

Stakeholder report: Human rights in the digital context in Namibia



The Association for Progressive Communications (APC), an organisation in consultative status with ECOSOC, advocates the strategic use of information and communications technologies to advance human rights. The APC network has 73 organisational members and 44 associates active in 74 countries.

Contact address: PO Box 29755, Melville 2109, Johannesburg, South Africa

Website: www.apc.org/en

Contact person: Verónica Ferrari, Global Policy Advocacy Coordinator (veronica@apc.org)

I. INTRODUCTION

1. This stakeholder report focuses on key issues relating to human rights in the digital context in Namibia, including digital connectivity and inclusion, freedom of speech and expression online and online disinformation, right to privacy, data protection, surveillance and cybersecurity and technology-facilitated gender-based violence (TFGBV).
2. This review marks the fourth cycle for Namibia in the Universal Periodic Review (UPR) mechanism. During the third cycle, Namibia received six recommendations related to these issues, including one related to data protection and the right to privacy, one addressing the need for digital rights, two on protecting freedom of expression and safeguarding journalists from attacks, one on access to information and one on hate crime legislation.¹ Namibia received over 30 recommendations on strengthening mechanisms to combat gender-based violence, with five of these referring to “all forms” of gender-based violence. However, none of the recommendations expressly addressed the issue of TFGBV.

II. CONTEXT OF THE SITUATION OF HUMAN RIGHTS ONLINE IN NAMIBIA

3. In 2024 Namibia faced persistent challenges in protecting human rights online, particularly regarding freedom of expression and privacy. Although the constitution guarantees these rights,² they are not explicitly extended to digital spaces. The Access to Information Act (2022)³ and the National Cybersecurity Strategy (2022-2027)⁴ aim to enhance transparency and privacy, but implementation has remained weak due to non-operationalisation of the former and the fact that the latter is a voluntary mechanism. Currently, Namibia remains lacking in comprehensive data protection and cybersecurity legislation.
4. Digital rights awareness is critically low.⁵ Civil society has raised concerns over mandatory SIM card registration, metadata retention without safeguards and opaque law enforcement access to communications.⁶ TFGBV and digital inequality – especially in rural and marginalised communities – remain unaddressed.⁷ Plans to pass the data protection bill have been in the pipeline;⁸ however this may pose a risk of weak oversight and increased surveillance.

1. Human Rights Council. (2021). *Report of the Working Group on the Universal Periodic Review: Namibia*. United Nations. <https://documents.un.org/doc/undoc/gen/g21/165/87/pdf/g2116587.pdf>

2. Namibian Constitution, articles 13 and 21. <https://namiblii.org/akn/na/act/1990/constitution/eng@2014-10-13>

3. The Namibian. (2022, 22 June). Historic access to information bill passed. *The Namibian*. <https://www.namibian.com.na/historic-access-to-information-bill-passed/>

4. <https://nam-csirt.na/download/national-cybersecurity-strategy-awareness-raising-plan-2022-2027/>

5. Paradigm Initiative. (2022). *Londa: Digital Rights and Inclusion in Africa Report 2022*. <https://paradigmhq.org/wp-content/uploads/2023/06/Namibia-Londa-2022.pdf>; Links, F. (2024, 25 March). Rights watered down in draft privacy and data protection bill in Namibia. *Association for Progressive Communications*. <https://www.apc.org/en/news/rights-watered-down-draft-privacy-and-data-protection-bill-namibia>

6. Links, F. (2023, 24 December). Namibia's Unfolding 'Identity Crisis'. <https://ippr.org.na/blog/namibias-unfolding-identity-crisis/>; Links, F. (2022, 26 September). New surveillance regulations lurk threateningly in Namibia. *Association for Progressive Communications*. <https://www.apc.org/en/news/new-surveillance-regulations-lurk-threateningly-namibia>

7. Gervasius, N. (2022). *Online Violence Against Women and Girls in Namibia. A country situational assessment*. Internet Society Namibia Chapter. <https://isocnamibia.org/wp-content/uploads/2022/05/Ovaw-Digital.pdf>

8. Menas, D. (2025, 14 August). Govt to introduce data protection bill in September. *The Namibian*. <https://www.namibian.com.na/govt-to-introduce-data-protection-bill-in-september/>

5. Despite ratification of key international treaties associated with digital rights, enforcement gaps hinder the realisation of such rights. The African Declaration on Internet Rights and Freedoms (2019)⁹ has yet to be fully integrated into the national framework in Namibia.
6. The 2024 national elections were marred by ballot shortages and technical failures, prompting a controversial voting extension.¹⁰ During this period, the digital environment was rife with misinformation and disinformation, amplified by social media platforms such as WhatsApp and Facebook. Youth voters, who rely heavily on these platforms, were particularly vulnerable due to low media literacy.¹¹
7. Namibia is a regional leader in press freedom, ranking 28th globally and second in the African continent in 2025, with a score of 75.35 out of 100.¹² This is an improvement from 2024 when Namibia's press freedom ranking had dropped to 34th globally due to concerns over lack of independence, political interference and insufficient protections for the media.¹³
8. Despite concerns over political interference, the judiciary has demonstrated its independence in key cases.¹⁴ In 2024, the Namibian High Court also ruled to decriminalise consensual same-sex relations.¹⁵

III. DIGITAL CONNECTIVITY AND INCLUSION

9. Namibia has made notable strides in digital connectivity since 2018, with internet access reaching 64.3% of the population and mobile broadband usage standing at 64% in mid-2025.¹⁶ The internet penetration rate in the country is cited as 64.4% at the beginning of 2025.¹⁷ In 2024, the Communications Regulatory Authority of Namibia (CRAN) auctioned 3500 MHz spectrum for 5G rollout, which is expected to enable

9. <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf>

10. Freedom House. (2025). *Freedom in the World 2025: Namibia*. <https://freedomhouse.org/country/namibia/freedom-world/2025>; Agence France-Presse. (2024, 28 November). Ballot counting slowly under way in Namibia after long delays. *The Namibian*. <https://www.namibian.com.na/ballot-counting-slowly-under-way-in-namibia-after-long-delays/>; Calitz, E. (2024, 28 November). Namibia's election chaos: Technical failures and ballot shortages spark outrage among voters and parties. *Daily Maverick*. <https://www.dailymaverick.co.za/article/2024-11-28-namibia-poll-slammed-after-after-delays-ballot-shortages-questions-over-id-cards/>

11. Santos, P. (2025). *Mis- and Disinformation in the Run-Up to Namibia's 2024 General Elections*. Office of the Media Ombudsman for Namibia. <https://www.nmt.africa/uploads/685d718d98626/Mis-andDisInformationin2024Elections.pdf>; Namibia Fact Check. (2024, 4 November). Election fake news surge in October 2024. <https://namibiafactcheck.org.na/news-item/election-fake-news-surge-in-october-2024/>; Namundjembo, A. (2025, 26 March). AI, WhatsApp fueled fake news in 2024 elections. *Windhoek Observer*. <https://www.observer24.com.na/ai-whatsapp-fueled-fake-news-in-2024-elections/>

12. Tafirenyika, T. (2024, 11 December). Namibia's press freedom rankings decline amid growing political interference. *The Namibian*. <https://www.namibian.com.na/namibias-press-freedom-rankings-decline-amid-growing-political-interference/>; Reporters Without Borders. (2025) *World Press Freedom Index: Namibia*. <https://rsf.org/en/country/namibia>

13. Tafirenyika, T. (2024, 11 December). Op. cit.

14. High Court of Namibia Main Division, Windhoek. (2020, 20 February). *Esau and Others v Director General: Anti Corruption Commission and Others*. <https://namiblii.org/akn/na/judgment/nahcmd/2020/59/eng@2020-02-20>; High Court of Namibia Main Division, Windhoek. (2025, 20 August). *Shanghala and Others v President of the Re-public of Namibia and Others*. <https://namiblii.org/akn/na/judgment/nahcmd/2025/474/eng@2025-08-20>

15. Kojoué, L. (2024, 25 June). Namibia Court Decriminalizes Consensual Same-Sex Conduct. *Human Rights Watch*. <https://www.hrw.org/news/2024/06/25/namibia-court-decriminalizes-consensual-same-sex-conduct>

16. Kemp, S. (2025, 3 March). Digital 2025: Namibia. *DataReportal*. <https://datareportal.com/reports/digital-2025-namibia>

17. Ibid.

smart cities and internet of things (IoT) deployment.¹⁸ Government initiatives, including an investment of NAD 145 million (USD 8,410,000) via the Universal Service Fund (USF) aimed at expanding information and communication technology (ICT) accessibility in underserved areas,¹⁹ have contributed to an evident shift to data-driven services, with internet-enabled SIM cards rising from 58% to 61% of active SIMs.²⁰ Fixed broadband is slowly growing, with 100,000 subscriptions and 44,000 fibre connections.²¹

10. Despite the increase in digital access in the country, stark disparities persist: only 16.2% of rural households have mobile internet, compared to 50.3% in urban areas, and smartphone ownership remains low at 28.5%.²² While 93% of Namibians have basic telecom access, many rural schools and clinics lack reliable infrastructure.²³ Affordability remains a persistent barrier: the mobile data and voice high consumption basket price represents 92.2% of gross national income (GNI) per capita while the fixed broadband basket price represents 75.9% of GNI.²⁴ Digital literacy²⁵ and gender disparities²⁶ further hinder inclusion, with women facing limited access and participation in ICT sectors. A 2020 report by the Internet Society Namibia Chapter found that only 47% of Namibian women had internet access.²⁷
11. Namibia introduced digital IDs, focusing on refugees in implementation, under the Civil Registration and Identification Act (2024), which is awaiting operationalisation.²⁸ While this law has been praised for containing essential elements of data protection, critics have highlighted the lack of a personal data protection law and raised concerns around exclusion.²⁹
12. Digital connectivity has improved but there are gaps in rural access to the internet, limited smartphone use and weak legal protections, thus underscoring the need for robust reforms to ensure inclusive digital rights and democratic integrity.³⁰

-
18. Connecting Africa. (2023, 29 May). Namibia to Auction 5G Spectrum. *Connecting Africa*. https://www.connectingafrica.com/author.asp?section_id=816&doc_id=785095; World Bank Group. (2022). *Creating Markets in Namibia*. <https://documents1.worldbank.org/curated/en/099850311112236455/pdf/IDU0ff2db1400403c046b2099a300571336f9a6d.pdf>
 19. The Brief. (2025, 19 March). Govt backs Universal Service Fund with N\$145 million in seed funding. *The Brief*. <https://thebrief.com.na/2025/03/govt-backs-universal-service-fund-with-n145-million-in-seed-funding/>
 20. Menas, D. (2025, 16 September). Internet SIM card use grows by 3 percentage points. *The Namibian*. <https://www.namibian.com.na/internet-sim-card-use-grows-by-3-percentage-points/>; Lazarus, S. (2025, 5 March). Namibians SMS less, WhatsApp more. *The Namibian*. <https://www.namibian.com.na/namibians-sms-less-whatsapp-more/>
 21. Market Watch. (2025, 13 June). Namibia embraces fibre and data as traditional telecoms shift gears. *Market Watch*. <https://market-watch.com.na/business/namibia-embraces-fibre-and-data-as-traditional-telecoms-shift-gears2025-06-13160023>
 22. Namibia Statistics Agency. (2024). *Namibia 2023 Population and Housing Census. Main Report*. <https://nsa.org.na/census/wp-content/uploads/2024/10/2023-Population-and-Housing-Census-Main-Report-28-Oct-2024.pdf>
 23. Hangala, N. (2025, 20 August). CRAN Assessment Reveals Deep Internet Connectivity Gaps. *The Villager*. <https://www.thevillager.com.na/national/2025/cran-assessment-reveals-deep-internet-connectivity-gaps/>
 24. International Telecommunication Union. (2023). *Measuring digital development. The ICT Development Index 2023*. <https://www.itu.int/itu-d/reports/statistics/idi2023/>
 25. Mhani, H. (2024, 25 June). Embracing the Digital Future: The Crucial Role of Digital Literacy in Namibia. *Communications Regulatory Authority of Namibia*. <https://www.cran.na/embracing-the-digital-future-the-crucial-role-of-digital-literacy-in-namibia/>
 26. GIP Digital Watch. (2020, 5 August). Women and the ICTs in Namibia. *GIP Digital Watch*. <https://dig.watch/updates/women-and-icts-namibia>
 27. Internet Society Namibia Chapter. (2020). *Women's Rights Online Report Card: Namibia. Measuring Progress, Driving Action*. <http://web-foundation.org/docs/2020/08/GenderReport-Namibia.pdf>
 28. Macdonald, A. (2024, 24 June). Namibia begins issuance of much-anticipated biometric ID cards to refugees. *BiometricUpdate.com*. <https://www.biometricupdate.com/202406/namibia-begins-issuance-of-much-anticipated-biometric-id-cards-to-refugees>; Maritz, Y. (2025, 3 September). Season 3: Namibia's Digital Identity Journey – From Vision to Reality. *UNDP Namibia*. <https://www.undp.org/namibia/blog/season-3-namibias-digital-identity-journey-vision-reality>
 29. Macdonald, A. (2024, 9 September). Namibia's new CRVS, national ID system reflects key data protection aspects. *BiometricUpdate.com*. <https://www.biometricupdate.com/202409/namibias-new-crvs-national-id-system-reflects-key-data-protection-aspects>
 30. Kemp, S. (2024, 23 February). Digital 2024: Namibia. *DataReportal*. <https://datareportal.com/reports/digital-2024-namibia>; Nangalo, N. (2024, 12 June). Digital Divide Hinders Growth – Theofelus. *Namibian Sun*. <https://www.namibiansun.com/local-news/digital-divide-hinders-growth-theofelus2024-06-12>

13. In the absence of a national artificial intelligence (AI) strategy or regulatory framework, there is limited scope for coordinated development on AI. There is a real risk that algorithmic bias could cause harm to vulnerable groups.³¹

IV. FREEDOM OF SPEECH AND EXPRESSION ONLINE AND ONLINE DISINFORMATION

14. Namibia generally maintains a favourable environment for freedom of expression, with a World Press Freedom Index ranking of 22 in 2023, 34 in 2024 and 28 in 2025.³² However, the 2024 presidential and parliamentary elections were accompanied by a surge in misinformation, particularly on social media.³³
15. Gendered disinformation targeted female candidates. This included AI-generated content falsely depicting President Netumbo Nandi-Ndaitwah falling, as well as fabricated religious messages aimed at presidential candidate Ally Angula, with “God asking her to withdraw” from the elections.³⁴
16. Namibia does not have laws to enforce content moderation. Google reports 44 items flagged by the government between 2011 and 2024, with three total removal requests.³⁵ The government did not request any data or content removal from Meta in 2024,³⁶ but shadow banning and content suppression – especially of Indigenous peoples, such as the Ovahimba – are persisting concerns.³⁷ An example of this is illustrated by the June 2025 decision of the Meta Oversight Board to overturn two cases of content removal by Meta involving bare-chested Indigenous Himba women. The Oversight Board highlighted that nudity is a socially and historically accepted aspect of Himba custom and that both posts showed sufficient indications of implicit consent to being photographed or recorded. It also recommended that Meta publish its Adult Nudity and Sexual Activity policy exception (applied on escalation only) allowing content depicting bare-chested Indigenous women in circumstances where it reflects socially accepted custom and belief and does not misrepresent such practices.³⁸

31. Shalihaxwe, E. (2025, 12 August). AI readiness stalled by policy shortfall – Steenkamp. *Windhoek Observer*. <https://www.observer24.com/na/ai-readiness-stalled-by-policy-shortfall-steenkamp/>

32. Reporters Without Borders. (2025). Op. cit.; Matthys, D. (2024, 6 May). Disappointment as Namibia loses top position on press freedom. *The Namibian*. <https://www.namibian.com.na/disappointment-as-namibia-loses-top-position-on-press-freedom/>

33. Shihepo, T. (2024, 26 November). Elections run by insults, fake news, influencers, paid propaganda. *The Namibian*. <https://www.namibian.com.na/elections-run-by-insults-fake-news-influencers-paid-propaganda/>; Links, F. (2025). *AI & 2024 Election Disinformation. Countering Electoral Disinformation*. Institute for Public Policy Research. <https://ippr.org.na/publication/ai-2024-election-disinformation/>

34. Namibia Fact Check. (2024, 4 November). Op. cit.

35. Google Transparency Report. (2024, July-December). *Government requests to remove content: Namibia*. <https://transparencyreport.google.com/government-removals/government-requests/NA>

36. Meta Transparency Center. (2024, July-December). *Government Requests for User Data: Namibia*. <https://transparency.meta.com/reports/government-data-requests/country/NA/>

37. Oversight Board. (2025, 3 June). *Images of Partially Nude Indigenous Women*. <https://www.oversightboard.com/decision/bun-s8141r-ab/>

38. Oversight Board. (2025, 3 June). *Ban on Showing Indigenous Nudity Disproportionately Limits Expression*. <https://www.oversightboard.com/news/ban-on-showing-indigenous-nudity-disproportionately-limits-expression/>

V. RIGHT TO PRIVACY, DATA PROTECTION, SURVEILLANCE AND CYBERSECURITY

17. Namibia lacks comprehensive laws on cybercrime, data protection and personal data privacy. A National Cybersecurity Strategy was adopted in March 2022,³⁹ but the absence of a national cybersecurity framework and the long-delayed Cybercrime Bill (drafted in 2014) hinder effective response and alignment with global standards.⁴⁰ There were around 2.7 million cyberattacks recorded in the country in 2022.⁴¹ Similar threats are faced by the telecommunications sector as well, such as the data breach affecting Telecom Namibia in late 2024, wherein sensitive information of over 619,000 clients was exposed.⁴² A data breach experienced by the Namibia Student Financial Assistance Fund in October 2025 exposed personal information of over 7,000 students.⁴³
18. Namibia has ratified the African Union's Malabo Convention, which came into force in June 2023, signalling regional commitment to cybersecurity and data privacy. However, domestic implementation remains slow. Efforts are still underway to revise the 2013 Data Protection Bill and update the Communications Act of 2009.⁴⁴
19. The 2023 mandatory SIM card registration law requires that biometric data be linked to national IDs and mandates telecoms to retain user metadata for five years. While framed as a security measure under the Communications Act of 2009, the policy lacks transparency and oversight, raising concerns about surveillance and self-censorship since there are no legal protections for encryption, pseudonymity or secure communication tools.⁴⁵ The resulting increase in biometric data collection and storage makes it even more urgent for Namibia to enact a strong data protection law.

VI. TECHNOLOGY-FACILITATED GENDER BASED VIOLENCE

20. Technology-facilitated gender-based violence (TFGBV),⁴⁶ such as cyberstalking, online harassment and doxxing, encompasses acts of gender-based violence that are committed,

39. <https://mict.gov.na/documents/869282/1009163/National+CyberSecurity+Strategy+and++Awareness+Raising+Plan+2022+-+2027++13+10+22.pdf/ea059f22-173f-ad8f-47a3-eb29cd0a0ee1?t=1757529184891>

40. Ajibade, A. (2024, 10 September). Namibia to finalise data and cybercrime bills soon. *Tech Point Africa*. <https://techpoint.africa/2024/09/10/namibia-finalise-data-cybercrime-bills/>; Amutenja, H.-M. (2023, 26 September). Namibia's Cybercrime Bill Undergoes Redrafting. *Windhoek Observer*. <https://www.observer24.com.na/namibias-cybercrime-bill-undergoes-redrafting>; Links, F. (2022). *Familiar Flaws – Unpacking Namibia's draft Cybercrime Bill*. Institute for Public Policy Research. <https://ippr.org.na/wp-content/uploads/2022/03/Familiar-Flaws-MHRC-Feb-2022-web-2.pdf>

41. Kangumine, V. (2024, 17 July). Namibia experiences over two million cyber attacks per year. *The Namibian*. <https://www.namibian.com.na/namibia-experiences-over-two-million-cyber-attacks-per-year/>

42. Lee, G. (2024, 18 December). Namibia Ransomware Attack: Sensitive Data of Government Officials and Citizens Leaked. *Security Daily Review*. <https://dailysecurityreview.com/news/namibia-ransomware-attack-sensitive-data-of-government-officials-and-citizens-leaked/>; Siririka, P. (2024, 16 December). Telecom hit by massive cyberattack ... over 400 000 files 'leaked'. *New Era Live*. <https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked/>

43. Namibia Economist. (2025, 3 October). NSFAF data breach exposes student personal information. *Namibia Economist*. <https://economist.com.na/101217/technology/nsfaf-data-breach-exposes-student-personal-information/>; Shipena, J., & Petersen, S. (2025, 3 October). Shocking Lapse: NSFAF clueless about cyberattack ... Over 7 000 students' data exposed online. *Windhoek Observer*. <https://www.observer24.com.na/shocking-lapse-nsfaf-clueless-about-cyberattack-over-7-000-students-data-exposed-online/>

44. Government Gazette of the Republic of Namibia. (2022). *Draft Data Protection Bill 2021*. <https://action-namibia.org/wp-content/uploads/2022/10/Data-Protection-Draft-Bill-March-2022....pdf>

45. Hubbard, D. (2024, 5 September). Namibia navigates biometric data privacy pending civil registration bill. *Association for Progressive Communications*. <https://www.apc.org/en/news/namibia-navigates-biometric-data-privacy-pending-civil-registration-bill>; The Brief. (2023, 26 May). CRAN bans mandatory biometric data collection for SIM card registration. *The Brief*. <https://thebrief.com.na/2023/05/cran-bans-mandatory-biometric-data-collection-for-sim-card-registration/>

46. In this submission, we primarily use the term "technology-facilitated gender-based violence" (TFGBV), while many other terms, such as "online gender-based violence" (OGBV), are in use in international human rights spaces. Since our early research in this area, we have understood that technology-related GBV includes a broader scope of harms to be addressed, including violence facilitated by technology in so-called "offline" or on-ground lives, rather than just violence that happens in an online space.

abetted or aggravated, in part or fully, by using ICTs, including phones, the internet, social media platforms and email. 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 occur in isolation, as women and gender-diverse people's lives online intersect frequently and in various complex ways with other areas of their lives, and harm in one domain can often produce harm across others.⁴⁷

21. Namibia has several laws aimed at curbing gender-based violence but lacks specific laws to address TFGBV. Non-consensual image sharing and sexualised hate speech have increased, as has online engagement on this topic.⁴⁸ A robust data protection law is also needed so women can combat such instances.⁴⁹
22. Though TFGBV is increasing, it remains underreported and poorly addressed. Law enforcement and social service sectors lack capacity, training, protocols and legal frameworks to respond effectively, causing many victims to retreat from online spaces and widening the gendered digital divide.⁵⁰
23. Women in leadership roles, including politicians, journalists, human rights defenders and influencers face disproportionate TFGBV.⁵¹ 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.⁵² Political leaders such as Sofia Shaningwa, secretary general of the South West Africa People's Organisation, and Emma Theofelus, who in March 2020 became the youngest Namibian deputy minister of information, communication and technology, have frequently been the target of such attacks.⁵³
24. A study conducted by Survey Warehouse revealed that that 94% of LGBT+ respondents faced online hate speech in 2024, with 59% experiencing multiple forms of discrimination.⁵⁴ The report pointed to an increase in hate speech, manifesting as harassment, threats, doxxing and derogatory language, leading to severe mental health impacts, and it highlighted that fewer than 20% of respondents were aware of legal protections and online safety measures.⁵⁵

47. Association for Progressive Communications. (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*. https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_O_0.pdf; Association for Progressive Communications. (2023). *Feminist Principles of the Internet: Advocacy brief on violence*. <https://genderit.org/node/5664>

48. Gervasius, N. (2022). Op. cit.

49. Ibid.

50. Internet Society Namibia Chapter. (2020). Op. cit.; Gervasius, N. (2022). Op. cit.

51. Gervasius, N. (2022). Op. cit.

52. Zviyita, I., & Mare, A. (2024). Same threats, different platforms? Female journalists' experiences of online gender-based violence in selected newsrooms in Namibia. *Journalism*, 25(4), 779-799. <https://journals.sagepub.com/doi/pdf/10.1177/14648849231183815>; Gervasius, N. (2022). Op. cit.; Maundu, C. (2025, 1 August). How Safety-by-Design tech can end technology-facilitated gender-based violence in Africa. *Global Voices*. <https://globalvoices.org/2025/08/01/how-africa-is-leading-the-charge-in-tackling-gender-based-violence-online/>

53. Gervasius, N. (2022). Op. cit.

54. Keulder, C. (2024). *The Digital Closet: Experiences of Hate Speech in Virtual Environments Among Namibia's LGBT+ Community*. Namibia Diverse Women's Association (NDWA) and NMT Media Foundation. <https://surveywarehouse.com.na/wp-content/uploads/2024/12/TheDigitalCloset-report.pdf>

55. Ibid.

VII. RECOMMENDATIONS

25. We recommend that the government of Namibia take the following measures to uphold human rights in the digital context:

Digital connectivity and inclusion

- Develop a national digital inclusion strategy, focusing on infrastructure, affordability and equitable access in rural areas. Mainstream a gender perspective in the strategy.⁵⁶ Expand digital literacy and rights awareness programmes, especially targeting women, youth and marginalised populations.
- Invest in infrastructure to extend broadband internet access to rural areas, including through partnerships with private sector providers and community-based networks.
- Strengthen regulatory frameworks, support community networks and prioritise inclusive ICT education and infrastructure financing.
- Fully implement the USF. Create enabling policy and regulatory environments for the development and sustainability of community-led networks as supported by Recommendation ITU-D 19.⁵⁷ This can include creating simple, affordable licensing and making public funding available to them and other small-scale networks, particularly through the effective use of the USF, supporting civic initiatives in small-scale infrastructure, providing training and capacity building for meaningful connectivity and content creation, offering tax incentives and providing access to financing.
- Implement programmes on early digital rights education and awareness activities, including prioritising digital literacy education in public primary and secondary schools to empower people with skills to navigate the digital space safely and critically.
- Offer targeted training programmes for adults, especially women, to equip them with the necessary digital skills for employment and participation in society. Implement mentorship programmes to increase the number of girls taking up ICT-related courses in school.
- Ensure that digital access is inclusive and equitable for all. Address barriers to accessing technology and the internet by marginalised communities, including rural communities, women and persons with disabilities. For this, the government should establish institutionalised bottom-up participation and multistakeholder decision-making processes to promote inclusive participation of communities in policy making concerning access and digital inclusion.

56. United Nations. (2024). *Global Digital Compact*. <https://www.un.org/global-digital-compact/en>

57. International Telecommunication Union. (2010). *Recommendation ITU-D-19*. https://www.itu.int/dms_pubrec/itu-d/rec/d/D-REC-D.19-201003-1!!PDF-E.pdf; International Telecommunication Union. (2021). *Digital trends in Africa 2021. Information and communication technology trends and developments in the Africa region, 2017-2020*. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG-TRENDS_AFR.01-2021-PDF-E.pdf

Freedom of speech and expression online and online disinformation

- Promote healthy information systems that include robust access to public information, plural, accessible and diverse media contexts, independent and qualified journalism and the possibility of expressing ideas safely to counter disinformation.⁵⁸ This includes encouraging social media platforms to take proactive measures to address disinformation and provide transparency on their algorithms and content moderation policies.
- Work with civil society organisations and community leaders on public awareness campaigns to promote tolerance, inclusivity and respect for diversity.
- Require internet intermediaries to ensure that in moderating or filtering online content, they mainstream human rights safeguards into their processes and adopt mitigation strategies to address all restrictions on freedom of expression and access to information online.
- Ensure that platforms provide transparency on requests for removal of content and incorporate appeal mechanisms and that they comply with their responsibilities under the United Nations Guiding Principles on Business and Human Rights (UNGP-BHR), including the right to freedom of opinion and expression.
- In line with the UNGP-BHR, ensure that social media companies exercise due diligence and conduct regular human rights assessments of their products, operations and policies, with a view to identifying, preventing or mitigating actual or potential adverse impacts on human rights and to provide remediation.⁵⁹

Right to privacy, data protection, surveillance and cybersecurity

- Enact cybersecurity and cybercrime-related frameworks, ensuring that these are aligned with Namibia's obligations under international human rights law. Cybersecurity-related policies must provide security in a way that reinforces human rights.⁶⁰
- Pass the Cybercrime Bill through ongoing open, inclusive and transparent approaches that involve all stakeholders, including civil society and human rights defenders. Specific gender impact assessments should be carried out before approval of the law. Refrain from using vague and overly broad terms in criminal definitions.⁶¹
- Enact a strong data protection law consistent with international standards, including necessary oversight mechanisms, recourse for breach of personal data and establishment of an independent data protection authority with investigative, enforcement and remedial powers.

58. Association for Progressive Communications. (2025). *APC policy explainer: Disinformation*. <https://www.apc.org/en/pubs/apc-policy-explainer-disinformation>

59. Khan, I. (2023). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Irene Khan. United Nations. <https://docs.un.org/en/A/78/288>

60. Association for Progressive Communications. (2024). *APC policy explainer: A human rights-based approach to cybersecurity*. <https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity>

61. Association for Progressive Communications & Derechos Digitales. (2024). *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks*. https://www.apc.org/sites/default/files/gender_considerations_on_cybercrime_0.pdf

- Encourage companies operating in Namibia to implement robust cybersecurity measures to protect personal data and prevent cyberattacks, in line with the government's obligations under the UNGP-BHR.
- Refrain from the use or transfer of new and emerging technologies, including artificial intelligence applications and spyware, where they are impossible to operate in compliance with international human rights law or pose undue risks to the enjoyment of human rights, unless and until the adequate safeguards to protect human rights and fundamental freedoms are in place.⁶² Set up an adequately resourced independent judicial mechanism with oversight of the state surveillance apparatus.
- Guarantee adequate independent oversight mechanisms that operate on principles of transparency and accountability, provide redress mechanisms to victims and control state surveillance practices to ensure they are limited and proportional in accordance with international human rights standards. Ensure that journalists and activists can operate without fear of digital surveillance or retaliation.
- Provide transparency reports on SIM card registration and data retention procedures, including clear limitations on retention duration and requirements for judicial authorisation prior to data access. Enable the use of encryption and anonymous communication tools to safeguard user privacy.
- Align surveillance and content regulation frameworks with human rights protections enshrined in the Namibian Constitution and in international legal standards, ensuring accountability, proportionality and respect for fundamental freedoms.

Technology-facilitated gender-based violence

- Enact and enhance measures and policies to prevent, prohibit, investigate and prosecute TFGBV. Engage with specialists in TFGBV, including civil society organisations, survivors and academics for such law reform. Ensure that legislative responses to tackle TFGBV are gender-responsive and in line with international human rights standards.
- Provide redress and reparation as an effective, efficient and meaningful way of aiding victims of TFGBV and ensuring that justice is achieved. Such measures should include forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic, material, individual and collective, depending on the circumstances and the preferences of the victim.
- Train judiciary personnel, lawyers, police and law enforcement officials and frontline workers to ensure their ability to investigate and prosecute perpetrators and foster public trust in obtaining justice for cases of TFGBV, in conjunction with broader sensitisation on addressing gender-based violence.

62. Human Rights Council. (2025). *Human rights defenders and new and emerging technologies: protecting human rights defenders, including women human rights defenders, in the digital age*. United Nations. <https://documents.un.org/doc/undoc/ltd/g25/048/80/pdf/g2504880.pdf>; Baltazar, F., & Martins, P. (2025, 23 April). A digital milestone: New resolution on human rights defenders and new technologies adopted by the UN Human Rights Council. *Association for Progressive Communications*. <https://www.apc.org/en/news/digital-milestone-new-resolution-human-rights-defenders-and-new-technologies-adopted-un-human>

- Ensure that online platforms comply with their responsibilities under the UNGP-BHR. Develop appropriate and effective mechanisms of accountability for social media platforms and other technology companies, with a focus on ensuring company transparency and remediation to ensure that hate speech and TFGBV are addressed on their platforms, there is appropriate response to such instances and safeguards and redress mechanisms are available for those affected.
- Promote the development of TFGBV lexicons in different local languages to be used in training AI algorithms and individuals for effective content moderation to curb TFGBV.
- Proactively facilitate collaboration between various stakeholders, including technology companies, women's rights organisations, researchers and civil society, to strengthen policy making and implementation aimed at preventing and addressing TFGBV.