APC submission to the Office of the High Commissioner for Human Rights

Input to the report of the UN High Commissioner for Human Rights pursuant to HRC resolution 58/23 on “Human rights defenders and new and emerging technologies: protecting human rights defenders, including women human rights defenders, in the digital age”

About APC

The Association for Progressive Communications (APC) is an international civil society organisation and a network of members dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communications technologies (ICTs). APC currently has 74 organisational members and 44 associates active in 74 countries, primarily in the Global South.

ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

MARCH 2026

Background:

- APC, through its network of members and partners, has documented how digital technologies that are so often framed as universal enablers of expression and participation have become a terrain where women human rights defenders (WHRDs), activists and marginalised communities are targeted, silenced and endangered.
- From gendered disinformation campaigns and algorithmic abuse that delegitimise women's voices, to intrusive surveillance and digital repression that mirror and amplify offline violence, APC's work with networks across Africa, Latin America, SWANA and Asia Pacific reveals a continuum of harms that violate rights to freedom of expression, privacy and association.
- Drawing on research, capacity building, submissions to UN processes and feminist holistic security strategies co-developed with grassroots WHRDs and documented through initiatives like the annual Global Information Society Watch (GISWatch) report, this submission situates protection of defenders squarely with the geopolitical and technological realities that shape their safety and participation in public life.

Questions:

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

- *For each of the questions listed above, please provide information on the national, regional or international laws or regulations referred to, case examples and other relevant illustrative data.*

- APC has documented how national security, counter-terrorism and cybercrime legislation and other measures, like defamation, libel laws and frameworks regulating civil society, are weaponised against WHRDs, including those who expose sexual harassment and violence or government corruption.
- APC's mapping of cybercrimes and internet-specific laws demonstrates how broadly drafted provisions with vague terminology empower discretionary enforcement that criminalises dissent and undermines human rights. These laws often fail tests of legality, necessity and proportionality, creating chilling effects for freedom of expression and association, particularly for marginalised groups, including women, LGBTQIA+ activists and HRDs.
- An APC exploratory report co-authored by Derechos Digitales documents how such frameworks are used to prosecute activists, deepening gender inequalities.
- Cybercrime and "online harm" legislation that lacks human rights safeguards and gender analysis is actively used to suppress critical voices. In Nicaragua, WHRDs have been prosecuted under special cybercrime laws for political content, while in the Democratic Republic of Congo, journalists and activists face defamation charges under Digital Code 2023, inhibiting scrutiny of government actions. In The Gambia, provisions on false publication and sedition have been repeatedly deployed to arrest human rights activists.
- In Kenya, proposed amendments to cybercrime law signal a legislative trend towards expanding state control of online spaces.
- These efforts may undermine rights to free expression, peaceful assembly and association, disproportionately impacting WHRDs and activists. Legal frameworks that criminalise false information, "immoral" content and digital dissent within one jurisdiction often lead to similar measures elsewhere.
- Civil society has called for essential human rights safeguards in the UN Cybercrime Convention negotiations, emphasising prior judicial authorisation, gender mainstreaming, and limits on procedural abuses. Without these,

international frameworks can legitimise surveillance and censorship powers that states may export, solidifying restrictive legal models across regions.

- Across these trends, the absence of gender-responsive legislation is a worrying gap. APC's Framework for Developing Gender-Responsive Cybersecurity Policy highlights that cyber-related laws rarely account for differentiated impacts on women and gender-diverse people, reinforcing systemic exclusion. Without gendered legal analysis, regulatory responses to information integrity and online safety can inadvertently perpetuate existing harms and inequality.

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?*
- *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?*
- *What specific risks to HRDs emerge via online platforms and communications services in situations of armed conflict, instability and/or elections?*
- *What specific risks do women HRDs and HRDs from groups affected by marginalisation and discrimination face on online platforms and communications services?*
- *How do companies' policies and practices relating to content moderation and engagement with law enforcement and government authorities affect HRDs' work and safety?*
- *How do advances in AI technologies exacerbate risks to HRDs' operations and presence on online platforms and communications services?*
- *For each of the questions listed above, where possible, please provide case examples, references to State or corporate policies, practices or initiatives, and other relevant illustrative data.*

- **Internet shutdowns and connectivity restrictions undermine WHRDs' work and safety**
    - APC's submission on internet shutdowns documents how deliberate disruptions to connectivity exclude entire communities from participating in civic life, block access to information, impede documentation of abuses, and prevent defenders from communicating and coordinating both online and offline. Shutdowns interrupt monitoring, reporting and early warning systems that HRDs depend on during critical events, including elections and protests, and disproportionately affect marginalised populations. Beyond total shutdowns, partial interference and platform blocks can isolate WHRDs, journalists and civil society at critical moments. Blocking social media not only constrains freedom of expression, but also impacts tools used for emergency communications and legal mobilisation. These restrictions often accompany political and security crises, reinforcing the chilling effect on civic engagement already documented in research.

- **TFGBV intersects with offline harms**
    - APC has been working with members and partners documenting and analysing technology-facilitated gender-based violence (TFGBV)[1] against HRDs and WHRDs.
    - TFGBV has the same roots as other forms of gender-based violence, and is part of the same continuum. Online and offline gender-based violence do not happen in vacuums separate from each other, and violence in any one domain can often produce harm across other domains.
    - Feminists and land defenders in Costa Rica face coordinated harassment on social media that aligns with offline attacks, including threats of arson for their land rights or gender advocacy.

[1] Defined by APC as "acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms and email." See: https://www.apc.org/en/glossary/technology-facilitated-gender-based-violence

    - Cases in Lebanon following the Freedom March involved doxxing of feminist activists across social media platforms, without accountability from authorities or platforms.
    - Cases in Namibia and The Gambia show how women in leadership roles, including WHRDs, face disproportionate TFGBV. Abuse typically occurs via social media and messaging apps, leading to withdrawal from digital spaces due to safety concerns and lack of access to justice.

- **Risks during conflict, instability and elections**
    - Shutdowns often form part of broader digital repression strategies that combine connectivity blackouts with surveillance and restrictive laws.
    - Upcoming research conducted by the Myanmar Internet Project (MIP) and APC reveals that after the February 2021 coup in Myanmar, there were various forms of digital repression, including surveillance, internet shutdowns and the amendment and enactment of laws affecting digital rights. The research refers to this as an "ecosystem" of digital repression, where all of these strategies are interdependent and work symbiotically to silence online dissent.
    - This ecosystem has a differential impact on WHRDs. Restrictions on free expression, pervasive doxxing, harassment on messaging platforms, and targeted extraction and dissemination of private data are tactics used to intimidate and silence WHRDs, deter reporting of abuses, and weaken community support networks during crisis and conflict.
    - APC's feminist research and submissions to human rights mechanisms emphasise that such attacks are shaped by intersecting discrimination, with algorithmic invisibility and content moderation failures further marginalising their voices.

- **Corporate content moderation and engagement with states affect WHRDs**
    - APC's advocacy highlights systemic failures in platform governance as content moderation systems frequently misclassify rights-affirming speech as harmful, disproportionately censor marginalised voices, and

lack transparency and accountability. Algorithms optimised for engagement can amplify hate and harassment rather than protecting users against them. Corporate policies often defer to government directives without independent human rights due diligence, putting HRDs at risk where states seek to suppress dissent.

- **AI and emerging technologies intensify risks**
    - APC's submission to the UN Working Group on discrimination against women and girls highlights how AI systems can exacerbate threats to gender equality by enabling deepfakes, reinforcing biased profiling, and aggravating harms against women and LGBTQIA+ people. AI-driven content moderation lacking contextual nuance increases the likelihood of wrongful removals and shadowbanning of critical speech, while AI-based surveillance technologies weaken privacy protections.

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?*
- *What risks have emerged for HRDs with the expansion of biometric surveillance infrastructure and increased monitoring of public and digital spaces?*
- *How have technological and regulatory developments relating to encryption eased or exacerbated risks to HRDs?*
- *How do advances in AI technologies exacerbate risks to the privacy and safety of HRDs?*
- *For each of the questions listed above, please describe, where possible, case examples, references to State or corporate policies, practices or initiatives, and other relevant illustrative data.*

- **Surveillance**
    - APC has documented how digital surveillance tools, ranging from commercially sold spyware to sophisticated interception systems and biometric data platforms, have been used by states and non-state actors to monitor, intimidate and suppress civil society, including HRDs and WHRDs. These systems often operate in the absence of adequate legal safeguards, violating rights to privacy, expression, association and peaceful assembly. APC's submission on the surveillance industry and human rights highlights the disproportionate impacts of such technologies on gender, sexual and political minorities, journalists and advocates.
    - APC and its partners in its 2024 Kenya UPR joint submission document extensive state digital surveillance that undermines privacy and civic space. It highlights mass data-collection systems, mandatory SIM registration, and national CCTV and social media monitoring as core enablers of pervasive communication interception. These tools operate alongside broad legal powers under national security and anti-terrorism laws, creating conditions for unchecked surveillance by state agencies.
    - Upcoming research supported by APC shows that Myanmar's military has built an expansive digital surveillance state that erodes privacy and targets human rights defenders through widespread collection of personal and biometric data. These pervasive practices have forced WHRDs and activists to alter their digital security behaviours, for instance, tightening privacy settings, using secure messaging apps like Signal, changing devices and adopting pseudonyms, often at additional financial cost.

- **Weaponisation of AI tools against defenders**
    - APC's research on AI and TFGBV documents how AI tools can be weaponised to spread manipulated narratives that discredit women politicians, academics and HRDs. These campaigns often intersect with racist, transphobic or xenophobic – and in certain contexts, religious or caste-based – content aimed at undermining credibility, inciting harassment and deterring political participation.
    - In humanitarian and conflict settings, AI-generated and AI-distributed disinformation can fuel escalation, destabilise communities and increase risks of conflict-related sexual violence. Feminist digital rights advocates have documented how gendered disinformation is used to discredit women peacebuilders and HRDs, exploit ethnic divisions, and legitimise gender-based harassment.

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?*
- *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?*
- *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?*
- *What steps should companies take to improve identification, assessment and prevention of risks posed to HRDs' work and safety on their platforms and services?*
- *For each of the questions listed above, please describe, where possible, case examples, references to corporate policies, practices or initiatives, and other relevant illustrative data.*

- APC has long emphasised that companies operating digital platforms must “use international human rights law as the authoritative global standard” for regulating content and user safety, rather than defaulting to inconsistent state laws or corporate interests. This includes integrating the UN Guiding Principles on Business and Human Rights (UNGPs) into platform governance and decision making. Platforms that fail to align content policies with human rights risk amplifying harm, including violence, silencing of dissent, and algorithmic bias against marginalised voices.
- Analysis by the Business and Human Rights Centre shows that tech companies have generally failed to meet their responsibilities to recognise and mitigate human rights risks, including those affecting HRDs. Over the past decade, less than half of tech companies engaged meaningfully with civil society on human rights allegations, with many lacking transparent human rights due diligence, grievance mechanisms, and accountability for harmful impacts linked to their products and services.
- APC’s work on digital rights and safety highlights that recourse to address grievances must be inclusive, transparent and responsive to the needs of marginalised individuals who face TFGBV, including WHRDs. We emphasise that “greater transparency, better established due process, and other procedural enhancements to company practices would greatly improve their ability to respect human rights, and should be considered a part of company human rights due diligence.”
- Civil society, including APC and its members and partners, face structural barriers when engaging with major tech companies, who often resist transparent dialogue or share limited information about how they address risk and assess impacts, particularly in non-Western, Global Majority contexts. For example, 7amleh, a Palestinian digital rights organisation, repeatedly reports the lack of or delay in response from the tech companies when reached for action regarding hate speech and censorship targeting Palestinian users, including WHRDs, on their platforms. Lebanon-based Social Media Exchange (SMEX) also reported

that social media platforms inadequately address hate speech and cyberbullying, while disproportionately censoring activists, especially in Arabic content.

- In our joint submission to the UN Expert Mechanism on the Right to Development, APC and Derechos Digitales highlight that AI governance must protect cultural rights and ensure accountability for algorithms that shape visibility and access to platforms. In the absence of transparency and safeguards, automated systems often reproduce historical bias and silence marginalised voices, and can amplify gendered, racialised or other discriminatory harms.
- APC's Safety for Voices initiative, grounded in an intersectional feminist holistic security framework, recognises corporate accountability as central to WHRD safety. The programme aims to document and address the ways in which state actions as well as corporate policies shape digital violence. It places emphasis on the amplification of WHRD voices by prioritising holistic safety to ensure that gendered and intersectional harms are understood and mitigated.
- Civil society research and policy advocacy, including submissions by APC to UN processes, argue that companies should conduct robust human rights impact assessments aligned with the UNGPs, and publish transparency reports on how human rights risks are addressed.
- Based on APC's and its members' and partners' expert advocacy and work with communities on the ground across the world, we believe that companies should take the following steps as an imperative starting point:
    - Embed human rights due diligence aligned with the UNGPs across all operations, including identification and mitigation of risks specific to WHRDs.
    - Ensure transparency and accountability in content moderation, algorithmic decision making and data governance policies so that affected communities understand how decisions are made.
    - Establish accessible, gender-responsive reporting mechanisms that are safe, independent and responsive to WHRDs' concerns.
    - Engage regularly and meaningfully with HRDs, WHRDs and civil society to inform risk assessments and policy design with lived experiences.

- Publish clear public commitments and reporting on how human rights risks are assessed and addressed, with specific indicators for WHRDs' safety and platform accountability.
- Avoid complicity with repressive state demands for user data, content takedowns or surveillance without due process and human rights safeguards.