End violence: Women's rights and safety online

Technology-related violence against women in Kenya

Mary Onyango

International Association of Women in Radio and Television

Association for Progressive Communications (APC)

July 2014

Ministry of Foreign Affairs

This research is part of the APC "End violence: Women´s rights and online safety" project funded by the Dutch Ministry of Foreign Affairs (DGIS) and is based on a strong alliance with partners in seven countries: Bosnia and Herzegovina, Colombia, Democratic Republic of Congo, Kenya, Mexico, Pakistan, and Philippines. For more information visit GenderIT.org and Take Back the Tech!

Table of Contents

Introduction

The research project is part of the remedies for victims/survivors of technology-related forms of violence against women (VAW). The project is an implementation by the Association for Progressive Communications (APC) in partnership with seven countries: Mexico, Colombia, Democratic Republic of Congo, Kenya, Philippines, Pakistan and Bosnia and Herzegovina. The main objectives were to:

- Map domestic legislation.
- Carry out desk review on corporate policies.
- Interview three to four case studies on victims/survivors of technology-based violence.
- Interview law enforcers.
- Interview NGO directly concerned with violence against women.
- Interview corporate representatives (ISPs, mobile phone companies, public policy departments).

Summary of research

The International Association of Women in Radio and Television (IAWRT) Kenya Chapter, carried out the research on "End violence: Women's rights and safety online". The aim was to find out the emotional and psychological effects on women who are violated on physically as well as through technology, and determine the legal redress mechanisms available for violations. Four case studies were selected for the research. Data was collected through interviews of purposive sampled real life victims/survivors; Non governmental organisation concerned with women's rights; and corporate organisations concerned with ICT infrastructure such as internet service providers and mobile telephone company. The research zeroed on Safaricom, Google and Communications Commission of Kenya (CCK) as key corporates. The data compiled for Safaricom and Google included general terms and conditions for use of the services the companies offer to customers such as policies prohibiting offensive comments, personal attacks, graphic violence and invasion of privacy. The policies however, do not specifically refer to gender, race or ethnicity. The research also carried out desk review of domestic laws which include: criminal laws, ICT related laws, and procedural laws. The research was carried out part of November 2013, then from 26th February, to 10th April, 2014.

Policy and political background

Women's rights in Kenya were not part of the development agenda before the third United Nations conference on women held in Nairobi in 1985. It was during this period that women in Kenya began to experience the need to advocate for various rights in governance, legal access, cultural practices that were retrogressive, and the promotion of gender equality. The experiences of 1985 led to the formation of women rights organisations like Federation of Women Lawyers (FIDA), with strategies to promote gender equality and fight for women who are abused physically, by seeking legal redress for the victims/survivors. Another organisation that emerged during this period is the Coalition on Violence Against Women (COVAW). According to the programme associate, the cases on assault have been increasing owing to the fact that more women are willing to speak out on violations against them. This makes follow-up on access to justice easier. COVAW has trained paralegals in the communities are able to handle gender-based violence. They reach out to the women and girls at community level, by assisting them to

acquire medical care, psychological support, which police station to report the matter to, and the necessary legal process.

There has been gain in recognizing women's rights, but implementation of the same has been the challenge. According to World Bank Data on Global Development: Women's rights and gender equality (February, 2013), Kenya scored a *NO* in all the legal concerns on domestic violence. Questions paused whether there is legislation specifically addressing domestic violence; specialized court for cases of domestic violence; legislation on emotional and physical abuse; all scored a *NO* as answer. Kenya only scored highly on sexual harassment where there are specific laws and criminal sanctions against perpetrators. The Constitution 2010 too was noted to be having non-discrimination clause on any gender and a guarantee of equality before the law.

Summary of key themes/trends in the cases

Dynamics of tech-related forms of VAW

The information super highway and new technologies has made it easier for people to communicate in dynamic and various ways. The computer technology allows the use of internet and communication through the available media of email, Facebook, Twitter, and blogs among others. According to the Communications Commission of Kenya (CCK) quarterly statistics report of October-December 2013/2014, released April 2014, estimated number of internet users rose by 11% to reach 21.2 million up from 19.1 million. In essence, internet penetration increased to 52.3% in a population of 40m countrywide. Other technologies are mobile telephony which experienced a marginal increase in the number of mobile subscriptions during the quarter to above 31 million. The number of short message services (SMS) grew significantly to 6.2 billion SMS compared to 5.0 billion posted in the preceding quarter.

This increase in access to information communication technologies (ICTs), while contributing to socio-economic and political development also provides increased avenues for stalking, abuse, intimidation and humiliation. According to the Kenya ICT Action Network (KICTAnet) research study of 2010 on *Women and cybercrime: the dark side of ICTs,* revealed that use of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women was rampant in Kenya.

The case studies on the technology-related violence documented use of social media, particularly Facebook as the common platform used by abusers. In the four cases under study, three of them reported violation committed through Facebook to implicate and intimidate the victims. In the other case SMS was used to also intimidate and harass the victim/survivor.

Harms

The victims/survivors of the case studies mostly experienced emotional distress and psychological harms exacerbated if they could not find explanations to the happenings around the violations. Other forms of harms included: feeling threatened due to the violation and political affiliation; financial strain because of loss of economic rights; low self–esteem; isolation when shunned or ridiculed by people in the community. In certain communities cultural values are pivotal in marriages, for example, where a woman is bound by the marriage to the man and cannot take any legal redress if being abused because it is considered a curse on the children. The victims/survivors experienced harassment, harm to reputation, withdrawal, intimidation, scare, fear, confusion, anger and some depressed to the point of seeking counseling services.

The harms were perpetrated through social media fora and short message services which according to the law are part of cyber bullying, the most common form of cyber crime. Cyber bullying has been defined variously as: the use of the internet vide computer or other devices to engage in obnoxious behavior directed at a specific person or group of persons, and involves threats, (cyber) stalking, insults. Defamatory/libelous statements, falsification and fraud among others. Cyber bullying can be effected through emails, tweets, through messages on social media fora, short messaging services, or actual phone/skype calls.

Kenya is a signatory to Universal Declaration on Human Rights. These are embedded in the Constitution which guarantees individuals human rights such as the right to privacy: "the right not to have their communications infringed"; right to freedom of expression; freedom of association; political, economic and social rights are all guaranteed. A violation of any of the rights is an abuse of human rights as noted in the case studies.

Actors

Out of the four cases under study, two sought legal remedies, while the other two responded to personal remedies. For the victim/survivor who reported violations of falsification on social media, the police (Officer in Charge of Police Division) promised to

carry out investigations under cyber crime offence and charge the offender accordingly. Cyber crime is handled by the Kenya Police Services Division of Criminal Investigation Department (CID) which mostly handles fraud cases. Meanwhile, pending investigations, the police offered the victim/survivor physical protection in case of pending threats. Victim declined the offer citing infringement on her privacy.

The victim/survivor of physical abuse which later turned to short messaging services was not accorded a similar treatment. The victim went to the police to report death threats and physical abuse by her husband but was sent away citing domestic affair encouraging the victim to discuss the same with the husband and seek services of a counselor. It was unfortunate this happened to the victim. Ideally the police were supposed to record the victim's case and give her a restraining order (Form P.3) as a legal injunction that would have restrained the perpetrator to stop further abuse or face charges should the victim report, after the issuance of the restraining order, that the perpetrator had violated her again.

The victim/survivor whose political rights were being abused did not report to the police nor any internet intermediary. Although the victim was psychologically affected by cyber bullying, had low self-esteem and doubted herself, she opted to seek counseling services. This was a turning point in the victim's life. She felt encouraged and gathered courage to respond to her bullies through social media.

The last case did also not report to the police or internet intermediary. Tied by cultural rights, the victim sought to separate from an abusive husband who was cyber bullying her with a view to denying her freedom of expression and association online.

The husband had demanded all her passwords to email, Facebook and even ATM. In her submission, the victim handed over all passwords to her own detriment.

Is the legal framework satisfactory?

Research by KICTAnet shows that Kenya's laws are unable to effectively prosecute cyber crime and online hate speech. The study further identified various challenges related to dealing with women. These included inappropriate policy and regulatory frameworks, inadequate training of legal and law enforcement professionals on cyber crime, insufficient resources for cyber crime prevention and enforcement.

The Constitution of Kenya, 2010 is the supreme law of the land and embodies legal frameworks upon which various legislative laws/policies that relate to violence against women have been enacted. A key provision in the Constitution is the Bill of Rights which spells out fundamental human rights to be enjoyed by all persons: right to life, equality, freedom from discrimination, including the right not to be subjected to any form of violence from either public or private sources. The various laws include:

Criminal laws

- The National Gender and Equality Commission Act 2011
- Penal Code, Cap 63 (Rev. 2009)
- Counter-Trafficking in Persons Act, No.8 of 2010
- Children Act, No.8 of 2001
- National Cohesion and Integration Act, No. 12 of 2008
- Sexual Offences Act of 2006
- Prevention of Organized Crimes Act, No. 6 of 2010

ICT related laws

- Kenya Information and Communications Act, Cap 411A (Revised 2012).
- Data Protection Act, 2012.
- Computer Emergency Response Team (CERT) – CCK, 2008; established to deal with cyber crime.
- The Internet Governance Forum Steering Committee (KIGFSC) now pushing for the Draft Cyber Crime and Computer Related Offences Bill 2014 to be signed into law.
- The Kenya Information and Communications (Amendment) Act, 2013 has brought into being the Communications Authority of Kenya to replace the Communications Commission of Kenya (CCK). The new regulatory body has a mandate to regulate the ICT industry.

Procedural laws

- Evidence Act, Cap. 80

Law enforcement agency

- The Kenya Police Service established under the provision of the Police Act

Despite the various laws and recognition of women's rights such as the right to access to justice, implementation is still a challenge. This is further aggravated by the fact that technology-related violence against women is a fairly new phenomenon to law enforcers. In some cases of gender-based violence, (for example rape) when "women go to report to the police stations they can sometimes be turned away and falsely accused that rape was as a result of the way they were dressed". Such incidences have in the past led to women opting to withdraw rather than report any sex offence. Despite such isolated negative reactions, the gender desks at police stations are now isolated from common areas of reporting cases. The personnel posted at the desks know how to handle survivors of sexual violence due to the counseling training they undergo. Furthermore the Sexual Offences Act, 2006 is applicable to sexual offences, particularly rape.

Sometimes victims report abuse directly to the non-governmental organisation concerned with violence against women. And for such cases the organisation has trained paralegals at community level who reach out to the women and girls under violations in terms of where they can acquire services: medical care, psychological support, legal assistance, which police station to report the matter to get a P.3. form (restraining order), file the case in court. Where a victim needs a lawyer, the organization has a database of probono lawyers who can be relied upon to help out the victims.

Victims/survivors of ICT infrastructure face challenges of not having direct laws to address ICT offences. The only law applicable for such offences is the Kenya Information and Communications Act, Cap 411A which has limitations. The law addresses certain criminal acts like: unauthorized access to computer data, access with intent to commit offences, interception of computer service, modification of computer material, denial of access, unauthorized possession of data, electronic fraud, and publishing of obscene information. The law enforcer may interpret the law to mean misuse of telecommunication system and use the same to institute a charge. There is no mention or definition of cyber bullying as an offence yet this is the most common form of cyber crimes.

When police receive cyber related cases, they are usually handed over to the Criminal Investigation Department (CID) in Nairobi, the Kenya Police Services Department which specializes in penetrating and dismantling criminal networks. Hence offences of criminal

nature like cyber crime would have to be sent to the CID headquarters for investigations before any charges can be instituted against a perpetrator. This may take long since the department is not decentralized. Although the department had 18 trained personnel in forensic investigations, they are scattered in various departments. This has further weakened the cyber crime unit to operate to capacity. Victims do not therefore feel confident enough to bring the issues into the limelight due to the long wait for the law to be enforced.

The Penal Code, Cap 63, can still be applied to charge offenders of cyber crime where the Kenya Information and Communications Act, 411A is inapplicable. It provides the general framework for criminal law and contains all the offences that are punishable by law in Kenya.

Another law that would be applicable is the National Cohesion and Integration Act, No 12 of 2008. However, this law only seeks to criminalize discrimination on the basis of ethnic or racial grounds. Under this law, hate speech is prohibited and it involves the use of threatening, abusive or insulting words intended to or likely to stir up ethnic hatred. Hence any speech or SMS should Cyber Crime and Computer related Offences Bill 2014 to be signed into law. The details of the draft bill are yet to be made public.

The participation of Kenya in the African Union Convention on Cyber Security[16] will provide the guidance and impetus for African Union countries to enact national level legislation dealing with digital security, personal data protection and effective mechanisms to combat cyber crime.

Is the corporate redress/response mechanism satisfactory?

Safaricom is one of the leading integrated communications companies in Africa with over 17 million subscribers. Safaricom provides a comprehensive range of services under one roof: mobile and fixed voice as well as data services on a variety of platforms.

Safaricom has several terms and conditions of use for the various services they offer. Safaricom's terms and conditions are comprehensive references to online crime against a person.

Terms and Conditions for the use of Safaricom:

"*The user name you choose must not be obscene, threatening, menacing, racist, offensive, derogatory, defamatory or in violation of any intellectual property or proprietary rights of any third party; and if we consider in our sole and absolute discretion that the user name selected by you is inappropriate, we reserve the right to reject and prevent your use of such user name at any time with or without notice to you.*"

Policy further states that:

"Abusive, indecent, defamatory, obscene, pornographic, offensive or menacing effect of causing the recipient to feel so harassed, abused or offended; or Designed to cause annoyance, inconvenience or needless anxiety to any person; or In breach of confidence, intellectual property rights, privacy or any right of a third party."

This policy captures and prohibits offensive comments, personal attacks, and invasion of privacy, graphic violence, and pornography. It however does not capture or reference harassment on basis of sex, gender, race, ethnicity, ability or religion.

Safaricom does not specify what information is permitted but it does however prohibit the use of abusive, indecent, defamatory, obscene, pornographic, offensive threatening, menacing, racist, offensive and derogatory word(s). It also does not highlight the punishment for such acts according to the existing laws like the Kenya Information and Communication Act, 411A. But it does mention in passing that the person's account will be terminated.

There is no mention of mechanisms to block or remove content which violates a person's privacy in its terms and condition. The following link however enables a user to seek some sought of redress through reporting directly with a company (Deloitte South Africa) which is completely independent of Safaricom.

https://www.safaricomethicsline.com/Disclosing.aspx

The services of Google are not limited to; Google Books, Google Finance, Google Image Search, Language Tools and Google Search.

Google does have a policy regarding the use of hate speech: "*Do not distribute content that promotes hatred or violence towards groups of people based on their race or ethnic origin, religion, disability, gender, age, veteran status, or sexual orientation/gender identity*."

This policy echoes what is contained in the National Cohesion and Integration Act, No 12 of 2008, which as mentioned earlier, only deals with ethnicity and not general hatred messages/speeches.

Other policies that negate violence include:

- **Sexually explicit material**

Do not distribute content that contains nudity, graphic sex acts, or sexually explicit material. Do not drive traffic to commercial pornography sites.

- **Harassment and bullying**

Do not harass or bully others. Anyone using Google+ to harass or bully may have the offending content removed or be permanently banned from the site. Online harassment is also illegal in many places and can have serious offline consequences.

- **Violence**

Do not distribute depictions of graphic or gratuitous violence.

There isn't a clear mechanism on removal of content; whether this is done after the victim/survivor complains. Google however has provided a channel where one can block the person or flag it. In its terms and conditions, Google does not mention if there is a specific department which decides on what content is taken down consequently, there are no mechanisms in place to deal with such a decision.

The data Google records and stores can be shared with companies, organisations or individuals outside of Google as long as it is to meet any applicable law, regulation, legal process or enforceable Governmental request. Such data is valuable when crime such as cyber crime is being investigated. Through off-the-cuff information gathered, internet service providers do not provide grievance mechanisms for victims of technology-based violence. What they expect is for victims/survivors to report to the police first who would then request for the said data for investigations.

Interviews of the internet intermediaries (Safaricom and Google) were very key in the case studies as mentioned earlier due to their fundamental roles in providing ICT related services. Through personal interviews we were to gather, for example, data on reports of rights violations and how the companies respond to offline violence facilitated by technology.

Dynamics of justice

In all the four cases under study, the women felt the legal procedures were inadequate. In certain instances of violence where tradition and culture were pivotal in decision making, the women felt the government and relevant organisations need to decentralize services for the benefit of women at grassroots who need to be educated on domestic violenceand reporting. Unless this is done then traditions and cultures usually supercede new aspects in development.

Other than culture, one victim strongly felt it would have been difficult to explain to the law enforcer what psychological/emotional distress she was going through. Her case she claims, "was not like verbal or physical abuse" that one could easily report. The victim further felt that cyber bullying could not form a strong basis for a report that could institute legal proceedings, it was more emotional than tangible.

In the other two cases there was a willingness to report to the police in pursuit of justice. The victim reported to the police who wrote a statement promising to investigate and charge the perpetrator under cyber crime. The case was reported in November, 2013. By the time of this study there was no feedback to the victim as to when the court proceedings would begin. The victim/survivors disappointed with delayed justice.

In the last case although the victim reported to the police, she was sent away citing a domestic affair that she and her husband could sort out It is unfortunate the victim was treated thus. She ought to have been issued with a restraining order (Form P.3) as a legal injunction that would have restrained the perpetrator to stop further abuse or face charges should the victim report continued attacks.

Recommendations

This study revealed that there is technology-based violence against women through ICT infrastructure;the social media (particularly Facebook) and short message services on mobile phone. The study also revealed that the increased use of ICT has enabled perpetuation of violence from physical to online. Perpetrators of violence now have more uncontrolled platforms for abuse than there has been in the past before advancement in technology. Lack of definite ICT laws to deal with such criminal activities has further contributed to online abuse. It would be therefore worthwhile:

1. To decentralize the cyber crime unit as a devolved service to facilitate investigations.

2. To revise Kenya Information and Communication Act, Cap 411A to address cyber bullying.

3. To have direct redress mechanisms from ISPs so that victims/survivors do not have to report to police first to institute investigations upon which ISPs can respond.

4. To have ISPs state punishment to offenders alongside the warnings stated in the terms and conditions.

5. To train law enforcers to manage psychological/emotional stress that is presented by online violence.

6. To have organisations that are directly concerned withviolence against women embrace technology-based violence as a new form of violence.

7. To train women on Take Back the Tech! safety online to reduce chances of cyber bullying, for example, stalking/trafficking.

8. For the government department responsible for ICT industry to push for enactment of a law that would regulate the ICT industry and deal directly with computer related offences.

9. For the government department in charge of the implementation of the Constitution to foresee implementation of Bill of Rights and freedom from discrimination including the right not to be subjected to any form of violence.

10. For the Internet Governance Forum to facilitate international treaties binding countries to curb ICT related offences.

Areas for further research

The case studies generally examined the technology-based violence against women. Further research could be done on why women prefer not to report cases of violence. Another area of research could be the prevalence of cyber crime in the country and come up with deterrent mechanisms.