International Cybersecurity Law Review (2024) 5:443–458
https://doi.org/10.1365/s43439-024-00126-0

Cyberstalking in Nigeria: An Exploratory Study of Section 24 of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024

Ifeoma E. Nwafor

Accepted: 10 June 2024 / Published online: 1 July 2024

Abstract The increase in internet use, interconnectivity, and affordability of data have intensified online harms, including cyberstalking on social media platforms and online generally. Victims of cyberstalking suffer severe harm, such as mental health issues, long-term psychological trauma, stigmatisation, depression, low self-esteem, job loss, fear and suicide. The Nigerian Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 made cyberstalking a crime under section 24 of the Act. However, the Economic Community of West African States Court of Justice ruled that section 24 (1) the Cybercrime Act of 2015 violates the right of freedom of expression and information. This paper evaluates the argument that the Cybercrime Act of 2015 violates free expression, a fundamental human right in the Nigerian Constitution vis-a-z the Nigerian Cybercrime (Prohibition, Prevention, Etc.) (Amendment) 2024. The findings reveal that the repealed provisions of section 24 of the Nigerian Cybercrime Act do not clearly define the offence of cyberstalking or stipulate the parameters or elements of the offence. Although, the amended provisions of section 24 make some improvement in protecting freedom of expression in Nigeria it does not fully ensure digital rights and press freedom. This paper canvasses for the further reform of section 24 of the Cybercrime Act to align with the constitutional rights of Nigerian citizens and offers recommendations for better protection for victims of cyberstalking in Nigeria.

Keywords Cyberstalking · Harassment · Cybercrime · Freedom of expression · Cyberstalking in Nigeria · Victim's protection

✉ Ifeoma E. Nwafor
Faculty of law, Godfrey Okoye University, Enugu, Nigeria
E-Mail: nwaforifeoma@gouni.edu.ng

Faculty of Business, Economics and Law, TH Köln, Cologne, Germany

1 Introduction

The virtual world is exploited for threatening, harassing, intimidating, and causing harm to others.[1] The content aimed at the target is often unsuitable and occasionally distressing, leading to the experience of fear, distress, anxiety, and concern. Cyberstalking reports exhibit the increasing prevalence of that form of cybercrime. Cyberstalking is the repetitive and deliberate use of information and communications technology (ICT) to harass, annoy, attack, threaten, intimidate, or verbally abuse individuals.[2] It frequently coincides with stalking that occurs in real-time or offline, and both acts are considered criminal offences. The motivations behind these actions are rooted in the desire to exert control, intimidate, or manipulate the victim. The perpetrator can be an unfamiliar individual encountered online or someone known to the target. They may choose to remain anonymous and may even seek the involvement of other online individuals without a connection to the victim.

Annually, an estimated 850,000 adults in the United States (US) fall victim to cyberstalking. Statista's 2021 report[3] provides that approximately 11% of US adults have personally encountered cyberstalking. Meanwhile, national statistics from the United Kingdom[4] indicate a significant surge of 24% in reported cases of cyberstalking in England and Wales throughout 2020. The Cyberbullying Research Centre[5] also observed a substantial increase, with cyberstalking cases rising from 6% in 2007 to 34% in 2019. Police records show that from April 2020 to March 2021, there were 98,863 reported instances of stalking, representing a staggering 300% surge compared to the previous year. Disturbingly, a review platform for software and digital services called Gitnux found that 47% of cyberstalking victims suffered from emotional distress, 38% experienced anxiety, and 19% reported symptoms of depression.[6] In most reported cases, women were more frequently targeted by stalkers than men, with many perpetrators being the victims' current or former intimate

[1] Recupero P.R 'Forensic Evaluation of Problematic Internet Use.' [2008] (36) *Journal of the American Academy of Psychiatry Law in* Steven D. Hazelwood & Sarah Koon-Magnin, 'Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. [2013] (7) (2) *International Journal of Cyber Criminology 155.*

[2] Sherri Gordon (2023) Cyberstalking: Definition, signs, examples and prevention. https://www.verywellmind.com/what-is-cyberstalking-5181466 accessed April 27 2024.

[3] S. Dixon, 'Global Opinions on Cyber stalking 2021, by age' [2022] https://www.statista.com/statistics/1306379/online-stalking-opinions-worldwide-by-age/ accessed March 24 2024.

[4] Office of National Statistics. Stalking: Findings from the Crime Survey for England and Wales https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/stalkingfindingsfromthecrimesurveyforenglandandwales accessed March 312024; Talia Shadwell (021) Stalking and harassment reports soared by 30% in England and Wales as Lockdown lifted https://www.mirror.co.uk/news/uk-news/breaking-stalking-harassment-reports-soared-23721399.amp accessed February 22 2024; Carsten Mapel, Emma Short& Antony Brown. Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey 2011. https://uobrep.openrepository.com/bitstream/handle/10547/270578/ECHO_Pilot_Final.pdf?sequence=1&isAllowed=y accessed February 27 2024.

[5] Justin W Patchin Cyberbullying 2019. https://cyberbullying.org/2019-cyberbullying-data accessed March 18, 2024.

[6] ibid.

partners.[7] Cyberstalking predominantly occurs on social media platforms, and charities and authorities have noted a surge in cyberstalking incidents over the past two years.

In Nigeria, numerous cyberstalking cases are reported, and the perpetrators have been taken to court, but most of these cases have remained undocumented and, therefore, difficult to monitor.[8] A study conducted on undergraduate students in Nigeria[9] provided that approximately 41.0% of the respondents expressed a fear of receiving threatening, insulting, and harassing emails.[10] This fear is not without basis. True Caller recently revealed that its community recorded a significant number of spam and unwanted calls in Nigeria, with a daily average of 120,000 such calls and a total of 2 million over a certain period.[11] These findings indicate that cyberstalking, although not extensively studied by scholars in Nigeria, continues to be a growing social issue that requires further investigation.

Various nations have laws that classify cyberstalking as a criminal offence, falling under anti-stalking, defamation, and harassment legislation. If convicted, the assailant can face legal consequences such as restraining orders, probation, criminal penalties, and imprisonment. In Nigeria, cyberstalking is an offence under the previous section 24 of the Cybercrime (Prohibition, Prevention, etc) Act [2] 2015 (the Principal Act) and section 24 of the Cybercrime (Prohibition, Prevention, etc) (Amendment) Act (Amended Act). It has been argued that the Section 24 of the Cybercrime Act of the Principal Act has been used to arrest and prosecute numerous journalists in Nigeria.[12] Government officials and authorities charge journalists based on subjective interpretations to trigger the application of section 24 of the Amended Act.

This study investigates the constitutionality of Section 24 of the Amended Act which also criminalises cyberstalking in Nigeria. It found the phrase "for the purpose of causing a breakdown of law and order" to be vague, ambiguous and susceptible to subjective interpretations. It makes recommendations for better protection of cyberstalking victims. The contribution of this work lies in illuminating the challenges of

[7] United States Department of Justice (1999). 1999 report on cyberstalking: A new challenge for law enforcement and industry. http://www.justice.gov/criminal/cybercrime/CS.htm accessed March 25, 2024.

[8] Okoye, Nwankwo, Obi et al. 'Stalking in the Criminal Legal System-Nigeria in Perspective' [2022] (13) (1) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* https://www.ajol.info/index.php/naujilj/article/view/225868/213139 accessed March 28, 2024.

[9] Philip N Ndubueze & ZAkariyya Muhammad Sarki 'Cyberstalking Awareness and Perception among Undergraduate Students in Nigeria' [2017] (2) (2) *Duste Journal of Humanities and Social Sciences.* https://www.researchgate.net/publication/325103033_Cyberstalking_Awareness_and_Perception_among_Undergraduate_Students_in_Nigeria accessed March 26, 2024.

[10] Ibid.

[11] Vanguard online, cited in Philip N Ndubueze & ZAkariyya Muhammad Sarki 'Cyberstalking Awareness and Perception among Undergraduate Students in Nigeria' [2017] (2) (2) Duste Journal of Humanities and Social Sciences. https://www.researchgate.net/publication/325103033_Cyberstalking_Awareness_and_Perception_among
_Undergraduate_Students_in_Nigeria accessed March 26, 2024.

[12] Emma Woollacott, Nigerian Cybercrime Law Ruled Illegal over Human Rights Concerns [April 2022] https://www.forbes.com/ accessed March 25, 2024.

the revised provision and enriching the ongoing debate on overly broad cybercrime enactments.

This paper is divided into four parts, commencing with the introduction. Part two covers the nature of cyberstalking and highlights the elements of the crime. Part three investigates the constitutionality of section 24 of the Cybercrime Act of the Principal and Amended Act, which criminalises cyberstalking in Nigeria. Part four offers recommendations for better protection for cyberstalking victims. Part five provides concluding remarks.

2 The nature of cyberstalking in Nigeria

Cyberstalking refers to unwanted and harassing behaviour where the perpetrator utilises electronic communication tools such as email, social media, and messaging apps to monitor, intimidate, or threaten another individual or individuals, often to cause fear or harm. It ranks among the top five global cybercrimes, and it is estimated that 850,000 adults in the United States fall victim to cyberstalking annually.[13] Rao[14] states that the terms 'cyber stalking' and 'cyber bullying' are often used interchangeably. The author posits that cyberbullying occurs among pre-teens and teenagers using digital technologies, particularly the internet and mobile phones. In contrast, cyberstalking is a more severe form of harassment, predominantly involving adults, and nearly 90% of cyberstalking cases are sexual. This research goes a little further to add that apart from including sexual content, the victims of such cyber-attacks are often subjected to threatening and intimidating messages, which may consist of text, images, or both. In almost all instances, the perpetrator's identity is either unknown or falsified.

Ndubueze[15] posits that cyberstalking is particularly prevalent among university undergraduate students. Hassan et al.[16] suggest that cyberstalking may include messages which constitute false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex or gathering infor-

[13] Janet Ogundepo, 'Experts Call for Vigilance as Cyberstalking Festers Online' https://punchng.com/experts-call-for-vigilance-as-cyberstalking-festers-online/ accessed March 28, 2024.

[14] Sam Rao, 'Disturbing Psycho-Social Trends in Social Media: The Phenomena of Cyber Bullying and Cyber Stalking'. [2022] (20) (47) *Global Media Journal.* https://www.globalmediajournal.com/open-access/disturbing-psychosocial-trends-in-social-media-the-phenomena-of-cyber-bullying-and-cyber-stalking.pdf accessed March 27, 2024.

[15] Philip N Ndubueze & Zakariyya Muhammad Sarki 'Cyberstalking Awareness and Perception among Undergraduate Students in Nigeria' [2017] (2) (2) *Duste Journal of Humanities and Social Sciences.* https://www.researchgate.net/publication/325103033_Cyberstalking_Awareness_and_Perception_among_Undergraduate_Students_in_Nigeria accessed March16, 2024.

[16] Anan Bijik Hassan, DI Funmi, and Julius Makinde, 'Cybercrime in Nigeria': Causes, Effects and the way out' [2012] (2) (7) *ARPN Journal of Science and Technology* in Oluremi Savage and Abiodun Ashiru, 'The Protection of Women against Cyberstalking and Cyberharassment in Nigeria, England and the United States: An Appraisal of the Legal Framework' [2021] https://www.researchgate.net/publication/350328200_The_Protection_of_Women_against_Cyberstalking_and_Cyber-Harassment_in_Nigeria_England_and_the_United_States_An_Appraisal_of_the_Legal_Frameworks accessed March 28, 2024.

mation to harass. Michael[17] asserts that cyberstalking is an evolution of traditional stalking, characterised by the stalker employing the internet to engage in harassment, threats, and disseminating distressing text and image content. For him, the significant difference between cyberstalking and offline stalking is that while one is done physically, the other is done using the internet.

There is a significant interrelationship between cyberstalking and offline Stalking, as cyberstalking is often accompanied by offline stalking. Bocij suggests that it is essential to develop a definition of cyberstalking that serves the needs of numerous stakeholders such as victims, law enforcement, internet service providers, researchers, etc.[18] He argues that although cyberstalking is related to offline stalking, it should be regarded as a new form of deviant activity. Sinwelski and Vinton provided a brilliant summary of stalking as follows:

> "Stalking behaviours range on a continuum of severity and intensity. They may begin with acts that, individually, may seem insignificant, such as repeated, unwanted contact in the form of telephone calls, beeper codes, email messages, or letters. If left unchecked, these contacts may escalate to unwanted physical contacts or the stalker's 'coincidental' appearance whenever the victim goes. Sometimes, the contacts are in the form of unwanted gifts, such as flowers or jewellery. At other times, stalkers spread false rumours about their victims to the victim's family members, friends, or employers or lie to frighten or coerce their victims."[19]

From the preceding, the authors suggest that stalking usually starts as acts that may appear trivial and harmless but may subsequently soar to unwanted physical contact or spreading rumours about the victim.

The history and criminalisation of stalking are tied to 'star stalking' that involves the fanatic quest of celebrities by psychologically unstable fans. The notoriety of stalking happened in the 1980s when it was perceived as the repeated imposition of unwanted communications or contact from the stalker to the victim.[20] Stalking patterns include repeated phone calls, sending gifts, letters or offensive materials, and loitering near/approaching the victim, the victim's friends, family members and co-workers.[21] Cyberstalking refers to "a process in which electronic communications, such as emails, instant messages, and any other form of electronic communications,

[17] Michael L. Pittaro, 'Cyber stalking: An Analysis of online harassment and Intimidation' [2007] (1) (2) *International Journal of Cyber Criminology* 180. https://www.ojp.gov/ncjrs/virtual-library/abstracts/cyber-stalking-analysis-online-harassment-and-intimidation accessed April 25 2024.

[18] Paul Bocij, *Cyberstalking: Harassment in the Internet Age and how to Protect your Family* (Greenwood Publishing Group). Victims want to be fully protected, law enforcement agencies want to catch and prosecute cyber stalkers, ISPs want to encourage their users on their safe services and researchers want to better understand the nature of cyberstalking.

[19] Shari A Sinwelski and Linda Vinton, 'Stalking: The Constant Threat of Violence' 2001 https://doi.org/10.1177/08861090122094136.

[20] Majid Yar, Cybercrime and Society, (London: Sage Publications Ltd 2013) 129.

[21] McGuire and Wraith cited in Yar, ibid.

contain psychologically threatening remarks that harass a recipient or cause victims to fear for their lives".[22]

Cyberstalking is an extension of offline/conventional stalking, where the critical difference lies in the utilization of the internet as a tool for engaging in harassment, threats, and the dissemination of fear-inducing messages and images.[23] Cyberstalking exhibits significant similarities to offline stalking, particularly in terms of the gender of the victim, the motivations of the stalker, the nature of the relationship between them, and their behaviours.[24] Both cyber stalkers and traditional stalkers are driven by an obsession with attaining power, control, and influence over their victims. However, a distinction between the two is that cyber stalkers possess computer skills and are adept at leveraging the internet. They may have knowledge about evading detection through techniques like maintaining anonymity by connecting through various internet service providers and creating multiple screen names. These tactics make it exceedingly difficult to trace the origin of emails and messages.

Cyberstalking behaviour encompasses several recurring traits, such as tracking the target's location, violating their data privacy, monitoring both online and offline activities, obsessively monitoring the victim's movements, and engaging in intimidating tactics. Additionally, social media stalking can involve actions like sending threatening private messages or fabricating manipulated images.[25] It can manifest in both direct and indirect forms.[26] In direct instances, perpetrators may contact their victims directly through emails, inundating their inboxes with messages. They may also harass them via instant messaging, voicemail, text messages, or other electronic communication methods. Utilising various technologies, they may engage in surveillance or follow their victims, often without their knowledge, frequently monitoring their online activities.[27] Cyberstalkers sometimes employ explicit, offensive,

[22] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (MA, USA: Anderson Publishing 2011) 133.

[23] Michael L. Pittaro, 'Cyber stalking: An Analysis of online harassment and Intimidation' [2007] (1) (2) *International Journal of Cyber Criminology* 180. https://www.ojp.gov/ncjrs/virtual-library/abstracts/cyber-stalking-analysis-online-harassment-and-intimidation accessed March 25 2024.

[24] Wei-Jung Chang 'Cyberstalking and Law Enforcement [2020] *Procedia Computer Science* https://www.researchgate.net/publication/346063813_Cyberstalking_and_Law_Enforcement accessed March 12 2024.

[25] Intellipatt 'What is Cyberstalking and how to protect yourself?' (2023) https://www.liebertpub.com/doi/10.1089/cyber.2020.0253 accessed March 27 2023.

[26] Rahul Awati. Cyberstalking (2023) https://www.techtarget.com/searchsecurity/definition/cyberstalking accessed March 17, 2023.

[27] In *People v Costales* 2d Crim.No B215915 (Court of Appeals of California, Second District, Division 6, 2010) in Oluremi Savage and Abiodun Ashiru, 'The Protection of Women against Cyberstalking and Cyberharassment in Nigeria, England and the United States: An Appraisal of the Legal Framework' [2021] https://www.researchgate.net/publication/350328200_The_Protection_of_Women_against_Cyberstalking_and_Cyber-Harassment_in_Nigeria_England_and_the_United_States_An_Appraisal_of_the_Legal_Frameworks accessed March 12 2024, the victim used an open profile to market her music, she received a large number of disturbing emails from a Michigan stranger; in *People v Coreleone* D052816 (Court of Appeals of Califonia, Fourth Appellant District, Division one, 2009), the perpetrator met the victim via an advertisement for "adult services" posted on Craigslist website; in *US v Sayer*, No. 2:11-CR-113-DBH (United States District Court, D. Maine, 2012), the harasser created a fake Facebook account for a former girlfriend, fictitious Internet advertisements and Social Media Profiles using the Victim's name and made postings purported to have originated from the victim, posting the victim's address and invitations to visit her for sexual encounters; in People and Rosa No F063748 (Court of Appeals of California,

or vulgar language, sending social media friend or follower requests or even outright threats. These actions can distress the victims, inducing fear for their safety and well-being. Additionally, cyberstalkers may expand their influence by targeting the victims' family members or friends.[28]

Alternatively, indirect cyberstalking occurs when the perpetrator's actions do not directly involve contacting the victim but still cause them anxiety or harm.[29] A good example are attacks that aim to damage the victim's device. This can be achieved by infecting it with ransomware, effectively locking its files and demanding a ransom for their release. Another method is the installation of viruses or keystroke loggers, which clandestinely monitor the victim's online behaviours and potentially steal data from their device. In addition, for indirect attacks, individuals responsible for cyberstalking may engage in harmful actions such as posting false or malicious information about their victims online.[30] This deliberate cyber-smearing act aims to tarnish their victims' social standing or professional reputation. Another strategy perpetrators' employ involves creating fraudulent social media or forum accounts using their victim's identity. Through impersonation, they can post content online on behalf of the victims, often with malicious intent.[31]

From the preceding definitions, it is evident that cyberstalking is interrelated with stalking. It frequently coincides with stalking that occurs in real-time or offline stalking. This study submits that apart from the general nature or mode of perpetrating these offences, cyberstalking preserves the anonymity of the perpetrator, who may use fake identities to attack their victims, making it challenging to track offenders. Cyberstalking is the dissemination of fear-inducing messages and images via technology or technological tools to cause the victim significant adverse outcomes such as anxiety, depression and social isolation.

2.1 Elements of the crime, cyberstalking

Cyberstalking refers to a pattern of behaviours and actions carried out over time with the intention of intimidating, alarming, frightening, or harassing the victim and their family, partner, and friends.[32] These actions include various methods such as overwhelming the victim's email inbox, frequently posting on their online platforms and social media accounts, repeatedly calling or texting them, leaving voicemails, send-

Fifth District, 2013), the perpetrator posted nude photographs of his ex-wife and an advertisement that she was willing to meet men for oral sex. In *Vrasie v Leibel* No 4D12-1289 (District Court of Appeal of Florida, Fourth District, 2013), the harasser sent offensive letters and the victim's nude to those on his contact list and created a website on victim's name to pre-sell her book and to post an excerpt that included defamatory statement s about him.

[28] Ibid.

[29] 'Cyberstalking and Cyberharassment', (2019), https://www.unodc.org/.

[30] In *US v Petrovic*, 701 F.3d 849 (2012), the perpetrator posted confidential pictures and information obtained from the victim during their relationship and shared pictures of the victim engaging in section activities to other people.

[31] ibid.

[32] United Nations Office on Drugs and Crime. University Module Series: Cybercrime https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html accessed March 26 2024.

ing follower and friend requests, joining the same online groups and communities as the victim, or monitoring their posts through acquaintances, colleagues, classmates, family members, or friends on social media.[33] Additionally, the perpetrators may continuously view the victim's online profile, with some websites notifying users when their page is accessed. These perpetrators can monitor and observe victims online and offline, sometimes without the victims' awareness. The behaviours and actions of cyber stalkers instil fear in the victims, making them concerned for their safety and well-being and, in some cases, the safety and well-being of their loved ones.

Generally, cyberstalking may be identified using three criteria: intent to harm, the power imbalance between the victim and perpetrators and the repetitive nature of the act.[34] Section 24 of the Cyber Crime (Prohibition, Prevention, etc.) Act, 2015 prohibits actions which amount to cyberstalking. The section provides thus:

> "Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that –
> (a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or
> (b) he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent:
> commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.
> (2) Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network
> (a) to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person;
> (b) containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; or
> (c) containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value:
> commits an offence."

Thus, to constitute this offence, the message must be grossly offensive, of an indecent, obscene or menacing character. It must be sent to cause annoyance, in-

[33] ibid.

[34] Timo Tapani Ojanen, Pimpawun Boonmongkon et al. 'Connections between Online Harassment and Offline Violence among Youth in Central Thailand' [2015] (44) *National Library of Medicine;National centre for Biotechnology Information.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4461520/.

convenience or needless anxiety to another.[35] Some other elements of cyberstalking include:

1. Knowledge and Intention: The intention to send an offensive, obscene, and unwanted message must be present.
2. Intimidation: Cyberstalkers engage in activities aimed at intimidating the victim. They may use various tactics to create fear, anxiety, and distress.
3. Persistence: Although one act may result in cyberstalking, it usually involves a persistent and prolonged pattern of behaviour. The perpetrator repeatedly and unwarrantedly contacts the victim through various digital channels, such as emails, direct messages, or comments, to cause distress or fear.[36]
4. Harassment: The purpose of cyberstalking is to harass the victim. This can take various forms such as sending threatening messages, posting derogatory comments, or spreading false information about the victim.
5. Invasion of Privacy: Cyber stalkers invade the victim's privacy by monitoring their online activities, accessing personal information, and infiltrating their digital space. They may gather information about the victim's daily life, routines, or personal relationships. They may also dox the victim.[37] Doxing is the act of publicly revealing or sharing private and personal information about the victim, such as their address, phone number, workplace, or financial details, without their consent.[38]
6. Online and Offline Targeting and Monitoring: Cyber stalkers may monitor the victim both online and offline. Cyber harassers specifically target individuals or groups online with the intention to intimidate, humiliate, or degrade them. They may track the victim's online presence, follow their social media accounts, and even physically observe their activities in real life.
7. Use of Multiple Platforms: Cyber stalkers utilise online platforms and technologies to target the victim. This can include email, social media, messaging apps, online forums, or any other digital platform where the victim is active.
8. Impact on Victims and their Relationships: Cyberstalking causes emotional distress and fear in victims. It can negatively affect their mental well-being, disrupt their daily lives, and strain their relationships with family, friends, and partners.[39]
9. Potential for Escalation: Cyberstalking has the potential to escalate into more serious forms of harassment or even physical harm. It is essential to address cyberstalking promptly to prevent further harm to the victim.
10. Offensive or Abusive Content: Cyber harassment often involves creating, disseminating, or sharing objectionable or abusive content. This can include hate speech, derogatory comments, threats, or explicit material.

[35] Muitanmi Olusola, Ogundere Samon et al., 'Cybercrimes and Cyber Laws in Nigeria' [2013] (2) (4) *The International Journal of Enginerring and Sciences,* 19.

[36] Gordon, (*n* 4).

[37] Sameer Hinduja, 'Doxing and cyberbullying'. https://cyberbullying.org/doxing-and-cyberbullying accessed March 18, 2024.

[38] The Cybersmile Foundation, 'Doxing' https://www.cybersmile.org/advice-help/doxing accessed March 28, 2024.

[39] Savage and Ashiru, (*n* 16).

11. Impersonation: Cyber harassers may impersonate the victim or create fake accounts in the victim's name, pretending to be them. This can lead to reputation damage, identity theft, or spreading false information.
12. Cyberbullying and online shaming: Cyberstalking often involves cyberbullying, where the perpetrator repeatedly targets an individual, using digital means to spread rumours, engage in social exclusion, or publicly shame the victim. Cyber harassers engage in public shaming of the victim, often by sharing embarrassing or private information about them to a broader audience, intending to cause social humiliation.

It is important to note that these elements may vary in different cyberstalking cases, and not all features may be present in every instance. In summary, Section 24 of the Cybercrime Act criminalises the sending of pornographic content, false, offensive and aggravating information, and cyberbullying, including stalking and insulting public/government officials online. However, the section does not define the key elements that constitute the crime of cyberstalking. The interpretation section of the Cybercrime Act does not specify the parameters or elements of cyberstalking for practical interpretation and implementation.

3 Section 24 of the cybercrime (prohibition, prevention, etc.) act of 2015 and the right of freedom of expression

The Economic Community of West African States Court of Justice (ECOWAS court) ordered the Federal Republic of Nigeria (FRN) to repeal or amend the Cybercrime Act to align with the obligation under Article 1 of the African Charter on Human and Peoples' Rights and the International Covenant on Civil and Political Rights (ACHPR). The court pronounced this in *Incorporated Trustees of Law and Rights Awareness Initiatives v Federal Republic of Nigeria (*ECOWAS case).[40] The applicant brought the action against the FRN for alleged violation of the fundamental human rights of freedom of expression of its members, associates and employees under the provisions of Articles 1 and 9 of the ACHPR[41] and 19 of the International Covenant on Civil and Political Rights (ICCPR)[42] due to the implementation of section 24 of the Cybercrime Act.

The applicant reiterated that section 24 of the Cybercrime Act limits freedom of expression on the internet or the use of any device and imposes fines and other penal sanctions. Since the enactment of the Act, the defendant had used it to intimidate the applicant, its members, associates and employees, thus violating their freedom of expression and digital rights on the internet and further violating their freedom of expression enshrined in the ACHPR as well as the defendant's obligation under the ECOWAS Revised Treaty. The applicant contended that as much as the Act

[40] Suit No ECW/CCJ/APP/53/2018.

[41] https://au.int/.

[42] United Nations (General Assembly), (1966). International Covenant on Civil and Political Rights, Treaty Series, 999. 171.

contained vague words such as "grossly offensive", it may give rise to arbitrary interpretation and application of the Act, making it a "low-quality law".

In deciding the issue before it, the court held that to avoid infringement of human rights, a law such as the Cybercrime Act should not be arbitrary but somewhat predictable, reasonable, and proportionate and pursue legitimate objectives. This is notwithstanding that the restrictions are established under the law, and the law must be formulated with enough precision. The court further stated that section 24 of the Cybercrime Act typifies criminal conduct, defines applicable sanctions, and must, in all its ramifications, be well written, legally and highlight its elements to avoid ambiguity. The court cited the Inter-American Court of Human Rights judgements in *Uson Ramires v Venezuela*[43] and *Khodorkovskiy and Lebedev v Russia*[44] as references.

The court concluded that when a law does not define the parameters or elements of the crime it prohibits, it cannot pass the test of legality since it will only lead to ambiguity. Thus, the expression "grossly offensive" used in the Act alone could be subject to varied interpretations. The court, however, took cognizance of the state's definition and prohibition of other conduct that qualified as a crime and held that the provision in question provided adequate information to individuals to adapt their conduct accordingly. It concluded that the section met the "law" requirement under Article 9 and the objectives pursued by the section were legitimate since they fell within the motives provided for in Article 19(3) of the ICCPR and 27(2) of the ACHPR and aim to safeguard due regard to the rights of others.

In determining the proportionality of the punishment and purported offence, the court stated that the provisions were not necessary for a democratic society, were disproportionate to the purported offence and violated the right to freedom of expression guaranteed under Article 9(2) of the ACHPR and 19 of the ICCPR. Article 9(2) of the ACHPR states, "Every individual shall have the right to express and disseminate his opinions within the law". Article 19 of the ICCPR provides that "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print, in the form of art, or through any other media of his choice".

The court espoused that penal defamation laws should include such defences as the defence of truth and should not be applied to those forms of expressions that are not by their nature subject to verification. States should, therefore, avoid excessively punitive measures and penalties. Finally, the court declared that by adopting the provisions of section 24 of the Cybercrime Act, the defendant State violated Articles 9 (2) of the ACHPR and 19 (3) of the ICCPR. The court ordered the defendant to repeal or amend section 24 of the Act following its obligations under these Articles.

It is submitted that section 24 of the Cybercrime Act does not align with the right to freedom of expression guaranteed under Article 9(2) of the ACHPR and 19 of the ICCPR because the section limits the right of individuals to express and disseminate

[43] (2009).

[44] Application no 11082/06/13772/05 Judgment (merits and just satisfaction), court (first section) 25/07/2013.

their opinions within the law. Additionally, the section's failure to define the parameters or elements of cyberstalking equates to failure of the legality test as it will only lead to ambiguity. The expressions such as "grossly offensive, menacing character, annoying, indecent, obscene", etc., were not clearly defined to convey the intended message of the law correctly, and this could be subject to varied interpretations.

A year after the ECOWAS case, the Court of Appeal in *Okedara v Attorney General of Federation*[45] held that the provisions of Section 24 of the Cybercrime Act are constitutional. The applicant, Solomon Okedara, filed an application before the Federal High Court (FHC) in Lagos, contesting the constitutionality of section 24(1) of the Cybercrime Act. He argued that the provisions of the Act were overbroad and vague and threatened his constitutional rights of freedom of expression and fair hearing protected in sections 29 and 36(12) of the 1999 Constitution of the Federal Republic of Nigeria (as amended) (the Constitution), respectively. The FHC, in dismissing the application, held that the restriction on freedom of expression as contained in section 24 of the Cybercrime Act was necessary in a democratic society as it relates to the interest of defence, public safety, public order, public morality or public health under Section 45 of the Constitution. The FHC found that the provisions of the section were explicit and, therefore, constitutional.

The applicant/appellant appealed the FHC decision at the Court of Appeal. The applicant/appellant put forward seven issues for determination, which are:

> "1. Whether the trial judge was right when he held that the offence contained in section 24(1) of the Cybercrime Act is quite clear and defined
> 2. Whether the learned trial judge was right when he held that section 24(1) of the Cybercrime Act does not in any way conflict with section 36(12) of the 1999 Constitution of the Federal Republic of Nigeria.
> 3. Whether the learned trial judge was right when he held that cybercrime is incapable of direct definition and dwelt on the same to determine the Appellant's case.
> 4. Whether the learned trial judge was right when he did not make a finding on the Appellant's issue as to the vagueness, ambiguity and over-breadth of section 24(1) of the Cybercrime Act but rather on issues not submitted for determination.
> 5. whether the vague and overbroad wording of section 24(1) of the Cybercrime Act, 2015 constitutes an interference to section 39 of the 1999 Constitution (as amended) and is inconsistent thereto.
> 6. Whether the learned trial judge was right when he held that section 24(1) of the Cybercrime Act is in the best interest of the generality of the public.
> 7. Whether the learned trial judge was right when he failed to rule on the issue as to whether provisions of section 24(1) of the Cybercrime Act are within the permissible restrictions stipulated in section 45 of the 1999 Constitution or whether section 45 of the 1999 Constitution can save section 24(1) of the Cybercrime Act."

[45] (2019) LCN/12768 (CA).

It is important to note that the right to freedom of expression is guaranteed under section 39 of the Constitution and cannot be derogated by legislation except to preserve the interest of defence, public safety, public order, public morality, and public health or to protect the rights and freedom of other persons. Section 45(1) of the Constitution provides thus:

> "(1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society.
> (a) In the interest of defence, public safety, public order, public morality or public health; or
> (b) For the purpose of protecting the rights and freedom of other persons."

After reviewing the issues for determination of both parties, the court streamlined it to one issue: whether section 24(1) of the Cybercrime Act was unconstitutional or not. The court relied on the constitutionality test developed by Nigerian courts over time to ascertain that "When an Act of Congress is appropriately challenged in the courts as not conforming to the constitutional mandate, the judicial branch of government has only one duty: to lay the article of the constitution which is invoked beside the statute which is challenged and to decide whether the latter squares with the former...". The court laid down the provisions of section 24(1) of the Cybercrime Act, sections 36(12) and 39 of the Constitution.

In its findings, the court stressed that the offence specified in the section is clearly defined, and the punishment prescribed is clearly stated. Although the court recognized the freedom of expression covered in section 39 of the Constitution, it reiterated that the right provided in section 39 is not open-ended or an absolute right and, therefore, subject to some restrictions by the provisions of section 45 of the Constitution. In dismissing the appeal, the court held that the limitation on freedom of expression provided in section 24(1) of the Cybercrime Act was necessary to protect public safety, public order, public morality, etc., under the Constitution. The court concluded that the provisions of section 24(1) of the Cybercrime Act do not conflict with sections 36(12) and 39 of the Constitution and, therefore, upholding its constitutionality.

Although, regional court judgments are not binding on national courts. The decision of the ECOWAS case would have served as a persuasive authority on the Court of Appeal's decision in *Okedara v Attorney General of Federation.* It is submitted that the legitimacy of the restriction posed by the provisions of Section 24 of the Cybercrime Act will be deemed constitutional only if it is reasonably justified in a democratic society. How does one determine what is reasonably justified in a democratic society? It has been argued that the answer to this question is the people, but the people need free speech to exchange their ideas and decide on a standard.[46] In other words, free speech drives the exchange of ideas, beliefs, opinions, standards, etc., to meaningfully participate in a democratic State. The provisions of section 24(1) of the Cybercrime Act did not clearly define the offence of cyberstalking. The vagueness and choice of words such as "grossly offensive,

[46] Ekojoka Aghedo, 'Interpreting 'Reasonably Justifiable in a Democratic Society': A Protective Standard for Free Speech in Nigeria', https://www.ajol.info accessed March 26, 2024.

menacing character, annoying, indecent, obscene", etcetera adopted by the section may lead to ambiguity, thus defeating the purpose of the legislation.

3.1 Section 24 of the Cybercrime (Prohibition, Prevention, Etc.) Act of 2024 and the Right of Freedom of Expression

The provisions of Section 24(1) of the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 was amended in February 2024 by the Nigerian government by substituting paragraphs "(a)" and "(b)". The amended provision provides thus:

> "Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that –
>
> (a) is pornographic; or
> (b) He knows to be false, for the purpose of causing a breakdown of law and order, posing a threat to life, or causing such message to be sent."[47]

The amended provision limits the scope of the offence of cyberstalking to messages that are pornographic, false, likely to lead to a breakdown of law and order or threatening to life. Thus, to constitute the offence of cyberstalking under the amended Act, the sender of the message must have the knowledge that the message is false and the intention to cause a breakdown of law and order or posing a threat to life. The amended provision is an improvement to the amended provision of section 24 of the Principal Act. However, the elements of "for the purpose of causing a breakdown of law and order" can still lead to ambiguity. The parameters of the element were not clearly defined. The words "for the purpose of causing a breakdown of law and order" is susceptible to more than one meaning and open to subjective interpretations. Ambiguity in a legislation arises from imprecise and vague language with unclear legislative intent that requires judicial interpretation to resolve the ambiguity.

The phrase "for the purpose of causing a breakdown of law and order" does not provide clear parameters on the scale and degree of "breakdown" that would prompt the application of the provision. Although, the amended provisions of section 24 of the Amended Act is narrower than the Principal Act, some elements of the provision are unclear and can pose a threat to freedom of expression and media freedom. This study, therefore, proposes the further reform of this section to properly define the generic words "for the purpose of causing a breakdown of law and order", to properly convey the intended message since the clarity of legislation is an enabling force for enforcement.

4 Better protection for victims of cyber stalking in Nigeria

Victims of cyberstalking suffer severe harm, such as mental health issues, long-term psychological trauma, stigmatisation, depression, low self-esteem, job loss,

[47] Cybercrime (Prohibition, Prevention, Etc.) Act of 2024.

fear and suicide. In Nigeria, the Cybercrime Act makes express provisions that criminalise all forms of cyberstalking. In determining cyberstalking cases, the judge may grant a restraining order against the defendant to protect the victim from further harassment.[48] One noteworthy provision is the court's authority under Section 24(3) of the Cybercrime Act to prevent further harassment. Section 24(3) of the Act provides that the court may, while sentencing, grant orders that may prevent further actions that may harass or cause reasonable apprehension in the victim.

A careful examination of the Cybercrime Act reveals that lawmakers are aware of the current risks associated with technology. This means the court can issue a restraining order forbidding the offender from contacting the victim. The law grants the court the power to impose a hefty fine of ten million naira or a prison sentence of up to three years on an offender who violates a court order prohibiting harassing behaviour or other specified conduct. Furthermore, subsection (6) states that the court can issue interim orders to safeguard the victim from the alleged crimes.

While these provisions are undoubtedly a step in the right direction, more must be done to relieve victims of these crimes. Nigerian criminal laws primarily focus on serving as deterrents or prescribing punishments for convicted offenders, with little consideration given to the interests of the victims. The lack of compensation and protection for victims has discouraged many from reporting cybercrimes such as cyberstalking. This study provides the following recommendations:

1. *Review and further amendment of section 24(1) of the Cybercrime Act to align with the constitutional rights of Nigerian citizens*. The first step to protecting victims of cyberstalking is the existence of a well drafted and effective legislation devoid of implementation gaps. The cyberstalking provision can be narrowly tailored to prohibit the offence of cyberstalking without infringing on the fundamental right of freedom of expression. It is important to balance the protection of individuals from cyberstalking incidents while recognizing the inalienable right of legitimate free speech
2. *Establishment of cyberstalking protection and support centres*: The government should establish multiple cyberstalking protection and support centres in the country where victims of cyberstalking who feel threatened for their lives and security can reside and report the incidents to the appropriate law enforcement body. These centres should work with law enforcement agencies and regulatory bodies to investigate and prosecute cyberstalking incidents respectively.
3. *Training/sensitizing law enforcement agents investigating cyberstalking cases to gain the victim's trust is crucial*. Law enforcement agents should receive periodic trainings on the intricacies, peculiarities and the dynamics of cyberstalking investigation. Owing to the sensitive nature of some cyberstalking cases, invasive requests for sensitive details of the cyberstalking incidents should be asked when the victim is ready to share with law enforcement.
4. Internet service providers and data controllers can redact obscene materials of cyberstalking victims.

[48] Section 23 (3).

5. *Establishment of cyberstalking counselling services with experts specializing in counselling victims of cyberstalking*.
6. *Establishing cyberstalking support hotlines where victims can report cyberstalking incidents*. Cyberstalking victims should be encouraged to document and preserve all the cyberstalking incidents and the medium of online and offline communication, which can be used as evidence in prosecuting the cyber stalker.

5 Conclusion

The contentious provision of section 24 of the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 has been a subject of academic discourse. This paper investigates the constitutionality of Section 24 of the Principal and Amended Act which criminalises cyberstalking in Nigeria. It found that although the Amended Act narrows the offence of cyberstalking, concerns regarding subjectivity of interpretation and violation of free speech still exist. The phrase "for the purpose of causing a breakdown of law and order" is vague, ambiguous and susceptible to subjective interpretations. This study found that the vagueness and choice of words adopted in the amended section 24(1) of the Act may lead to ambiguity, thus defeating the purpose of the legislation. It therefore proposes the further amendment of this section to properly define the generic words "for the purpose of causing a breakdown of law and order", to convey the intended message of the law correctly. The cyberstalking provision can be narrowly tailored to prohibit the offence of cyberstalking without hampering on the fundamental right of freedom of expression. It is important to balance the protection of individuals from cyberstalking incidents while recognizing the inalienable right of legitimate free speech. This paper canvasses for better protection for victims of cyberstalking in Nigeria.