Journal of Culture, Society and Development
ISSN 2422-8400 An International Peer-reviewed Journal
Vol.56, 2020

Background Paper-Safe Digital Spaces: Protection of Women and Girls from Technological Violence

UN Women East and Southern Africa Regional Office in Nairobi-Kenya
esaro.publications@unwomen.org

Abstract

The rapid advancement of information and communication technologies (ICTs) increased the opportunities for communication and use of ICTs in a number of innovative ways. However, ICTs are also harming and threatening women and girls in a number of ways. Technology-assisted Violence against Women and Girls is emerging as a global problem with serious implications for societies and economies around the world. Reports now suggest that an incredible 73 percent of women have been exposed to some form of violence online. The statistics pose risks to the peace and prosperity for all enshrined in the Charter of the United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement.

As the use of information and communication technologies has become more omnipresent, the use of these technologies as a weapon against women has also become ubiquitous. In addition, the internet and social media have also become environments where women are often made to feel unsafe and are threatened. Violence against women is being committed through the use of media such as texting, email, Facebook, Twitter, YouTube and just about any other internet or social media platform you can think of. More so, data shows that cyber-violence against women is very prevalent among the youth. This is very well showcased by media stories of many young girls affected by aggravated sexual assault and sexting.

This paper analyses the ways in which technology helps women and contributes to achieving Sustainable Development Goals (SDGs) , examines the various forms of technology-assisted violence against women and their impact and consequences in the light of the global and Africa region frameworks, how this type of violence impacts women's lives, where various African governments are in terms of policy provision to access justice for victims, and proposed recommendations to end the vice. The paper argues that making accessible ICTs and filling the gender divide is important in achieving the Sustainable Development Goals (SDGs). It also seeks to offer a collective understanding of what technology-assisted violence against women and girls constitutes. It further makes recommendations to address tech-violence against women and girls with an emphasis on the transformative change in making the digital world accessible and safe for women and girls.

Keywords: Tech Violence, VAW, UN Women, youth, student leaders, SDGs, gender equality, women's empowerment, cyber bullying, ICT, TVAW

DOI: 10.7176/JCSD/56-08
Publication date: February 29th 2020

1.0 Background and Context

Information and communication revolution joined by globalization have tended to shrink space in recent years. Technology makes everyone's life easier, especially students and researchers, benefit immensely from the world of web. Advancements in science and technology envisaged at making available the physical, educational, social and environmental health if not regulated systematically can be devastating. There's no denying that we have gained from technological advancements, however, if not regulated, may cause havoc to the future generations[i]

Cybercrime is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime and their victims can be located in different regions, and it can have a ripple effect through societies around the world, highlighting the need to mount an urgent, dynamic and international response.

As observed by the United Nations Office on Drugs and Crime (UNODC) in its recent study, "Fast-paced technological innovation and widespread and increasing accessibility of ICTs, including high-speed Internet and mobile devices with Internet connectivity, have transformed societies around the world. Children, in particular, have increased access to ICTs and, in recent decades, have tended to adopt these technologies from an early age,

resulting in ICTs becoming thoroughly embedded in their lives. This context facilitates opportunities for the misuse of ICTs to abuse and exploit children. Children can easily engage with strangers and exchange large data files, while the possibilities for parental supervision and monitoring are restricted. Children are also at particular risk as they often do not fully understand threats associated with the use of ICTs, or are not sufficiently aware that, once shared, control over such material is effectively waived."

2.0 Women's Right to ICTs: Tool for Empowerment

Technological innovation has profoundly transformed societies around the world. Harnessing Information and Communication Technology (ICTs) to advance gender equality and women's empowerment is not only vital for women and girls, but critical for achieving the 2030 Agenda for Sustainable Development. The United Nations Sustainable Development Goals (SDGs) 5 and 9 call for prioritizing "Support to gender equality in internet and broadband access and use as an enabler of women's empowerment (SDG 5)" and; to "Increase access to information and communications technologies and strive to provide universal and affordable access to the internet (SDG 9)." The United Nations Sustainable Development Goals (SDGs),[ii] a collective global effort to address global development priorities for the next 15 years, includes a goal on gender equality which places women's access to technology for their empowerment as one of the core indicators for progress. In September 2013, the Broadband Commission for Digital Development[iii] set an ambitious new target calling for gender equality in broadband access by 2020.

By the end of 2013, according to UNODC,[iv] almost 40 percent of the world's population, i.e., 2.7 billion people, and 78 percent of households in developed countries had access to the internet. Although only 28 percent of households currently have access to the internet in developing countries, between 2009 and 2013, there were annual internet access growth rates of 27 per cent in Africa and 15 per cent in Asia and the Pacific, the Arab States and the Commonwealth of Independent States. The percentage of use of social media by women and girls is higher. Along with the rising use of mobile phones, texting by Short Message System (SMS) has emerged as a common means of communication. Between 2007 and 2010, the number of SMSes sent globally tripled from 1.8 trillion to 6.1 trillion a year, equaling an average of 200,000 text messages sent every second. Facebook had 1.44 billion monthly active users. This translates to 50 percent of Internet users worldwide.

There is a gender gap in access to ICTs. For example, the GSMA[v] examined the ownership and use of mobile phones in its report: 'Bridging the Gender Gap', and it found that 200 million fewer women than men own a mobile phone across low- and middle-income countries. Even when women own a mobile phone, they are far less likely than men to use it, especially when it comes to the more transformational services like mobile internet and mobile money services. This represents a significant lost market opportunity. Our research shows that closing the gender gap in mobile phone access and usage in low and middle-income countries could unlock an estimated cumulative revenue opportunity of USD 170 billion for the mobile industry from 2015–2020.

Similarly, there are gaps identified in access to internet by people in general and women in particular due to various reasons. In 2016, the United Nations Human Rights Council passed a resolution condemning the practice of preventing and/or disrupting individuals' access to the Internet.[vi] While universal access to the Internet is not recognized as a human right in international human rights law, there are State obligations to promote Internet connectivity that can be derived from a number of human rights, such as freedom of expression[vii]. Internet access is essential for the realization of many other rights as well, including the rights to freedom of association, freedom of assembly, to education and health, to full participation in social, cultural and political life, to social and economic development.[viii] These obligations include "adopting effective and concrete policies and strategies in consultation with individuals from all segments of society, including the private sector as well as relevant Government ministries to make the Internet widely available, accessible and affordable to all."[ix] Here, "a comprehensive human rights-based approach in providing and in expanding access to the Internet [should be followed], and states [should make every] effort to bridge the many forms of the digital divide."[x] More specifically, the United Nations Human Rights Committee states that "States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto".[xi]

3.0 Legal Frameworks for Promotion of ICTs

An analysis of the existing global and regional frameworks for the regulation of cyber security reveals the limited consensus among the global actors and preparedness to tackle the cybercrimes. Much of the focus is laid on addressing economic offences. Often States are also hesitant to commit themselves to take a position on the regulatory frameworks and thus to express their *opinio juris*. It took until 2013 for state representatives to agree on the rudimentary threshold assumption that international law actually applies to cyberspace.[xii] The absence of a cyber-specific system of rules of international law does not mean that there are no legal rules that would apply to cyber activities. As we have seen, states accept that generally applicable rules of international law apply to states' conduct in cyberspace, too. This is undoubtedly correct. If international law is to be an efficient governance structure, it must be adaptable to new phenomena without the need to reinvent an entire regulation framework on each occasion.[xiii]

The United Nations Human Rights Council has repeatedly affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[xiv] The obligations of States under international human rights treaties have been interpreted by courts and other expert bodies as requiring States parties not only to ensure that State parties take appropriate measures to prevent the infliction of violence by private actors, to investigate and punish such actions, and to provide protection and support for the survivors of violence. Similarly, the Convention on the Rights of the Child (CRC) obliges States parties[xv] to take all appropriate legislative, administrative, social and educational measures to protect all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse.[xvi] Other forms of exploitation are addressed in articles 35 and 36 of the CRC. At the UN level, the Committee on the Elimination of Discrimination against Women (the CEDAW Committee) has articulated the obligations of States parties to the Convention on the Elimination of All Forms of Discrimination against Women (the CEDAW Convention) to eliminate violence against women, in particular in its General recommendation 19 (1992).[xvii] Other UN human rights treaty bodies, such as the Human Rights Committee[xviii] and the Committee against Torture,[xix] have also made clear that States parties' obligations under the International Covenant on Civil and Political Rights 1966 (ICCPR)[xx] and the Convention against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment 1984 (CAT)[xxi] include eliminating public and private violence against women.

Further, in the wake of the Beijing+25[xxii] taking place in 2020, it is time to revisit Section J of the Beijing Platform for Action-on women and the media, which needs to be reprioritized in the context of the post-2015 development agenda. Advocacy for the reprioritization of Section J at the CSW asked governments to recognize the critical role that the media and information and communications technologies (ICTs) play in both advancing and stifling women's rights. The Secretary-General's Report included a detailed assessment of progress and gaps and several priorities forward- looking recommendations. The Association for Progressive Communications (APC)[xxiii] has also developed 10 points on Section J, which describes the growing impact of ICTs on a variety of women's rights issues from access and agency to economics and ecology.

The 2013 CSW outcomes recommended that States should support the development and use of ICT and social media as a resource for the empowerment of women and girls, including access to information on the prevention of, and response to violence against women and girls and develop mechanisms to combat the use of ICT and social media to perpetrate violence against women.

The freedom of expression is viewed as a right that enables and facilitates the enjoyment of other essential economic, social, cultural, civil and political rights, including the right to freedom of peaceful assembly and association, the right to education, and right to participate in cultural life. The United Nations General Assembly also recognized "that the exercise of the right to privacy is [also] important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society".[xxiv] In addition to the generally applicable rules of international law, as provided under the UN Charter[xxv] and other human rights treaties, certain sectoral and regional treaties, have been adopted to regulate the cyber activities. These include, among others, the 1992 Constitution of the International Telecommunication Union;[xxvi] the 2001 Budapest Convention on Cybercrime[xxvii] and its 2006 Protocol on Xenophobia and Racism;[xxviii] the 2009 Shanghai Cooperation Organization's Information Security Agreement;[xxix] the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa 2003 (Maputo Protocol); and the 2014 African Union's Cyber Security Convention.[xxx] Although important in their own right, these international agreements govern only a small slice of cyber-related activities (such as criminal offences committed by means of computer systems[xxxi] or operations interfering with existing telecommunications networks),[xxxii] or have a very limited membership (six states in the case of the Shanghai Cooperation Organization's agreement[xxxiii] and none yet in that of the African Union's convention).[xxxiv] The European Court on Human Rights has extended the positive

obligation to protect vulnerable persons (namely, children) online by stating that countries are required to implement measures that safeguard them from harm through legislation.[xxxv]

4.0 Technological Violence Against Women and Girls

Violence against women and girls is a grave violation of human rights. The 1993 Declaration on the Elimination of Violence against Women became the first international instrument explicitly addressing violence against women, providing a framework for national and international action. It defines violence against women as any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.

Although violence is often equated with physical abuse, it can take many different forms. Consequently, different or new forms of Violence against women and girls may increase or arise when societies undergo demographic, political and economic changes, or social and cultural shifts. This includes when new Information, Communications and Technology tools enter the scene.

Statistics on violence against women showed that more than 1 in 3 women (36.6 per cent) in Africa report having experienced physical, and/or sexual violence by a partner or a non-partner. Technology-assisted violence against women and girls could significantly increase this staggering number, as reports suggest that 73 per cent of women have already been exposed to or have experienced some form of online violence in what must still be considered a relatively new and growing technology. Cybercrime is an evolving form of transnational crime impacting the society in general and women and girls in particular.[xxxvi]

The exponential growth and developments in technology have created new ways to connect, share resources and experiences, and build communities. However, it is often said that technologies such as the internet or mobile phones are a double-edged sword, since these digital spaces have also provided tools and platforms for the replication and continuation of the perpetration of violence against women and girls. They can be used by abusers to deepen their control.

5.0 Various Forms of Cyber Violence Against Women and Girls

There is no uniform definition of Cyber Violence against Women in many jurisdictions. However, Cyber Violence Against Women and Girls (VAWG) includes hate speech (publishing a blasphemous libel); hacking (intercepting private communications); identity theft; online stalking (criminal harassment); and uttering threats. It can entail convincing a target to end their lives (counseling suicide or advocating genocide). The Internet also facilitates other forms of violence against girls and women, including trafficking and sex trade. Not only does commercialized sex on the Internet drive the demand for the sex industry overall, but it also allows traffickers to use the legal aspects of commercial sex on the Internet as a cover for illegal activities. Some of the main uses of the Internet by traffickers include: advertising sex, soliciting victims on social media, exchanging money through online money transfer services, and organizing many of the logistical operations involved in transporting victims.[xxxvii] The complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response.

Technology-assisted Violence Against Women and girls encompasses acts of gender-based violence that are committed using information and communication technologies (ICTs), such as phones, the Internet, social media platforms and emails among others. On the flip-side, women can, and have been using ICT platforms to inform, denounce and strategize, and to demand their right of a life free from violence, examples include advocacy campaigns such as the *#MeToo* movement against sexual harassment and sexual assault and the *#TotalShutDown* movement in South Africa, against gender-based violence especially acts of murder, kidnap and abuse of women, children, and gender non-conforming people.

Impacts of violence against women range from immediate to long-term multiple physical, sexual and mental consequences for women and girls, including death. It negatively affects women's general well-being and prevents women from fully participating in society. Violence has negative consequences for not only women and girls but also their families, the community and the country at large. It has tremendous costs, from greater health care and legal expenses and losses in productivity, impacting national budgets and overall development.

For those who may never have been exposed to this kind of violence, it is difficult to imagine what cyber

VAWG might look like, or indeed what its effects might be. Hate speech (publishing a blasphemous libel), hacking (intercepting private communications), identity theft and online stalking (criminal harassment) are the most common forms of cyber-VAWG. Threats of rape, death and stalking are emotionally draining, and financial stress can include legal fees, online protection services as well as missed earnings.

The rapid proliferation of information and communication technologies (ICTs) expands opportunities to address VAWG, providing victims with access to information and reporting mechanisms. However, technological advances continue to outpace legal developments and the reality in many countries is that the existing international or national legal framework fails to provide timely or effective legal remedies.

The Broadband Commission for Sustainable Development guided by the UNESCO and the ITU established a working group on the digital gender divide and on Gender, which came out with the paper on "Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call." It provided statistics and identified the priority areas for action.

6.0 Forms and Manifestation of Violence Against Women and Girls in a Digital World

Social networking websites, for example, make it easier for perpetrators to monitor their targets, obtain personal information, and repeatedly send unwanted messages. The internet provides perpetrators with anonymity not afforded in real space and a larger platform for the spread of harassment. Online threats of violence against women, however, are often trivialized or minimized by the public, with perpetrators experiencing little or no consequences for their behavior. Technology, therefore, facilitates the proliferation of gendered hate and harassment.[xxxviii]

All technology-related violence is concerning and unacceptable.[xxxix] It affects children and adults and can be perpetrated by females and males and both can be victims/survivors of this violence. However, women and girls are disproportionately targeted and affected by technology-assisted violence on a complex number of intersecting factors such as age, race, class and disability. The UN estimates that 95 percent of aggressive behavior, harassment, abusive language and denigrating images in online spaces are aimed at women and come from a partner or former male partners.[xl]

Young women and their peers are likely to spend more time using and use more technologies than any other age group. Consequently, young women are at increased risk for all types of technology-related violence, popularly referred to as known as cyber misogyny-the various forms of gendered hatred, harassment, and abusive behavior targeted at women and girls via the internet.[xli] Cyber misogyny is most commonly manifested as: Revenge porn, cyberstalking, gender-based hate speech online, non-consensual sharing of intimate images and child sexual exploitation.

Take Back the Tech-a collaborative campaign to reclaim information and communication technology (ICT) to end violence against women (VAW)-organizes cyber misogyny/technology related violence against women into several broad categories:

1. **Online harassment and cyberstalking**, which constitutes one of the most visible forms of technology related VAW. This ranges from harassing SMS messages and online comments to tracking women's networks, friends, movements and activities through mobile phones, social networking spaces like Facebook and Twitter.
2. **Intimate partner violence**, where technology is used in acts of violence and abuse in intimate or spousal relationships. For example, women are afraid to leave abusive relationships due to threats of disclosure of private and intimate communications by their partners.
3. **Culturally justified violence against women**, where culture or religion is used as a reason to justify, ignore or accept acts of VAW, or when technology plays a role in creating a culture of VAW. It can be something as thoughtless as forwarding a sexist joke that supports the idea that women are less valuable than men, to starting a Facebook group that promotes different ways to rape girlfriends.
4. **Rape and sexual assault**, where technology is used to track the movement and activities of a victim/survivor, to provide location information or when an act of violence is digitally recorded and distributed. In other cases, the internet is used to lure women into situations of sexual assault.
5. **Violence targeting communities**, where communities face targeted online attacks and harassment because of their gender, sexual identity or political views. For example, the websites of many women's rights organizations have been hacked because of their stance on gender equality and feminism. Women bloggers who are outspoken about discrimination have also faced overwhelming attacks and messages that aim to disrupt their ability to express themselves online.

6. **Recruitment**, which uses technology to lure potential victims into violent situations. e.g., fraudulent postings and advertisements (dating sites; employment opportunities); traffickers using chat rooms, message boards, and websites to communicate/advertise, among others.

Unfortunately, cyber misogyny has real, tangible, and often devastating consequences for the safety and security of women and girls. Cyber misogyny also violates women's and girls' rights to equality and freedom from discrimination and contributes to the normalization of violence against women in mainstream culture.[xlii] Consequences experienced by victims/survivors include but are not limited to: Suicide, emotional and psychological distress, violation of privacy, public humiliation and exposure, damage to reputation, Job loss and financial losses, damage to personal relationships, violation of personal dignity and autonomy, fear for physical and/or psychological safety among others.

7.0 Enabling Factors of How VAW Manifests in the Digital Space

According to the Association for Progressive Communications Women's Networking Support Programme (APC WNSP), there are several factors which affect how VAW can manifest in the digital age. These include but are not limited to:

- **Anonymity:** Widespread usage of digital technology has increased the potential for an abuser to remain anonymous. An intimate partner, acquaintance, work colleague or stranger can commit abuses without physically entering public spaces.
- **Automation:** Automation refers to the use of information technologies to reduce human work in tasks. In the context of ICTs, automation is useful for monotonous tasks (e.g., distribution of information), time-consuming (e.g., monitoring victim/survivor behaviour or movement) and involve specialized work (such as a film production or image manipulation). It is particularly relevant for surveillance and stalking. Although the surveillance and policing of women's movements as a tactic to control and regulate women's behaviour is not new, the automation enabled by ICTs allows abusers to check their partners' mobile phones for SMSs, monitor social networking activity, check their browser history and log into their personal accounts with little effort. Furthermore, these technologies usually do not require any special knowledge or skills to use.[xliii]
- **Action at a distance:** ICTs permit sexual harassers to send abusive messages from anywhere in the world to anywhere in the world. This makes it more difficult for a survivor to identify and take action against an abuser.
- **Affordability:** New ICTs have also significantly reduced the difficulty and cost of production and propagation of information. Anyone with a mobile phone can take and upload images or videos and distribute quickly via an email application, Facebook or YouTube, which allow the images to be replicated thousands of times at little or no cost.
- **Propagation:** In cyber-space settings, abuse can happen every day, all year round. The internet records everything and never forgets. The continuous traffic of harassing text and images makes it hard, if not impossible, to track down and stop further circulation. Moreover, the propagation of texts and images can lead to the revictimization of women. It can follow victims/survivors everywhere–at home, work and school, whenever their computer or mobile phone is turned on, without a break or relief.

8.0 Access to Justice: The Situation in Africa

Victims/survivors of technology-assisted VAW often struggle in seeking adequate recourse and claiming their rights. Legal and regulatory agencies and law enforcement bodies are very often in a quandary on what law to use to punish perpetrators. Police and judicial officials maneuver across laws ranging from anti-VAW laws, to cybercrime bills or laws on privacy rights, to stop violence and provide remedies for victims/survivors.

ICT policy and legal frameworks are in different stages of development in different countries in Africa. However, policies and laws on ICT are for, the most part, gender-blind and do not focus on how men and women are impacted differently. Even less do they consider violence against women and girls. For example, and as indicated in table 1 below, most of the national ICT legislation on cybercrimes only focus on high-profile crimes such as phishing scams, identity theft, hacking and copyright infringement, and not on the violation of the women specific human rights.

As at July 2018, 12 African States (Botswana, Cameroon, Côte d'Ivoire, Ghana, Kenya, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) seemed to have basic substantive and procedural law provisions in place, although implementing regulations may still be missing in a few of these countries.

However, most African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. In addition, draft laws or amendments to existing legislation had reportedly been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). In some instances, bills had been presented to national parliaments; in others the fate of draft laws is uncertain.

Table 1 below provides a cursory overview of Africa in terms of specific criminal law provisions on technology-assisted VAW.[xliv]

Country	Status of specific criminal law provisions on technology-assisted violence against women and girls (as at July 2018)	
Algeria	Partial	• Partial legislation in force • Law No. 09-04 of 14 Chaabane 1430. Corresponding to 5 August 2009 containing specific rules on the prevention and fight against information technologies and communications crimes - enacted in 2009
Angola	No	• No legislation in force • Penal Code amendments including substantive criminal law provisions under discussion
Benin	Partial	• Act against cybercrime (draft law) • No specific procedural law provisions
Botswana	Yes	• Cybercrime and Computer Related Crimes (no 22) Act 2007 • Electronic (Evidence) Records Act 2014 for admissibility of electronic evidence
Burkina Faso	No	• Draft law on cybercrime. No specific legislation in force
Burundi	No	• Partial substantive law provisions in Penal Code Act No. 1/95 of 22 April 2009
Cape Verde	No	• No specific legislation in force • Penal Code – Decree Law No. 4/2003
Cameroon	Yes	• Cybersecurity and Cybercrime Law from 2010 - Loi No 2010/012
Central African Republic	No	• No specific legislation in force
Chad	TBC	• Loi relatifs à la cyber sécurité et la lutte contre la cybercriminalité (July 2014)
Comoros	No	• No specific legislation in force
Congo Brazaville	No	• No specific legislation in force
Côte d'Ivoire	Yes	• Law 2013-451 (19 June 2013)
Democratic Republic of Congo	No	• No specific legislation in force
Djibouti	No	• No specific legislation in force • Draft Law on cybercrime
Egypt	No	• No specific legislation in force
Equatorial Guinea	No	• No specific legislation in force
Eritrea	No	• No specific legislation in force
Ethiopia	No	• Draft Ethiopian Cybercrime Law • Criminal Code of the Federal Democratic Republic of Ethiopia 2004
Gabon	No	• No specific legislation in force
Gambia	Partial	• Information and Communications Act No. 2 of 2009 with substantive criminal law provisions
Ghana	Yes	• Electronic Transactions Act, 2008 (ETA) for substantive and procedural law • Mutual Legal Assistance Act, 2010 (MLAA) with specific provisions on international cooperation on cybercrime and electronic evidence
Guinea	No	• Draft law (projet de loi relative à la cybercriminalité) adopted by the Government in April 2016
Guinea-Bissau	No	• No specific legislation in force
Kenya	Yes	• Computer Misuse and Cybercrimes Law, 16 May 2018. Criminal law

		provisions in section 37 of the Act
Lesotho	No	• No specific legislation in force • Bill on computer crime and cybercrime 2013
Liberia	No	• No specific legislation in force
Libya	No	• No specific legislation in force
Madagascar	Partially	• Loi n°2014-006 sur la lutte contre la cybercriminalité
Malawi	No	• No specific legislation in force
Mali	No	• No specific legislation in force • Draft Law on cybercrime; Loi n° 01-079 du 20 août 2001 portant code pénal du Mali
Mauritania	Yes	• Loi 2016-007 relative à la cybercriminalité (20 January 2016) • Implementing regulations pending
Mauritius	Yes	• The Computer Misuse and Cybercrime Act (No. 22) 2003
Morocco	Partial	• Partial legislation in force • Amendments to criminal and criminal procedure codes underway • with specific provisions on cybercrime and electronic evidence
Mozambique	Partial	• Partial substantive law provisions in amended Penal Code of 2015
Namibia	No	• Use of Electronic Transactions and Communication Draft Bill from September 2010. No specific legislation in force
Niger	No	• No specific legislation in force
Nigeria	Yes	• Cybercrime Act 2015 • Evidence Act as amended in 2011 for admissibility of electronic evidence
Rwanda	Partial	• Substantive law provisions in Penal Code No. 01/2012/OL of 02/05/2012 • Law No. 18 of 2010
Sao Tome and Principe	No	• No specific legislation in force in Penal Code cover illegal interception and child pornography
Seychelles	No	• No specific legislation in force
Senegal	Yes	• loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité
Sierra Leone	No	• No specific legislation in force
Somalia	No	• No specific legislation in force
South Africa	Partial	• Partial legislation in force • Electronic Transactions and Communications Act 2002 • Draft law (Cybercrimes and Cybersecurity Bill) in National Assembly following public consultations in December 2015.
South Sudan	No	• No specific legislation in force
Sudan	Partial	• Law No. 14 on Information Technology Crime • Cyber Crimes Act 2007
Swaziland	No	• No specific legislation in force
Tanzania	Yes	• Cybercrimes Act 2015 (20 February 2015)
Togo	No	• No specific legislation in force • Draft law on cybercrime; Le projet de texte relatif à la lutte contre la cybercriminalité
Tunisia	Partial	• Criminal Code • Law no 83 of 2000 on Electronic Commerce and Exchanges • Cybercrime Bill, 2014
Uganda	Yes	• Computer Misuse Act, 2011 (14 February 2011)
Zambia	Yes	• Electronic Communication and Transactions Act (ECT Act) 21 2009
Zimbabwe	Partial	• Computer Crime and Cyber Crime Bill • Criminal Law (Codification and Reform) Act - Act 23/2004

9.0 Key Trends and Issues

ICT policies and laws are, for the most part, gender-blind and do not focus on how men and women are impacted differently. Even less do they consider violence against women and girls. For example, some of the national ICT

legislation on cybercrimes only focus on high-profile crimes such as phishing scams, identity theft, hacking and copyright infringement, and not on the violation of the women specific human rights.

ICT enables secondary victimization: Secondary victimization can take the form of anonymous victim blaming and insensitive and harassing comments on images and clips that have been distributed virally. The ability to share images via social networking sites or mobile phones in a very short space of time and at low cost has serious implications for the extent to which women are re-victimized. Vicious responses to sexual assault often revive for victims/survivors their recently lived-through trauma and emotions of panic, insecurity, loss of control and pain.

10.0 Towards Creating Gender Equal and Safe ICT Spaces: Way Forward and Conclusions

One of the most significant challenges for eliminating and preventing VAW/G remains the persistence of attitudes and behaviours of men and women in a society that accept or condone violence against women, as well as beliefs that women and girls are less valuable or weak. This includes leaders such as politicians and decision-makers, service providers, police, justice officials, health workers, community leaders, as well as faith-based leaders.

Over the past two decades, there has been a growing momentum to eliminate and prevent all forms of violence against women, mainly due to the sustained efforts of the women's rights movement. Governments have demonstrated their obligations and commitments to address VAW/G through the further elaboration of international and regional policy and legal agreements. Decades of mobilizing by civil society and women's movements have put ending gender-based violence high on national and international agendas. There have been several internationally agreed norms and standards relating to ending violence against women and girls. These include the 1979 Convention on the Elimination of all Forms of Discrimination against Women (CEDAW) and the 1995 Beijing Platform for Action that identifies specific actions for Governments to take to prevent and respond to violence against women and girls. Moreover, in 2013, the Commission on the Status of Women (CSW) adopted, by consensus, Agreed Conclusions on the elimination and prevention of all forms of violence against women and girls. Similarly, an unprecedented number of countries have laws against domestic violence, sexual assault and other forms of violence. The recently agreed agenda on the SDGs included ending VAW/G and harmful practices, as target areas, confirming that they need to be urgently addressed in order to achieve gender equality.[xlv]

As the internet evolves and social media and networking tools increasingly become an intrinsic part of people's lives around the globe, attitudes and norms that contribute to cyber VAWG must be addressed with urgency. A collective global effort, led by the United Nations system, has put in place the pillars for a 21st century sustainable development paradigm. The Sustainable Development Goals (SDGs) establishing the global development priorities for the next 15 years includes a goal on gender equality, which places women's access to technology for their empowerment as one of the core indicators for progress.

In conclusion, in enhancing the fight against ICT-facilitated women and child abuse and exploitation, governments and national authorities need to focus on: a women and child protection approach that fully respects human rights; on ensuring that legislation keeps pace with technological innovation; on recruiting, training and maintaining specialized personnel; on gaining access to state-of-the-art technological resources; developing effective mechanisms for accessing third party data and conducting undercover investigations that are consistent with the rule of law; as well as developing policy guidance on harmful conduct committed by youth. The formulation of policies in this area is best based on a multidisciplinary approach that draws on research findings and best practices from social science, legal policy and public policy. Efforts to effectively and comprehensively combat ICT facilitated child abuse and exploitation necessitate a multi-stakeholder approach, including and actively involving children, families, communities, governments, members of civil society and the private sector.

11.0 Recommendations

Through the SDGs, the world leaders have committed to promoting "Gender Equality and the Empowerment of Women" and that No One is Left Behind. The SDGs, through their targets, call for accelerating efforts to fill the gender gap in all the areas, including women's access to ICTs and creating an enabling environment for achieving the SDGs by 2030. The prevention and response to cyber violence require a multi-sectoral and multi-faceted accelerated approach involving all key stakeholders focusing on sensitization, safeguards, and sanctions.

- **Partnerships:** Implementation and attainment of the Agenda 2030 for Sustainable Development is key in ending violence against women and girls, especially technology-assisted violence. Goal 17 calls for

strengthening the means of implementation and revitalizing the global partnership for sustainable development. In this regard, Technology-assisted VAW demands the attention of all stakeholders involved in shaping online spaces, and/or addressing VAW. This includes ICT users' communities, internet intermediaries, government policy makers, organizations working on VAW and the media. Each of these actors relates to technology- related VAW in different ways and has different roles. For instance, the state, including policymakers and law enforcers, is the primary duty bearer and has obligations under a number of treaties and policy frameworks to enact, implement and monitor legislation addressing all forms of VAW. Similarly, we cannot over emphasize the need to engage with private sector companies who develop and operate mobile phones and internet platforms. The internet intermediaries are powerful players in ICT policy, influencing national and transnational debates that shape internet governance and regulatory measures. Secondly, they can play an important role in shaping anti-VAW policies and strategies that empower rather than protect and victimize women.

- **Wholistic Legislative and ICT policies amendments:** Legislative review and the enactment of new laws and policies to deal with technology-assisted violence is vital. Governments need to ensure that laws responding to technology- related VAW are in place, implemented and monitored. This means that existing laws protecting women, such as anti-VAW laws, need to be expanded to account for technology -related violence. Furthermore, laws that deal with ICT related crime (privacy laws, pornography laws) need to account for gender differences and inequalities. Responding effectively to any VAW requires a holistic legislative approach,[xlvi] which assesses and balances all women's rights and recognizes that various discriminations can intersect. To ensure a holistic approach to technology related VAW, inter-thematic dialogue and research with a range of actors, from women's rights advocates to state actors and private companies, and which covers the range of issues that affect women's rights and ICTs is necessary. Similarly, tackling unequal gender power relations through "increasing women's participation in decision-making positions and political power is critical in order to influence policies and institutional practices that perpetuate impunity and tolerance for violence against women." As it is now, women are under-represented in ICT policy decision-making and within the ICT industry.
- **Advocacy to ensure women's participation:** Advocacy and initiatives by the youth, women's rights organizations and other civil society actors are important to ensure policy and law makers take into account ICT related VAW and that women participate in policy making dialogues. Advocates have an opportunity to influence these processes to ensure the development or renewal of national policies considers gender equity and addresses VAW within the framework of new ICTs. The participation of women and young people in forums such as the annual Transform Africa Summit will allow women's rights advocates to raise their concerns in contexts where women's perspectives are usually absent.
- **Evidence building: Collecting data on ICT related violence against women:** In order to ensure that policies continually respond to women's experiences, there is a need for more systematic reporting and monitoring of technology related VAW. Currently, there is a scarcity of information on VAW, ICTs and the intersection of the two. More systematic documentation of these violations, including in-depth case studies, is necessary to identify effective remedies and new policies.
- **Making online spaces safer: Internet intermediary policies and strategies:** Internet and mobile phone service providers need to play a role in ensuring women's and girls' privacy and safety when using their services by creating an online culture of zero tolerance to VAW and their responsibility in protecting users' rights. A victim/survivor of technology related VAW needs to know how to ensure her security online, including how to stop the violence, how to remove abusive comments or images from online platforms and prevent similar violations in the future. Moreover, they implement measures and policies that leave users more vulnerable to privacy breaches and security violations. For example, Facebook is well-known for making changes to its privacy policy that dismiss completely the original settings of users. Many online services stores, analyze and sometimes sell our search queries, social relationships, sites we "like" or tweet about, and other data for profit. Engaging with internet intermediaries and demanding that they develop corporate policies, practices and tools that respect women's rights is a critical part of our future.[xlvii]
- **Youth action:** Data shows that cyber-violence against women is very prevalent among youth. This is very well showcased by media stories of many young girls affected by aggravated sexual assault and sexting. Therefore, like other prevention programs, there is a need to target prevention programs at youth and engage youth in the creation of such programs. Examples of this could include social media literacy programming led by youth, for youth, on the consequences of sharing sexual images through social media and other forms of cyber-violence against women commonly experienced by young people.

REFERENCES

[i]Sadiq Syed, "Role of Law in Building a Peaceful, Inclusive and Sustainable Society for Future Generations," ICMF publication, p69 (2018).
[ii]See details at https://sustainabledevelopment.un.org/topics.
[iii]See details at http://www.broadbandcommission.org/Pages/default.aspx.
[iv]World Drug Report, 2012 accessed at https://www.unodc.org/documents/data-and-analysis/WDR2012/WDR_2012_web_small.pdf (26th February 2020).
[v]The GSM Association is a trade body that represents the interests of mobile network operators worldwide.
[vi]A/HRC/RES/32/13.
[vii]A/HRC/17/27.
[viii]A/HRC/17/27.
[ix]A/HRC/17/27, para. 66.
[x]A/HRC/32/L.20, para. 5.
[xi]General Comment No. 34, para. 15; See also, https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html.
[xii]Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24 June 2013) ('GGE Report 2013') 8 [19].
[xiii]Cf US, International Strategy for Cyberspace (n 24) 9.
[xiv]e.g., A/HRC/RES/20/8; A/HRC/RES/38/7; see also GA resolution A/RES/68/167 for the same affirmation for the right to privacy.
[xv]Article 19, Convention on the Rights of the Child, 1989, entered into force on 2 September 1990.
[xvi]Office of the United Nations High Commissioner for Human Rights, Legislative History of the Convention on the Rights of the Child (United Nations 2007), vol II, 512-521.
[xvii]Among others, it defines sexual harassment "Sexual harassment includes such unwelcome sexually determined behaviour as physical contact and advances, sexually colored remarks, showing pornography and sexual demands, whether by words or actions. Such conduct can be humiliating and may constitute a health and safety problem; it is discriminatory when the woman has reasonable ground to believe that her objection would disadvantage her in connection with her employment, including recruitment or promotion, or when it creates a hostile working environment." (Art. 11.18)
[xviii]"OHCHR | Human Rights Committee." https://www.ohchr.org/en/hrbodies/ccpr/pages/ccprindex.aspx (February 26, 2020).
[xix]"OHCHR | Committee against Torture." https://www.ohchr.org/en/hrbodies/cat/pages/catindex.aspx (February 26, 2020).
[xx]International Covenant on Civil and Political Rights, 1996
[xxi]Convention against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment, 1984.
[xxii]In 2020, the global community will mark the twenty-fifth anniversary of the Fourth World Conference on Women and adoption of the Beijing Declaration and Platform for Action (1995). A five-year milestone will be reached towards achieving the Sustainable Development Goals of the 2030 Agenda for Sustainable Development.
[xxiii]"Association for Progressive Communications | Internet for Social Justice and Sustainable Development." https://www.apc.org/ (February 26, 2020).
[xxiv]UN-GA resolution A/RES/68/167.
[xxv]The Charter of the United Nations of 1945 is the foundational treaty of the United Nations, an intergovernmental organization. See details at https://www.un.org/en/sections/un-charter/un-charter-full-text/ accessed on 28th November 2019
[xxvi]Constitution of the International Telecommunication Union (concluded 22 December 1992, entered into force 1 July 1994) 1825 UNTS 143 (hereinafter 'ITU Constitution').
[xxvii]Council of Europe, Convention on Cybercrime (signed 23 November 2001, entered into force 1 July 2004) ETS 185.
[xxviii]Council of Europe, Additional Protocol concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (opened for signature 28 January 2003, entered into force 1 March 2006) ETS 189.
[xxix]Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security ('Yekaterinburg Agreement') (signed 16 June 2009, entered into force 5 January 2012).
[xxx]African Union Convention on Cyber Security and Personal Data Protection (signed 27 June 2014) AU Doc EX.CL/846(XXV).

[xxxi]Convention on Cybercrime, European Treaty Series No. 185 of 23.XI.2001 (n 42) Arts 2–10.
[xxxii]ITU Constitution (n 41) Art 45 (prohibiting harmful interference) and Annex (defining harmful interference).
[xxxiii]Yekaterinburg Agreement (n 44), *Ibid*.
[xxxiv]See also, Henry Rõigas, 'Mixed Feedback on the "African Union Convention on Cyber Security and Personal Data Protection"', CCD COE INCYDER Database (20 February 2015) https://ccdcoe.org/ mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html; also see, Kubo Mačák, Is the International Law of Cyber Security in Crisis?, 2016 © NATO CCD COE Publications, Tallinn.
[xxxv]e.g., see *Mouvement raelien Suisse v. Switzerland* , 2012; *M.C. v. Bulgaria* , 2003; *Perrin v. United Kingdom* , 2003 *; K.U. v. Finland* , 2008.
[xxxvi]UNESCO, "Cyber Violence against Women and Girls: A World-Wide Wake-Up Call" (2015)
[xxxvii]See, https://ucollege.wustl.edu/files/ucollege/imce/iap.kabance.drp_.pdf; See also, https://en.unesco.org/sites/default/files/genderreport2015final.pdf
[xxxviii]http://www.vawlearningnetwork.ca/sites/vawlearningnetwork.ca/files/LN_Breif_28.pdf
[xxxix]Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences
[xl]The Association for Progressive Communications, p. 1
[xli]Cyber Misogyny http://www.vawlearningnetwork.ca/sites/vawlearningnetwork.ca/files/LN_Breif_28.pdf
[xlii]Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences
[xliii]Jan Moolman "Tracking violence against women in online spaces" Inter Press Service (IPS) Africa 2011 www.ips.org/africa/2011/04/tracking-violence-against-women-in-online-spaces/
[xliv]The above table is a quick overview of the existing provisions undertaken through desk research and is not exhaustive list.
[xlv]Source: UN Women global flagship program initiative (FPI).
[xlvi]Rashida Manjoo Report of the Special Rapporteur on violence against women, its causes and consequences
[xlvii]Gus Hosein "Privacy and Security", in *The APC ICT policy handbook* ed. David Souter (Association for Progressive Communications, 2009) www.apc.org/en/system/files/APCHandbookWeb_EN.pdf

Acknowledgements
This background paper has been informed by the discussions from an International Youth Conference co-organized by UN Women and other UN agencies in Africa and hosted at the United Nations Office in Nairobi in October 2018. The conference involved Six UN agencies and other external stakeholders. The agencies collaborating on the initiative included: Regional Service Centre, UNFPA, UNICEF, UNESCO, UN Environment, UNIC, FAWE, Africa Alliance of YMCA and Youth Agenda. These partnerships yielded high impact programming through development of a joint theory of change that petitioned African governments to prioritize investment in youth in light of the SDGs. The conference was a three-day continental conference which brought together 370 youths with 60 per cent being female. In addition, 81 per cent of the panelists and moderators were below 35 years of age, with 65 per cent of the being female. The conference was spearheaded by a 21 Member-Youth Only Steering Committee. It was further strengthened by a Knowledge Seminar on the Role of Student Leadership in Ending Technology-assisted Violence Against Women and Girls (TVAW) in Universities and the Academia. The seminar convened 70 student leaders from 30 universities across Kenya to dialogue on their role in ending technology-assisted violence against women and girls in Kenya and Africa. The seminar was co-hosted by UN Women and Maseno University Institute of Gender Studies-led by Dr. Karen Nyambura, Director for the Institute of Gender Studies, Maseno University. We appreciate the review and inputs by various stakeholders who reviewed and provided technical inputs in the finalization of the paper. This paper has been developed by Sadiq Ahamad Jilani Syed, Jack Onyisi Abebe, Michael Faraday Awino, Susan Kariuki and Martha Wanjala under the overall leadership of Zebib Kavuma-Deputy Regional Director-UN Women East and Southern Africa.

The research is funded and led by UN Women East and Southern Africa Regional Office. UN Women is the UN Agency dedicated to gender equality and the empowerment of women. As a global champion for women and girls, UN Women was established to accelerate progress on meeting their needs worldwide. With a vision of equality enshrined in the Charter of the United Nations, UN Women works for the elimination of discrimination against women and girls; the empowerment of women; and the achievement of equality between women and men as partners and beneficiaries of development, human rights, humanitarian action and peace and security. UN Women also coordinates and promotes the UN system's work in advancing gender equality, and in all deliberations and agreements linked to the 2030 Agenda. The entity works to position gender equality as fundamental to the Sustainable Development Goals, and a more inclusive world. It supports UN Member States as they set global standards for achieving gender equality and works with governments and civil society to design laws, policies, programmes and services needed to ensure that the standards are effectively implemented

and truly benefit women and girls worldwide. It works globally to make the vision of the Sustainable Development Goals a reality for women and girls and stands behind women's equal participation in all aspects of life. It has invested in its commitment to end all forms of violence, including child marriage, Female Genital Mutilation and other harmful practices against women and girls across the globe. UN Women envisions a world where societies are free of gender-based discrimination, where women and men have equal opportunities, where the comprehensive economic and social development of women and girls is ensured so that they can lead the change that they want to see, where gender equality and women's empowerment are achieved, and where women's rights are upheld in all efforts to further development, human rights, peace and security.