Nnamdi Azikiwe University Awka Journal of Private and Property Law, volume 3 (2) April, 2026

CYBERCRIME, GENDER, AND LEGAL PROTECTIONS: A COMPARATIVE STUDY OF NIGERIA AND THE UNITED STATES

Muinat Oluwaseun Mustapha[1]

Abstract

Cybercrime has emerged as one of the most significant threats in the digital age, transcending national boundaries and affecting individuals, institutions, and governments alike. While cybercrime is often discussed in terms of financial loss and technological vulnerability, its gendered dimensions remain largely underexplored, particularly in developing jurisdictions. Women and gender minorities are disproportionately affected by certain forms of cybercrime such as cyberstalking, online harassment, sextortion, and the non-consensual dissemination of intimate images. These harms are not merely technological but deeply social and legal, raising critical questions about access to justice, victim protection, and the adequacy of existing legal frameworks. This study undertakes a comparative analysis of Nigeria and the United States in order to examine how both jurisdictions address cybercrime through a gender-sensitive legal lens. The paper analyses statutory provisions, judicial responses, institutional mechanisms, and enforcement challenges in both countries. It argues that while the United States has developed more comprehensive victim-oriented legal protections, Nigeria's framework remains largely offender-focused, with significant gaps in gender-sensitive enforcement. The paper concludes by recommending legal reforms, policy interventions, and institutional strengthening to enhance gender protection within cybercrime regulation, particularly in Nigeria.

Keywords: Cybercrime, Gender-Based Violence, Nigeria, Cyberstalking, Legal Protection

1. Introduction

Cybercrime has evolved from being primarily a technical or economic issue into a serious social and human rights concern. Online platforms have become sites where misogyny, harassment, and abuse are perpetrated with relative anonymity and speed. The permanence and borderless nature of digital communication make it difficult for victims to escape or seek effective remedies. Once harmful content is shared online, it can be replicated endlessly, causing long-term psychological, reputational, and social harm.[2] As a result, cybercrime affecting women is no longer merely an issue of criminal law but also one of privacy, dignity, equality, and freedom of expression.

Globally, research indicates that women are disproportionately subjected to online harassment and abuse compared to men. Women are more likely to receive threats of sexual violence, persistent stalking, and attacks aimed at silencing their voices in public discourse.[3] Female journalists, activists, politicians, and professionals often report coordinated online harassment campaigns intended to intimidate and discourage their participation in civic life. In many cases, these abuses force women to withdraw from digital platforms or self-censor their expression, undermining democratic participation and gender equality.

[1] **Muinat Oluwaseun Mustapha, PhD**, Lecturer, Department of Public Law, Faculty of Law, University of Abuja, Nigeria. Email: muinat.mustapha@uniabuja.edu.ng, muinatmustapha@gmail.com.

[2] UNODC, *Comprehensive Study on Cybercrime* (Vienna: United Nations Office on Drugs and Crime 2021) 42.

[3] Pew Research Center, 'The State of Online Harassment.' https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/&ved=2ahUKEwiJ0oKT-NuTAxXgX0EAHfGDGdoQFnoECBYQAQ&usg=AOvVaw1qi2UOCshBV8kcPeY08Jiu retrieved on April 7, 2026.

In Nigeria, the growth of internet penetration and social media usage has coincided with rising reports of cyberstalking, sextortion, and online harassment, particularly targeting women and young girls. Reports from civil society organizations show alarming levels of online abuse directed at Nigerian women, with many incidents involving threats of sexual violence or the unauthorized publication of personal images.[4] Cultural stigma surrounding sexual matters, limited digital literacy, and fear of victim-blaming often prevent victims from reporting such crimes. Additionally, legal remedies remain unclear or difficult to access for many victims.

Similarly, in the United States, studies reveal high levels of online harassment directed at women and marginalized groups.[5] The rise of image-based abuse, cyberstalking, and online exploitation has prompted legislative and judicial responses at both federal and state levels. However, challenges remain in enforcement, platform accountability, and jurisdictional coordination. Despite having more developed digital infrastructures and legal systems, victims in the USA still encounter obstacles when seeking justice for gendered online harms.

The intersection of cybercrime and gender therefore presents a unique legal challenge. Traditional criminal laws were not designed to address the complexities of digital abuse that can occur anonymously, across borders, and on a massive scale. Many existing laws struggle to capture the nuances of non-consensual image sharing, coordinated online harassment, and digital stalking.[6] As technology evolves, perpetrators find new methods of exploiting victims faster than legal systems can adapt. This creates significant gaps in legal protection, particularly for women and girls who are most vulnerable to these harms.

Nigeria and the United States offer interesting comparative case studies in this regard. Nigeria operates under a centralized cybercrime framework through the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended, which criminalizes a range of online offenses including cyberstalking.[7] However, critics argue that the Act contains vague provisions and does not explicitly address modern forms of gendered cyber abuse such as non-consensual intimate image distribution or deep fake exploitation. Enforcement capacity, judicial interpretation, and victim awareness also present challenges.

In contrast, the United States addresses cybercrime through a combination of federal statutes, such as the Computer Fraud and Abuse Act and the Interstate Stalking and Prevention Act, as well as numerous state laws that criminalize cyber harassment, cyberstalking, and revenge porn.[8] The layered nature of U.S. law provides multiple avenues for legal redress, including criminal prosecution and civil remedies. Nonetheless, the fragmented nature of federal and state jurisdiction can create enforcement complexities.

[4] M Olugbode, 'Actionaid: 45% of Women in Nigeria Experience Cyberstalking.' https://www.thisdaylive.com/2025/12/06/actionaid-45-of-women-in-nigeria-experience-cyberstalking/ retrieved on April 7, 2026.
[5] Pew Research Center (n 3).
[6] UNDP, 'Analysis of the legislation related to Technology Facilitated Gender Based Violence.' https://www.undp.org/sites/g/files/zskgke326/files/2024-12/final-analysis-tf-gbv.pdf retrieved on April 7, 2026.
[7] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 s 24 (Nigeria).
[8] Computer Fraud and Abuse Act 1986 (USA) 18 USC § 1030; Interstate Stalking and Prevention Act 1996 (USA).

This comparative study is important because it highlights how two different legal systems respond to the same global problem of gendered cybercrime. By examining both jurisdictions, it becomes possible to identify strengths, weaknesses, and areas for reform. It also sheds light on how cultural, institutional, and legal differences influence the protection of victims in digital spaces.

The central argument of this research is that although both Nigeria and the USA have taken steps to address cybercrime, the extent to which their laws recognize and respond to gender-specific online harms differs significantly. While the USA has developed more explicit legal responses to issues such as revenge porn and interstate cyberstalking, Nigeria's framework remains broader and less tailored to gendered digital abuse. Both systems, however, face enforcement challenges that limit the effectiveness of legal protections.

1.0 Conceptual Framework

1.1 Meaning and Scope of Cybercrime

Cybercrime has been defined as offences committed against computer data, computer data storage media, computer systems, service providers.[9] The concept usually covers categories of offences

such as illegal access, interfering with data and computer systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringement

The United Nations Office on Drugs and Crime (UNODC) defines cybercrime as "any criminal conduct carried out by means of computer systems or networks."[10] Cybercrime refers to criminal activities committed through the use of computers, digital devices, or internet-based platforms.[11] It includes offences where the computer is either the target of the crime or the instrument used in committing the offence. These definitions demonstrate that cybercrime is not confined to a single type of offence but rather encompasses a wide range of unlawful behaviours enabled by digital technologies.

The scope of cybercrime has expanded significantly with increased global internet penetration, social media usage, mobile connectivity, and digital financial systems.[12] Activities that were once physical in nature are now conducted in virtual spaces, creating new opportunities for criminal conduct. Cybercrime may therefore be broadly classified into three main categories:[13]

---

[9] Interpol, 'INTERPOL National Cybercrime Strategy Guidebook.' (2020), https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf retrieved on April 7, 2026.

[10] UNODC (n 2) 50.

[11] A A Ajibade, 'Cybercrime.' https://tau.edu.ng/assets/media/docs/cybercrime-css414_1716305602.pdf retrieved on April 8, 2026.

[12] P Mohamadpour, 'Cybercrime in 2026: Deep Trends, Real Numbers & How We Fight Back.' https://medium.com/@pmpr.ir/cybercrime-in-2026-deep-trends-real-numbers-how-we-fight-back-a1138d8d607f retrieved on April 8, 2026.

[13] Cybertalents, 'What is Cybercrime? Types, Examples, and Prevention.' https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention#:~:text=Cybercrimes%20can%20be%20classified%20into%20four%20categories:,property%20rights%20*%20**Society%20cybercrimes**%20Includes%20cyber%2Dterrorism retrieved on April 8, 2026.

a) Crimes against individuals, such as cyberstalking, identity theft, online harassment, cyberbullying, sextortion, and non-consensual sharing of intimate images.
b) Crimes against property, including hacking, ransomware attacks, data breaches, online fraud, and intellectual property theft.
c) Crimes against government or society, such as cyberterrorism, espionage, and attacks on critical infrastructure.

Although financial crimes such as phishing, hacking, and online scams dominate public discourse on cybercrime, there is a growing recognition that crimes against individuals, particularly women and girls, represent one of the most harmful and underreported dimensions of cybercriminal activity.[14] These crimes often cause psychological trauma, reputational damage, social exclusion, and long-term emotional distress that may be more devastating than financial loss.

One important characteristic of cybercrime is its anonymity and borderless nature. Perpetrators can operate behind pseudonyms, fake profiles, or encrypted networks, making detection and prosecution difficult. Victims, on the other hand, may experience repeated and continuous abuse that transcends geographical boundaries. Unlike traditional crimes, cybercrime can occur at any time, persist indefinitely, and reach a wide audience instantly. Harmful content posted online can be copied, reshared, and stored permanently, leaving victims unable to fully escape the consequences.

Furthermore, cybercrime often exploits the speed and virality of digital communication.[15] A single act of abuse, such as the release of a private image, can be disseminated globally within minutes. This creates a form of harm that is amplified by technology, making legal remedies complex and sometimes ineffective even when perpetrators are identified and prosecuted.

In this context, the understanding of cybercrime must go beyond technical offences and include interpersonal abuses that disproportionately affect vulnerable groups. It is within this broader understanding that gendered cybercrime emerges as a critical area of study.

1.2 Gender and Legal Vulnerability

Gender refers not merely to biological differences between men and women but to socially constructed roles, behaviours, expectations, and power relations that shape how individuals experience society. Feminist legal theory argues that laws are often created within social systems that reflect dominant male perspectives, and as a result, may unintentionally reinforce gender inequalities.[16] When applied to cyberspace, this theory suggests that digital platforms are not neutral spaces but environments where offline gender hierarchies and power imbalances are reproduced and sometimes intensified.

Women and girls often experience the internet differently from men due to higher exposure to harassment, sexual threats, and intimidation. Studies consistently show that women are more likely to be targeted with abuse that is sexualized, degrading, or aimed at silencing their

[14] Europol, 'Internet Organised Crime Threat Assessment IOCTA(2024).' https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 retrieved on April 8, 2026.

[15] S Shoro, 'Cyber Attacks Impacting on Communication Using Social Media: Systematic Review Using Data Cluster Ball.' https://www.researchgate.net/publication/354849301_Cyber_Attacks_Impacting_on_Communication_Using_Social_Media_Systematic_Review_Using_Data_Cluster_Ball retrieved on April 8, 2026.

[16] C. MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 23.

participation in public discourse.[17] Female journalists, activists, politicians, and professionals frequently report coordinated online attacks designed to intimidate them and force them out of public spaces. As a result, many women limit their online presence, self-censor, or withdraw from digital engagement altogether.

This pattern of abuse has led to the development of the concept of technology-facilitated gender-based violence (TF-GBV). TF-GBV refers to acts of harassment, abuse, coercion, or exploitation carried out through digital means that disproportionately affect women and girls.[18] These acts include cyberstalking, doxing (publishing private information), online sexual harassment, sextortion, impersonation, and the non-consensual distribution of intimate images.[19]

Gender-based cybercrime is therefore not simply technological misconduct but a form of structural violence that manifests through digital means. It often intersects with issues of patriarchy, cultural stigma, victim-blaming, and institutional neglect. For example, victims of image-based abuse are frequently blamed for taking private photos rather than perpetrators being held accountable for distributing them. This cultural response discourages reporting and limits access to justice.

Another aspect of gender vulnerability in cyberspace is the power imbalance created by digital literacy and access. In many developing countries, including Nigeria, women may have less access to digital education and resources, making them less equipped to protect themselves from online threats. Even when abuse occurs, lack of awareness about legal rights and reporting mechanisms further increases vulnerability.

The legal system's response to gendered cybercrime is often inadequate because many traditional laws were not designed to address the nuances of digital abuse. Laws addressing stalking, harassment, and defamation were developed for physical environments and may not fully capture the scale and persistence of online abuse.[20] As a result, victims often struggle to find clear legal remedies, and perpetrators exploit these legal gaps.

Moreover, the stigma attached to sexual content and online harassment means that women may be reluctant to pursue legal action due to fear of public exposure, family shame, or professional consequences. This creates a situation where gendered cybercrime is both underreported and under-prosecuted, allowing perpetrators to act with impunity. International human rights bodies now recognise online gender-based violence as a violation of rights to dignity, privacy, equality, and freedom of expression.[21] The digital space, once viewed as a platform for empowerment, has therefore become a site of exclusion for many women due to fear of abuse.

[17] Pew Research Center (n 3).
[18] *Ibid.*
[19] D K Citron and M A Franks, *Cyber Civil Rights: Rights, Remedies, and Support for Technology-Facilitated Gender-Based Violence* (Cambridge University Press 2020) 58.
[20] S. Herman, *Cyber Law: Text and Materials* (Oxford University Press 2019) 112.
[21] Report of the UN Human Rights Council, Online Gender-Based Violence and Rights (UN Doc A/HRC/41/43 2019) 7.

2.0 Forms of Gender-Based Cybercrime

Gender-based cybercrime refers to criminal activities conducted through digital platforms that disproportionately target individuals on the basis of their gender.[22] Although cybercrime affects all users of digital technology, empirical evidence demonstrates that women and gender minorities experience certain categories of cyber harm more frequently and more severely. These forms of cybercrime often replicate existing social power imbalances and extend offline patterns of gender-based violence into the digital sphere.

Gender-based cybercrime is distinct from ordinary cyber offences because its primary objective is not merely financial gain but psychological domination, reputational destruction, sexual exploitation, and social control. The consequences of such crimes extend beyond digital platforms, often leading to long-term emotional trauma, social exclusion, and economic vulnerability.

2.1 Cyberstalking

Cyberstalking involves the repeated use of digital communication to harass, threaten, monitor, or intimidate a person. It typically includes persistent messaging, online surveillance, impersonation, and unsolicited digital contact that causes fear or distress to the victim. Unlike traditional stalking, cyberstalking allows perpetrators to maintain anonymity, operate across geographical boundaries, and reach victims continuously through multiple platforms.[23]

Women constitute the majority of cyberstalking victims globally. Studies conducted by the Pew Research Center reveal that women are twice as likely as men to experience severe online harassment, including threats of physical harm and sustained stalking.[24] The psychological effects of cyberstalking include anxiety, depression, and fear of public participation in digital spaces.

From a legal perspective, cyberstalking undermines fundamental human rights such as the right to privacy, dignity, and personal security. In Nigeria, cyberstalking is criminalised under section 24 of the Cybercrimes Act 2015, which prohibits knowingly sending grossly offensive or indecent messages intended to cause annoyance or anxiety.[25] However, the provision focuses on punishment without addressing victim protection or rehabilitation. Victims often struggle to obtain restraining orders or digital protection, leaving them exposed to repeated harm.

In contrast, the United States treats cyberstalking as both a criminal and civil offence, allowing victims to seek protective injunctions, compensation, and offender monitoring. U.S. courts increasingly recognize cyberstalking as a form of digital continuation of domestic abuse.[26]

2.1 Non-Consensual Dissemination of Intimate Images

The non-consensual dissemination of intimate images — commonly referred to as revenge pornography — involves the distribution of private sexual content without the consent of the

[22] T Paovic, 'Unite to End Digital Violence Against Women and Girls.' https://www.undp.org/turkmenistan/blog/ending-gender-based-violence-digital-age-empowering-women-and-youth retrieved on April 8, 2026.

[23] Pew Research Center, 'The State of Online Harassment.' (2021) https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/&ved=2ahUKEwitxNur2N6TAxXdT0EAHZteCWYQFnoECAwQAQ&usg=AOvVaw1qi2UOCshBV8kcPeY08Jiu retrieved on April 8, 2026.

[24] *Ibid*

[25] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 24.

[26] Violence Against Women Act 1994; Interstate Stalking and Prevention Act 1996.

individual depicted.[27] This offence primarily targets women and is often perpetrated by former intimate partners or online predators.

This form of cybercrime constitutes a violation of the right to privacy and bodily autonomy. Victims frequently experience humiliation, social stigma, and mental health distress. In conservative societies such as Nigeria, the consequences may include family rejection and social ostracism. Despite its severity, Nigerian law does not explicitly criminalize revenge pornography. Victims are forced to rely on general provisions under the Cybercrimes Act, defamation laws, or the Violence Against Persons (Prohibition) Act 2015 (VAPP Act), none of which adequately capture the distinct nature of digital sexual exploitation. The absence of a specific offence creates enforcement gaps and discourages reporting. By contrast, several U.S. states have enacted specific statutes criminalizing the non-consensual dissemination of intimate images, often accompanied by civil remedies allowing victims to compel removal of content and obtain damages.[28]

2.2 Sextortion

Sextortion refers to digital extortion where perpetrators threaten to release sexual images or information unless the victim provides money, additional content, or engages in sexual acts.[29] Such crimes often begin with online grooming, where offenders establish emotional relationships with victims before coercion.

Women and adolescent girls are particularly vulnerable to sextortion due to societal pressures, emotional manipulation, and fear of public shame. Sextortion has been associated with severe psychological distress among victims.

Legally, sextortion occupies an ambiguous space in Nigerian law. While it may fall under extortion or blackmail provisions, there is no specialized offence for digital sexual exploitation. Law enforcement agencies frequently lack the technical capacity to trace offenders across international jurisdictions.

The United States treats sextortion as a federal offence involving sexual exploitation and cybercrime statutes, providing victims with both criminal and civil pathways for redress.[30]

2.3 Doxxing

Doxxing involves the public release of private personal information — such as home addresses, phone numbers, and workplace details — with the intent to intimidate or harm the victim.[31] Doxxing is often used against female journalists, activists, and public figures.

Doxxing can lead to real-world danger, including physical harm, identity theft, and social harassment.[32] It disproportionately silences women in political and professional spaces. Most Nigerian legal frameworks do not explicitly address doxxing; victims must resort to data protection or defamation claims, which are often procedurally complex and slow.[33] By contrast,

[27] *Ibid.*
[28] See California Penal Code § 647(j)(4) (revenge porn statute).
[29] UNODC, Comprehensive Study on Cybercrime (Vienna: UNODC 2021) 55.
[30] 18 USC § 2422 (Sexual Exploitation).
[31] *Ibid.*
[32] *Ibid.*
[33] Nigeria Data Protection Act 2023.

U.S. law increasingly recognises doxxing as a form of cyber harassment, and courts have issued protective orders and damages in relevant cases.

2.4 Deepfake Abuse

Deepfake technology allows the creation of artificial images or videos that convincingly depict individuals engaging in acts they did not commit.[34] This emerging form of cybercrime enables perpetrators to fabricate explicit material without the victim's consent.

Deepfake abuse poses unprecedented legal challenges, as it blurs the line between real and fabricated harm.[35] Victims suffer reputational destruction and emotional trauma. Most legal systems, including Nigeria's, currently lack specific legislation addressing *deepfake* abuse, leaving significant regulatory gaps.

Gender-based cybercrime represents one of the most urgent legal challenges of the digital era. These offences demonstrate that cybercrime is not merely technological misconduct but a continuation of structural gender violence in digital spaces. Without gender-sensitive legal frameworks, victims remain exposed to harm while perpetrators exploit regulatory gaps.

3.0 Cybercrime and Gender Protection in Nigeria

Nigeria has experienced rapid growth in internet penetration, digital financial services, and social media usage over the past decade. While these developments have facilitated economic growth and social connectivity, they have also increased exposure to cybercrime. Nigeria has gained international notoriety for cyber fraud; however, the gendered dimensions of cybercrime remain largely under-examined in Nigerian legal discourse.

3.1 Legal Framework Governing Cybercrime in Nigeria

4.1.1. Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The principal legislation regulating cybercrime in Nigeria is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. The Act was enacted to provide a unified legal framework for the prevention, detection, and prosecution of cyber-related offences. It criminalizes identity theft, computer-related fraud, cyberterrorism, online harassment, and child pornography.[36]

Section 24 of the Act specifically addresses cyberstalking and online harassment, making it an offence to knowingly send messages or material that are grossly offensive, indecent, or intended to cause annoyance or anxiety. While this provision appears broad, its application in practice has been inconsistent and largely limited to politically motivated speech rather than gender-based abuse.

Notably, the Act lacks explicit recognition of gender-based cybercrime. It does not distinguish between financial cyber offences and sexual or psychological cyber harms. As a result, offences such as revenge pornography, sextortion, and doxxing are prosecuted under general provisions that fail to capture their unique social and emotional consequences.[37]

4.1.2. Violence Against Persons (Prohibition) Act, 2015

The Violence Against Persons (Prohibition) Act 2015 (VAPP Act) represents Nigeria's most progressive attempt at addressing gender-based violence. The Act criminalizes emotional, psychological, and sexual abuse and provides for victim compensation and protection orders.

[34] D. K. Citron, 'Deepfakes and Digital Harm' (2020) 16 *Journal of Internet Law* 6.
[35] *Ibid.*
[36] Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
[37] *Ibid.*

However, the VAPP Act suffers from two major limitations. First, it is not uniformly applicable across Nigeria, as several states have yet to domesticate it. Second, it was not designed specifically for cyber contexts, making enforcement against digital offences procedurally difficult. Victims of online abuse are often forced to pursue claims under both the Cybercrimes Act and the VAPP Act, creating legal uncertainty and procedural complexity.[38]

4.1.3. Nigerian Case Law and Judicial Attitudes

Judicial interpretation of cybercrime laws in Nigeria remains underdeveloped. Most reported cases focus on financial fraud rather than gender-based harm.[39] For example, in *FRN v Daramola*, the court upheld conviction for cyber fraud but made no reference to victim impact or digital harm.[40] Similarly, in *Okoli v Okoli*,[41] the court recognized privacy rights but failed to establish enforceable digital protection mechanisms.

The absence of reported decisions on revenge pornography, sextortion, or cyberstalking highlights a systemic failure in legal recognition. This judicial silence reinforces the perception that digital sexual abuse is not a serious legal issue, discouraging victims from seeking justice.

4.2. Institutional and Enforcement Challenges

One of the most significant barriers to effective regulation in Nigeria is weak institutional capacity. Law enforcement agencies such as the Nigerian Police Force and the Economic and Financial Crimes Commission lack specialised cyber forensic units and trained personnel capable of investigating digital evidence.[42]

Digital crimes require advanced technical skills such as IP tracing, metadata analysis, and digital authentication. However, most police stations lack infrastructure to preserve or analyse electronic evidence, resulting in low conviction rates.

Institutional corruption further undermines public trust. Victims frequently report being asked to pay bribes to initiate investigations or being discouraged from pursuing cases involving influential perpetrators.[43]

4.3. Cultural and Social Barriers

4.4. Cultural norms significantly influence enforcement of cybercrime laws. Patriarchal social attitudes often blame victims for sexual abuse, particularly in cases involving intimate images. Women may be accused of immorality, regardless of consent. Religious and

[38] Violence Against Persons (Prohibition) Act 2015 (Nigeria).

[39] J Ade, 'Cybercrime Governance and Legal Accountability in Nigeria: A Critical Appraisal of Enforcement Rights and Digital Sovereignty.' https://www.researchgate.net/publication/397579094_Cybercrime_Governance_and_Legal_Accountability_in_Nigeria_A_Critical_Appraisal_of_Enforcement_Rights_and_Digital_Sovereignty retrieved on April 23, 2026.

[40] *FRN v Daramola* (2018) Federal High Court Nigeria (unreported); *Okoli v Okoli* (2019) Federal High Court Nigeria (unreported).

[41] *Supra.*

[42] Economic and Financial Crimes Commission Act 2004; Nigerian Police Force Act 2004.

[43] Transparency International, 'Corruption Perceptions Index.' (2024) https://www.transparency.org/en/cpi/2024&ved=2ahUKEwioipO3yIaUAxXUXUEAHfzeN5kQFnoECBcQAQ&usg=AOvVaw3_fZdgNL-XPsSzJLanDiFC retrieved on April 24, 2026.

cultural stigma further silence victims, as reporting cyber abuse can lead to social ostracism or reputational damage.[44]

5.Comparative and International Legal Framework: Cybercrime, Gender, and Legal Protection in Nigeria and the United States

5.1. Cybercrime Legal Framework in the United States

The United States operates one of the most developed cybercrime regulatory systems globally.[45] Cybercrime in the U.S. is regulated through a combination of federal statutes, state legislation, and judicial precedents. The cornerstone federal statute is the Computer Fraud and Abuse Act 1986 (CFAA), which criminalises unauthorised access to computer systems, identity theft, digital extortion, and online fraud.[46]

A distinguishing feature of the CFAA is its dual enforcement structure.[47] It allows criminal prosecution by the state and civil actions by victims, empowering individuals to seek compensation, injunctions, and damages for digital harm. From a gender perspective, victims of cyberstalking, revenge pornography, and sextortion may pursue both criminal and civil remedies.

Beyond the CFAA, the Violence Against Women Act 1994 (VAWA) plays a crucial role in addressing gender-based cybercrime.[48] VAWA recognises cyberstalking, online harassment, and digital coercion as extensions of domestic violence, allowing victims to obtain restraining orders, legal aid, and counselling.[49]

At the state level, jurisdictions such as California, New York, and Texas have enacted specific statutes criminalising non-consensual dissemination of intimate images, sextortion, and doxxing, often coupled with civil remedies enabling victims to compel removal of harmful content.

Decisions such as *People v Bollaert*,[50]where a revenge pornography operator was prosecuted — and *Elonis v United States*,[51] where the U.S. Supreme Court acknowledged psychological harm in online threats while balancing free speech demonstrate judicial willingness to interpret cybercrime laws in victim-centred ways.[52]

5.2 Cybercrime Legal Framework in Nigeria

In contrast, Nigeria's cybercrime framework remains primarily offender-focused and technologically oriented. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 criminalises a wide range of digital offences, including identity theft, online harassment, cyberterrorism, and

[44]OHCHR, 'A/HRC/38/47: Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.' https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and retrieved on April 24, 2026.

[45] H Agarwal, 'A Glance at the United States Cyber Security Laws https://www.appknox.com/blog/united-states-cyber-security-laws retrieved on April 24, 2026.

[46] Computer Fraud and Abuse Act 1986 (USA) 18 USC s 1030.

[47] SJKP Law Firm LLP, 'The Computer Fraud and Abuse Act (CFAA).' https://www.daeryunlaw.com/us/practices/detail/cfaa retrieved on April 24, 2026.

[48] Congress.gov, 'The Violence Against Women Act (VAWA): Historical Overview, Funding, and Reauthorization.' https://www.congress.gov/crs-product/R45410 retrieved on April 24, 2026.

[49] Violence Against Women Act 1994.

[50] No. D067863, (Cal. Ct. App., 4th Dist. June 28, 2016).

[51] 575 U.S. 723 (2015)

[52] *People v Bollaert* 248 Cal App 4th 699 (2014); *Elonis v United States* 575 US 723 (2015).

child pornography.[53] However, the Act does not explicitly recognise gender-based cybercrime as a distinct category. Unlike the CFAA, the Nigerian Act does not provide civil remedies for victims. Victims are entirely dependent on state prosecution, which is often slow, under-resourced, and politically constrained. There are no statutory provisions for victim compensation, digital protection orders, or content removal.

The Violence Against Persons (Prohibition) Act 2015 offers limited relief by criminalising emotional and psychological abuse.[54] However, it is not uniformly applicable across Nigerian states and was not designed specifically for digital contexts. Consequently, victims of cyber sexual abuse often fall into legal gaps where neither statute provides effective remedies.[55] Comparatively, while US law conceptualises cybercrime as both a criminal and human rights issue, Nigerian law conceptualises it largely as a technical offence against public order and national security.[56]

6. Comparative Analysis: Nigeria and the United States

The comparative analysis reveals fundamental differences in legal philosophy, institutional capacity, and victim protection:

1. **Legal Philosophy** – US cybercrime law adopts a human-centred approach, integrating technological regulation with gender equality and human rights principles. Nigerian cybercrime law adopts a state-centred approach, focusing on punishment rather than victim rehabilitation.[57]
2. **Victim Remedies** – In the US, victims may seek civil damages, restraining orders, counselling, and content removal. In Nigeria, victims rarely obtain any remedy beyond criminal prosecution, which may take years and often collapses due to evidentiary weaknesses.[58]
3. **Institutional Capacity** – US law enforcement agencies possess advanced cyber forensic infrastructure, specialised digital units, and trained prosecutors. Nigerian institutions lack adequate technical resources, trained personnel, and digital evidence management systems.[59]

[53] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria) ss 6–24.

[54] Violence Against Persons (Prohibition) Act 2015 (Nigeria) ss 1–5.

[55] UN 'Women, Online and ICT-Facilitated Violence Against Women and Girls.' (2023) https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19&ved=2ahUKEwiC5IqqzYaUAxX2QkEAHccNA6YQFnoECA0QAQ&usg=AOvVaw0djsYDrx1LCGoRwHd8gSEu retrieved on April 24, 2026.

[56] D. K. Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 52–54.

[57] M. A. Franks, *The Cult of the Constitution* (Stanford University Press 2019) 103–107.

[58] Pew Research Center, 'The State of Online Harassment.' (2021) https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/&ved=2ahUKEwivrLmp0IaUAxXnT0EAHaxSHJcQFnoECA0QAQ&usg=AOvVaw1qi2UOCshBV8kcPeY08Jiu retrieved on April 24, 2026.

[59] Europol, 'Internet Organised Crime Threat Assessment.' (2024) https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 retrieved on April 24, 2026.

4. **Cultural Context** – In the US, public discourse increasingly recognises digital abuse as real harm. In Nigeria, cultural stigma, victim-blaming, and patriarchal norms discourage reporting and silence victims.[60]

This comparison demonstrates that Nigeria's regulatory framework remains structurally incapable of addressing the gendered realities of cybercrime.

7, International Legal Framework

Both Nigeria and the United States operate within an international legal environment shaped by global conventions and human rights instruments.

The Budapest Convention on Cybercrime 2001 represents the first comprehensive international treaty addressing cybercrime. It establishes standards for criminalisation, investigation, international cooperation, and digital evidence. The United States is a signatory and actively implements its provisions. Nigeria, although not a party, has drawn indirectly from its principles in drafting the Cybercrimes Act.[61]

The Convention on the Elimination of All Forms of Discrimination Against Women 1979 (CEDAW) obliges states to eliminate discrimination and violence against women in all spheres, including digital environments. Gender-based cybercrime clearly falls within the scope of this obligation.[62]

At the regional level, the African Union Convention on Cyber Security and Personal Data Protection 2014 provides a framework for African states to regulate cybercrime and protect digital rights. However, implementation remains weak due to lack of political will and institutional capacity.[63]

International law therefore establishes a clear normative expectation: states must protect individuals from digital harm and ensure gender equality in cyberspace. Nigeria's current legal framework falls short of these standards. This comparative and international analysis demonstrates that effective cybercrime regulation requires more than criminalisation; it requires a human rights-oriented legal philosophy that prioritises victim dignity, gender equality, and social justice.[64]

8. Challenges in the Enforcement of Gender-Based Cybercrime Laws

Despite the existence of statutory frameworks at national and international levels, enforcement of gender-based cybercrime laws faces multiple challenges that are legal, institutional, technological, cultural, and socio-political.

[60]S Ejike, 'ActionAid raises alarm over rising digital violence.' https://tribuneonlineng.com/actionaid-raises-alarm-over-rising-digital-violence/ retrieved on April 24, 2026.

[61] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No 185 (2001).

[62] UN General Assembly, Convention on the Elimination of All Forms of Discrimination Against Women, 18 December 1979, 1249 UNTS 13.

[63] African Union, 'Convention on Cyber Security and Personal Data Protection,' https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection retrieved on April 24, 2026.

[64] *Ibid*; UN Women (n 3)

8.1 Underreporting of Gender-Based Cybercrime

One of the most significant obstacles is underreporting. Many victims do not report digital abuse to law enforcement due to fear of stigma, victim-blaming, and social consequences.[65] In Nigeria, patriarchal norms and cultural pressure discourage women from filing complaints. Underreporting also creates the false perception that cyber sexual abuse is rare, reducing political urgency and institutional response.

8.2 Jurisdictional and Cross-Border Complexity

Cybercrime often transcends national boundaries.[66] Offenders may operate from one country while targeting victims in another, creating complex jurisdictional challenges for investigation, prosecution, and extradition. Differences in legal standards, evidentiary rules, and privacy laws further complicate enforcement. Developing countries like Nigeria frequently lack the diplomatic and technical capacity to pursue cross-border cybercrime cases.

8.3 Evidentiary and Technical Challenges

Digital evidence is volatile.[67] Online content may be deleted, altered, or encrypted quickly. Many law enforcement agencies lack the expertise to preserve metadata, authenticate digital records, or trace IP addresses. Courts may exclude evidence due to procedural errors or unfamiliarity with digital forensic standards, disproportionately affecting gender-based cybercrime victims.

8.4 Institutional Weakness and Resource Constraints

Effective enforcement requires specialised institutions, trained personnel, and technological infrastructure.[68] However, many Nigerian police units operate without cyber forensic laboratories or secure data systems, resulting in delayed investigations and lost evidence.

8.5 Cultural and Social Barriers

Cultural norms often trivialise gender-based digital harm.[69] Women may be blamed for possessing intimate content or "provoking" abuse, shifting responsibility away from perpetrators and reinforcing gender inequality.

8.6 Lack of Victim Support Mechanisms

Many legal systems lack structured victim support, including counselling, legal aid, financial compensation, and digital safety resources.[70] Without these, victims may abandon legal processes, internalise trauma, and withdraw from public life, perpetuating systemic exclusion.

---

[65] UN Women, 'Online and ICT-Facilitated Violence Against Women and Girls.' *op. cit.*

[66] Council of Europe, 'Budapest Convention on Cybercrime.' (2001) https://www.coe.int/en/web/cybercrime/convention-on-cybercrime&ved=2ahUKEwiJkL7w1IaUAxUed0EAHdf0GiUQFnoECC0QAQ&usg=AOvVaw3QLdbmzxVutQGs8SvsrIKv retrieved on April 24, 2026.

[67] Interpol, 'Digital Evidence and Cybercrime Guide.' https://www.interpol.int/content/download/15731/file/Guide%2520for%2520Criminal%2520Justice%2520Statistics%2520on%2520Cybercrime%2520and%2520Electronic%2520Evidence.pdf&ved=2ahUKEwjdreKu1YaUAxWndUEAHQ0JNfUQFnoECBYQAQ&usg=AOvVaw2QDU6m70XoTAE_S8ZAlA6z retrieved on April 24, 2026.

[68] UNODC, Cybercrime Technical Assistance Report (2020) https://www.unodc.org/documents/NGO/CSU-CyberCrime-240731-WEB.pdf&ved=2ahUKEwiwxvHp1YaUAxW1W0EAHWOaIz0QFnoECBYQAQ&usg=AOvVaw1OG7xOb1QQHx8xJJLmT73l retrieved on April 24, 2026.

[69] UN Human Rights Council, 'Online Violence Against Women.' *Op. cit.*

9. Conclusion

Cybercrime is no longer merely a technical or financial issue; it is a profound human rights and social justice challenge. This study has highlighted that its gendered dimensions are particularly severe, as women and gender minorities face disproportionate harm through cyberstalking, non-consensual dissemination of intimate images, sextortion, doxxing, and emerging forms of abuse like deepfake pornography. These crimes do not merely cause emotional or reputational damage—they undermine victims' autonomy, dignity, and participation in both digital and public spheres.[71]

Comparative analysis shows that legal frameworks alone are insufficient unless designed to address the lived experiences of victims and the structural inequalities that make certain groups more vulnerable. The United States demonstrates a model of a comprehensive, victim-oriented approach, combining federal statutes like the CFAA with the Violence Against Women Act and state-specific laws addressing revenge pornography, cyberstalking, and online harassment. Victims are recognised as active agents, with access to civil remedies, restraining orders, compensation, and psychological support. Judicial interpretation in cases such as People v Bollaert and *Elonis v United States* illustrates an evolving understanding of digital harm and a socially responsive, victim-centred legal approach.[72]

Nigeria, however, illustrates the limitations of an offender-focused and technologically oriented model. The Cybercrimes Act 2015 primarily prioritises punitive measures over victim protection. Section 24, which criminalises cyberstalking and offensive communications, is applied inconsistently and fails to address gender-specific harms. While the Violence Against Persons (Prohibition) Act attempts to fill gaps, uneven domestication, procedural challenges, and cultural barriers limit its practical impact. Judicial engagement with gendered cybercrime remains minimal, and institutional capacity including forensic expertise and specialised units is weak. Patriarchal norms, victim-blaming, and social stigma further discourage reporting. Consequently, victims face prolonged exposure to harm with limited access to timely and meaningful remedies.[73]

The comparative analysis highlights that effective gender-sensitive cybercrime regulation depends on legal philosophy, institutional capacity, cultural context, and adherence to international obligations. U.S. law exemplifies a human-rights oriented philosophy, integrating technological enforcement with social and gender justice. Nigerian law remains state-centred, focusing on offender punishment rather than victim empowerment. Closing this gap requires legislative reform, institutional strengthening, judicial training, public awareness, and alignment with international instruments such as the Budapest Convention, CEDAW, and the African Union Convention on Cyber Security.[74] Addressing gendered cybercrime is therefore a legal, social, and ethical imperative. Without robust gender-sensitive frameworks, digital spaces risk perpetuating offline inequalities, silencing women, and enabling impunity. Nigerian law must evolve to provide explicit statutory recognition of online sexual abuse, sextortion, and emerging forms of digital exploitation. Civil remedies, protective orders, victim support services, and regional

[70] Amnesty International, Digital Safety for Women (2021) 6.
[71] D. K. Citron, Hate Crimes in Cyberspace (Harvard University Press 2014) 101.
[72] People v Bollaert 248 Cal App 4th 699 (2014); Elonis v United States 575 US 723 (2015).
[73] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria) s 24; Violence Against Persons (Prohibition) Act 2015 (Nigeria).
[74] Council of Europe, Budapest Convention on Cybercrime (2001); CEDAW (1979); African Union Convention on Cyber Security and Personal Data Protection (2014).

cooperation are essential. Strengthening enforcement mechanisms, aligning with international best practices, and promoting public awareness will transform Nigeria's legal approach from punitive to victim-centred, safeguarding human dignity and equality in the digital age.[75]

9.2 Recommendations and Policy Reform

Based on comparative analysis and enforcement challenges, this study proposes the following practical recommendations primarily for Nigeria:

a.Enactment of Gender-Specific Cybercrime Legislation

Nigeria should enact laws explicitly criminalising revenge pornography, sextortion, doxxing, and deepfake abuse.[76] Such legislation should frame these offences as violations of human dignity, privacy, and gender equality, moving away from fragmented provisions.

b. Establishment of Victim-Centred Remedies

Legal reform should include civil remedies alongside criminal sanctions.[77] Courts should issue digital protection orders, restrain perpetrators, and enable content removal. Victims should access compensation and counselling, promoting restorative justice.

c. Creation of Specialised Cybercrime Courts

This would improve judicial efficiency and public confidence.[78] Specialised courts or judicial divisions trained in digital forensic evidence, international cyber law, and gender-sensitive adjudication should be established.

d. Institutional Capacity Building

Partnerships with international organisations and tech companies can enhance competence and resources.[79] Law enforcement agencies require cyber forensic infrastructure, secure evidence management, and continuous professional training.

e. Public Awareness and Digital Literacy

Education campaigns should reduce underreporting and stigma, inform citizens of digital rights, and integrate cyber safety into school curricula.[80]

f. Regional and International Cooperation

Nigeria should join international frameworks like the Budapest Convention and strengthen African regional collaboration through shared databases, extradition agreements, and joint investigations.[81]

g. Integration of Feminist Legal Perspectives

Legal reform should integrate feminist legal theory, recognising structural gender inequalities in cybercrime.[82] Gender impact assessments should guide legislative drafting and judicial policy.

[75] UN Women, Online Violence Against Women and Girls (2021) 25
[76] Cybercrime and Gender Bill Draft (Nigeria, 2023).
[77] *Ibid*.
[78] ibid.
[79] UNODC, Capacity-Building for Cybercrime Enforcement (2020) 15.
[80] UNESCO, Digital Literacy and Safety for Youth (2019).
[81] Council of Europe, Budapest Convention on Cybercrime (2001).
[82] C. MacKinnon, *Feminism Unmodified* (Harvard University Press 1987) 75.