DIGITAL SEXUAL VIOLENCE IN NIGERIA: CRIMINAL LAW RESPONSES AND VICTIM PROTECTION CHALLENGES

Ashikodi Phebe Ogheneyome*

Abstract

Digital technologies have transformed communication, social interaction, and commercial activities in Nigeria. However, the same technologies have also facilitated new forms of sexual violence perpetrated through cyberspace. Nigerian criminal law has increasingly responded to digital sexual violence through statutes such as the Constitution of the Federal Republic of Nigeria, 1999, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, among others. Despite these interventions, victims continue to face serious obstacles in obtaining effective legal protection and remedies. This article critically examines the adequacy of Nigerian criminal law responses to digital sexual violence and analyses the practical challenges confronting victims within the criminal justice system. The article argues that although Nigeria possesses fragmented legal mechanisms capable of addressing aspects of digital sexual violence, significant doctrinal, institutional, and enforcement gaps persist. It recommends legislative reform, specialised investigative mechanisms, stronger victim-centered procedures, and improved digital evidence frameworks.

Keywords: Digital Sexual Violence, Cybercrime, Victim Protección

1.0 INTRODUCTION

The rapid expansion of internet usage and social media platforms in Nigeria has fundamentally altered the nature of interpersonal interaction.

* Email: phebeashikodi@gmail.com

There is a significant impact on contemporary culture with Information and communication technologies (ICTs) as individuals all over the globe rely on ICTs, which have revolutionised how public and private spheres are interconnected.[1] While digital technologies have promoted economic growth and communication, they have simultaneously created opportunities for technology-facilitated abuse, particularly sexual violence committed through digital means[2]. Women and girls are disproportionately affected[3], although men and children are also victims of online sexual abuse and exploitation. DSV refers to acts of sexual abuse, harassment, or exploitation perpetrated through information and communication technologies. These include revenge pornography, cyberstalking, online grooming, sextortion, deepfake pornography, non-consensual[4] image sharing, and digitally facilitated sexual harassment. The anonymity, speed, and transnational nature of cyberspace complicate both prevention and prosecution.

In Nigeria, incidents of online harassment and cyber-enabled sexual abuse have increased due to new digital technologies, rapid technical innovation, the transnational character of internet services, and the likelihood that victims and perpetrators live in various countries, making it harder for

[1] N Henry and A Powell, Sexual Violence in The Digital Age: The Scope and Limits of Criminal Law (Springer Nature, London 2017) 7-9.
[2] S Burke, M Wallen, K Vail-Smith and D Knox, 'Using Technology to Control Intimate Partners: An Exploratory Study of College Undergraduates' (2011) 27 Computers in Human Behaviour 1162–1167.
[3] Committee on the Rights of the Child (CRC Committee), General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021 (CRC General Comment No. 25 (2021)), para. 3
[4] P Patella-Rey, 'Beyond Privacy: Bodily Integrity as an Alternative Framework for Understanding Non-Consensual Pornography' (2018) 21 Information, Communication and Society 5, 786-791.

governments to protect abuse victims[5]. Civil society organisations and advocacy groups have repeatedly highlighted the growing prevalence of digital gender-based violence.[6] Recent reports have also warned about rising incidents of cyberstalking, online harassment, sextortion, and image-based abuse.[7]Despite these developments, Nigerian criminal law was not originally designed to address technologically mediated sexual offenses. Existing laws are often fragmented, outdated, or insufficiently adapted to the realities of digital abuse. Victims also encounter institutional weaknesses, evidential difficulties, stigma, and procedural obstacles within the criminal justice process. This article critically evaluates the Nigerian legal framework governing DSV and examines the challenges confronting victims seeking protection and justice. To safeguard victims, new means for investigating, storing, and preserving electronic evidence, access to justice for victims, and independent oversight of children's digital rights to protection are required.[8]The article adopts a doctrinal and analytical methodology relying on statutes, judicial authorities, international instruments, and contemporary scholarly materials.

2.0 DEFINITION AND NATURE OF DIGITAL SEXUAL VIOLENCE (DSV)

[5] United Nations Children's Fund 'Legislating for the Digital Age: Global Guide on Improving Legislative Framework to Protect Children from Online Sexual Exploitation and Abuse' (UNICEF, New York 2022)10-12.
[6] Project Alert, 'Project Alert seeks stronger laws as femicide, online abuse rise' Vanguard (25 November 2025). Vanguard News
[7] Lift Africa Foundation, 'Group seeks passage of Kano VAPP Law, warns against digital GBV' Premium Times (30 November 2025). Premium Times Nigeria
[8] Cybercrimes (Prohibition, Prevention, Etc) Act 2015.

DSV is generally understood as sexual abuse perpetrated, facilitated, or amplified through the use of information and communication technologies (ICTs).[9] A variety of technologies being used by perpetrators to procure and facilitate sexual assaults includes mobile devices, email, social networking sites, chat rooms, and online dating services, which are just a few of the platforms included in these technologies.[10]This encompasses a spectrum of behaviours, ranging from the dissemination of sexually explicit material without consent to online grooming and sexual extortion. The term has evolved to reflect a more comprehensive understanding of the harm, moving beyond narrower definitions such as 'revenge porn' which often carried victim-blaming connotations.[11]

International scholarship frequently uses the term “technology-facilitated sexual violence” to encompass a broad spectrum of online sexual harms.[12]As defined by the World Health Organization, the term embraces a range of technologically-enabled behaviours.[13] These forms of DSV include: cyberstalking and online sexual harassment; non-consensual sharing of intimate images; revenge pornography; sextortion; deepfake

[9] F.A. Tunrayo, 'Legal Framework for Regulating Online Gender Based Violence in Nigeria: A Case for Stronger Cybercrime Legislation' (2025) SSRN.
[10] N Henry and A Powell, ‘Beyond the Sext: Technology Facilitated Sexual Violence and Harassment Against Adult Women’ (2014) 48 Australian and New Zealand Journal of Criminology, 1, 1104-1118.
[11] D Fido, 'Understanding how survivors of non-consensual intimate image-sharing' (2025) ScienceDirect’.
[12] N Henry and A Powell, ‘Sexual Violence in the Digital Age’ in The Routledge International Handbook of Technology-Facilitated Violence and Abuse (Routledge 2021).
[13] N Henry and A Powell, ‘Sexual Violence in The Digital Age: The Scope and Limits of Criminal Law’ (2016) 25 Social and Legal Studies, 4, 397-418.

sexual imagery;[14]online grooming of minors; cyber exploitation; dissemination of sexually explicit content without consent; digitally facilitated trafficking and exploitation. The psychological and social consequences of such violence are severe. Victims often experience depression, anxiety, reputational damage, social exclusion, economic loss, and suicidal ideation. The permanence and replicability of online content intensify the harm because abusive materials may continue circulating indefinitely. DSV also implicates constitutional rights, including the dignity of the human person, privacy, freedom from discrimination, and security of the person under the Constitution of the Federal Republic of Nigeria.[15]

Several key terminologies are integral to conceptualizing DSV:

i. Sextortion:

This refers to the act of coercing an individual into performing sexual acts, providing sexual images, or engaging in other sexual exploitation by threatening to expose sensitive or intimate information, often obtained through digital means.[16] Perpetrators typically exploit trust or

[14] B Chesney and D Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 6, 1753– 1820. *Police v. Ravshan Usmanov* (2011) NSWLC 40, the accused was also charged with an indecency offence of publishing indecent articles. on appeal, the 6-month home detention sentence was overturned and was reduced to a suspended sentence only.

[15]The Constitution of the Federal Republic of Nigeria (as amended) Cap C23 Laws of the Federation of Nigeria 2004 (CFRN) 1999.

[16] E Agnew, 'Sexting among Young People: Towards A Gender Sensitive Approach' (2021) 29 The International Journal of Children's Rights 1, 3-30.

vulnerability, using the threat of public humiliation or reputational damage as leverage.[17]

ii. Non-Consensual Sharing of Intimate Images (NCSII) / Image-Based Sexual Abuse (IBSA)

This involves the distribution of sexually explicit or intimate images or videos of an individual without their consent[18]. The term NCSII is increasingly preferred over 'revenge pornography[19] to accurately reflect the abusive nature of the act and to avoid implying that the victim is somehow responsible for the sharing.[20]IBSA is a broader term that includes NCSII but also encompasses threats to share, image manipulation, and voyeurism through digital means.[21]

iii. Cyberstalking and Cyber Harassment

These terms describe persistent and unwanted online contact or behavior that causes fear, distress, or annoyance. While not exclusively sexual, they frequently involve sexually suggestive or explicit content, threats of sexual violence, or the dissemination of intimate details to harass and

---

[17] P Patella-Rey, 'Beyond Privacy: Bodily Integrity as an Alternative Framework for Understanding Non-Consensual Pornography' (2018) 21 Information, Communication and Society 5, 786-791.
[18] *ibid*
[19] M Hall and J Hearn, Revenge Pornography. (1st edn, Routledge, London 2017)1- 12.
[20] Stand to End Rape, 'Non-Consensual Image Sharing vs. Revenge Porn' (2023) <https://standtoendrape.org/revenge-porn-vs-non-consensual-image-sharing/> accessed 22 May 2026.
[21]RAINN, 'Let's call it what it is, Image Based Sexual Abuse (IBSA)' (2024) <https://www.facebook.com/RAINN01/posts/-lets-call-it-what-it-is-image-based-sexual-abuse-ibsaalternative-langauge-like-/829608299212129/ >accessed 22 May 2026.

intimidate victims.[22] The Nigeria's Cybercrimes Act[23] specifically addresses cyberstalking, criminalizing the sending of messages that are grossly offensive, pornographic, or menacing in character or of an indecent or obscene nature.[24]

iv. Doxing

This involves the online publication of private or identifying information about an individual, such as their home address, workplace, or personal contact details, often with malicious intent. In the context of DSV, doxing can be used to facilitate offline harassment, intimidation, or to amplify the impact of NCSII by making victims easily identifiable.[25]

The unique nature of DSV, compared to traditional sexual violence, lies in several factors. Firstly, the anonymity and distance afforded by the internet can embolden perpetrators, reducing perceived risks of apprehension. Secondly, the speed and permanence of digital dissemination mean that intimate content, once shared, can be almost impossible to fully remove, leading to long-term psychological trauma and reputational damage for victims. Thirdly, DSV often involves a wider audience than traditional forms of sexual violence, as content can be viewed, shared, and re-shared globally, amplifying the victimisation

[22] Nigeria Police Force National Cybercrime Centre, 'Cyberstalking and cyberbullying are crimes under the law' <https://www.facebook.com/npfnccc/posts/cyberstalking-and-cyberbullying-are-crimes-under-the-law-behind-every-screen-is-/750053457996924/> accessed 22 May 2026

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

[24] *ibid*

[25] A. Ochoga, 'Legal Implications of Cyber-Bullying and Online Harassment in Nigeria' (2025) AOC Solicitors <https://aocsolicitors.com.ng/legal-implications-of-cyber-bullying-and-online-harassment-in-nigeria/> accessed 22 May 2026.

experience. Finally, the lack of physical contact can sometimes lead to a misconception that DSV is less severe than physical sexual violence, a notion that undermines the profound harm it inflicts.[26] Understanding these distinctions is paramount for crafting legal frameworks that are not only punitive but also preventative and victim-centered.

3.0 LEGAL FRAMEWORKS ADDRESSING DIGITAL SEXUAL VIOLENCE IN NIGERIA

Nigeria has made strides in developing legislative frameworks to combat cybercrime and gender-based violence, some of which are directly applicable to DSV. However, the evolving nature of DSV often outpaces legislative responses, creating challenges for enforcement and victim protection. This section critically examines the primary legal instruments in Nigeria that address DSV.

3.1 Constitution of the Federal Republic of Nigeria, 1999

The Constitution[27] guarantees fundamental rights relevant to victims of DSV, including the right to the dignity of the human person under section 34[28] and the right to privacy under section 37[29]. However, constitutional enforcement in DSV cases remains limited due to weak implementation mechanisms.

---

[26] `M Mustapha, 'Cybercrime, Gender, And Legal Protections: A Comparative Study of Nigeria and the United States' (2026) Nnamdi Azikiwe University Journal of Private and Property Law,15.22-36

[27] *ibid* (n.15)

[28] *ibid* s. 34

[29] *ibid* s. 27

3.2 The Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act[30] is Nigeria's principal legislation addressing online misconduct. The Act criminalises child pornography[31]. The provision prohibits producing, distributing, procuring, or possessing child pornography through computer systems. This is particularly significant given the increasing online exploitation of minors. The Act also criminalises cyberstalking and offensive online communication. The provision prohibits knowingly sending grossly offensive, pornographic, indecent or menacing messages through computer systems or networks.[32] Section 24 has become the most frequently invoked provision in addressing online harassment and digital abuse. Recent prosecutions under the amended Act demonstrate the growing reliance on cyberstalking provisions in criminal proceedings.[33] Specifically, it targets messages sent to cause criminal intimidation, annoyance, inconvenience, obstruction, insult, injury, enmity, hatred, ill will, danger, or needless anxiety.[34] While not explicitly mentioning sexual violence, these provisions have been widely used to prosecute cases involving online sexual harassment, bullying, and the non-consensual sharing of intimate images, particularly when such acts cause significant distress or intimidation to the victim.

Notwithstanding these provisions, section 24 has generated controversy for vagueness and potential misuse against journalists, activists, and social commentators. The ECOWAS Community Court of Justice in *SERAP v*

[30] The Cybercrimes (Prohibition, Prevention, etc.) Act 2015
[31] Cybercrimes Act s.23
[32] *ibid* s.24
[33] Interior Minister sues activist for cyberstalking' The Star (4 March 2026). The Star
[34] Cybercrimes Act, s. 24(1)(b)

Federal Republic of Nigeria[35] criticised section 24 as arbitrary, vague, and a violation of the right to freedom of expression[36], ordering the Nigerian government to repeal or amend it. The application of section 24 is against online expression.[37]The broad language of the section creates uncertainty regarding the threshold for criminal liability and risks conflating legitimate expression with genuine harmful conduct. The Act addresses persistent online harassment, which can often have sexual undertones or be a component of DSV. This is aimed at deterring individuals from engaging in repeated acts of communication that cause distress or fear.[38]

Furthermore, section 27 criminalizes cybersquatting and impersonation, which may intersect with DSV where perpetrators create fake accounts to harass or sexually exploit victims. As deterrents, the Cybercrimes Law stipulates 10 years' imprisonment and fines of 25 million naira. The Act[39] does not provide for many forms of technology-facilitated sexual violence, and the criminal and penal legislation don't cover most forms of technology-enabled sexual violence. Current Nigerian legislation does not effectively address how to prevent and respond to online sexual offenses. Considering our laws do not encompass digital sexual offenses, Nigerian offenders cannot be held liable for the majority of the sexual assaults facilitated by the technology listed above. When there is no statutory

[35] *SERAP v Federal Republic of Nigeria* ECW/CCJ/APP/09/19.
[36] CFRN s.39
[37] Socio-Economic Rights and Accountability Project, 'SERAP sues Nigerian govt at ECOWAS Court over misuse of Cybercrimes Act' Premium Times (12 January 2025). Premium Times Nigeria
[38]Cybercrimes Act, s.26
[39] *ibid*

provision for a crime, courts are frequently compelled to dismiss the charges. It is often argued that where there is no law, there is no crime.[40]

The Cybercrimes Act 2015[41] was a landmark piece of legislation that established a comprehensive legal framework for the prohibition, prevention, detection, response, investigation, and prosecution of cybercrimes in Nigeria. Despite its significance, the 2015 Act faced criticism for its broad wording, particularly concerning Section 24, which some argued could be used to stifle free speech and legitimate online expression. This led to calls for amendments to refine its scope and ensure a clearer distinction between criminal behaviour and protected speech.

3.3 The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024

In response to the criticisms and the evolving landscape of cybercrime, President Bola Ahmed Tinubu signed the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 into law in February 2024.[42] This amendment sought to address some of the ambiguities and concerns raised by the 2015 Act. While the full implications are still being analysed, key changes include a more refined definition of cyberstalking under Section 24, aiming to narrow its application to focus more explicitly on actual threats, harassment, and malicious intent, rather than inadvertently capturing legitimate online discourse. This amendment is

[40] CFRN, s.36(12); *Faith Okafor v. Lagos State Government and Anor* (2016) LPELR-41066(CA);
[41] Cybercrimes Act.
[42] 'Tinubu Signs Cybercrime Amendment Bill into Law' Premium Times (1 March 2024) <https://www.premiumtimesng.com/news/top-news/670356-tinubu-signs-cybercrime-amendment-bill-into-law.html>accessed 22 May 2026.

crucial for ensuring that the law effectively targets perpetrators of DSV without infringing on fundamental rights.

3.4 Violence Against Persons (Prohibition) Act (VAPP)2015

The VAPP Act[43] is another critical legislative tool, primarily designed to eliminate violence in private and public life and ensure maximum protection for victims. While the VAPP Act was initially conceived to address physical and domestic violence, its broad definitions and provisions make it applicable to certain forms of DSV, particularly those involving psychological and emotional harm. The VAPP Act significantly expanded protection against gender-based violence in Nigeria. The Act prohibits various forms of sexual and psychological abuse, including stalking, intimidation, and emotional abuse. The Act,[44] criminalises stalking, including conduct involving electronic communication. This provision is particularly relevant to DSV involving persistent online harassment or threats. The VAPP Act also broadens the concept of rape and sexual violence beyond traditional definitions under the Criminal Code[45] and Penal Code[46]. It recognises psychological violence and harmful conduct occurring within domestic relationships. However, the VAPP Act applies directly only within the Federal Capital Territory unless domesticated by states. Although many states have adopted equivalent legislation, uneven domestication creates inconsistent protection across Nigeria.[47]

---

[43] Violence Against Persons (Prohibition) Act 2015.
[44] VAPP, s.17
[45] Criminal code Act, Cap C38 LFN 2004
[46] Penal code (1962) Cap 89, Laws of Northern Nigeria
[47] Zulum signs child protection bill into law' The Cable (11 January 2022)

It is important to note that the VAPP Act primarily applies to the Federal Capital Territory (FCT), but many Nigerian states have domesticated the Act, thereby extending its protections across various jurisdictions. This domestication is vital for providing a more uniform and comprehensive legal response to gender-based violence, including its digital manifestations.

3.5 Criminal Code and Penal Code

While the Cybercrimes Act and VAPP Act are the most direct legislative responses, other laws play a supplementary role in protecting victims. A careful understanding of the Criminal Code Act reveals the presence of some elements of revenge pornography. Nonetheless, if the act is committed without using the Internet, it will not be applicable. The Criminal Code Act[48]applicable in Southern Nigeria and the Penal Code[49] applicable in Northern Nigeria contain provisions criminalising obscenity, defamation, intimidation, and sexual offences. Section 170 (b) Criminal Code Act[50] provides:

> Any individual who knowingly sends, or attempts to send, by post anything which:
> (b) encloses an indecent or obscene print, painting, photograph, lithograph, engraving, book, card, or article, or which has in it, or on it, or on its cover, any indecent, obscene, or offensive words that are gross, marks, or designs; is guilty of a misdemeanour and one year imprisonment is liable.

[48] Criminal Code Act, s.170(b)
[49] The Penal Code
[50] Criminal Code Act

It is important to understand that this Act was enacted in 1990. However, these statutes predate modern digital realities and contain limited provisions specifically addressing online abuse. Many victims believe that the criminal code is insufficient to prevent revenge pornography.[51] The absence of explicit recognition of offences such as revenge pornography,[52] deepfake pornography and sextortion exposes significant legislative gaps. Prosecutors are therefore compelled to rely on general provisions that may inadequately capture the technological dimensions of the offences.

3.6 Evidence Act 2011

The Evidence Act[53] governs the admissibility of electronic evidence in Nigeria. Section 84 provides conditions for the admissibility of electronically generated evidence. DSV prosecutions frequently depend on screenshots, chats, emails, videos, and metadata. Nigerian courts have repeatedly affirmed the admissibility of electronic evidence where statutory conditions are satisfied. In *Kubor v Dickson*,[54] the Supreme Court clarified requirements for admissibility of computer-generated evidence. Nevertheless, practical difficulties persist regarding authentication, preservation, and forensic examination of electronic evidence.

3.7 Nigeria Data Protection Act 2023

The Nigeria Data Protection Act[55] provides additional protections relevant to victims of DSV. Unauthorised processing or dissemination of intimate images may constitute violations of data privacy rights. Although

[51] G Udonnah, Protecting Sexual Violence Victims in the Digital Age (2023) 2 *Cavendish University Law journal* 1.
[52] M Hall and J Hearn, Revenge Pornography. (1st edn, Routledge, London 2017)1- 12.
[53] The Evidence Act, Cap C Laws of the Federation of Nigeria 2011
[54] *Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534,
[55] The Nigeria Data Protection Act 2023

primarily regulatory rather than criminal, the Act strengthens privacy protection and may support civil or administrative remedies for victims.

3.8 African Union Convention on Cyber Security and Personal Data Protection

African Union Convention on Cyber Security and Personal Data Protection.[56]However, domesticated laws in line with section 12 (1)[57] of the Constitution are enforceable.

4.0 CRIMINAL LAW RESPONSES TO DIGITAL SEXUAL VIOLENCE

The effectiveness of any legal framework is ultimately determined by its application in practice. In Nigeria, the prosecution of DSV cases, while still nascent, has begun to yield some significant judicial precedents, particularly under the Cybercrimes Act. These cases offer insights into the courts' interpretation of the law and the challenges inherent in prosecuting digital offences.

The principal criminal law response remains the Cybercrimes (Prohibition, Prevention, etc.) Act as amended in 2024, especially section 24, with the VAPP Act and general criminal law provisions supply supplementary protection in cases involving psychological abuse, coercion, threats, and victim remedies. Cyberstalking also remains the most visible criminal law response to online abuse in Nigeria. Law

[56] The African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014 (EX.CL/846 (XXV). The Convention imposes obligations on Member States to establish legal, policy, and regulatory measures to promote cybersecurity governance and control cybercrime.
[57] The Constitution

enforcement agencies increasingly prosecute individuals accused of threatening or harassing victims online.[58]However, cyberstalking provisions often prioritise protection of public officials and politically exposed persons rather than vulnerable victims of sexual abuse. It is argued that enforcement patterns reveal selective prosecution. The broad scope of section 24 of the Cybercrimes Act also raises constitutional concerns regarding section 39 of the Constitution relating to freedom of expression under.[59] Yet the present framework still shows conceptual and practical weaknesses: there is no fully elaborated, stand-alone national offence structure for all forms of image-based sexual abuse, enforcement capacity is uneven, evidential demands for electronic proof are exacting, and victim protection measures remain fragmented across institutions and jurisdictions.

The Cybercrimes Act 2015, and its subsequent 2024 amendment, have been the primary legal instruments for addressing various forms of online misconduct, including those with sexual undertones. A notable case that illustrates the application of Section 24 (cyberstalking) is the *Federal Republic of Nigeria v. Okoye Blessing Nwakaego*.[60] This case involved a TikToker, Okoye Blessing Nwakaego, who was prosecuted and convicted by the Federal High Court in Lagos for cyberstalking Nollywood actress Eniola Badmus. The defendant was sentenced to three years' imprisonment, with an option of a fine.[61] While the specific details of the

[58] Police Arrest Three for Cyberstalking and Online Fraud, Nigeria Info FM (19 August 2025). Nigeria Info, Let's Talk!
[59] The Constitution s.39
[60] *Federal Republic of Nigeria v. Okoye Blessing Nwakaego* (2023)
[61] 'Court Sentences Lady to Three Years in Prison for Cyber-Stalking Eniola Badmus' Channels Television (2 August 2023) <https://www.channelstv.com/2023/08/02/court-

cyberstalking might not have been explicitly sexual in nature, the case is significant as it demonstrates the judiciary's willingness to apply the Cybercrimes Act to address online harassment and bullying perpetrated through social media platforms. It sets a standard for holding individuals accountable for their online conduct, which can be extended to cases involving DSV where the elements of harassment, intimidation, or offensive communication are present.

Beyond cyberstalking, law enforcement agencies, for example, the Economic and Financial Crimes Commission (EFCC) and the National Agency for the Prohibition of Trafficking in Persons (NAPTIP) have actively pursued cases involving sextortion. These cases often involve complex digital forensics to trace perpetrators and gather evidence. For instance, NAPTIP has reported busting several sextortion rings, leading to arrests and prosecutions.[62] While specific detailed judicial pronouncements on sextortion cases are not always widely publicised, the increasing number of arrests and convictions indicates a growing capacity within the Nigerian justice system to tackle this form of DSV. The VAPP Act primarily focused on physical and domestic violence, offers avenues for prosecuting DSV, particularly in states where it has been domesticated. The broad definitions of psychological and emotional abuse under Section 14, and intimidation under Section 18, can be invoked in cases where DSV leads to significant mental distress or fear. However, the application of the VAPP Act to purely digital forms of violence is still evolving, and more judicial interpretations are needed to solidify its role in this context.

---

sentences-lady-to-three-years-in-prison-for-cyber-stalking-eniola-badmus/>accessed 22 May 2026.

[62] NAPTIP, 'eDigest – April 2023'<https://naptip.gov.ng/edigest-april-2023/> accessed 22 May 2026.

The Criminal Code Act, the Cybercrimes Act, and the VAPP Act are Nigerian legislation that protects victims. A careful understanding of the Criminal Code Act reveals the presence of some elements of revenge pornography. Nonetheless, if the act is committed without using the Internet, it will not be applicable.

Furthermore, Nigeria has also intensified efforts against online child pornography and exploitation through collaboration between International Organisations, the Nigerian Police Force, and the Economic and Financial Crimes Commission[63]. Yet enforcement remains constrained by inadequate digital forensic infrastructure, poor reporting mechanisms, and low public awareness. Nigeria lacks comprehensive legislation specifically criminalising revenge pornography or image-based sexual abuse. Prosecutors typically rely on cyberstalking, obscenity, or privacy-related provisions. This fragmented approach weakens victim protection because existing laws do not adequately address consent, digital permanence, rapid dissemination, platform responsibility, and removal procedures. International scholarship increasingly recognises image-based abuse as a distinct form of sexual violence requiring specialised legal responses.[64]

[63] M Bello, investigating cybercriminals in Nigeria: a comparative study. <https://core.ac.uk/download/199214443> accessed May 20 2026

[64] Li Qiwei and others, 'Platforms as Crime Scene, Judge, and Jury: How Victim-Survivors of Non-Consensual Intimate Imagery Report Abuse Online' (2025) arXiv:2512.13500v1 <https://doi.org/10.48550/arXiv.2512.13500> accessed 22 May 2026.

5.0 INSTITUTIONAL RESPONSES TO DIGITAL SEXUAL VIOLENCE

Judicial engagement with DSV in Nigeria remains relatively limited. Nonetheless, recent cases demonstrate increasing judicial recognition of digital sexual abuse. In *Charlotte Dehli v Federal Republic of Nigeria*[65], the Court of Appeal affirmed the jurisdiction of Nigerian courts over allegations involving online dissemination of nude images for extortionary purposes. The case reflects growing judicial willingness to apply cybercrime legislation to image-based sexual abuse. Similarly, Nigerian courts have imposed sanctions for online defamatory conduct involving social media platforms. In 2024, a Federal High Court convicted a Tik`Tok user for cyberstalking and defamation under the Cybercrimes Act.[66]Although the case primarily concerned defamation, it demonstrates the judiciary's readiness to apply cybercrime laws to digital misconduct. However, judicial responses remain inconsistent. Courts frequently struggle with evidentiary issues related to digital authentication, the admissibility of electronic evidence, and jurisdiction over transnational offenses.

The Nigerian Police Force National Cybercrime Centre has expanded cybercrime enforcement activities.[67] However, institutional responses remain hindered by inadequate funding, shortage of trained personnel, corruption, weak inter-agency coordination, and limited victim support structures. Victims frequently report dismissive attitudes from law

[65] *Charlotte Dehli v Federal Republic of Nigeria* (CA/PH/32CR/2023, Court of Appeal, 24 May 2024).

[66]Federal High Court conviction involving cyberstalking and online defamation. Pulse Nigeria +1

[67] 'Cyberstalking, cyberbullying are serious crimes, police warn Nigerians' The Nation (24 September 2025). The Nation Newspaper

enforcement officials, especially in cases involving intimate images or online harassment. Nigeria needs an effective internet policing framework to assist law enforcement in investigating, prosecuting, and punishing these violators.[68]

6. THE CHALLENGES IN DSV PROTECTION: LEGAL AND PROCEDURAL GAPS

Despite these legal frameworks and emerging judicial precedents, the prosecution of DSV cases in Nigeria faces several formidable challenges. DSV is a new wave of criminality in Nigeria, making it difficult for law enforcement agencies to catch up with criminals who use the internet for nefarious intent. The Nigerian Criminal Justice System and its counterparts in other countries face cybercrime concerns, including jurisdictional issues and digital evidence.[69]

i. Anonymity of cybercriminals

The anonymity of cybercriminals remains one of the most significant obstacles in advancing global efforts to stem the growing epidemic of cybercrime, which includes DSV. There are no simple methods for identifying and apprehending perpetrators or determining who is doing what and where a user of the Internet is located at any given moment; access to the global information system is free, and there are no prerequisites that must be met before a user can log on and connect with anyone and anywhere in the world. Thus, the unrestricted freedom of information and communication enables cybercriminals to conceal their

[68] T Akpoghome, 'Analysis of the Domestic Legal Framework on Sexual Violence in Nigeria' (2016)4 Journal of Law and Criminal Justice 2, 17-30.
[69] G Walker, E Adomi, and S Igun, 'Combating Cyber Crime in Nigeria' (2008) 26 The Electronic Library, 5, 716–725.

identity using various telecommunications devices so they cannot be tracked, identified, and apprehended.[70]

ii. Underreporting:

One of the greatest obstacles confronting victims is underreporting. A pervasive culture of victim-blaming and stigmatisation surrounding sexuality and victimisation discourages many victims from seeking legal remedies. Victims fear: public humiliation; reputational harm; victim-blaming; retaliation; family rejection. Women are particularly vulnerable because patriarchal social norms often place disproportionate scrutiny on female sexuality.

iii. Evidentiary Hurdles:

The reliance on digital evidence presents significant challenges. Digital evidence is highly volatile and susceptible to alteration or deletion. Victims may lack the technical knowledge necessary to properly preserve evidence. Investigators also face difficulties tracing anonymous perpetrators, encrypted communications, and foreign-based platforms. The requirements of section 84 of the Evidence Act may further complicate admissibility where victims cannot obtain the necessary certification for digital materials. Section 84 requires strict adherence to conditions for the admissibility of computer-generated evidence, including certification and proof of the computer's operational integrity.[71] This often necessitates specialised forensic analysis, which can be costly, time-consuming, and beyond the current technical capabilities of many law enforcement agencies.

---

[70] E Ajayi, 'Challenges to Enforcement of Cyber-Crimes Laws and Policy' (2016) 6 Journal of Internet and Information Systems 1, 1-12.
[71] Evidence Act 2011, s 84.

iv. Jurisdictional Complexities:

Cross-jurisdictional challenges are another obstacle to prosecuting online crimes. DSV frequently transcends territorial boundaries. Perpetrators may operate from foreign jurisdictions while content is hosted on servers outside Nigeria.[72] These transnational characteristics complicate investigation, extradition, evidence gathering, and enforcement of judicial orders, making investigation and prosecution difficult. Nigeria's mutual legal assistance mechanisms remain relatively underdeveloped in cybercrime enforcement. The United Nations Convention Against Transnational Organized Crime[73]is aimed at preventing and combating transnational organized crime, including cybercrime. In general, prosecuting online crimes entails navigating complicated legal challenges relating to conflict of laws. The territoriality concept states that the country where the crime was committed applies its laws. Other international treaties and conventions promote international cooperation in pursuing online crimes. It necessitates collaboration across multiple jurisdictions to ensure that perpetrators are held accountable for their activities. Extradition is a remedy, but extradition is a lengthy and expensive procedure.[74]

v. Lack of Specialised Training and Resources:

Many law enforcement officers, prosecutors, and even judicial officers lack adequate training in digital forensics, cybercrime investigation, and the psychological impact of DSV, nor are they trained to recognise the

[72] N Henry and A Powel, 'Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives' (2018) 28 Policing and Society 291 – 307.
[73] D Johnson, and D Post. 'Law and Borders: The Rise of Law in Cyberspace' (1996) Stanford Law Review (1996): 1367-1402.
[74]*ibid*

different types of violence affecting victims online, and many of them do not know how to handle these procedures.[75]Most victims are unaware that they can record abusive content if accessible to file charges, despite the necessity of doing so. The criminals may delete or hide evidence from the victim. Criminal evidence may be kept in the cloud, abroad, or on private devices. Keeping track of abuse evidence may assist in prosecuting the crime.[76]The Cyber Crimes (Prohibition, Prevention, Etc.) The Act protects individuals against internet-related crimes, but it provides little protection against sexual offenses, which is a major challenge.

vi. Inadequacies and Inconsistencies in Legislative Coverage

Inconsistencies between Federal and State Laws. The VAPP Act is not uniformly adopted across all Nigerian states, creating a fragmented legal landscape. Existing Nigerian laws also inadequately address deepfake pornography, AI-generated sexual imagery, sextortion, doxxing, and coordinated online sexual abuse. The absence of specialized legislation creates uncertainty and inconsistent prosecution.

vii. Limited Availability and Accessibility of Services

The lack of adequate protection and prevention of sexual offences continues to jeopardise victims' safety.[77] Nigeria lacks robust victim support structures for survivors of DSV. There is a severe shortage of specialised psychological, legal, and social support services tailored to the unique needs of DSV victims. Counselling, legal aid, shelter services, and

[75] S Dunn,'Technology-Facilitated Gender-Based Violence: An Overview' (2020) Centre for International Governance Innovation: Supporting a Safer Internet Paper No. 1

[76] T Palmer, 'Rape Pornography, Cultural Harm and Criminalization' (2018) 69 Northern Ireland Legal Quarterly 1, 37–58.

[77] T Starr, and T Lavis, 'Perceptions of Revenge Pornography and Victim Blame' (2018) 12 International Journal of Cyber Criminology 2, 427-438.

digital safety assistance remain limited and unaccessible. Victims often navigate the criminal justice process without adequate psychological or financial support.

viii. Delayed Justice

Criminal proceedings in Nigeria are frequently characterised by delay. Prolonged trials may intensify victims' trauma, especially where harmful content remains accessible online during litigation.

7.0 COMPARATIVE PERSPECTIVES

Several jurisdictions have adopted specialised legislation addressing DSV. In the United Kingdom, the Criminal Justice and Courts Act[78] criminalises disclosure of private sexual photographs without consent and with intent to cause distress. Similarly, Australia and Canada have enacted legislation specifically targeting non-consensual sharing of intimate images. South Africa's Cybercrimes Act[79]criminalizes the disclosure of intimate images without consent and provides enhanced victim protection mechanisms. Nigeria may draw lessons from these jurisdictions by adopting clear statutory definitions and victim-centered remedies.

8. RECOMMENDATIONS

Despite progress in certain jurisdictions, much more needs to be done in Nigeria. Hence, this work recommends that Nigeria enact specialized legislation expressly criminalising all forms of sexual abuse. Clear statutory definitions would enhance certainty and improve prosecution. Reform Section 24 of the Cybercrimes Act to eliminate vague language,

[78] The United Kingdom Criminal Justice and Courts Act 2015, s.33
[79] South Africa's Cybercrimes Act 2020

ensure compliance with constitutional free expression standards, and preserve protection against genuine online abuse. Law enforcement agencies should develop specialised DSV units staffed with trained cyber investigators, forensic analysts, and victim-support personnel.

Nigeria should simplify evidential requirements for electronically generated evidence and improve forensic infrastructure. Judicial officers also require continuous training on cybercrime and digital evidence. The government should establish counselling centres, emergency reporting mechanisms, legal aid services, and digital safety assistance programs. Partnerships with civil society organisations are essential.

Public education campaigns should address online safety, consent, digital ethics, reporting mechanisms, and harmful gender stereotypes. Through public education programs, social networking is used to eliminate sexual violence in Nigeria. These programs raise public awareness of sexual assault by providing resources, refuting myths, or sharing information that facilitates in-depth conversations and behavior modification. The effectiveness of social media safety measures can be reduced if parents are aware of their children's privacy settings[80]. Preventive techniques should be used to strengthen children's resilience to internet dangers rather than strict security and control procedures. The best preventative measure is to promote social media literacy and awareness.[81] Lastly, mutual legal

[80] L Baughman, 'Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators (2009) 19 Widener Law Journal 3, 933-966.

[81] S Duncan, 'My Space Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social-Networking Sites' University of Louisville School of Law Legal Studies Research Paper Series No. 2008-13(2008) Kentucky Law Journal 96.

assistance frameworks and cross-border cybercrime mechanisms should be strengthened to enhance International Cooperation.

9.0 CONCLUSION

DSV represents one of the most complex manifestations of gender-based violence in the digital age. Although Nigeria has adopted important legislative measures and related statutes, substantial legal and institutional deficiencies remain. The existing framework is fragmented, inconsistently enforced, and inadequately responsive to emerging technological harms such as deepfake pornography and image-based abuse. Victims continue to face stigma, evidential barriers, weak institutional support, and procedural delays within the criminal justice system. An effective response requires comprehensive legislative reform, victim-centered criminal justice procedures, specialized cyber enforcement mechanisms, and enhanced digital rights protection. Without such reforms, Nigerian law will remain insufficiently equipped to protect victims from evolving forms of DSV. A victim-centered approach, prioritising the safety, dignity, and recovery of those affected, must underpin all efforts.