Cybercrime and Cybersecurity: An Appraisal of Gender Based Offences

Kelvin Bribena PhD

Faculty of Law, Niger Delta University
Wilberforce Island, Bayelsa State, Nigeria.

Abstract

Despite the advancement and development of society, crime is nonetheless pervasive and destructive. As technology and crime detection techniques advance, criminals also come up with new strategies to circumvent these systems. Internet Service Providers (ISPs) and access points have significantly increased in Nigeria as a result of the country's rapidly growing internet usage, which has benefited the socioeconomic and educational development of the nation. Although cyberspace provides women with safe spaces for private communication, information access, and freedom of expression, the same anonymity and privacy also allow those who abuse information and communication technology (ICT) to commit crimes, including violence against women. By including cyber-based abuse and emphasising the difficulties women encounter in addressing this changing manifestation of gender inequality, this work explored new analytical viewpoints on violence against women. In order to ensure thorough analysis, the study used doctrinal research strategy, that is, consulting primary and secondary legal sources, including legislation, official statistics, treaties, conventions, protocols, court rulings, and declassified government papers. The results showed that violence against women is still pervasive, that women continue to face obstacles as workers and business owners, and that in many communities, women do not participate equally in household, community, workplace, and national decision-making. As a result, the study suggested that individuals in charge of digital content creation, technology infrastructure, and the larger enabling environment of cyberspace should make protecting the safety and dignity of women and girls a top priority. Ignoring this obligation compromises the internet's ability to promote women's empowerment and gender equality. In order to guarantee proper protection and efficient remedies, the study also underpinned the necessity of comprehensive criminal law that specifically targets the many types of online violence against women.

Keywords: Cybercrime, cybersecurity, violence, women, gender-based, internet, charter, Convention.

Introduction

One of the most pervasive human rights violations is still violence against women and girls. Numerous women worldwide suffer from gender-based violence in online environments, especially on social media sites. Such mistreatment has occasionally resulted in fatalities, severe health issues, and drawn-out court cases.

Millions of women and girls around the world are specifically targeted because of gender-related vulnerabilities. Beyond national borders, racial, cultural, and social divides, violence against women and girls (VAWG) causes severe harm to victims as well as to their families, communities, and society at large.[1]

There are now more options to fight VAWG due to the growing usage of the internet and the quick development of information and communication technologies (ICTs), and the broad use of social media. [2]At the same time, these technologies are being used more and more as abusive tools. Cybercrime has grown to be a major worldwide issue and a relatively recent but significant worry in Africa, with far-reaching effects on both social stability and economic growth. Growing numbers pose a threat to international peace and prosperity, as well as the fulfilment of rights guaranteed by the UN Charter, especially the goal of inclusive and sustainable development that places a high priority on women's empowerment and gender equality. This work examines the connection between cybercrime and gender-based violence, takes into account the rising frequency of these crimes, suggests solutions to lessen their occurrence, and describes how women and girls can better defend themselves against these ubiquitous dangers.

Cyber Crime

One of the most pervasive human rights violations in the world is violence against women and girls.[3] Many women worldwide have been victims of gender-based abuse in cyberspace, especially on social media sites. In certain cases, these abuses have resulted in death, major health issues, and protracted legal disputes. Beyond national borders, racial, cultural, and socioeconomic divides, violence against women and girls (VAWG) causes severe harm to victims as well as to their families, communities, and society at large.[4]

The extensive use of social media, the quick development of mobile information and communication technologies (ICTs),[5] and the internet's growing reach have all opened up new avenues for creative solutions to VAWG. Simultaneously, these technologies are being used more frequently to harm women and girls. With far-reaching effects on social stability and economic

---

[1] United Nations Secretary General's Campaign to End Violence Against Women.
<http://www.who.int/mediacentre/factsheets/fs239/en/,http://www.un.org/en/women/endviolence/index.Shtm>1; and
<http://www.un.org/en/women/endviolence/factsheets.shtml> accessed 4 February 2024.
[2]Reports of the Broadband Commission http://www.broadbandcommission.org/resources/Pages/default.aspx>accessed 6 February 2024.
[3] Flavia Fascendini, "Small Thoughts Around Cybercrime and Legislation and gender" Gender centered thematic bulletin, 11.
<http://www.genderit.org/newsletter/cybercrime-legislations-and-gender>accessed 10 February 2024
[4] Ibid 11
[5] The Convention on Cybercrime also known as the Budapest Convention on Cybercrime 1877.
nations6gb.http://www.coe.int/en/web/conventions/treaty/185 accessed on 7 February 2024.

development, cybercrime has become a major worldwide concern and a relatively new but rapidly expanding phenomena in Africa.[6]

Global peace and prosperity, as well as the realization of rights enshrined in the UN Charter—particularly the pursuit of inclusive and sustainable development, which places a premium on gender equality and women's empowerment—are all at risk due to current trends and statistics.[7]

Because cybercrime is becoming more common, this paper investigates the connection between it and gender-based violence. It also suggests ways to lessen their frequency and provides information on steps that women and girls can take to protect themselves from these ongoing online dangers.[8]

Gender Based Violence

Information and communication technologies (ICTs) have significantly reduced gender gaps, but they have also made them worse by enabling cybercriminals to use these platforms in ways that violate women's rights. The safety and privacy of digital communication spaces are increasingly threatened by cybercrime, which limits women's capacity to use ICTs for development and empowerment with confidence due to increased security concerns.[9]

Acts of violence against women because of their social disadvantage are referred to as gender-based violence (GBV). It includes any threat or action that harms women and girls physically, sexually, or psychologically because of their gender, frequently committed by men or male-dominated institutions. Such violence is justified and maintained in many countries by cultural values, social conventions, and established institutions. GBV can take many different forms, such as physical, sexual, and psychological abuse like domestic violence; sexual assault, including rape and incest; forced pregnancy; sexual slavery; and damaging customs like acid attacks, female genital mutilation, and abuse related to dowries. Along with emotional abuse through compulsion, intimidation, and demeaning language,[10] it also encompasses brutality during military confrontations, such as rape and murder. Other instances include forced marriage, sexual harassment, workplace intimidation, and the trafficking of women and girls for prostitution.

Both the public and private domains are affected by gender-based violence. In addition to occurring inside the family or the larger community, it can also be sustained by the state through discriminatory laws or the acts of state representatives like the military, immigration officials, or the police. Every society and social class experiences GBV, with women most frequently at

---

[6] Kristen v. Brown, United Nations Report on Cyber Violence against women has set off another battle over free speech online' (30 May 2015) <http://fusion.net/story/206207/u-n-cyber-harassment-against-women> accessed 30 February 2024

[7] Flavia Fascendini, (n 3) 111

[8] *Ibid*, Kari, Kabance 'The Globalization of Sex Trafficking (2014) P.34.https://ucollege.wustl.edu/files/ucollege/imce/iap.kabance.drp_.pdf> accessed 12 February 2024.

[9] A Report of Women and Cybercrime the dark side of ICT April 2011, <http://www.internetsociety.org/women-cybercrime-kenya-dark-side-icts> accessed 7 February 2024.

[10] Defining Gender-Based Violence, Gender-based violence (GBV) or violence against women (VAW)? <http://www.genderit.org/en/index.shtml?apc=r90501-e96137-1> accessed 10 February 2024.

danger from men they know.[11] During times of war and conflict, organized targeting of women and girls is also a common tactic.[12]

Prior to roughly forty years ago, sexual harassment and domestic abuse were primarily considered personal issues rather than societal issues. However, these types of violence have changed recently and are now present in digital environments, where women are the targets of online harassment, cyberstalking, and voyeurism. Civil rights advocates fought to have these problems acknowledged as significant social issues in the 1970s and 1980s. Violence against women was not initially covered under the 1979 United Nations Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), the first significant international convention on women's rights; however, this gap was filled in 1992.[13] General Recommendation No. 19, which was then accepted by the CEDAW Committee, made it clear that gender-based violence is a type of discrimination against women and is thus covered by the Convention.[14] GBV was defined as violence against women because of their gender or violence that disproportionately impacts them, highlighting the fact that these acts are not random but rather stem from gender inequality. Furthermore, the recommendation acknowledged that GBV encompasses acts that result in physical, mental, or sexual harm in addition to threats, coercion, and limitations on personal freedom. It also confirmed that such violence is a violation of fundamental human rights, such as the right to life, equality before the law, equality within the family, and the best possible standard of physical and mental health.[15]

Similar to this, violence against women is defined by the United Nations Declaration on the Elimination of Violence Against Women (DEVAW) as a violation of women's human rights and the outcome of uneven power relations between men and women.[16] Even though the UN officially recognized the problem in the early 1990s, more than 20 years later, there hasn't been enough improvement. Large sums of money and concerted efforts from all facets of society— governments, non-governmental organizations, legislators, law enforcement, social service providers, educators, the media, trade unions, international organizations, donors, and the

---

[11] Kristen v. Brown, United Nations Report on Cyber Violence against women has set off another battle over free speech online 'Supra

[12] Http://womensenews.org/story/war/110619/gadhafi-said-order-forces-rape-villagers> accessed 2 February 2024

[13] CEDAW General Recommendation No. 19 on VAW,1992). <http://www.healthgenderviolence.org/sites/default/files/download/m2_handout_cedaw_rev2013_1.pdf> accessed 11 February 2024.

[14] Citron, Danielle Keats. (2009). "Law's expressive value in combating cyber gender harassment" Michigan Law Review, Vol. 108:253. 14 October 2009. <http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgiarticle=1687&context=fac_pub> accessed 24 February 2024

[15] No. 19 on VAW (GR 19) http <://www.healthgenderviolence.org/sites/default/files/download/m2_handou t_cedaw_rev2013_1.pdf>accessed 9 February 2024.

[16] Ibid

international internet community[17]—are still needed to prevent violence against women and guarantee effective protection, redress, and support services.[18]

Cyber Crime and Gender Based Violence

Due to their increased susceptibility, women and girls are disproportionately affected by internet crimes. A sizable fraction of these acts are classified as romantic scams. A romance scam is a type of fraud in which the perpetrator claims to have sincere romantic intentions, establishes emotional trust with the victim, and then takes advantage of that confidence to commit fraud. Gaining access to the victim's financial resources, bank accounts, credit cards, passports, email accounts, or national identifying information, or forcing victims to commit financial crimes on the perpetrator's behalf, are examples of such fraudulent acts.[19]

Beyond concerns about gender disparity, internet crimes like fraud, data privacy violations, partner-seeking schemes, and hate speech that is sexist have become more common. Women's ability to utilise the internet as a tool for empowerment and personal or socioeconomic growth is limited by these new types of cybercrime, which threaten formerly protected venues.[20] This change is important because, whereas violence against women was formerly thought of in terms of physical acts like rape or battery, it is now more frequently seen in digital contexts.

Crucially, discrimination and gender inequality continue to be major causes of violence against women. These are influenced by long-standing structural and historical power disparities between men and women, which continue to exist to varied degrees in countries all over the world.

Six major categories can be used to classify cyberviolence against women and girls:[21]

1. Hacking is the use of technology to achieve unauthorised or illegal access to data or systems, usually in order to change content, obtain personal information, or disparage the victim or organisations that combat violence against women and girls. Password breaches and taking over a victim's computer's operations, including freezing the machine or forcing the user to log out, are two examples.[22]

2. Impersonation is the practice of using digital resources to pretend to be someone else in order to get private information, embarrass or shame the victim, make unwelcome contact, or provide false identification. To get around blocking, this can entail making anonymous calls or sending offensive emails from the victim's account.[23]

---

[17] CEDAW General Recommendation No. 19 (Article 2).

[18] See preamble to DEVAW. Article 3 lists examples of these rights, such as the right to life, the right to equality, the right to the highest standard attainable of physical and mental health, or the right not to be subjected to torture, or other inhuman or degrading treatment or punishment. (Source: 1993 UN Declaration on the Elimination of Violence Against Women).

[19] 19 Romans Scams, Action Fraud <http://www.actionfraud.police.uk/fraud-az-romance-scams>, accessed 13 February 2024.

[20] *Ibid*

[21] VAW Learning Network. (2013)
 <http://www.learningtoendabuse,ca/sites/default/files/Baker_Campbell_Bar   reto_Categories_Technology-Related_VAW_.pdf> accessed 1 February 2024.

[22] Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call, A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender, 2015.

[23] Ibid

3. The use of technology to track or observe a victim's actions and behaviour, either in real time or after the fact, is known as surveillance or tracking. Examples include keyboard logging to recreate a survivor's computer activities or GPS tracking via mobile devices.[24]

4. The persistent use of digital communication to threaten, harass, terrify, or annoy a victim is known as harassment or spamming. This entails recurring behaviours as opposed to one-off occurrences, including bombarding voicemail systems to stop other contacts or making unending calls or texts.

5. Recruitment: The use of technology to lure people into abusive or dangerous circumstances. This might happen as a result of false employment offers, phoney dating profiles, or misleading internet ads. Traffickers can also use websites, chat rooms, and message boards to find and recruit victims.

6. The alteration and distribution of harmful, illegal, or defamatory content about the victim or organizations that address violence against women and girls is known as malicious distribution. Examples include the use of internet media to normalise or encourage violence against women, as well as threats to leak or the actual publication of private photos or recordings. [25]

Additionally, as online abuse has become more common, several terms related to cyber violence against women and girls have emerged, such as sexting and revenge pornography.[26]

The act of posting a person's private photos or videos online without that person's permission with the goal of degrading, shaming, or seriously harming the victim's offline life—for example, by causing them to lose their job or social standing—is known as revenge pornography. Another name for this practice is non-consensual pornography. Sexting, which is the exchange of sexually graphic or naked photographs, usually over text messages, is closely connected.[27] Drawing on long-standing social conventions surrounding heterosexual relationships, male entitlement, and standards of female beauty, sexting is frequently influenced by gendered expectations that put pressure on females to give nude photographs. Notably, girls who engage in sexting typically experience more severe social repercussions, and photographs of them are more likely to be shared outside of the intended receiver.[28]

Because of the anonymity provided by the internet, pimps and exploiters have also been able to get around laws that prohibit sexual exploitation and violence, especially in places with lax or nonexistent regulations.[29] The exploitation and abuse of women in the industry have not decreased, despite the fact that the mainstreaming of pornography was once presented as a way to

---

[24] Ibid

[25] *Ibid*

[26] Revenge Porn: The Facts A new criminal offence to tackle Revenge Porn is being introduced in England & Wales as part of the Criminal Justice Courts Bill

[27] Revenge Porn: The Facts, a new criminal offence to tackle Revenge Porn is being introduced in England & Wales as part of the Criminal Justice Courts Bill. ibid

[28] Sexting, Online and Mobile Safety.
 <https://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx>assessed 12 February 2024.

[29] Ibid

empower performers and acknowledge their rights. Conversely, as websites depend more and more on extreme and graphic content to draw viewers, increased competition among online platforms has resulted in a steady increase in violent and misogynistic content. The sheer amount and accessibility of such content—an ordinary internet user can now come across more violent and demeaning content in a matter of minutes than they might have in a lifetime just fifteen years ago—is what sets the present landscape apart.

On the other hand, the anonymity of the internet can also be used to reveal and stop cyberviolence against girls and women. Due to the availability of inexpensive performers from Eastern and Central Europe, a number of American and European pornographic producers have moved their operations to locations like Budapest, Hungary, throughout the previous ten years. In addition to being a destination and transit route for women trafficked from nations including Ukraine, Moldova, Russia, Romania, and the former Yugoslavia, Budapest has surpassed more established hubs like Amsterdam and Copenhagen to become Europe's largest centre for the production of pornography. Authorities discovered an online marketplace in 2014 that linked traffickers and potential buyers through a number of websites, forums, and about 30 groups on a significant Chinese messaging app. Up to 200,000 boys and girls are reportedly kidnapped and sold online each year in China.[30]

Because the type and severity of violence women endure is strongly correlated with their gender, cybercrime impacts them in fundamentally different ways than it does males. Women are more commonly the targets of sexualized insults and character attacks than men, who may be accused of corruption or misbehaviour. Because of this, women are disproportionately harmed by online harassment, and many of them decide to completely avoid digital environments. While only a tiny percentage are able to withstand the abuse and continue to be active online, this retreat can have a substantial impact on their professions and social engagement.

It is crucial to remember that strategies like threats, intimidation, and the improper use of private data are not brand-new in the context of domestic abuse. But the use of technology has increased the intrusiveness, persistence, and psychological damage of this kind of abuse. One in five women in developing nations believe the internet is an unsafe or inappropriate place for them, and one in three women worldwide will encounter violence at some point in their lives, according to a BBC investigation. According to the findings, women between the ages of 18 and 24 are disproportionately affected by serious kinds of online harassment: 25% have been the victim of online sexual harassment, and 26% have been the victim of online stalking.[31]

---

[30] Ibid

[31][31] 23.3 per cent of women in an online survey reported being blamed for the violence done to them. One woman writes, "Most people blamed me for the abuse saying I deserved it. Others ignored it", and another responded, "no help no support at all. I was told that being online is a risk and if I'm being harassed it's my own fault.

When it comes to responding to cyberviolence, a sizable percentage of female victims decide not to report instances. About 65% of people choose not to disclose because they are afraid of social rejection or negative consequences.[32] Of those who do react, 22% report the incident to the appropriate website or online service provider, 47% confront the offender online, 44% block the offender, and only 5% escalate the situation to law enforcement.[33]

It is therefore important to note that, cyber violence against women cuts across all ages. It is not limited to a certain age of women.

Recommendation

It is advised that criminal laws should specifically address all types of cyber violence against women in order to provide victims with adequate protection and access to the legal system. However, legal provisions are not enough on their own. Sustained education, the creation of efficient coping and protection strategies, and an adaptable judicial system that can handle cyberviolence without subjecting victims to more harm or secondary victimization are all necessary.

Policymakers and gender and development activists must carefully weigh privacy and information security considerations when assessing cybercrime laws. On the one hand, information and communication technologies (ICTs) have made it possible to challenge inequality by using online communities and collective movements to raise awareness of situations that were previously thought to be private, such sex trafficking and domestic abuse. However, by giving hackers the ability to illegally access, alter, and use personal data to target vulnerable groups, these same technologies can exacerbate already-existing disparities. The nature of the internet and cybercrime must be critically examined, especially in light of their consequences for social justice and human rights, as ICTs rapidly blur the lines between private and public life.

Therefore, in addition to utilizing ICTs to restructure power relations in ways that advance equality, legal frameworks should explicitly establish the criteria governing access to, use of, and engagement with ICTs. In order to increase public awareness, encourage thoughtful discussion, and guarantee that online violence against women stays firmly on the public and policy agendas, this strategy should be supplemented by cooperation with the media.

Conclusion

Women continue to face major obstacles as employees and business owners, and violence against them is still widespread. They continue to have unequal access to and influence over national, workplace, community, and family decision-making processes in many nations. For individuals in charge of producing digital material, maintaining technical infrastructures, and influencing the larger digital ecosystem, protecting the safety, security, and dignity of women and girls must thus be their top priority. If these obligations are not met, the internet's ability to promote gender equality and women's empowerment could be jeopardized.

---

[32] West, Jessica (2014) <http://www.bwss.org/wp content/uploads/2014/05/CyberVAWReportJessicaWest.pdf> accessed 20 February 2024.

[33] According to Cambridge dictionary, A man who controls prostitutes especially by finding customers for them, and takes some of the money that they earn. <http//: www. Dictionary, cambridge.org> accessed 10 February 2024, see also Merriam -Webster's Learners Dictionary: A criminal who exerts control over, and lives off the earnings of one or more prostitutes" <www.merriam-webstar.com> accessed 10 February 2024.

The need for strong legal, social, and normative controls on online attitudes and illegal behaviour is becoming more and more apparent as internet access continues to spread throughout the world. Concerns about the conflict between protecting internet users' privacy and protection and preserving freedom of expression continue to exist. For the internet to become a safe, respectful, and empowering space—not just for women and girls, but eventually for all users, including boys and men—effective oversight and rigorous enforcement of laws that forbid cyber violence against women and girls are essential.