

SUPPORTED BY:

Luminate



POLICY BRIEF

Strengthening Platform Accountability for AI-Facilitated Gender-Based Violence in Nigeria



Key Message

Platform accountability means holding AI companies responsible not only for the content they host, but also for the algorithms, design choices, and governance systems that enable or amplify technology-facilitated gender-based violence (TFGBV) against women and girls. A survivor-centred, gender-responsive AI governance framework can ensure that digital innovation expands women's participation online in Nigeria rather than reinforcing violence, exclusion, and inequality.

The key priorities are:

Move accountability upstream: Require platforms to assess and mitigate foreseeable AI-related harms before deployment, not only remove harmful content after it is reported.

Strengthen reporting and redress: Establish survivor-centred, time-bound, and trauma-informed reporting and appeals systems that provide timely remedies.

Modernize Nigeria's legal framework: Update the 2024 Cybercrimes Amendment Act, the 2015 VAPP Act, and related legislation to explicitly address generative AI, deepfakes, and AI-generated and manipulated image-based abuse.

Improve institutional coordination: Create a shared complaint, evidence, and referral pathway linking NITDA, the NCC, the NHRC, NAPTIP, and civil society organizations.

The policy problem

TFGBV includes online stalking, cyber-harassment, non-consensual sharing of intimate images, doxxing, hate speech, impersonation, and AI-generated sexualised content targeting women and girls. In this brief, platforms refer to AI-enabled digital and social media services that host user-generated content,¹ facilitate online communication, or use algorithmic recommendation systems; the recommendations therefore apply to all platforms operating in Nigeria that meet this description, rather than to any specific company.

AI intensifies these harms along three dimensions. First, creation: generative AI tools produce realistic deepfakes, cloned voices, and

manipulated abusive content that are increasingly indistinguishable from authentic media.² These generative tools now require little specialised technical skill to produce convincing harmful content, sharply lowering the barrier to perpetration.³ Second, amplification: recommendation algorithms are optimised for engagement and can prioritise emotionally charged or harmful content, including misogynistic abuse, increasing its reach even where platforms did not intend to promote it. Third, automation: coordinated harassment campaigns, including networks of fake accounts and bot-assisted pile-ons can now be generated and deployed rapidly using AI tools, overwhelming both victims and platform moderation capacity.⁴

1 These include TikTok, Facebook, YouTube, Snapchat, Instagram, and X which together reach tens of millions of Nigerian users and increasingly embed generative AI and algorithmic recommendation features into their core products. DataReportal, Digital 2026: Nigeria, 2026, <https://datareportal.com/reports/digital-2026-nigeria>

2 UNESCO, "Technology Facilitated Gender-Based Violence in Times of Generative AI," 2023, op. cit.; UN Women, How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls, 2026, <https://www.unwomen.org/sites/default/files/2026-01/how-ai-is-exacerbating-technology-facilitated-violence-against-women-and-girls-en.pdf>.

3 Canadian Women's Foundation, Challenging Gendered Digital Harm: Research Report on Impacts and Solutions to Digital Harm Facing Women, Gender-Diverse People, and Gender Equality Organizations, February 2025, p. 32 <https://canadianwomen.org/help-end-gender-based-digital-harm>.

4 UNESCO, Guidelines for the Governance of Digital Platforms, 2023, op. cit.

Women in politics, journalism, activism, and other forms of public life are disproportionately targeted, which drives self-censorship, psychological harm, economic loss, and withdrawal from digital and civic spaces.⁵ BBYDI's own Violence Against Women in Elections (VAWIE) research documents this dynamic during Nigeria's 2026 election cycle, including coordinated online attacks and AI-generated and manipulated content targeting women candidates, journalists, and election observers.⁶ The scale in Nigeria and the wider region is substantial. More recent, Nigeria-specific evidence points in the same direction: the 2024 Nigeria Demographic and Health Survey, the country's first nationally representative estimate, found that 1.6 per cent of women aged 15–49 had ever experienced TFGBV, with strangers the most common perpetrators (60 per cent of cases); civil-society research published in 2025 puts the figure considerably higher, finding that 58 per cent of documented online harms in Nigeria target women and that half of Nigerians report facing online abuse regularly. These sources use different definitions and samples and are not directly comparable, but together with the regional survey evidence below they confirm that the problem is substantial and persistent. A 2020 Plan

International survey of 14,000 girls and young women aged 15–25 across 22 countries, including Nigeria, found that 58 per cent had experienced online harassment or abuse.⁷ Domestically, African Polling Institute research cited in the same reporting found that 50 per cent of women in Nigeria had encountered gender-based hate speech online, directly or indirectly, compared with 36 per cent of men, and that more than 60 per cent of Nigerians are aware of others experiencing online violence evidence that such abuse is becoming normalised in the country's digital spaces.⁸

United Nations reporting corroborates this pattern regionally: UN agencies describe ending digital violence as "Africa's next chapter" in the pursuit of gender equality, while civil-society monitoring has documented how weak platform response mechanisms and legal gaps leave Nigerian women and girls exposed to escalating harm, including image-based abuse and AI-generated content.^{9,10} TFGBV is not unique to Nigeria: it is a globally documented problem affecting women's safety and participation online, which underscores the urgency of a Nigeria-specific response.

Why platform accountability matters

Traditional approaches focus on removing illegal content after harm has already occurred, leaving the burden of detection, reporting, and evidence-gathering on the victim. Platform accountability shifts responsibility upstream by requiring technology companies to anticipate and reduce foreseeable risks before they materialise.

UNESCO and the OECD both argue that platforms should conduct human-rights risk assessments before deploying major AI systems and should regularly evaluate the impact of their products on women and girls rather than responding only after harm is reported.

5 OECD, "Mapping Policy Responses to Technology-Facilitated Gender-Based Violence in the G7 Countries," 2025, op. cit.

6 Brain Builders Youth Development Initiative (BBYDI), Violence Against Women in Elections (VAWIE): Power & Actors Analysis – Evidence Brief Framework, 2026, https://thebrainbuilders.org/wp-content/uploads/2026/08/BBYDI-BBYDI_VAWIE_Power_Analysis_and_Evidence_Brief.pdf; BBYDI, Policy Brief: VAWIE Osun, 2026, https://thebrainbuilders.org/wp-content/uploads/2026/08/BBYDI-Policy_Brief_VAWIE_Osun_2026.pdf.

7 Plan International, Free to Be Online?, 2020, as reported in West Africa Weekly, "58% of Women and Girls Across 22 Countries, Including Nigeria, Face Online Harassment," <https://westafricaweekly.com/58-of-women-and-girls-across-22-countries-including-nigeria-face-online-harassment/>.

8 African Polling Institute data, as reported in West Africa Weekly, ibid.

9 Africa Renewal / UN Office of the Special Adviser on Africa, "Ending Digital Violence Is Africa's Next Chapter in Equality for Women and Girls," <https://africarenewal.un.org/en/magazine/ending-digital-violence-africas-next-chapter-equality-women-and-girls>; UN Nigeria, Mohamed M. Fall, "Voices Unbroken: Ending Digital Violence Against Women and Girls," <https://nigeria.un.org/en/306078-voices-unbroken-ending-digital-violence-against-women-and-girls-mohamed-m-fall>.

10 Global Voices Advox, "When Technology Fails Women: Online Abuse and Nigeria's Digital Weak Points," April 2026, <https://advox.globalvoices.org/2026/04/10/when-technology-fails-women-online-abuse-and-nigerias-digital-weak-points/>.

11 UNESCO, Guidelines for the Governance of Digital Platforms, 2023, op. cit.; OECD, "Mapping Policy Responses to Technology-Facilitated Gender-Based Violence in the G7 Countries," 2025, op. cit.

TABLE 1 - Shifting from a reactive content-moderation model to an accountability model that governs AI design, algorithms, and redress systems.

Traditional model	Accountability model
Remove harmful posts after the fact	Prevent foreseeable harms through safer design, built in before launch
Users must report abuse themselves	Platforms proactively detect systemic and emerging risks
Responsibility falls on perpetrators alone	Shared responsibility that extends to platform architecture and incentives
Limited or voluntary transparency	Mandatory transparency reporting and independent audits
Weak, slow, or inaccessible victim remedies	Accessible reporting, appeal, and redress within defined timelines

International standards emerging

Three complementary international frameworks provide guidance for national policy. UNESCO's ethics-of-AI and platform-governance instruments call for human-rights-based AI, transparency, gender-impact assessment, algorithmic accountability, and independent auditing of high-risk systems.¹² The OECD's TFGBV policy framework, published in June 2025, identifies four pillars for effective national responses: national strategic and legal frameworks, regulation of online platforms, systematic data collection, and capacity-building for justice-sector actors, and finds that while G7 countries have made visible progress, significant gaps remain in harmonisation, enforcement, and evidence.¹³

In March 2026, the Council of Europe Committee of Ministers adopted Recommendation

CM/Rec(2026)2 on accountability for technology-facilitated violence against women and girls. The Recommendation is the first international standard dedicated specifically to this issue. It recommends comprehensive legal, administrative and policy responses; safety-by-design in digital products and services; effective reporting and redress; improved data collection; and survivor-centred access to justice designed to avoid secondary victimisation. Although it applies formally within the Council of Europe system, it offers useful comparative guidance for Nigeria.¹⁴

A fourth, closely related reference point is the European Union's Digital Services Act, which requires "very large online platforms" to conduct annual systemic-risk assessments, including risks to gender equality and to fundamental rights and

¹² UNESCO, Guidelines for the Governance of Digital Platforms, 2023, op. cit.; UNESCO / Global AI Ethics and Governance Observatory, "Tackling Gender Bias and Harms in Artificial Intelligence (AI)," <https://www.unesco.org/en/articles/tackling-gender-bias-and-harms-artificial-intelligence-ai>.

¹³ OECD, "Mapping Policy Responses to Technology-Facilitated Gender-Based Violence in the G7 Countries," 2025, op. cit.

¹⁴ Council of Europe, Committee on Crime Problems, "Accountability for Technology-Facilitated Violence Against Women and Girls: New Council of Europe Recommendation," 2026, <https://www.coe.int/en/web/cdpc/-/accountability-for-technology-facilitated-violence-against-women-and-girls-new-council-of-europe-recommendation>; <http://search.coe.int/cm?i=09125948802acd83>

to mitigate risks identified, subject to independent audit and regulatory enforcement under Article 34. Commentators have noted that this systemic-risk framework is one of the clearest existing legal hooks for treating TFGBV as a structural,

design-level obligation rather than a case-by-case moderation issue, and it offers Nigeria a tested legislative model to adapt rather than build from scratch.¹⁵

What should platforms be accountable for?

Drawing on these frameworks, seven areas of platform conduct should carry enforceable obligations rather than remain matters of voluntary corporate policy.¹⁶

TABLE 2 - Platform obligations across the AI and content lifecycle, from design through to redress.

Accountability area	Expected obligation
AI design	Assess gender-specific risks before deploying generative or recommendation systems
Algorithms	Reduce algorithmic amplification of misogynistic and abusive content
Content moderation	Deploy proportionate measures to detect, assess and disrupt deepfakes, image-based abuse and coordinated harassment, supported by accuracy testing, privacy safeguards, human review and accessible appeals.
Transparency	Publish TFGBV enforcement statistics and independent AI audit findings
User safety	Provide fast, survivor-centred reporting channels and appeal processes
Data access	Share anonymised data with accredited, vetted researchers
Redress	Restore wrongly removed accounts, remove harmful content, and preserve evidence for survivors and law enforcement

Source: UNESCO (2023) and OECD (2025)¹⁷

15 Digital Services Act, Article 34 (systemic risk assessment), https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html; DSA Observatory, "Platform Governance and Technology-Facilitated Gender-Based Violence: Positioning the DSA in the EU's Legal Framework," 2026, <https://dsa-observatory.eu/2026/07/13/platform-governance-and-technology-facilitated-gender-based-violence-positioning-the-dsa-in-the-eus-legal-framework/>.

16 UNESCO, Guidelines for the Governance of Digital Platforms, 2023, op. cit.; OECD, "Mapping Policy Responses to Technology-Facilitated Gender-Based Violence in the G7 Countries," 2025, op. cit.

17 UNESCO. (2023). Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach. Paris: UNESCO. ISBN 978-92-3-100620-3; OECD. (2025). Mapping Policy Responses to Technology-Facilitated Gender-Based Violence in the G7 Countries. OECD Publishing, Paris. <https://doi.org/10.1787/b0887189-en>

Nigeria's current legal and institutional landscape

Nigeria is increasingly making progress to address TFGBV through its policy and legal reforms. Several instruments now touch on TFGBV, but efforts remain a work in progress: most were not designed with generative AI in mind, and none explicitly addresses AI-generated or manipulated forms of abuse, leaving material gaps. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, assented to on 28 February 2024, amended section 24 of the principal Act.¹⁸ The amendment narrowed section 24(1) to communications that are pornographic or knowingly false and intended to cause a breakdown of law and order or pose a threat to life.¹⁹ Section 24(2) continues to criminalise communications used to bully, threaten or harass another person where they place that person in fear of death, violence or bodily harm. These provisions may provide partial remedies for serious forms of TFGBV, but they do not expressly address AI-generated or manipulated media, deepfakes or non-consensual intimate-image abuse.²⁰

The Violence Against Persons (Prohibition) Act 2015 provides for offences including stalking, intimidation, indecent exposure, and emotional, verbal and psychological abuse.²¹ It applies directly in the Federal Capital Territory and requires equivalent state legislation or domestication elsewhere. However, it does not expressly criminalise non-consensual intimate-image distribution or AI-generated and manipulated intimate imagery. It may therefore offer partial remedies in individual cases but does not provide a clear, comprehensive statutory response to image-based TFGBV.²²

NITDA's enabling legislation, the NITDA Act 2007, provides a broad mandate to develop information-technology standards, guidelines and regulatory instruments in Nigeria. This has supported its role, alongside the Federal Ministry of Communications, Innovation and Digital Economy and other institutions, in the development of Nigeria's National Artificial Intelligence Strategy. While the Strategy advances broad commitments to responsible, inclusive and human-centred AI, its treatment of gender-differentiated harms and TFGBV remains largely high-level and does not yet establish detailed, enforceable safeguards. Nigeria also does not yet appear to have a single, fully operational body with a clear, adequately resourced mandate to conduct systemic algorithmic audits, receive and coordinate systemic TFGBV complaints, and sanction non-compliant platforms. Although the Nigeria Data Protection Commission has relevant data-protection oversight functions, the Nigeria Data Protection Act's General Application and Implementation Directive 2025 principally requires Data Privacy Impact Assessments for high-risk personal-data processing.²³ In 2026, the NDPC also announced an AI System Impact Assessment initiative. These measures are relevant to anticipatory oversight, but they do not create a complete TFGBV complaint-handling, platform-audit or sanctions regime.²⁴

NITDA has also begun developing an online-safety architecture. Its 2024 White Paper on the Framework for Online Harms Protection proposes platform obligations relating to age assurance,

18 <https://www.wipo.int/wipolex/en/legislation/details/22699>

19 <https://eprints.gouni.edu.ng/5624/1/CYBERSTALKING%20IN%20NIGERIA-%20AN%20EXPLORATORY%20STUDY%20OF%20S.%2024%20OF%20NIGERIAN%20CYBERCRIMES%20ACT.pdf>

20 <https://liradnigeria.org/tag/cybercrime-act-2015-vs-2024-nigeria/>

21 <https://naptip.gov.ng/violence-against-persons-prohibition-department/>

22 <https://techsociety.org/wp/blog/how-the-vapp-act-falls-short-on-protecting-against-ncii-image-based-abuse-in-nigeria/>

23 <https://ndpc.gov.ng/beyond-compliance-ndpc-introduces-ai-system-impact-assessments-at-national-ai-summit/>

24 <https://stransact.com/insights/the-road-to-trust-how-gaid-2025-will-shape-nigerias-digital-economy>; National Information Technology Development Agency Act 2007; National Artificial Intelligence Strategy (NAIS), Nigeria, 2024, tracked at OECD.AI, <https://oecd.ai/en/dashboards/policy-initiatives/national-artificial-intelligence-strategy-nais>.

protection against harmful content, and regular risk assessments, initially with a strong focus on child protection.²⁵ The proposed Online Harm Protection Bill, publicly discussed in 2025, would further establish institutional mechanisms for online-harm oversight, including an Online Harm Protection Centre, a Multi-Stakeholder Council, a Redress Panel, and an Independent Oversight Forum. These developments provide an important

foundation for platform accountability in Nigeria. However, the framework remains broader than TFGBV and does not yet establish a dedicated, gender-responsive mechanism for AI-enabled violence against women and girls. The emerging architecture should therefore be expanded to explicitly incorporate TFGBV, gender-impact assessment, platform transparency, survivor-centred redress, and accountability for AI-enabled harms.

25 <https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf>



Policy recommendations for Nigeria

1

Introduce mandatory AI gender-impact assessments

The National Assembly and NITDA should require platforms deploying generative AI or recommendation systems in Nigeria to conduct Gender and Human Rights Impact Assessments before major product releases, with assessments for high-risk systems reviewed by an independent regulator rather than self-certified.²⁶ Assessments should be updated whenever a platform materially changes its recommendation algorithm or launches a new generative-AI feature capable of producing AI-generated or manipulated media, mirroring the systemic-risk review cycle already required of very large platforms under the EU's Digital Services Act.

2

Establish platform transparency obligations

Platforms operating in Nigeria should be required to publish quarterly reports disclosing the number of TFGBV complaints received, average response and removal times, the volume of deepfake and AI-generated abuse detected and actioned, the outcomes of appeals and account reinstatements, and any algorithmic changes affecting content recommendation that materially affect user safety. Standardising these disclosures would allow NITDA, the NCC, and independent researchers to compare platform performance over time and would improve both regulatory oversight and public accountability.²⁷

3

Regulate AI-generated intimate image abuse explicitly

Nigeria should amend its cybercrime and violence-against-persons statutes to explicitly criminalise the creation, possession for distribution, and dissemination of AI-generated non-consensual intimate imagery, regardless of whether the depicted person or image is wholly or partly AI-generated or manipulated. As documented in Section 5 above, neither the 2024 Cybercrimes Amendment Act nor the 2015 VAPP Act currently contemplates deepfake or AI-manipulated imagery, which means prosecutors must currently rely on general harassment or defamation provisions that were not designed for this harm and carry weaker evidentiary pathways and penalties.²⁸

4

Require safety-by-design standards

Rather than relying solely on after-the-fact content removal, platforms should be required to embed preventive safeguards directly into product design. These should include default technical detection of AI-generated or manipulated intimate images at the point of upload, visible watermarking or provenance indicators on AI-generated media, stronger default protections and rapid-response channels for women in public life who face elevated targeting, and friction mechanisms, such as warning prompts or delayed sending before a user shares content flagged as potentially abusive. Safety-by-design, pioneered by regulators such as Australia's eSafety Commissioner, is increasingly recognised internationally as the most effective preventive approach because it reduces harm before it reaches a victim rather than after.²⁹

26 UNESCO / Global AI Ethics and Governance Observatory, "Tackling Gender Bias and Harms in Artificial Intelligence (AI)," op. cit.

27 UNESCO, Guidelines for the Governance of Digital Platforms, 2023, op. cit.; comparable practice illustrated by TikTok's Digital Services Act transparency reporting on content moderation in Europe, <https://newsroom.tiktok.com/en-eu/digital-services-act-our-fifth-transparency-report-on-content-moderation-in-europe>.

28 Analysis based on Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 and Violence Against Persons (Prohibition) Act 2015, op. cit.

29 eSafety Commissioner (Australia), "Safety by Design," <https://www.esafety.gov.au/industry/safety-by-design>; Council of Europe, "Accountability for Technology-Facilitated Violence Against Women and Girls," op. cit.

5

Build survivor-centred reporting, response, and redress systems

Nigeria should require digital platforms to establish survivor-centred, trauma-informed, and time-bound reporting and redress systems for victims of TFGBV. Reporting mechanisms should be accessible through multiple channels, including local-language interfaces and partnerships with accredited civil society organizations, with priority response timelines for image-based abuse and credible threats of violence.

Platforms should integrate technologies such as hash-matching to prevent the re-upload of non-consensual intimate images, ensure moderators receive mandatory trauma-informed training, preserve digital evidence for legal proceedings, and provide transparent appeals and account reinstatement processes. A coordinated referral pathway linking platforms with NITDA, the NCC, the NHRC, NAPTIP, and law enforcement should provide survivors with a single entry point for both platform action and formal justice.

6

Establish a statutory digital-safety coordination and oversight mechanism

Nigeria should establish a statutory, multi-agency Digital Safety Coordination and Oversight Mechanism with a clear lead institution, published protocols, dedicated funding, due-process protections and independent civil-society and technical-advisory participation. The mechanism should receive and analyse systemic complaints, coordinate survivor referrals, set standards for high-risk platform transparency and risk assessment, commission independent audits, publish aggregate compliance findings, and refer violations to the authority with legal power to investigate or sanction.

The mechanism should coordinate not duplicate existing mandates. NITDA could lead technical AI and digital-service standards; NDPC could address unlawful personal-data processing; NCC could apply its regulatory powers to licensed communications and internet-service providers where relevant; NHRC could monitor rights impacts; NAPTIP and law-enforcement agencies could investigate offences within their mandates; and civil society could provide survivor support, independent monitoring and research input.

7

Use existing enforcement powers to hold platforms and AI developers accountable now

While the reforms above are being developed, Nigeria already has usable levers to hold platforms and AI developers accountable for TFGBV. The Nigeria Data Protection Commission has existing powers under the Nigeria Data Protection Act 2023, including cease-and-desist and erasure orders, that can be used to compel the takedown of non-consensual and AI-generated or manipulated intimate imagery and to sanction platforms or AI developers that unlawfully process personal data in producing or hosting such content. The Commission should use these powers actively, publish the outcomes of enforcement actions as precedent, and prioritise cases involving AI-generated abuse and insider data leakage, while NITDA and sector regulators apply existing consumer-protection and licensing powers to non-compliant platforms. This provides an immediate accountability mechanism that does not depend on the legislative and institutional reforms recommended above.

References

- Africa Renewal / UN Office of the Special Adviser on Africa. (n.d.). Ending digital violence is Africa's next chapter in equality for women and girls. United Nations.
<https://africarenewal.un.org/en/magazine/ending-digital-violence-africas-next-chapter-equality-women-and-girl>
- African Polling Institute. (2020). Data on gender-based hate speech online in Nigeria. As cited in West Africa Weekly. (2020). 58% of women and girls across 22 countries, including Nigeria, face online harassment.
<https://westafricaweekly.com/58-of-women-and-girls-across-22-countries-including-nigeria-face-online-harassment/>
- Brain Builders Youth Development Initiative (BBYDI). (2026). Policy brief: VAWIE Osun 2026. BBYDI.
https://thebrainbuilders.org/wp-content/uploads/2026/08/BBYDI-Policy_Brief_VAWIE_Osun_2026.pdf
- Brain Builders Youth Development Initiative (BBYDI). (2026). Violence Against Women in Elections (VAWIE): Power & actors analysis – Evidence brief framework. BBYDI.
https://thebrainbuilders.org/wp-content/uploads/2026/08/BBYDI-BBYDI_VAWIE_Power_Analysis_and_Evidence_Brief.pdf
- Brown, V. (2026, April 10). When technology fails women: Online abuse and Nigeria's digital weak points. Global Voices Advox.
<https://advox.globalvoices.org/2026/04/10/when-technology-fails-women-online-abuse-and-nigerias-digital-weak-points/>
- Canadian Women's Foundation. (2025, February). Challenging gendered digital harm: Research report on impacts and solutions to digital harm facing women, gender-diverse people, and gender equality organizations (p. 32).
<https://canadianwomen.org/help-end-gender-based-digital-harm>
- Council of Europe, Committee on Crime Problems. (2026). Accountability for technology-facilitated violence against women and girls: New Council of Europe recommendation. Council of Europe.
<https://www.coe.int/en/web/cdpc/-/accountability-for-technology-facilitated-violence-against-women-and-girls-new-council-of-europe-recommen>
- dation
- Cyberstalking in Nigeria: An exploratory study of s. 24 of Nigerian Cybercrimes Act [PDF]. (n.d.). Godfrey Okoye University ePrints Repository.
<https://eprints.gouni.edu.ng/5624/1/CYBERSTALKING%20IN%20NIGERIA-%20AN%20EXPLORATORY%20STUDY%20OF%20S.%2024%20OF%20NIGERIAN%20CYBERCRIMES%20ACT.pdf>
- DataReportal. (2026). Digital 2026: Nigeria. DataReportal.
<https://datareportal.com/reports/digital-2026-nigeria>
- DSA Observatory. (2026, July 13). Platform governance and technology-facilitated gender-based violence: Positioning the DSA in the EU's legal framework.
<https://dsa-observatory.eu/2026/07/13/platform-governance-and-technology-facilitated-gender-based-violence-positioning-the-dsa-in-the-eus-legal-framework/>
- eSafety Commissioner (Australia). (n.d.). Safety by design.
<https://www.esafety.gov.au/industry/safety-by-design>
- European Union. (n.d.). Digital Services Act, Article 34 (systemic risk assessment).
https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html
- Fall, M. M. (2025, November 24). Voices unbroken: Ending digital violence against women and girls. United Nations Nigeria.
<https://nigeria.un.org/en/306078-voices-unbroken-ending-digital-violence-against-women-and-girls-mohamed-m-fall>
- Federal Republic of Nigeria. (2007). National Information Technology Development Agency Act, 2007. Government of Nigeria.
- Federal Republic of Nigeria. (2015). Violence Against Persons (Prohibition) Act, 2015. Government of Nigeria.
- Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. WIPO Lex.
<https://www.wipo.int/wipolex/en/legislation/details/22699>
- Lex Initiative for Rights Advocacy and Development (LIRAD). (n.d.). Cybercrime Act 2015 vs. 2024, Nigeria.

<https://liradnigeria.org/tag/cybercrime-act-2015-vs-2024-nigeria/>

National Agency for the Prohibition of Trafficking in Persons (NAPTIP). (n.d.). Violence Against Persons (Prohibition) Department. <https://naptip.gov.ng/violence-against-persons-prohibition-department/>

National Information Technology Development Agency (NITDA). (2024). National Artificial Intelligence Strategy (NAIS), Nigeria. Tracked at OECD.AI. <https://oecd.ai/en/dashboards/policy-initiatives/national-artificial-intelligence-strategy-nais>

National Information Technology Development Agency (NITDA). (2024, December). Framework for Online Harms Protection: White paper. <https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf>

Nigeria Data Protection Commission (NDPC). (n.d.). Beyond compliance: NDPC introduces AI System Impact Assessments at National AI Summit. <https://ndpc.gov.ng/beyond-compliance-ndpc-introduces-ai-system-impact-assessments-at-national-ai-summit/>

OECD. (2025). Mapping policy responses to technology-facilitated gender-based violence in the G7 countries. OECD Publishing. <https://doi.org/10.1787/b0887189-en>

Plan International. (2020). Free to be online? As cited in West Africa Weekly. (2020). 58% of women and girls across 22 countries, including Nigeria, face online harassment. <https://westafricaweekly.com/58-of-women-and-girls-across-22-countries-including-nigeria-face-online-harassment/>

Stransact. (n.d.). The road to trust: How GAID 2025 will shape Nigeria's digital economy. <https://stransact.com/insights/the-road-to-trust-how-gaid-2025-will-shape-nigerias-digital-economy>

TechSocietal. (n.d.). How the VAPP Act falls short on protecting against NCII image-based abuse in Nigeria. <https://techsocietal.org/wp/blog/how-the-vapp-act-falls-short-on-protecting-against-ncii-image-based-abuse-in-nigeria/>

TikTok. (n.d.). Digital Services Act: Our fifth transparency report on content moderation in Europe. <https://newsroom.tiktok.com/en-eu/digital-services-act-our-fifth-transparency-report-on-content-moderation-in-europe>

UN Women. (2026). How AI is exacerbating technology-facilitated violence against women and girls. UN Women. <https://www.unwomen.org/sites/default/files/2026-01/how-ai-is-exacerbating-technology-facilitated-violence-against-women-and-girls-en.pdf>

UNESCO / Global AI Ethics and Governance Observatory. (n.d.). Tackling gender bias and harms in artificial intelligence (AI). UNESCO. <https://www.unesco.org/en/articles/tackling-gender-bias-and-harms-artificial-intelligence-ai>

UNESCO. (2023). Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach. UNESCO. ISBN 978-92-3-100620-3

UNESCO. (2023). Technology facilitated gender-based violence in times of generative AI. UNESCO.



Email: brainbuilderedu@gmail.com **Tel:** 07068775529

Headquarters: 2 Catchment Road, Opposite Forest, Along Sydney Restaurant, GRA, Ilorin

Abuja Address: No. 12 T.O.S. Benson Crescent, Utako Abuja, 900108, FCT

Cameroun Address: Yaoundé- Montee Jouvence, Patmos Church Street 8.560

US Address: 1301 S Bowen Rd STE 450 Arlington TX 76013

www.thebrainbuilders.org