can be evidenced throughout the world, where hyper-scaled data-centre models operate using a predictable cycle:

Stage	Description	Human Rights Impact
1. Promise	Developers promise jobs, investment, and economic development	Municipalities are incentivised to approve projects without rigorous assessment
2. Approval	Municipalities grant rezoning and grid connections without independent resource impact assessments	Communities are not consulted; cumulative impacts are not evaluated
3. Extraction	Developers extract public resources (water, electricity) at below-market rates	Public resources are diverted from residential and agricultural needs
4. Socialisation	Costs (grid strain, water depletion, environmental damage) are borne by municipalities and communities	Vulnerable communities bear the burden of resource scarcity
5. Repatriation	Profits are repatriated to global headquarters	No lasting local benefit; community displacement and resource depletion remain
6. Repetition	Success of one project is used to justify the next, without cumulative impact assessment	The cycle repeats, compounding human rights violations

This is not a failure of regulation, it is a feature of the business model. Hyper-scaled data-centres are designed to extract, not to contribute and build.

3.3 Corporate Complicity and Conflicts of Interest

South Africa's contracts with global tech giants create a serious conflict of interest. These same companies are implicated in grave human rights violations globally. UN Special Rapporteur Francesca Albanese documented such occurrences in her report, "From Economy of Occupation to Economy of Genocide." She named 48 corporations, including Amazon, Microsoft, Google, IBM, and Palantir, as complicit in Israel's genocide in Gaza. The report finds that these firms are no longer passive suppliers. They are embedded in an economy of genocide.

Yet South Africa continues to award them lucrative contracts for cloud and software services. Our public funds flow to corporations enabling war crimes. This violates the state's constitutional duty to protect human rights (Sections 7, 8, and 39). The state cannot profess human rights while subsidising their violation. We call for immediate transparency on all such contracts and for mandatory human rights due diligence in public procurement. Any company found complicit in international crimes must be disqualified from bidding for government contracts.

3.4 The Full Value Chain Impact

The human rights burden extends beyond the data-centre itself:

Stage	Impact	Rights Affected
Raw Material Extraction	Rare earth mining, environmental degradation, conflict minerals	S24 (Environment), S27 (Health), S10 (Dignity)
Manufacturing	E-waste, hazardous materials, labour exploitation, unsafe working conditions	S23 (Labour), S24 (Environment), S10 (Dignity)
Construction	Land displacement, community disruption, unsafe labour practices	S25 (Property), S26 (Housing), S23 (Labour)
Operation	Energy/water consumption, heat pollution, community displacement, grid strain	S24, S27, S25, S23
Data Labour	Content moderation trauma, algorithmic management, outsourcing, low pay	S23 (Labour), S10 (Dignity), S12 (Security)
Decommissioning	E-waste management, data sanitisation failures, toxic waste disposal	S24, S14 (Privacy), S27 (Health)

3.5 The Cognitive Autonomy Crisis and Epistemicide

Beyond physical resource extraction, hyper-scaled AI systems powered by these centres threaten a more subtle but equally fundamental right: **cognitive autonomy**, the right to form one's own understanding without undue manipulation.

Hyper-scaled data centres ultimately embed Western epistemologies into AI systems. This drives epistemicide, the systematic erasure of indigenous knowledge. As scholars argue, generative-AI reproduces colonial hierarchies. It extracts non-Western knowledge, strips its origins, and repackages it as Western. This epistemic violence becomes physical at the River Club development in Cape Town. The destruction of heritage sites obliterates the material anchors of indigenous memory and identity. Cognitive autonomy becomes impossible when heritage is obliterated.

When citizens are subjected to unmediated automated decision-making powered by opaque, hyper-scaled infrastructure:

- Their interpretive agency is fundamentally infringed (S10, S12)
- They cannot understand or challenge decisions affecting them (S32)
- They face "hermeneutic collapse", the irreversible contraction of multiple possible meanings into singular, often dangerous, certainty

This is not hypothetical. It is the same psychological mechanism that has, throughout history, caused individuals consulting authoritative texts in desperation to interpret random fragments as divine instruction, sometimes with fatal consequences. In the AI age, the speed, fluency, and apparent authority of large language models dramatically amplifies this risk.

4 Technical Root Cause: Hyper-Scaling Is a Business Model, Not a Technical Necessity

4.1 The Economics of Hyper-Scaling

Frontier AI developers build hyper-scaled server farms because their profitability and control strategies rely on:

1. **Continuous, compute-heavy retraining loops** that require ever-increasing infrastructure
2. **Opaque statistical wrappers** that resist interpretability and lock in vendor dependence
3. **Privatising technological benefits** while socialising ecological and infrastructure costs
4. **Securing first-mover advantage** through massive capital expenditure that creates barriers to entry
5. **Creating monopolistic control** over AI infrastructure, preventing competition and democratic alternatives

This "brute-force" paradigm treats intelligence as a function of raw compute rather than allowing the development towards "architectural elegance". Hyper-scaling is not a technical necessity, it is a business strategy.

4.2 The Distributed Infrastructure Alternative

The brute-force paradigm is not the only option. The idea of implementing distributed, scaled-down data-centre infrastructure models offers a viable alternative:

Feature	Hyper-Scaled Model	Distributed Model
Scale	100MW+, billions of litres water	10-20MW, minimal water usage
Location	Centralised, often in water-scarce areas	Distributed, located near renewable energy sources
Cooling	Water-intensive (evaporative cooling)	Air-cooled, closed-loop, or geothermal
Grid impact	Massive strain on municipal grids	Can operate off-grid or with renewable microgrids
Community impact	Displacement, resource competition	Local employment, skills transfer

Feature	Hyper-Scaled Model	Distributed Model
Profit repatriation	Profits leave the country	Can support local data sovereignty and ownership
Resilience	Single point of failure	Redundant, resilient infrastructure
Accountability	Opaque, distant governance	Transparent, local governance
Ownership	Corporate monopolies	Public, co-operative, or community-owned alternatives

4.3 The Right to Data Sovereignty

South Africa's data should be stored on South African owned infrastructure that serves the public interest, not global corporate profit. Distributed data-centres can be owned and operated by public entities, co-operatives, or local consortia, ensuring that data sovereignty is not just a legal concept but a material reality.

The Draft National AI Policy (Notice 3880 of 2026) acknowledges the importance of data sovereignty. However, without regulatory intervention, data sovereignty will remain a rhetorical commitment while hyper-scaled infrastructure extracts public resources and sends data, and profits, overseas.

4.4 Opposition to Corporate Monopolies

AI and data infrastructure ownership should be decentralised and democratised. Public resources, water, electricity, land, should not be used to entrench corporate monopolies that:

- Control access to AI infrastructure
- Set prices for compute and storage
- Determine which applications and services can be developed
- Extract data from South African citizens without meaningful consent
- Repatriate profits while socialising costs

The concentration of AI infrastructure in the hands of a few global corporations is a threat to democratic governance, economic sovereignty, and human rights.

5 Constitutional & Human Rights Analysis

The rapid expansion of hyper-scaled data-centres directly vitiates several core rights enshrined in our Bill of Rights:

Constitutional Section	Right Protected	Impact of Hyper-Scaled data-centres	How Distributed Infrastructure Mitigates
Sections 10 & 12	Human Dignity; Freedom and Security of	Opaque AI systems powered by these centres can produce decisions that	Distributed, locally accountable infrastructure enables transparent

Constitutional Section	Right Protected	Impact of Hyper-Scaled data-centres	How Distributed Infrastructure Mitigates
	Person	strip individuals of agency and dignity. Cognitive autonomy is fundamentally infringed. Autonomous weaponry systems delegate life and death decisions to machines without human control, attacking human dignity and security of person.	governance and community oversight. Citizens can challenge decisions affecting them. Inherent application of Ubuntu
Section 14	Privacy	Storage and use of data to train AI models without consent; public databases commodified; unclear responsibility for data cleansing at system decommissioning.	Local data governance ensures privacy protections are enforced; community-controlled infrastructure prevents data commodification.
Section 23	Fair Labour Practices	Data workers and content moderators subjected to unethical labelling work (viewing violence, trauma) via third-party outsourcing contracts; algorithmic management without recourse; precarious employment.	Transparent labour standards in AI value chain; psychological care mandates for data labourers; right to unionise; collective bargaining.
Section 24	Environment Not Harmful to Health	Massive energy and water consumption harms environment, impacting health and well-being. Allocation of vast electrical capacity and scarce water resources violates state's duty to protect environment.	Low-power, air-cooled architecture; no hyper-scaling required; resource prioritisation protects environment.
Section 25	Property	Land displacement of vulnerable communities; conversion of agricultural land to industrial use; loss of livelihoods; destruction of heritage sites.	Distributed infrastructure can be located on non-agricultural, non-residential land; community consent required.
Section 26	Housing	Community displacement; pressure on housing in areas adjacent to data-centres; increased cost of living.	Distributed infrastructure reduces displacement pressure; community benefit agreements.
Section 27	Water, Health	Diverting scarce water and	Minimal infrastructure

Constitutional Section	Right Protected	Impact of Hyper-Scaled data-centres	How Distributed Infrastructure Mitigates
	Care, Basic Necessities	energy resources for industrial cooling directly threatens access to basic necessities. "People cannot eat or drink data."	footprint; resource prioritisation for residential/agricultural/healthcare needs.
Section 32	Access to Information	Opacity of AI systems makes it difficult for individuals to know how decisions affecting them are made, undermining right to understand and challenge automated outcomes.	Full audit trails of data governance; explainability focused on user vulnerability, not just model transparency.

5.1 The Interconnected Nature of These Rights

These rights do not operate in isolation. The diversion of water (S27) for data-centre cooling exacerbates environmental harm (S24), which impacts health (S27), which undermines dignity (S10), which is compounded when opaque AI systems make decisions affecting that individual's access to services (S32). The conversion of agricultural land (S25, S26) for data-centre infrastructure threatens food security (S27), which disproportionately affects low-income and rural communities (S10, S23). The destruction of heritage sites (S25) destroys the material anchors of indigenous memory and identity, making cognitive autonomy (S10, S32) impossible. This interconnectedness demands a holistic regulatory approach.

6 Human Rights Due Diligence & Regulatory Gaps

Current municipal and national approval processes for digital infrastructure suffer from severe structural gaps:

6.1 Siloed Governance

- Municipal planning tribunals frequently evaluate data-centre proposals purely as commercial real-estate or zoning applications (e.g., granting rezoning approvals while deferring environmental, water, and power impact assessments to remote future "Site Development Plans").
- Developers often obtain municipal rezoning approvals before comprehensive Environmental Impact Assessments (EIAs) are completed.
- Water, energy, land, heritage and agricultural impacts are assessed in isolation, not as an integrated nexus.

6.2 Absence of Human Rights Impact Assessments (HRIAs)

- Developers are rarely required to perform comprehensive UN Guiding Principles on Business and Human Rights (UNGPs) due diligence regarding cumulative resource depletion on surrounding informal, working-class, and poor settlements.
- We assert that none of the 56 data centres have conducted adequate, publicly-available environmental and human rights impact assessments. Should this assertion be contested, developers must provide verifiable proof of high-quality consultation with affected communities and impacted persons. Any gaps identified must be remedied within a strict, pre-defined period (e.g., 3 months), failing which operations must be suspended.
- While South Africa has supported the UNGP framework, it has yet to adopt mandatory human rights due diligence legislation, underscoring the need for the SAHRC's recommendations.

6.3 Failure to Assess Autonomous Weapons Systems and Military AI

- Autonomous weaponry systems (AWS) pose an urgent and under-addressed human rights threat.
- They shift warfare from traditional arms to drones, digital attacks, and AI driven systems.
- Delegating life and death decisions to machines without human control attacks human dignity (S10) and security of person (S12).
- South Africa has acknowledged this danger. Parliament has called for a binding treaty that bans AWS not under human supervision, yet the country simultaneously embraces the very infrastructure, hyper-scaled data centres, cloud platforms, and AI supply chains, that enables these systems globally.
- The same corporations building data centres in South Africa, e.g. Amazon, Microsoft, Google.
- They provide cloud and AI technologies that enhance surveillance and data processing in conflict zones.
- South Africa must advocate for a global ban on AWS. At the same time, we demand that it stop hosting the enabling infrastructure of these corporations within its borders. We must apply the precautionary principle across the full AI value chain.

6.4 Lack of Full Public Disclosure

- Developers are not required to disclose electricity demand, water use, cooling technologies, backup generation, emissions, air pollution, noise pollution, land-use impacts, energy contracts, public incentives, grid dependencies, ownership structures, or end-user arrangements.

- Communities cannot meaningfully participate in decisions when they lack access to such essential information.

6.5 Decoupling Governance from Infrastructure

- Regulators treat data protection (POPIA) and environmental protection (NEMA and the National Water Act) as entirely separate domains, failing to recognise that compute-heavy AI safety methods directly cause localised environmental degradation.
- Off-site energy generation, wheeling arrangements, grid connections, substations, and backup generation are often excluded from impact assessments.

6.6 Insufficient Corporate Accountability

- Corporate Social Responsibility (CSR) principles, while evolving, are often insufficient to prevent human rights harms without robust state regulation.
- "Green claims" (carbon neutral, green cloud) are not subject to independent verification or scrutiny.
- South Africa's contracts with global tech giants create a serious conflict of interest, while endorse these same companies who are complicit in grave human rights violations

6.7 Failure to Consider Distributed Alternatives

- Municipalities approve hyper-scaled projects without requiring developers to demonstrate why distributed, scaled-down alternatives are not viable. The default assumption is that hyper-scaling is necessary, rather than a choice.
- Public resources and regulatory support for data-centres are not justified by demonstrable public benefit, but merely by private computational capacity or corporate cloud expansion.

6.8 Failure to Protect Food-Producing Land and Rural Livelihoods

- Data-centre-linked energy projects in agricultural regions are not assessed for impacts on high-potential agricultural land, maize production, farm workers, smallholder producers, water users, agro-processing, grain storage, and local food economies.
- Rural livelihoods and food security are jeopardised without adequate assessment or mitigation.

6.9 Failure to Protect Heritage Sites and Indigenous Knowledge

- Our courts have recognised the threat of irreparable harm to indigenous living heritage, yet development upon these very sites goes ahead unchecked.

- This is nothing short of a heritage and environmental crime in Amazon's name.
- Indigenous knowledge systems are systematically erased by Western epistemological dominance embedded in hyper-scaled AI systems.

7 Policy Recommendations to the SAHRC

The DSC Working Group respectfully submits the following recommendations for inclusion in the SAHRC's report and subsequent guidance to Parliament and state organs.

Recommendation 1:

7.1 (High Priority) Mandate Distributed Infrastructure and Community Consent

Action: The SAHRC should recommend that all future data-centre developments be required to demonstrate that hyper-scaling is the **only** viable option, and that distributed, scaled-down alternatives have been fully considered and rejected on technical and economic grounds.

7.1.1 Requirements: Distributed Infrastructure Analysis:

- Developers must submit a detailed analysis of distributed alternatives, including cost-benefit analysis, resource impact assessment, and community benefit plan.
- The analysis must demonstrate why distributed alternatives are infeasible, with the burden of proof resting on the developer.
- Indigenous communities must have specific protections for heritage sites, with mandatory community consent grounded in the Right to Say No.

7.1.2 The Right to Say No (RTSN):

- Communities must have genuine veto power over data-centre projects that affect their resources and livelihoods.
- Consultation must be early, meaningful, accessible, and informed.
- Communities must be told clearly where a project fits within the data-centre value chain and who benefits from it.

7.1.3 Opposition to Corporate Monopolies:

- AI and data infrastructure ownership should be decentralised and democratised.
- Public resources should not be used to entrench corporate monopolies.
- Preference should be given to public, co-operative, or community-owned infrastructure.

Rationale: Hyper-scaling is a business model, not a technical necessity. Communities have the right to determine what happens to their resources and livelihoods. Democratic oversight must replace opaque corporate control.

Responsible Bodies: SAHRC (guidance), Municipalities (approval processes), DCDT (policy alignment), National Treasury (funding conditions).

Recommendation 2:

7.2 (High Priority): Mandate Comprehensive Human Rights, Ecological, Agricultural, Heritage and Nexus Impact Assessments

Action: No data-centre or digital infrastructure project should receive municipal rezoning, environmental authorisation, or grid-connection approval without a mandatory, independent Human Rights Impact Assessment (HRIA), Ecological Impact Assessment (EIA), Heritage Impact Assessment, Agricultural Impact Assessment, and Water-Energy-Food Nexus Assessment.

7.2.1 Requirements: Full Public Disclosure:

- Developers must disclose electricity demand, water use, cooling technologies, backup generation, emissions, air pollution, noise pollution, land-use impacts, energy contracts, public incentives, grid dependencies, ownership structures, and end-user arrangements.
- Off-site energy generation, wheeling arrangements, grid connections, substations, and backup generation must be included in disclosures.
- All disclosures must be publicly accessible and subject to community review.

7.2.2 Human Rights and Environmental Due Diligence:

- Evaluate cumulative impacts on water, energy, land-use, community well-being, and agricultural livelihoods under Sections 10, 23, 24, 25, 26, 27, and 32 of the Constitution.
- Must take cognisance of the perspicacious legal ruling laid down by the Ecuadorian Constitution (2008) which establishes the Rights of Nature (Pachamama) under Articles 71-73, providing a legal framework that can guide South Africa's approach. These principles include: the right to exist and regenerate; the right to restoration; the precautionary principle applied to activities that might lead to extinction or ecosystem destruction; and public legal standing to enforce the rights of nature. This framework reinforces our argument for mandatory HRIAs and the precautionary principle.
- Apply the UN Guiding Principles on Business and Human Rights (UNGPs) framework.
- Include mitigation plans that prioritise basic human needs over industrial cooling.
- **The precautionary principle must apply:** the burden of proof must rest on developers to demonstrate safety and community benefit. No deployment without proven safety and demonstrated community benefit.

7.2.3 Protection of Food-Producing Land and Rural Livelihoods:

- Data-centre-linked energy projects in agricultural regions must be assessed for impacts on high-potential agricultural land, maize production, farm workers, smallholder producers, water users, agro-processing, grain storage, and local food economies.
- Food sovereignty and rural livelihoods must be protected.

7.2.4 Protection of Heritage Sites and Indigenous Knowledge:

- An immediate moratorium must be placed on data centre developments on heritage sites.
- Heritage impact assessments must be mandatory and binding.
- Indigenous knowledge systems must be integrated into AI governance. An African AI epistemology, rooted in Ubuntu's relational ethics, must guide our future.

7.2.5 Water-Energy-Food Nexus Assessment:

- Approvals must assess electricity, water, land, and food impacts in an integrated manner, not in isolation.
- Cumulative and climate-related impacts must be central to decision-making.
- Climate adaptation and resilience must be considered.

7.2.6 Protection of Vulnerable Communities:

- Assessments must ensure that low-income communities, rural areas, farm workers, smallholder producers, indigenous communities and under-served municipalities do not bear disproportionate environmental, water, energy, land-use, heritage, or tariff burdens while benefits accrue mainly to large technology companies and corporate users.
- Equality, dignity, and non-discrimination must be central to all assessments.

Rationale: Current approval processes deliberately avoid/ignore comprehensive assessment of human rights, ecological, agricultural, heritage, or nexus impacts, thus allowing developers to externalise costs onto vulnerable communities and ecosystems.

Responsible Bodies: SAHRC (guidance), National Treasury (funding conditions), DCDT (policy alignment), Municipalities (approval processes), Department of Agriculture, Land Reform and Rural Development, Department of Water and Sanitation, Department of Mineral Resources and Energy, Department of Sports Arts and Culture (heritage protection).

Recommendation 3:

7.3 (High Priority): Enforce Resource Prioritisation and Scrutinise Some of the Purported Green Claims

Action: Governing authorities must enforce strict resource prioritisation, ensuring municipal water and electricity are reserved for residential, agricultural, and public healthcare needs over industrial cooling for hyper-scalers.

7.3.1 Requirements: Resource Prioritisation:

- Industrial data-centres must prove 100% off-grid energy self-sufficiency and closed-loop, non-potable cooling technologies prior to operation.
- Municipalities must conduct cumulative impact assessments before approving new data-centre projects.
- Water use licences must be subject to public scrutiny and community consent.

7.3.2 Scrutiny Some of the Purported Green Claims:

- Renewable energy procurement claims should not be accepted as a complete answer to environmental and human rights concerns.
- "Carbon neutral" or "green cloud" claims must be tested against land, water, grid, waste, and community impacts.
- Independent verification of all environmental claims must be required.
- Carbon offset schemes must be scrutinised for their actual environmental and social impacts.

7.3.3 Infrastructure Assessment:

- Assessments must include off-site energy generation, wheeling arrangements, grid connections, substations, and backup generation.
- Cumulative grid impacts must be assessed, including effects on load-shedding and grid stability.

Rationale: The diversion of public resources for private profit violates the state's duty to protect access to basic necessities under Section 27 of the Constitution. Green-washing must not be permitted to obscure real resource extraction.

Responsible Bodies: Municipalities, Department of Water and Sanitation, Department of Mineral Resources and Energy.

Recommendation 4:

7.4 (High Priority): Adopt a Whole-Infrastructure-Chain and Full Lifecycle Approach

Action: The SAHRC must recommend that all AI policy and regulations adopt a whole-infrastructure-chain and full lifecycle perspective, from raw material extraction to decommissioning, ensuring human rights protections apply at every stage.

7.4.1 Requirements: Whole-Infrastructure-Chain Assessment:

- Data-centre assessments must include off-site energy generation, wheeling arrangements, grid connections, substations, backup generation, water infrastructure, e-waste streams, and cumulative impacts.
- Supply chain due-diligence requirements for AI developers.
- Transparency requirements for subcontractors and third-party suppliers.

7.4.2 Full Lifecycle Accountability:

- Full lifecycle waste accountability from extraction and processing through construction, operation, and maintenance.
- E-waste management and data sanitisation standards.
- Decommissioning plans must be required prior to construction approval.
- Liability for environmental damage must extend throughout the lifecycle.

7.4.3 Workers' Rights to Organise:

- Unionisation of workers must be protected and promoted throughout the AI value chain.
- Labour rights protections must apply to all workers, including subcontractors and gig workers.
- Collective bargaining rights must be guaranteed.

Rationale: Current regulatory approaches focus narrowly on data centres as infrastructure, overlooking the upstream (mining, manufacturing) and downstream (e-waste, data labour) human rights impacts. Meanwhile, data labelers and other gig workers across the AI value chain have faced persistent employer hostility toward unionisation, despite laws that explicitly affirm their right to organise.

Responsible Bodies: SAHRC (guidance), DCDT (policy alignment), DTIC (industrial policy), Department of Mineral Resources and Petroleum (mining standards), Department of Employment and Labour.

Recommendation 5:

7.5 (Medium Priority): Protect Data Labour Rights

Action: The SAHRC should recommend specific protections for data workers and content moderators, including:

7.5.1 Requirements:

- Transparency about the nature of labelling work (e.g., viewing violent content, child sexual abuse material, graphic violence)
- Mandatory psychological care and support, including counselling and trauma recovery
- Fair compensation standards aligned with South African labour law
- Right to unionise and collective bargaining for platform workers
- Protection against algorithmic management and surveillance
- Right to disconnect and limits on working hours
- Regular independent audits of working conditions

Rationale: The AI value chain relies on human labour that is often outsourced, underpaid, and psychologically harmful. This violates Section 23 (fair labour practices) and Section 10 (dignity).

Responsible Bodies: SAHRC (guidance), Department of Employment and Labour (enforcement), DCDT (policy alignment). The Trade Union Movement must embrace this challenge of organising these “new” workers.

Recommendation 6:

7.6 (Medium Priority): Enforce POPIA Section 71 Through Transparent Governance Standards

Action: The Information Regulator and SAHRC should jointly establish clear standards for compliance with POPIA Section 71 (automated decision-making oversight), ensuring that algorithmic accountability is achieved through transparent governance rather than compute-intensive, opaque retraining pipelines.

7.6.1 Requirements:

- Full audit trails of automated decision-making.
- Clear explainability standards for high-risk AI systems.
- Independent oversight mechanisms for public-facing AI systems.
- Right to human review of automated decisions.
- Regular independent audits of AI systems for bias and discrimination.
- Transparency requirements for data sources, training data, and algorithmic design.

Rationale: Current approaches to "explainability" often require massive computational resources, perpetuating the brute-force paradigm. Distributed, transparent governance provides a lightweight, privacy-preserving alternative.

Responsible Bodies: Information Regulator, SAHRC, DCDT.

Recommendation 7:

7.7 (Medium Priority): Support Research into Distributed, Low-Power Infrastructure

Action: The SAHRC should recommend that the National AI Safety Institute (proposed in Draft National AI Policy) prioritise research into distributed, low-power data-centre architectures over hyper-scaled, resource-intensive models.

7.7.1 Requirements:

- Funding for research into air-cooled, closed-loop, and geothermal cooling technologies.
- Research into off-grid renewable energy systems for data-centres.
- Development of local manufacturing capacity for data-centre components.
- Skills development and training programmes for distributed infrastructure.
- Application of the concept of Ubuntu and research into public, co-operative, and community ownership models.
- Research into an African AI epistemology rooted in Ubuntu's relational ethics.

Rationale: South Africa must play a leading role as a progressive Global South country in establishing a digital infrastructure model that defends both human rights and the environment—but this requires strategic investment in infrastructure that actively upholds those rights.

Responsible Bodies: SAHRC (guidance), DSTI (research funding), CSIR (applied research), DCDT (policy alignment).

Recommendation 8:

7.8 (High Priority) Mandate Human Rights Due Diligence in Public Procurement

Action: The SAHRC should recommend that all government contracts with technology companies be subject to mandatory human rights due diligence.

7.8.1 Requirements:

- Immediate transparency on all existing government contracts with global technology companies.
- Mandatory human rights due diligence in public procurement processes.

- Disqualification from bidding for government contracts for any company found complicit in international crimes.
- Compliance with UN Guiding Principles on Business and Human Rights as a condition of contract.

Rationale: South Africa cannot profess human rights while subsidising their violation. Public funds must not flow to corporations enabling war crimes.

Responsible Bodies: SAHRC (guidance), National Treasury (procurement policy), DCDT (policy alignment).

8 Conclusion

The expansion of digital infrastructure should never come at the expense of human dignity, environmental justice, agricultural sustainability, heritage preservation, or democratic resilience. South Africa stands at a crossroads:

- **Path A:** Continue endorsing the hyper-scaled paradigm, data-centres that extract vital public resources for private profit, hijack social and human rights, promote ecological devastation, while projecting agricultural costs onto vulnerable communities. This path is driven by the circular financing trap, where developers promise jobs and investment while depleting water, straining grids, displacing communities, destroying heritage sites and jeopardising food security. This path entrenches corporate monopolies, enables autonomous weapons systems and undermines democratic sovereignty.
- **Path B:** Embrace distributed, accountable infrastructure, scaled-down data-centres that prioritise resource sovereignty, community benefits, environmental sustainability, agricultural protection and heritage preservation. This path requires regulatory intervention: mandatory HRIAs, resource prioritisation, community consent, heritage impact assessments, public procurement due diligence and a whole-infrastructure-chain approach to policy design. This path democratises AI infrastructure development and places it in the service of the people, respective to other life forms and the ecology at large.

The choice is not technical. It is political. And it must be made now.

We continue to draw enduring inspiration from the principles of the ancients, from spiritual wisdom, and from our shared contribution to world civilizations—turning away decisively from the growth-greed, extractivist logic and practice of colonialism. By pairing a robust constitutional rights framework with a commitment to distributed, resource-efficient infrastructure, South Africa can lead the Global South in forging a digital model that defends both human rights and the environment on which all life depends. The tools exist. The constitutional imperative is clear. The future is ours to choose.

9 Request for Engagement

We respectfully request:

1. That these recommendations form part of the SAHRC's report to Parliament;

2. An opportunity to present this framework to the SAHRC's stakeholder engagement process;
3. Collaboration on developing technical guidelines for distributed infrastructure certification.

We are available for engagement at the Commission's behest, in order to put forward our case.

10. AI Principles to Guide Action

In the spirit of constructive engagement, the DSC Working Group offers the following principles as a foundation for a new national AI and digital infrastructure policy. These principles have been developed through extensive consultation and reflection on the human rights implications of AI:

1. **The Right to Say No (RTSN):** Communities must be able to accept or reject data centre projects that affect their resources, livelihoods, and environments. Consent must be early, meaningful, accessible, and informed.
- **Full Lifecycle Waste Accountability:** AI and data centre waste (E-Waste – covering noise pollution – radio wave pollution – electronic garbage, etc.) must be accounted for from extraction and processing through construction, operation, and maintenance. Decommissioning plans must be required prior to approval.
- **Worker's Rights to Organise:** Unionisation must be protected and promoted throughout the AI value chain, including mining, manufacturing, and data labour. Collective bargaining, fair compensation, and psychological care must be guaranteed.
- **Opposition to Corporate Monopolies:** AI ownership should be decentralised and democratised. Public resources should not be used to entrench corporate monopolies. Preference must be given to public, co-operative, and community-owned alternatives.
- **Precautionary Principle:** No deployment without proven safety and demonstrated community benefit. Corporations must bear the burden of proof. The absence of evidence of harm is not evidence of safety.
- **Collective Ownership and Democratic Oversight:** Transparency and accountability must replace opaque corporate control. Communities must have genuine decision-making power over infrastructure that affects them.
- **Community Empowerment:** Affected populations must shape AI development and deployment. Infrastructure must serve community needs, not corporate profit.
- **Algorithmic Justice and Equity:** Systems must be designed to eliminate bias and inequality. Discrimination and exclusion must be actively prevented.
- **Resource Sovereignty:** South Africa's water, energy, land, and data resources must serve the people, not global corporate profit. Resource prioritisation must protect basic human needs.

- **Full Supply Chain Accountability:** The human rights burden of AI infrastructure must be accounted for at every stage of the value chain, from the mine to the server rack to the e-waste dump. Developers must be held accountable for the upstream impacts of their supply chains.
- **Protection of Indigenous Knowledge Systems:** An African AI epistemology, rooted in Ubuntu's relational ethics, must guide our future. Indigenous knowledge systems must be integrated into AI governance, not erased by Western epistemological dominance.
- **Heritage Protection:** Data-centre developments on heritage sites must be prohibited. The material anchors of indigenous memory and identity must be protected as fundamental to cognitive autonomy and human dignity.
- **Interpretive Governance:** The right to cognitive autonomy—the ability to form your own understanding without being unfairly manipulated—must be protected as a basic human right. AI systems must be built and used in ways that protect each person's ability to interpret information for themselves. This means people should not be subjected to unchecked automated decisions that take away their dignity, freedom, or their ability to understand and question outcomes that affect them. Interpretive governance calls for AI that is transparent, checkable, and designed around human needs—prioritising clear explanations, the right to challenge decisions, and the recognition that there can be multiple valid perspectives, rather than offering closed, fixed, or one-size-fits-all answers.
- **Global Regulation of Military AI:** Enforceable limits on autonomous weapons systems must be established through international agreement. South Africa should support and advocate for binding international treaties that prohibit the development, deployment, and use of autonomous weapons systems that operate without meaningful human control. The use of AI for surveillance, repression, and military purposes must be subject to rigorous human rights and people-driven oversight and accountability mechanisms. We abhor the silences surrounding the use of AI for surveillance, repression, and military purposes and call for immediate global action.
- **Public Procurement Accountability:** No public funds shall flow to corporations enabling war crimes or grave human rights violations. Mandatory human rights due diligence must be embedded in all government procurement processes.

11 Annexure 'A' - South African Constitutional Provisions (Plain-Language Summary)

Section	Right	Relevance to data-centres
S10	Human Dignity	Opaque AI systems strip individuals of agency; cognitive autonomy is a dimension of dignity; autonomous weapons systems delegate life and death decisions to machines
S12	Freedom and Security	Algorithmic decision-making can produce harmful

Section	Right	Relevance to data-centres
	of Person	outcomes without recourse; AWS attacks security of person
S14	Privacy	Data commodification and surveillance without consent
S23	Fair Labour Practices	Exploitation of data workers and content moderators
S24	Environment	Resource depletion, energy and water consumption
S25	Property	Land displacement; conversion of agricultural land; destruction of heritage sites
S26	Housing	Community displacement; pressure on housing
S27	Water, Health, Basic Necessities	Diversion of scarce resources for industrial cooling
S32	Access to Information	Opacity of automated decision-making

11.1 Annexure 'B': Sources & Citations

1. Constitution of the Republic of South Africa, 1996
2. Protection of Personal Information Act 4 of 2013 (POPIA)
3. National Environmental Management Act 107 of 1998 (NEMA)
4. National Water Act 36 of 1998
5. UN Guiding Principles on Business and Human Rights (2011)
6. Draft National AI Policy, Notice 3880 of 2026 (*Repealed June 2026 - now subject to new request*)
7. City of Cape Town Water Demand Projections (2025) - City of Cape Town, *Water and Sanitation Department: Bulk Water Resource Planning Report 2025*
8. Eskom Integrated Resource Plan (2023) (*Eskom Integrated Resource Plan (IRP 2019 / 2023 Draft Update)*)
9. UN Global Digital Compact (2024) (*Adopted UNGA Resolution 79/1*)
10. African Union Convention on Cyber Security and Personal Data Protection (2014) (*Awaiting ratification status*)
11. ILO Draft Convention on Decent Work in the Platform Economy (Expected adoption 2025/2026, ILC Agenda)
12. Data Workers Collective & ILO Platform Work Initiative (2025). Policy Report: Decent Work in the Platform Economy.
13. Schroedingers Bible - On Observation, Meaning, and the Ethics of Interpretation (*Dr. Gabrielle H. Tucker and Nicholas H. Tucker*)

14. Constitution of the Republic of Ecuador (2008), Articles 71-73 - Rights of Nature (Pachamama)
15. UN Special Rapporteur Francesca Albanese (2026). *"From Economy of Occupation to Economy of Genocide"* - Documentation of 48 corporations complicit in human rights violations
16. South African Parliamentary Resolutions on Autonomous Weapons Systems Treaty
17. River Club Development Court Interdict Proceedings - *Recognition of irreparable harm to indigenous living heritage*

This submission represents genuinely collaborative intellectual partnership amongst activists. The philosophical foundations emerged through extended dialogue amongst the authors; the strategic framework was developed in consultation with the collective's expertise in constitutional law, public health, and digital rights, systems development and AI-ethics and philosophy. The principles and recommendations represent a synthesis of multiple intellectual traditions, all united by a common commitment to human dignity, environmental justice, and democratic accountability.

Forward to resource sovereignty. Forward to distributed accountability. Forward to digital infrastructure that serves the people. Forward to a future where technology serves humanity, not profit.

