Policy Brief

MINDING THE GAPS: IDENTIFYING STRATEGIES TO ADDRESS GENDER-BASED CYBER VIOLENCE IN KENYA

The main objective of this policy brief is to call attention to emerging trends in gender based cyber violence in Kenya and to start discussions on strategies to address the same. This paper recognizes the wide array of issues related to cyber-violence in Kenya and globally and does not present itself as a full compilation of those issues or of proposed solutions.

Issue

Violence against women and girls is one of the most rampant human rights violations. This violence knows no boundaries, and cuts across borders, race, culture and income groups, profoundly harming victims, people around them, and society as a whole.

The growing reach of the internet, the rapid spread of mobile information and communications technologies and the wide diffusion of social media have presented new opportunities and enabled various efforts to address violence against women and girls. However, these same technologies are also increasingly being used to expose women and girls to new and emerging threats. Cyber-violence against women and girls is emerging as a global problem with serious implications for societies and economies around the world. The statistics pose risks to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement. The research that fed this policy brief explored the understanding that Kenyans have towards Gender Based Cyber Violence and focused on identifying promising strategies for preventing and combating the same.

Background to the Research

Gender based Cyber Violence is a problem of pandemic proportions. Research asserts [1]that one in three women will have experienced a form of violence in her lifetime. Cyber Violence against Women and Girls could significantly increase this staggering number, as reports suggest that 57% of Americans experiencing harassment online are women.[2] In Europe, [3]nine million girls have already experienced some kind of cyber violence by the time they are 15. Despite the ubiquity of this problem, in many countries, women are often reluctant to report their victimization for fear of social repercussions[3]. According to new research by the Web Foundation, young people are most likely to have suffered harassment online, with over 6 in 10 poor urban women and men in developing countries aged 18 – 24 who use the Internet saying they had suffered online abuse. Cyber violence is just as damaging to women as physical violence, according to a new U.N. report dubbed the "wake-up call", which warns that women are growing even more vulnerable to cyber violence as more and more regions gain internet access.

The report estimates that 73% of women have endured cyber violence, and that women are 27 times more likely than men to be harassed online. While fewer women than men access the Internet today, Intel's 2013 report, Women and the Web, estimates that 450 million new female Internet users could come online within the next three years. Given the ubiquity of the Internet and its wide-ranging impact, particularly on the younger generation, it becomes imperative to ensure it is a safe place for both current and future generations.

The Extent of the Problem in Kenya

According to the Kenya National Bureau of Statistics, mobile telephone subscriptions in Kenya stand at 33.6 million. As of 2014, the estimated internet users stood at 26.2 million users. This large number is due to the reduction in data bundle prices and availability of affordable internet enabled telephones in the country.

According to a survey conducted by the Google Consumer Barometer, 89 percent of people located within Kenya go online to visit social networks, which include the likes of Facebook, Twitter, as well as Instagram. In addition, 81 percent of users utilize the internet in order to check e-mail as well as access instant messenger services. The growing use of the Internet and other technologies in Kenya and across the world today suggests that cyber violence is likely to become an increasing problem.

In the recent past, Kenya has witnessed gender based attacks on the cyber space platform, including social media. Some of it has resulted in death, health challenges and court cases. Women across the board have been affected, ranging from senior government officials, politicians, media and entertainment personalities, and students, among others.

Recent research by the African Development Bank related to the incidence of gender based cyber violence in Kenya has found:

• There are a wide range of perspectives on what constitutes gender based cyber violence. Young women spoke about how cyber violence unfolds in their everyday lives, expressing their views about a wide range of experiences, from personal hate speech to revenge porn to online intimidation. A majority of the respondents understood gender based cyber violence to refer to misogynist comments posted on one's social media profiles. More than half of the respondents referred it to mean posting of someone else's pictures online without their consent and also soliciting for sexual favors online.

• More than a third of the respondents interviewed indicated that they had experienced harassment online. Another third had been contacted by imposters online, experienced personal hate speech, cyber bullying and trolling while online. The majority of these victims are women, and the repercussions can be severe. 7% of the respondents had experienced revenge porn whereby explicit images (taken with or without consent) are distributed without consent. It is clear that pervasive online misogyny and harassment of women is too often normalized. The perceived (often wrongly) anonymity of online posting and evolving cyber norms that suggest that

misogyny that is unacceptable offline is somehow more OK online may together contribute to the proliferation and acceptance of gender-based cyber violence.

• Of those that had experienced some form of cyber violence, a majority proceeded to block the aggressor from the social media platform. A quarter of the victims exited the platform and a further 23% went ahead to contact the owner of the platform to report the abuse. Very few people preferred to report the victimization to the police.

Cyber violence takes on various forms ranging from cyber stalking, defamation, email spoofing, cyber pornography, cyber morphing, harassment via emails, hacking, to trolling. Some of these can be prevented by creating awareness on how individuals can protect themselves when online.

Research was conducted to gauge how aware the respondents were of online safety tips and procedures.

Key findings were as follows:

• A majority of the respondents indicated that they avoided engaging with strangers online. However, only a few changed their social media passwords often. Most respondents used the same password for multiple site logins. This increases their security risk because if that password was hacked or exposed there would be nothing to stop the hacker/thief from trying it in other places.

• A majority of the respondents indicated that they did not read the policy guidelines, conditions and terms of networking websites before entering into contract with these sites. This hinders their ability to protect themselves and their privacy while online. In addition, few of the respondents read through the permissions they granted the applications installed on their phones. The problem is that users do not always understand why an app wants a specific permission and it can be difficult to distinguish between a valid reason and a suspicious request.

• Only a few of the respondents checked the publisher of their mobile phone applications before installing them. This increases their vulnerability to data mining, hacking and phishing or spam emails.

Users of the internet need to understand their roles and responsibilities in safeguarding their data while also reducing or eliminating their risk to cyber-attacks.

How does Cyber Violence impact victims?

A UN report indicates that gender-based cyber violence puts a premium on emotional bandwidth, personal and workplace time, financial resources and missed wages. The impacts of cyber-violence against women are psychological, social, physical and economic. The most prevalent are psychological impacts (e.g. anxiety, damaged self-image and to the most extreme, thoughts of suicide and engaging in self-harming behavior), which are felt by most women who experience cyber-violence.[4]

Policy Implications: A call to Action

Granted, it is challenging to govern gender-based cyber violence without treading on civil liberties such as freedom of expression. Moreover, the global nature of cyberspace makes it more difficult to develop a shared ideology or norms over what constitutes gender-based violence. The conversation over the governance of the Internet therefore remains fiercely debated on a global scale. However, action must be taken at the country and regional level to curb the growth of cyber violence especially against women and girls.

Cyber violence (e.g. cyberbullying, Internet luring and cyberstalking) is a complex problem that requires a nuanced and multi-pronged approach. There is a pressing need to involve girls and women in discussion with the wider community to define the problem, break down the institutional barriers that support it, and devise strategies to combat and eliminate it.

Globally, there has been action to reduce and prevent the occurrence of cyber violence. In the US, 48 states have laws against electronic harassment while 22 states have definitive laws about cyberbullying. In the UK, Europe and in South Africa, there are several laws about cyberbullying that can help protect an individual from being victimized. Although there is regulation on hacking and electronic fraud in Kenya, it is far from adequate. The Government of Kenya is yet to amend the statute books to legislate against cyber-bullying and its derivatives.

The research on gender based cyber violence in Kenya was devoted to identifying promising strategies for combating gender-based (cyber) violence in the country. These strategies may include (but are not limited to):

- Placing special emphasis on strong legislation to address and provide avenues of redress for cyber violence against women.

- Capacity building at the grass root level on what constitutes gender based cyber violence and how women can protect themselves from it.

- Creating awareness amongst law enforcement and the judiciary for better understanding of such kinds of victimization and quick responses towards the complaints.

- Creating digital spaces that are secure and empowering (e.g. working with digital industries).

- Exploring the use of digital social spaces as tools, taking advantage of their strengths and uniqueness to create positive interactive change (e.g. tackling issues related to online anonymity, victim blaming, cyber rights).

- Fostering knowledge-sharing and strengthening coordination among those working to prevent or eliminate cyber violence (e.g. police services, community agencies and educational institutions to better recognize and respond to cyber violence, promote data collection, and explore ways to facilitate the exchange of knowledge about cyber violence).

- Additionally, Kenya must embrace and join international cybercrime agreements that reach the regional and global level.

These steps will have the most immediate effect in curbing the growth of cybercrime in Kenya and Africa.

Conclusion

The potential for using technology to facilitate positive change cannot be overstated and, within Kenya and Africa as a whole, women have harnessed technology for various positive purposes. Yet, at the same time, the victimization of women within a sphere that is increasingly important and ungoverned, makes it a cause for concern. Balancing these two integral values therefore needs to become a national imperative.

Contact

Gloria Muhoro g.muhoro@afdb.org

References

1. http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures
2. http://www.onlineharassmentdata.org/release.html
3. http://www.unwomen.org/en/digital-library/publications/2015/9/cyber-violence-against-women-and-girls
4. CyberVAWReportJessicaWest.pdf