

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) welcomes the Human Rights Council's initiative under Resolution 58/23 to examine the risks that digital technologies pose to human rights defenders (HRDs) and to identify best practices for their protection. Responses are presented in bullet form under the questions:

---

## Background

Digital technologies have transformed both the work of human rights defenders (HRDs) and the nature of the threats and attacks they face. HRDs operate at the forefront of public engagement, increasingly relying on digital tools for communication, monitoring, documentation and advocacy. As these tools evolve, so does the nature of the threats and attacks HRDs face – impacting their safety online and offline. In April 2025, the Human Rights Council adopted **resolution 58/23** mandating OHCHR to conduct consultations to assess the risks created by new and emerging technologies to HRDs and to identify effective practices to address these risks across different geographical contexts. It also requested OHCHR to prepare a report on the outcomes of these consultations, which may include recommendations on due diligence and improved responses to digital technology-related risks faced by HRDs.

## Key questions and types of input/comments sought

Inputs are sought to gather information on the ways in which the work and safety of HRDs are affected by digital technologies. We will look at overarching trends which we have identified as particularly relevant to protection of HRDs: how digital technologies affect the communications, privacy and safety of HRDs; how legislative and regulatory measures impact digital spaces; and how companies have responded to identified risks affecting HRDs on their platforms and services.

We would appreciate receiving inputs in response to some or all of the questions listed below.

### 1. Legislative and regulatory measures

- What impacts have recent trends in legislative and regulatory efforts at local, regional and global levels – including, for example, on information integrity, online safety and cybercrime – had on the work and safety of HRDs offline and online?

Across Africa, recent laws have ostensibly been designed to operate as [weapons against HRDs](#). While most of these laws are often considered necessary for cybersecurity, counter-terrorism, data protection, or checking on disinformation, misinformation and fake news, they are routinely applied to curtail engagements and suppress dissent and activities of HRDs. Where the laws exist such as on data protection, they are not sufficient and, in most cases, fall short of the minimum regional and international human rights standards. State authorities in Africa often use and deploy vague and overbroad legislative provisions to exercise wide discretionary powers to determine what constitutes prohibited online speech and to selectively enforce the laws. In a largely minimal judicial oversight environment and inadequate due process protections, the chilling effect extends way beyond those actually prosecuted, which widely [undermines the work of HRDs in defending human rights](#).

- What legal or regulatory instruments and institutional procedures are commonly used to restrict the rights to freedom of expression, association and privacy of HRDs online?

Computer and cyber security related laws, and [national security legislation and anti-terrorism laws are](#) often broadly deployed and used to levy charges against HRDs. Laws in countries such as Eswatini, Nigeria, Somalia, [Tanzania](#), [Uganda](#), [Zambia](#), [Zimbabwe](#) are [largely repressive, marred](#) with criminal defamation, and sedition, [libel and slander](#) and other criminal charges aimed at prosecuting HRD over expressions considered protected speech under international human rights law. Human rights defenders (HRDs) face systematic intimidation through arrest,

detention, and prosecution under various laws. In countries like [Uganda](#), authorities routinely file charges against HRDs—not to secure convictions, but to trap them in lengthy court proceedings, divert their attention from human rights work, and deter others from similar advocacy. Digital taxation measures such as imposition of social media taxes, most notably Uganda’s Over-the-Top (OTT) tax, introduced in 2018 and restructured in subsequent years, impose financial barriers on access to the digital platforms through which HRDs communicate, organise, and publish. These taxes disproportionately widen the exclusion gap and limit online participation and public engagement. They represent a structural narrowing of accessible civic space that operates at the intersection of economic policy and digital rights.

- How have legislative and regulatory efforts in one country or region impacted similar legal and regulatory measures in other countries or regions?

Legislative measures that curtail the civic space for HRDs such CSOs and journalists are rapidly mirrored across the continent. The [Computer Misuse Act](#) which outlawed offensive communication in Uganda in 2011 was mirrored in the [Cybercrimes law](#) of Tanzania in 2015. This trend inspired punitive cybercrimes laws in [Ethiopia, Malawi, Rwanda, South Sudan, Burundi, and Kenya](#). Incidentally, continental instruments like the Malabo Convention and regional frameworks at the East African Community (EAC) frameworks, and Southern African Development Community (SADC) such as model laws which sought to standardize digital security frameworks allowed states such as [Zimbabwe, Nigeria, Eswatini, Somalia, Zambia, Mozambique, Mauritius, Namibia, Lesotho, Madagascar, Seychelles, South Africa, Botswana, Angola, Comoros, Algeria, and Egypt](#) to adopt laws that had overlaps which undermine human rights standards and safeguards.

## 2. Digital communications

- Which risks do internet shutdowns, network interferences, geo-blocking or other forms of restrictions of connectivity and communications pose to HRDs’ work and safety?

Internet shutdowns have become a regularized instrument of state control across Africa especially during elections and periods of political unrest. Most of the African countries have set [internet controls, disruptions, and shutdowns as a tool for repression](#). Amongst the affected countries include Chad (2016 and 2024), Burundi (2020), Cameroon (2018), Comoros (2024), Democratic Republic of Congo (2016), [Ethiopia \(2021\)](#), Guinea (2020), [Gabon \(2023\)](#), Nigeria, Mali (2020), Mauritania (2019), Republic of the Congo (2016 and 2021), [Senegal, Sudan](#), Tanzania (2020), Togo, Uganda (2016, 2021 and 2026) and Zimbabwe (2018 & 2019).

Internet shutdowns severely undermine HRDs ability to communicate, mobilize support, document violations, and report to international bodies. These shutdowns serve as powerful tools of state repression, silencing dissent and entrenching authoritarianism.

Shutdowns isolate HRDs from protective networks, cut off communities from documentation efforts, and disable emergency communications—creating windows of impunity where violations occur without witnesses. While the economic costs are substantial, the human rights impact on HRDs in fragile or conflict-affected areas is often irreversible. In high-risk environments, governments weaponize connectivity control for targeted attacks. Information blackouts conceal war crimes and electoral abuses, directly endangering HRDs on the ground. Vulnerable communities are left defenceless against state excesses, with their democratic rights completely undermined.

- What forms of technology-facilitated attacks do HRDs face on social media platforms and digital communications services? How do these online attacks intersect with offline events?

HRDs across Africa face an escalating spectrum of digital attacks. These range from state-sponsored campaigns to coordinated individual efforts designed to attack, mislead, and disinform the public. Common tactics include doxing, spear-phishing, deepfake abuse, sextortion, and systematic trolling. Technology-Facilitated Gender-Based Violence (TFGBV) against women HRDs has particularly intensified. These attacks follow documented patterns across the continent, with countries including [Uganda, South Africa, Ethiopia, Tunisia, Sudan, and Gabon](#) reporting widespread tech-facilitated harassment campaigns. Content moderation

systems exacerbate these vulnerabilities by prioritizing high-resource languages and Global North contexts. Harmful content including coordinated harassment, incitement to violence, and state-sponsored disinformation proliferates unchecked in African languages due to inadequate detection and removal systems. This creates structural inequality in protection: HRDs communicating in English or French receive imperfect but greater platform safety than those using Swahili, Amharic, Shona, or Luganda. African HRDs are thus rendered more vulnerable precisely because of their linguistic and cultural context

- What specific risks to HRDs emerge via online platforms and communications services in situations of armed conflict, instability and/or elections?

During situations of armed conflict, instability and/or elections, the digital civic space is often turned into a battle ground. Worse still, the state especially those with authoritarian governments weaponise the digital landscape by using malware and spyware to limit and curtail activities of HRDs.

Communications are usually intercepted to effectively limit assembly and association and frustrate any activities and plans by HRDs. The resulting effects are often arrests of HRDs and cutting off information access. Amongst the affected countries include Cameroon, Democratic Republic of the Congo (DRC), Ethiopia, Mali, Nigeria, Senegal, Sudan, [Uganda](#), and Zimbabwe. In other cases, telecommunications infrastructure in countries like Ethiopia and Sudan have [been routinely weaponised](#) to sever connections as a shield to hide grave human rights abuses from regional and international scrutiny. Similarly, state and non-state actors have often used [data protection and localized content moderation](#) to carry out cyber-attacks and doxing campaigns against HRDs, especially civic monitors.

- What specific risks do women HRDs and HRDs from groups affected by marginalisation and discrimination faced on online platforms and communications services?

Women human rights defenders (WHRDs) face a compounded threat. Technology-facilitated gender-based violence (TFGBV) including non-consensual intimate image abuse, sexual harassment, doxing, and coordinated pile-on campaigns has become a primary instrument of silencing women in digital public spaces across East and Southern Africa. TFGBV is not an ancillary concern but a systematic strategy of exclusion that drives WHRDs offline, effectively privatising and shrinking civic space along gendered lines. Some of the attacks are [reputational](#) targeting integrity of HRDs through smear campaigns. As a result, HRDs are often discouraged from doing their work and distressed since the trust of their communities and relationships with the international community and development partners is compromised.

- How do companies' policies and practices relating to content moderation and engagement with law enforcement and government authorities affect HRDs' work and safety?

In Africa, there's inadequacy of understanding of regional political nuances and most platforms rely on languages of the global north. This means state sponsored and other source-based disinformation, hate speech targeting HRDs cannot be removed easily by automated systems. This means censorship of human rights documentation under [vague community guidelines](#). Coupled with tech companies' compliance with government requirements and requests for real time surveillance and decryption of content and information in transmission, HRDs are stripped of their privacy and integrity of information. Platforms are therefore effective tools of control and repression with [no clear lines for transparency and accountability](#).

- How do advances in AI technologies exacerbate risks to HRDs' operations and presence on online platforms and communications services?

Advances in artificial intelligence (AI) account for the weaponisation of the digital ecosystem against Human Rights Defenders (HRDs) in Africa. State surveillance, disinformation and algorithmic bias against marginalised voices is now more pronounced. Countries such as [Uganda](#), [Nigeria](#), and [Zimbabwe](#), have had their governments deploy AI-powered facial recognition and

biometric surveillance systems often procured under questionable manner. The systems are further used in monitoring and surveillance of work of HRDs which later puts a chilling effect on the activities of HRDs. Generative AI is also associated with deep fakes and coordinated as well as state sponsored disinformation campaigns which are primarily designed to discredit HRDs and manipulate public perceptions. In countries like [Kenya, Namibia, and South Africa](#), recent political unrest is attributed to the wide deployment of AI. Again the platforms deploy automated content moderation systems trained predominantly on Western norms and high-resource languages which perpetuates bias and discrimination based on [algorithms](#). This has the effect of failure to detect hate speech on incitement of violence in African languages while at the same time silencing legitimate documentation of human rights such as in [Senegal, Tunisia, and Egypt](#). It may also lead to skipping of human rights impact assessments which creates a fertile ground for authoritarianism, control of the digital spaces and curtailing fundamental human rights and freedoms and the activities of HRDs to defend human rights.

### 3. Digital restrictions to privacy

- What risks have emerged for HRDs with the increasing procurement, use and abuse of digital surveillance tools, including spyware and interception technologies, by State and non-State actors?

The [CIPESA State of Internet Freedom in Africa 2025 report](#) documents a continent-wide pattern of governments deploying AI-enabled surveillance tools against HRDs.. Facial recognition systems integrated with digital identity infrastructure and closed-circuit television (CCTV) networks, biometric tracking is expanding rapidly across the region. These systems which include biometric border management systems, AI-assisted policing tools, and smart city surveillance infrastructure are increasingly deployed in the name of national security to identify, monitor, track, and suppress civic dissent. Governments including Ethiopia, Kenya, Nigeria, Rwanda, Tanzania, South Africa, Uganda, Zambia, and Zimbabwe among others have heavily invested in the largely surveillance enabling [smart city infrastructure](#) procured from tech companies such as Huawei.

The overwhelming procurement of surveillance systems have perpetuated unchecked deployment of AI-powered surveillance especially by authoritarian governments [against HRDs](#). Moreover, the civic environment is largely dominated by opaque content moderation practices-with limited judicial oversight. This trend accounts for the increasingly [dismantled space for democratic participation](#) across the African continent.

With the heavy deployment of AI enabled systems, monitoring, identifying and tracking of HRDs and their activities has become the norm. Policing of HRDs and their activities and interception of their communications has never been easy like it is now. In Kenya for example, AI technologies and systems including surveillance tools like spyware were used to track and [identify protectors in the Gen Z demonstrations](#), while countries like Tanzania, Uganda and Mozambique are known to have deployed AI surveillance tools to monitor and check activities of the political critics and dissidents. The sum effect has been the creation of a chilling effect on the exercise of fundamental human rights and freedoms like privacy, freedom of expression, assembly, association, and access to information. In most cases, HRDs have gone into [self-censorship](#) and withdrawn from digital platforms due to state overreach.

- What risks have emerged for HRDs with the expansion of biometric surveillance infrastructure and increased monitoring of public and digital spaces?

Expansion of biometric surveillance is made possible by enhanced biometric data collection including finger prints, thumb prints, iris and facial recognition. Technologies deployed in this mass data protection have put [HRDs at risk](#) since data is easily available and data subjects can be easily monitored and identified. It is even worse for HRDs who are key targets of the state and its operatives and agencies. Biometric surveillance has made [monitoring of HRDs work systematic](#). The integration of [centralized biometric digital ID systems](#) which is mandatory accounts for disenfranchisement of marginalized populace and exposure of activists to potential and massive data breaches which in turn perpetuates a chilling effect on human rights and freedoms and self-censorship.

With at least 49 countries on the continent including among others, [Algeria, Egypt, Kenya, Mauritius, Mozambique, Nigeria, Rwanda, Senegal, Uganda, Zambia, and Zimbabwe](#), [Ghana, Malawi, Morocco, South Africa, and Tanzania](#), adopting biometric tracking systems, state surveillance will continue, be more enhanced and put a chill on the exercise of digital rights and freedoms.

- How have technological and regulatory developments relating to encryption eased or exacerbated risks to HRDs?

A critical risk for HRDs is the continuous attempt by States to weaken digital security through outlawing encryption. States are banning encryption under justifications such as national security, cybercrime prevention, and law enforcement. Countries such as Democratic Republic of Congo, Malawi, Mali, Namibia, South Africa, and Uganda, have embarked on mandating access to encrypted communications. Similarly in other countries, cryptography providers using regressive laws such as cybersecurity and crimes laws and regulation of interception of communications laws are required to flag some types of encryption while others are required, to ensure that information flowing through their services is decrypted. These measures undermine end-to-end encryption of HRDs including journalists and whistleblowers communications since they facilitate interception of communications and render them easy offline targets. The requirement for assistance in interception of communications and decryption measures by service providers, creates weak points for erosion of privacy and [exploitation of HRDs by cyber criminals](#). End-to-end encryption is a non-negotiable security requirement for HRDs operating under conditions of state surveillance and repression. Regulatory proposals that mandate "backdoors," data localisation, or retention requirements pose an existential threat to HRDs' work by enabling blanket monitoring and eliminating secure communication channels. Technological developments that increase the accessibility and strength of encryption tools offer an important counterbalance to the expansion of state surveillance capacity.

- How do advances in AI technologies exacerbate risks to the privacy and safety of HRDs?

Beyond surveillance, HRDs in Africa including the [Democratic Republic of the Congo \(DRC\)](#), [Kenya](#), [Tunisia](#), and Uganda among others face a growing threat from AI-generated disinformation campaigns designed to discredit, intimidate, and silence them. [Africa's democracies](#) are widely facing AI driven disinformation. The use of synthetic multimedia content, deepfakes, AI-generated social media posts, and manipulated images to spread false narratives about activists, journalists, and civil society organisations is now more elevated. These attacks are particularly acute during election periods, with documented cases in Namibia and Kenya, where AI tools amplified disinformation targeting credible voices in public discourse. An overwhelming majority of African countries lack comprehensive AI legislation or AI-specific regulatory frameworks. While several countries have developed or are developing national AI strategies and the African Union adopted a Continental Artificial Intelligence Strategy in July 2024, the translation of strategic ambition into binding, enforceable, rights-protective regulation remains nascent. This regulatory vacuum has direct consequences for HRDs. In the absence of mandatory human rights impact assessments for AI deployments, pre-deployment review requirements for high-risk AI systems, and independent oversight mechanisms with genuine investigative and enforcement powers, governments and private actors face no binding obligation to assess or mitigate the harms their AI deployments impose on HRDs and civic space. CIPESA's research calls for the enactment of comprehensive AI legislation aligned with international human rights standards, the establishment of empowered and independent AI governance institutions, and the mandating of algorithmic transparency and accountability mechanisms.

#### **4. Corporate responses**

- How are companies meeting their responsibilities to identify, assess, mitigate and respond to risks posed to HRDs on their platforms and services?

Companies efforts to comply with and align with the UN Guiding Principles on Business and Human Rights are largely [inadequate](#). Human rights due diligence is lacking and business risks to human rights are still high. [Internet shutdowns by ISPs and telecoms](#) have been predominant on the continent on orders of the State, and tech facilitated gender based violence continues to be

perpetuated due to lack of [local cultural and linguistic context](#). Telcos and ISPs have also been cited in [transferring data of HRDs and dissidents](#) to the state operatives

- Are existing corporate models and approaches to risk assessment, due diligence, remedial mechanisms and engagement with HRDs on protection concerns and reports of violations sufficient and/or effective?

Corporate models and approaches to risk assessment, due diligence, remedial mechanisms and engagement with HRDs remain largely insufficient and ineffective. Most companies operating in Africa have not been able to comply with UN Guiding Principles on Business and Human Rights (UNGPs) with clear failure to identify and mitigate common risks. In addition, structural imbalances cannot allow local communities access mechanisms for redress of abuses. For instance, [Uganda's oil sector](#) and mining in the [DRC](#) and [South Africa](#) have witnessed violent targets on HRDs.

- What challenges do civil society and companies face in ensuring corporate policies, processes and initiatives – including in relation to internal mechanisms and external engagement – adequately and effectively address the range and extent of risks faced by HRDs in the digital age?

Civil society organizations [face](#) weak digital security, a rapidly shrinking civic space, and chronic underfunding. Governments in countries like Malawi and [Uganda](#) increasingly monitor human rights defenders, undermining their work. Meanwhile, tech companies struggle to align their business models and processes with human-rights due diligence and lack [adequate](#) accountability and transparency. This gap, along with pressure from states, makes it difficult for telecoms across the continent (e.g., Tanzania, Togo, Uganda, [Zimbabwe](#)) to resist onerous orders such as [internet shutdowns](#). Companies have also [failed to counter](#) smear campaigns and address localized digital threats because their content and security approaches prioritize digital capitalism and surveillance over community needs.

- What steps should companies take to improve identification, assessment and prevention of risks posed to HRDs' work and safety on their platforms and services?

Companies should:

- ❖ Substantially expand content moderation capacity, staffing, and AI detection tools for African languages, recognising the differential protection gap that current practices create.
- ❖ Implement 'rights-by-design' principles across the product development lifecycle, with HRD-specific protections embedded in privacy settings, account security features, and data governance policies.
- ❖ Publish disaggregated, country-level transparency reports on government data requests and content removal decisions, including for African markets.
- ❖ Establish accessible, well-resourced, and geographically sensitive rapid-response mechanisms for HRDs experiencing coordinated online attacks, including TFGBV.
- ❖ Look deeply into government requests for user data, content takedowns, or platform blackouts and weigh them against international human rights standards. Companies should adhere to the UN Guiding Principles on Business and Human Rights and stop complying with regressive directives in the name of local compliance when local laws violate fundamental human rights.
- ❖ Establish channels for secure reporting of human rights abuses including coordinated smear campaigns, cyber harassment, attacks and doxxing. These should be multilingual, gender-sensitive, and highly accessible to HRDs.