

Fighting Violence Against Women Online:

# A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda



Fighting Violence Against Women Online:  
**A Comparative Analysis of  
Legal Frameworks In Ethiopia, Kenya,  
Senegal, South Africa, and Uganda**

By Chioma Nwaodike and Nerissa Naidoo  
August 2020

This report was written and funded by Internews,  
in partnership with Pollicy.



**POLLICY**

# TABLE OF CONTENTS

04   Introduction	11   South Africa General Gender Equality Laws Criminal Laws Civil Remedies
05   Limitations	
06   International Instruments	14   Uganda General Gender Equality Laws Criminal Laws Civil Remedies
07   Overview of Domestic Regulatory Frameworks	
07   Ethiopia General Gender Equality Laws Criminal Laws Civil Remedies	15   Regulatory Issues
	18   Conclusion
08   Kenya General Gender Equality Laws Criminal Laws Civil Remedies	19   Recommendations
	20   Acknowledgments
10   Senegal General Gender Equality Laws Criminal Laws Civil Remedies	21   About the Authors
	22   Footnotes

# I. INTRODUCTION

Gender-based violence (GBV) remains one of the most pervasive structural issues across cultures, classes, and countries.<sup>1</sup>The Internet is not exempt from this, and the so-called real world inequalities and vulnerabilities borne by women are reflected in the digital sphere. In some cases, they are even exacerbated by it. Studies show that women are more likely than men to experience online violence and face more severe and consequential forms of it.<sup>2</sup>

Although a universal definition of online GBV does not exist, it can be described as “an action facilitated by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms, which is carried out by using the internet or mobile technology.”<sup>3</sup>Online GBV has the familiar manifestations of existing gender-based oppression, including stalking, harassment, intimidation, defamation, bullying, exploitation and blackmail. Rooted in the same patriarchal systems, online GBV should not be seen as a separate phenomenon but as occurring on the continuum of GBV in society, with online and offline violence facilitating and mimicking each other. At the same time, the “borderless” nature of the Internet, its potential as a tool for rapid dissemination and wide access, and the relative anonymity it affords perpetrators means that the impact of online GBV is particularly acute and far-reaching.<sup>4</sup>

Policymakers tasked with addressing GBV at a regulatory level are required to reconcile both the common and exceptional characteristics of online GBV; GBV is not unique to the Internet, but laws have to be designed to accommodate the unique capabilities of the Internet in furthering GBV both online and offline. The effective achievement of these demands reflects an appreciation of the role of the Internet in the social, economic, and political lives of women and the different ways in which different women interact with it. However, research on the existence and impact of online GBV is outpaced by the frequency with which it occurs, raising the question of whether national-level regulatory frameworks are at all equipped to protect women’s rights online.

Pollicy’s latest endeavor, “Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet,”<sup>5</sup> documents and analyzes the online experiences of women in Ethiopia, Kenya, Senegal, South Africa, and Uganda. To support advocacy and policy change, this report looks at the legal frameworks governing online GBV or the lack thereof. Since none of these countries have an online GBV-specific statute, this report considers each country’s general provisions on gender equality; its criminal laws, including cybercrime laws, which can be construed to cover certain acts of online GBV; and the civil remedies available to victims of online GBV.

## II. LIMITATIONS

This report is an overview of the legal frameworks governing online GBV in Ethiopia, Kenya, Senegal, South Africa, and Uganda and is not to be considered legal authority. It includes national-level legislation, regulations, policies, and cases, where available. Legal resources from these countries are not always readily accessible online, and cases of this nature are not always publicly reported. Our research suggests that online GBV cases rarely make it to the courtroom at all. These factors have limited our analysis of the implementation of these frameworks.

Similarly, we recognize that legal frameworks are rarely fully representative of the practical realities in any country. South Africa, for example, boasts “progressive” GBV laws yet maintains one of the highest GBV incidence rates in the world. Specific laws addressing online GBV are not the ultimate solution to a systemic problem and need to be adopted in conjunction with other measures, such as socio-economic upliftment and awareness-raising programs.



We recognize that legal frameworks are rarely fully representative of the practical realities in any country.

### III. INTERNATIONAL INSTRUMENTS

All five countries have ratified the International Covenant on Civil and Political Rights (ICCPR), which explicitly requires states to ensure that both men and women have equal enjoyment of the rights set out therein.<sup>6</sup> Article 26 asserts that the law must prohibit discrimination on the basis of, among other grounds, sex, and guarantees equal and effective protection from such discrimination. The ICCPR also recognizes the right to privacy, as well as the protection of honor and reputation.<sup>7</sup>

The African Charter on Human and People's Rights, to which all studied countries are party, also affirms equal enjoyment of fundamental rights regardless of, among other grounds, sex.<sup>8</sup>

All five countries have ratified the Convention on the Elimination of Discrimination Against Women (CEDAW). However, Ethiopia, Kenya, and Uganda have not ratified the CEDAW optional protocol, which grants authority to the CEDAW Committee to hear complaints from individuals and groups relating to violations of the CEDAW by a State Party. CEDAW requires all signatories to adopt gender equality laws. Although it does not mention online GBV specifically, in 2017, the CEDAW Committee issued General Recommendation No. 35, which recognized the following:



Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private. These include the family, the community, the public spaces, the workplace, leisure, politics, sport, health services, educational settings and *their redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the internet and digital spaces.* [emphasis added]<sup>9</sup>

## IV. OVERVIEW OF DOMESTIC REGULATORY FRAMEWORKS

### ETHIOPIA

#### GENERAL GENDER EQUALITY LAWS

The Constitution of Ethiopia enshrines the right to equality and guarantees equal protection under the law generally.<sup>10</sup> Article 35, however, explicitly asserts that women are entitled to the same rights as men, and additional “affirmative measures” address their historical inequality and discrimination.<sup>11</sup> Women, therefore, have a constitutional right to governmental action, which is specifically designed to protect and advance their position in society. Further, Article 35(4) prohibits any “[l]aws, customs and practices that oppress or cause bodily or mental harm to women.”<sup>12</sup> Therefore, the constitution broadly outlaws GBV and places a duty upon Ethiopian authorities to enact a regulatory framework that conforms to this stipulation.

#### CRIMINAL LAWS

The Criminal Code prohibits acts that cause bodily injury or impairment of health, including mental health.<sup>13</sup> It also prohibits intimidation,<sup>14</sup> threats,<sup>15</sup> coercion,<sup>16</sup> defamation,<sup>17</sup> extortion,<sup>18</sup> blackmail,<sup>19</sup> and instigation to commit suicide.<sup>20</sup> Article 710 acknowledges that these acts remain crimes punishable under the Criminal Code even when committed through the use of a computer.<sup>21</sup>

The Computer Crime Proclamation recognizes that existing laws inadequately address crimes committed through the use of information and communications technology (ICT). Article 13 criminalizes online activities that intimidate; threaten;<sup>22</sup> or cause fear, threat, or psychological strain.<sup>23</sup> As such, this article applies to online GBV. The dissemination of content that damages reputation or honor is also prohibited.<sup>24</sup> In addition, the Computer Crime Proclamation places a duty on Internet service providers (ISPs) to remove any criminal content once they are aware that it exists.<sup>25</sup>



*The Criminal Code prohibits acts that cause bodily injury or impairment of health, including mental health*

In 2020, the legislature enacted the Hate Speech and Disinformation Prevention and Suppression Proclamation, which prohibits “speech that deliberately promotes hatred, discrimination or attack against a person or a discernable group of identity, based on ethnicity, religion, race, gender or disability” on social media via text, audio, images, or video.<sup>26</sup> However, political speech and religious teachings are exempt from this.<sup>27</sup> The proclamation also imposes harsher punishments on perpetrators who have more than 5,000 social media followers.<sup>28</sup> Furthermore, it states that ISPs should work to suppress or prevent the dissemination of disinformation and hate speech online but does not impose an obligation on them to do so.<sup>29</sup> Article 8(5) places a duty on the Ethiopian Human Rights Commission to conduct public awareness campaigns on hate speech; however, as of this report, these campaigns have not yet been conducted.

## CIVIL REMEDIES

Victims may also bring a civil suit for defamation under the Civil Code.

# KENYA

## GENERAL GENDER EQUALITY LAWS

The Constitution of Kenya places a duty on all state organs and public officials to address the needs of vulnerable groups, including women.<sup>30</sup> Men and women have the right to equal treatment and opportunities,<sup>31</sup> and discrimination on the basis of sex is prohibited.<sup>32</sup> The state has a further duty to enact legislation designed to redress any historical disadvantages suffered by marginalized groups, including women.<sup>33</sup>

## CRIMINAL LAWS

The Penal Code outlaws incitement to violence,<sup>34</sup> threats to kill,<sup>35</sup> intimidation,<sup>36</sup> and any general act that causes harm to another.<sup>37</sup> These could apply to acts of online GBV, but the Penal Code does not explicitly state this nor is it clear the extent to which these offences apply to the digital sphere. Article 181 of the Penal Code prohibits the circulation of “obscene” photographs, videos or other media; this is replicated in the Computer Misuse and Cybercrimes Act, which prohibits the digital transfer or publication of “intimate or obscene” images.<sup>38</sup> Definitions are not provided for obscene or intimate in either statute, and the court has held that what constitutes “obscene” or “intimate” is to be judged on a case-by-case basis.<sup>39</sup>

The Computer Misuse and Cybercrimes Act also prohibits the intentional publication of false information that amounts to an advocacy of hatred on the basis of, among other grounds, gender<sup>40</sup> as well as the publication of false information that results in panic or violence or discredits the reputation of a person.<sup>41</sup> Article 27 deals with cyber harassment and states the following:

- (1) A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—
- (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or
  - (b) detrimentally affects that person; or
  - (c) is in whole or part, of an indecent or grossly offensive nature and affects the person.<sup>42</sup>

Cyber harassment carries a penalty of up to 10 years in prison and/or a fine.<sup>43</sup> The court may order an ISP to provide information relevant to identifying the accused.<sup>44</sup>

The Sexual Offences Act prohibits sexual harassment,<sup>45</sup> but this crime is narrowly defined to apply only in situations of power or authority imbalances, such as in the workplace. Furthermore, it is unclear whether this applies to online conduct as well.

## CIVIL REMEDIES

In addition to criminal cyber harassment proceedings, a victim may approach the court for an order that the accused refrain from further harassing or attempting to harass him/her.<sup>46</sup> Victims may also bring a civil suit for defamation under the common law supported by the provisions of the Defamation Law.

**The Sexual Offences Act prohibits sexual harassment, but this crime is narrowly defined to apply only in situations of power or authority imbalances, such as in the workplace**

# SENEGAL

## GENERAL GENDER EQUALITY LAWS

The Preamble of the Constitution of Senegal expressly affirms the country's adherence to, among other international human rights instruments, the CEDAW. It also assures the equality of all citizens under the law without distinction on the basis of origin, race, sex, or religion.<sup>47</sup> Article 7 states that men and women have equal rights and that the law promotes equal access to these rights.

## CRIMINAL LAWS

Senegal's Criminal Code criminalizes libel, which is loosely defined as "injury to honor."<sup>48</sup> It also outlaws threats of violence and threats for the purposes of solicitation.<sup>49</sup> Article 319bis prohibits harassment for sexual favors by someone with authority.

Article 256 prohibits the manufacture, distribution, or making available of content that is "contrary to good morals."<sup>50</sup> This is further affirmed by the 2016 Law Amending the Criminal Code, which specifically prohibits the online production and dissemination of documents or images that are "contrary to good morals."<sup>51</sup> In such cases, the court may order the blocking of the website or the infringing of the content and restrain the guilty party from further electronic communication.<sup>52</sup> In addition, the Cybercrime Law outlaws "immoral content" and designates pornography as the subset of this content that attracts the highest penalty.<sup>53</sup> The 2008 Decree on Electronic Communications requires ISPs to inform authorities of any "manifestly illicit content," including "content of a pornographic character" and content that is "clearly attacking the public order or good morals."<sup>54</sup> However, the standard of "good morals" is not defined in any of these statutes.

The Cybercrime Law generally outlaws xenophobic and racist content<sup>55</sup> and specifically mentions threats to commit hate crimes on the basis of race, color, ancestry, nationality, ethnicity, or religion<sup>56</sup> and abuse on these grounds.<sup>57</sup> This is also reflected in the 2016 Law Amending the Criminal Code.<sup>58</sup> Hate on the grounds of gender is not recognized in Senegalese criminal law.

Under the 2016 Law Amending the Criminal Code, it is a crime to intentionally violate other people's right to privacy by sharing their private images without their consent.<sup>59</sup> This includes the editing of their private images.

## CIVIL REMEDIES

Victims can sue for defamation under Senegalese common law.

# SOUTH AFRICA

## GENERAL GENDER EQUALITY LAWS

Non-sexism is one of the founding values upon which South Africa's post-apartheid constitutional dispensation was built.<sup>60</sup> The South African Constitution upholds equality under the law and equal protection of the law<sup>61</sup> and places a duty on the state to enact legislation that outlaws unfair discrimination on the basis of gender.<sup>62</sup>

One of those laws is the Promotion of Equality and Prevention of Unfair Discrimination Act, commonly known as the Equality Act. The Equality Act is a legislative recognition of the systemic inequalities caused by the patriarchy, and it affirms South Africa's obligations under CEDAW. Both considerations are relevant in interpreting the provisions of the Equality Act<sup>63</sup> to ensure the eradication of gender discrimination and inequality "in all spheres of life."<sup>64</sup>

The Equality Act explicitly outlaws GBV,<sup>65</sup> and harassment.<sup>66</sup> Gender is also one of the grounds on which hate speech is prohibited.<sup>67</sup> The remedies under the Equality Act are wide ranging and civil in nature, including monetary damages for pain and suffering,<sup>68</sup> restraining orders,<sup>69</sup> and unconditional apologies.<sup>70</sup> The Equality Court may also refer the matter to other institutions for further investigation.<sup>71</sup> The provisions of the Equality Act have previously been applied to online behavior related to other grounds of discrimination, such as race and sexual orientation. As such, these provisions would presumably extend to online GBV as well.

The South African government explicitly acknowledged online GBV in the National Strategic Plan on GBV & Femicide 2020–2030. Online violence against women is defined as:

any act of gender-based violence against a woman that is committed, assisted or aggravated in part or fully by the use of Information and Communications Technology (ICT), such as mobile phones and smartphones, the internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.<sup>72</sup>

Within the next five years, the government plans to conduct studies on the impact of online violence against women and roll out cyber violence awareness programs and strategies to respond to online GBV.

## CRIMINAL LAWS

The South African common law offence of assault includes not only physical impairment of another but also an act that inspires the belief or fear that such impairment is imminent. Online GBV that manifests as threats to the bodily integrity of women can fall under this category.

Another applicable common law offence is *crimen injuria*: the unlawful and intentional impairment of another's dignity. *Crimen injuria* has been applied to online activity in recent years, most notably to racist tweets and Facebook posts; this would presumably extend to certain instances of online GBV as well.

Part II of the Cybercrimes Bill, which has yet to successfully pass both houses of Parliament, governs malicious communications. The bill proposes a prohibition on the sending or making available of data messages with the intention of inciting violence against a person or group.<sup>73</sup> A message need not actually incite the violence contemplated; the intention of the sender is sufficient for a crime to occur. The bill also proposes a prohibition on the sharing of data messages that threaten a person or group with violence.<sup>74</sup>

The non-consensual sharing of intimate images via data messages is also outlawed under the malicious communications section of the proposed bill.<sup>75</sup> An offence is committed if the image is shared without the consent of the person who can be identified in the data message,<sup>76</sup> the person who is described as displayed in the data message even if he/she cannot be identified in the message alone,<sup>77</sup> and any person who, from other information, can be identified as being displayed in the data message.<sup>78</sup> This protection for victims is extended further, as "intimate images" include both real and simulated images.<sup>79</sup> They also include images in which the victim is not nude but his/her body is nevertheless displayed "in a manner that violates or offends" his/her sexual integrity or dignity<sup>80</sup> as well as other images for which the victim retains a reasonable expectation of privacy.<sup>81</sup>

The Cybercrimes Bill also proposes punishing those who assist in the commission of these crimes.<sup>82</sup> Commission of one of the crimes under malicious communications carries a sentence of up to three years of imprisonment,<sup>83</sup> and the court is also obligated to order the convicted person to destroy the data message in question or refrain from further distribution of it.<sup>84</sup> The court may also order ISPs to disable access to the message.<sup>85</sup> If the court is of the opinion that the behavior of the accused falls under the definition of harassment, as stipulated in the Protection from Harassment Act, the court may issue a protection order to the victim in accordance with the terms of the Harassment Act regardless of whether the accused is convicted or acquitted.<sup>86</sup>

Even before the finalization of the criminal proceedings, the victim may approach the court for an order restraining the accused or compelling ISPs to disable access to the content.<sup>87</sup> ISPs that fail to comply are also subject to criminal penalties.<sup>88</sup>

The Cybercrimes Bill also proposes the inclusion of the crime of “harmful disclosure of pornography” in the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.<sup>89</sup>

Although the Cybercrimes Bill has not yet been enacted, non-consensual sharing of intimate photography and film is currently outlawed under the Film and Publications Amendment Act.<sup>90</sup>

## CIVIL REMEDIES

In addition to the Equality Act’s civil remedies, a number of other avenues are available to victims of online GBV. The Protection from Harassment Act includes “electronic” communication under its definition of harassment, which also encompasses sexual harassment. A victim of harassment, referred to as a complainant, may approach the court for a protection order,<sup>91</sup> which restrains the other party from engaging in harassment<sup>92</sup> and enlisting others to assist in harassment of the complainant,<sup>93</sup> or any other order the court deems necessary for the safety of the complainant.<sup>94</sup> ISPs have a duty to furnish the court with the Internet Protocol (IP) address, identity of the sender of the harassing communications, or any other information relevant to determining the sender’s identity.<sup>95</sup>

Victims may also bring a civil suit for defamation under common law.

The Cybercrimes  
Bill also proposes  
the inclusion of the  
crime of “*harmful  
disclosure of  
pornography*”

# UGANDA

## GENERAL GENDER EQUALITY LAWS

Uganda's Constitution affirms that all people are equal under the law, have equal protection of the law, and are equal in all spheres of life.<sup>96</sup> It also prohibits discrimination on the basis of sex.<sup>97</sup> Section 33 enshrines the rights of women; the state has a constitutional duty to protect women and their rights,<sup>98</sup> and any laws, cultures, customs, or traditions contrary to women's dignity and interest are prohibited.<sup>99</sup> The constitution further provides that, if a person's fundamental right is infringed, his/she is entitled to approach a competent court for redress.<sup>100</sup>

## CRIMINAL LAWS

Under the Penal Code, it is an offence to threaten violence,<sup>101</sup> incite violence on the basis of, among other grounds, sex,<sup>102</sup> traffic in obscene publications for the purpose of trade,<sup>103</sup> cause another to die by suicide due to threats of violence,<sup>104</sup> or attempt extortion by threats.<sup>105</sup> Libel is also a crime in Uganda, and it applies to content which "exposes a person to hatred, contempt, or ridicule."<sup>106</sup> Although these offences do not target online GBV specifically, if the Penal Code is found to apply to online conduct, then threats, the non-consensual sharing of intimate images, or misogynistic speech against women, can be addressed under the Penal Code.

The Computer Misuse Act prohibits cyber harassment, which is defined as using a computer to make "any request, suggestion or proposal which is obscene, lewd, lascivious or indecent" or to threaten to injure someone.<sup>107</sup> However, definitions of obscene, lewd, lascivious, and indecent are not provided.

The Act also outlaws offensive communication, which amounts to the intentional and repeated disturbance of the peace or a person's privacy with no purpose of legitimate communication.<sup>108</sup> Cyber stalking, defined as the willful, malicious, and repeated use of electronic communication to harass or threaten, is prohibited.<sup>109</sup>

The Anti-Pornography Act states that it is an offence for a person to "produce, traffic in, publish, broadcast, procure, import, export, sell or abet [pornographic material] in any form."<sup>110</sup>

## CIVIL REMEDIES

Under the Computer Misuse Act, in addition to the prescribed punishments ranging from fines to years of imprisonment, the court must order the payment of compensation to the victim.<sup>111</sup> Victims of online GBV may bring a civil suit for defamation under the common law.

## V. CHALLENGES IN REGULATION

Ethiopia, Kenya, Senegal, South Africa, and Uganda have mechanisms in place to address the kinds of conduct that characterize online GBV. However, the absence of specific laws to address online GBV can be read as a failure of these countries to live up to their constitutional obligations. The constitution of each country explicitly affirms both gender equality and non-discrimination and places a duty on the government to enact legislation that addresses historic inequalities in society—specifically those faced by women. The urgent and imperative nature of this issue is not reflected in government action; general criminal or GBV laws do not adequately account for how the architecture of the Internet exacerbates the impact of certain conduct, while general cyberlaws center on the technical aspects of the crime rather than its human consequences. Provisions that are scattered across different statutes require more than an average person’s knowledge of the law to piece together, and it is unreasonable to expect women to meet this standard simply in order to protect themselves.

The loose provisions also engender a lack of legislative recognition that online GBV warrants an authoritative response or, worryingly, a lack of will to address it.<sup>112</sup> This, in turn, dilutes the possible deterrence effects that criminal laws might have on infringing behavior and reduces the efficacy of prescribed remedies. The ineffectiveness of these ambiguous laws is also apparent from the absence of case law regarding online GBV in the studied countries; the laws may exist, and, in some instances, the laws may be commendable—such as placing a duty on ISPs to assist the court with overcoming the anonymity hurdle—however, cases are nevertheless severely underreported or trivialized by law enforcement and social media platforms. In research by Pollicy, women reported that they either did not know there were remedies available to them or were insulted or laughed at by authorities when they tried to lay a complaint.<sup>113</sup> This careless, corrupt attitude is only perpetuated by the failure to throw the might of the law behind combatting online GBV.

Furthermore, the limited portfolio of civil remedies means that the governmental strategies for eliminating online GBV are not survivor-centered. Instead, online GBV is mostly left up to a criminal justice system designed on philosophies of punishment—a system in which women are often the victims.

Defamation is the civil remedy against online GBV that is available to women across all five countries; however, even this remedy is not designed to adequately respond to online GBV. Defamation compensates a victim for injury to his/her honor and reputation—standards defined in the context of the patriarchal society and standards to which women are often held hostage. Online GBV is deeper than this; honor and reputation are weaponized online through “slut”-shaming and other abuses; by forcing women to seek redress by upholding these standards, we further perpetuate them. Online GBV is not merely an injury to a woman’s dignity in the eyes of a society; online GBV is an injury to a woman’s dignity because of the society in which she is marginalized by virtue of being a woman. Cyberviolence has a long-term impact on the mental health of women, some of whom have reported psychiatric hospitalization, addiction, and suicide attempts in response to harassment, malicious rumors, and threats online.<sup>114</sup> Women live in fear for their safety and self-censor themselves, due to online threats, and some even lose their jobs because of content shared without their consent. Sometimes, all of these consequences manifest from a single act of online GBV. Defamation is an expensive tool that simply does not have the necessary range.<sup>115</sup>

In addition, reaching out to ISPs and social networks has not been a fruitful endeavor. Similar to the content-based restrictions imposed in countries, such as Senegal, social networks and ISPs operating in Africa tend to prioritize the removal of hate speech on the grounds of ethnicity and religion rather than gender.<sup>116</sup> Moreover, many of the cybercrime laws fall short of obligating ISPs to actively monitor and disable access to misogynistic speech or to provide assistance in combating online GBV. In South Africa, a 13-year-old girl approached the High Court for an order requiring Facebook, Inc. to reveal the identity of the person who sent her graphic threats of gang rape and murder on Instagram.<sup>117</sup> It took months of costly legal maneuvers to simply have the High Court serve papers on the company in California. If governments lack the capacity to monitor content on social media or investigate these crimes, they should be leveraging companies operating within their jurisdiction that do have this capacity. A failure in this regard further limits the avenues for redress available to women.

On a broader level, a limited understanding of the profound impact of GBV on women, and the failure to take appropriate action to restore their agency is likely to actively harm them. For example, provisions, such as those that prohibit “obscene” content or consensual pornography, are rooted in patriarchal conceptions of “morality” in which the sexuality of women is policed rather than protected. For example, an artist in Senegal was arrested and charged with “indecent and violation of good morals” because of the clothing she wore in a Snapchat video.<sup>118</sup> The complaint was laid by a religious organization, and, although the Cybercrime Code recognizes the role of religion in other forms of prejudice, this evidently does not extend to women.

Laws enacted under the auspices of protecting vulnerable groups, such as women, including hate speech and disinformation laws, have also been used to silence them. Legitimate limitations on free expression are exploited by governments to target dissidents, especially human rights defenders and journalists who speak out against abuses of power or maladministration. It is well documented that journalists who are women disproportionately face harassment, death threats, and doxxing for their reporting, jeopardizing their physical safety and job security. In 2019, Ugandan activist and writer Stella Nyanzi was sentenced to 18 months in prison for cyber harassment for posting a poem about the president on Facebook. In 2020, those charges were quashed on procedural grounds. Previously, Nyanzi had been jailed for 33 days for criticizing the president after he backed out on a promise to provide free sanitary towels for schoolgirls.<sup>119</sup>

Moreover, there are explicit and implicit qualifications to the provisions that purport to protect women but actually further entrench their vulnerability, including exceptions related to religious teachings and the criminalization of homosexuality and sex work. Minorities bear the brunt of vague punitive laws, and it is worse for women with intersecting oppressions.

Governments are effectively outsourcing to women the duty to protect themselves from violence—a nod to the victim blaming that so often occurs in the “real” world.<sup>120</sup> Women already have to overcome the digital divide stemming from the money, time, and skills needed to access the Internet at all; they now also have to fight for their right to remain there at great cost,<sup>121</sup> including by changing their passwords, using Virtual Private Networks (VPNs), and censoring their opinions and sexuality. Specific online GBV laws are therefore necessary to provide tailored relief to women, including appropriate measures to genuinely mitigate the impact of online GBV on their social, economic, political, and emotional lives.

## VI. CONCLUSION

The highest levels of regulation, from international treaties to constitutions, are unambiguous about creating an environment in which women thrive. However, this egalitarian space must be progressively realized, and one aspect of this work is eliminating discrimination, including in relation to GBV. Whether authorities care to admit it or not, the Internet is an inseparable part of the society in which we live, and online GBV demands a resolute hand. Unfortunately, the gaps in legal frameworks, not to mention deficient law enforcement, are forcing women to self-censor online or even wholly abandon platforms that could be used for legitimate expression and the exercise of other fundamental rights. Unless governments take urgent, comprehensive action, the inadequate protection of women's rights online will continue to erode any other legislative attempts to achieve equality across different spheres of life.

The highest levels of regulation, from international treaties to constitutions, are unambiguous about creating an environment in which women thrive

## VII. RECOMMENDATIONS

We recommend that governments take the following actions to strengthen their legal frameworks and response to combatting online GBV:

- Enact women-centered legislation that specifically targets online GBV; protects the legitimate expression of women, including consensual sexual expression; and includes defined parameters and swift, simple enforcement and redress mechanisms;
- Review all laws that regulate online activity to ensure that they are consistent with and support the elimination of online GBV;
- Commission human rights civil society groups, think tanks, and other non-governmental organizations (NGOs) to conduct regular national-level research on online GBV and the effectiveness of laws and law enforcement;
- Enact stricter regulations requiring social media platforms and ISPs to adhere to international human rights standards, including CEDAW;
- Ratify the CEDAW Optional Protocol;
- Conduct training for law enforcement and the judiciary on the severity of online GBV, online GBV regulations, and how to effectively and sensitively handle online GBV cases;
- Provide all women, including those with added vulnerabilities, with information on how to recognize online GBV and the remedies available to them;
- Design the aforementioned measures in consultation with all affected parties, especially women across all classes and identities, civil society groups, and the ICT sector;
- Ensure all measures are grounded in the rights of freedom, autonomy, and the self-determination of women instead of moralistic or paternalistic values that essentialize “womanhood.”



*Provide all women, including those with added vulnerabilities, with information on how to recognize online GBV and the remedies available to them*

## ACKNOWLEDGEMENTS

Chioma is grateful to the experts who offered their time and insights for this report, and wishes to thank Haley Slafer, Neema Iyer, and Laura Schwartz-Henderson for their guidance, feedback, and support during this process.

Nerissa wishes to thank Vidaisha Naidoo and Grant Baker for their advice and positivity.

## ABOUT THE AUTHORS



### CHIOMA NWAODIKE

---

*Chioma Nwaodike* is the Internet policy fellow with Internews, an international non-profit organization that works to empower people worldwide with the trustworthy, high-quality news and information they need to make informed decisions, participate in their communities, and hold power to account. Previously, Chioma was a Legal Officer with Media Rights Agenda (MRA), a Nigeria-based

non-profit, where she worked extensively on freedom of information (FOI) litigation, research, capacity building, advocacy, and campaigns, as well as reviewing the Declaration on Principles of Freedom of Expression with the Special Rapporteur on Freedom of Expression and Access to Information in Africa. She was also part of the team of experts developing the FOI Civil Procedural Rules for High Courts in Nigeria. Chioma received her LL.M from the University of Lagos, and her bachelors' degree in law (LLB) from Babcock University in Nigeria.



### NERISSA NAIDOO

---

*Nerissa Naidoo* is a human rights fellow at SMEX, an NGO in Beirut that works regionally to defend digital rights across the Middle East and North Africa. Born and raised in South Africa, Nerissa received her undergraduate law degree summa cum laude from the University of KwaZulu-Natal. In 2018, she was awarded a Fulbright scholarship to attend Harvard Law School, where she received her LL.M

and was active in the International Human Rights Clinic, working on corporate accountability of mining companies in West Africa. She will be attending Oxford University beginning in the Fall of 2020 as a Rhodes Scholar, pursuing a Master of Science degree in the Social Science of the Internet program.

## FOOTNOTES

<sup>1</sup>United Nations (UN) Broadband Commission for Digital Development Working Group on Broadband and Gender (2015) *Cyber violence against women and girls: A world-wide wake-up call*. Available at:

[https://www2.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber\\_violence\\_gender%20report.pdf?v=1&d=20150924T154259](https://www2.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259)

<sup>2</sup>Womankind Worldwide (2018) *Breaking the silence: Ending online violence and abuse against women's rights activists*. Available at:

<https://www.womankind.org.uk/docs/default-source/default-document-library/breaking-the-silence-policy-briefing.pdf?sfvrsn=0>

<sup>3</sup>Pollicy (2020) *Alternate realities, alternate internets: African feminist research for a feminist internet*. Available at: insert link.

<sup>4</sup>UN High Commissioner for Human Rights (2018) *The impact of online violence on women human rights defenders and women's organisations*. Available at:

<https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23238&LangID=E>

<sup>5</sup>Pollicy (2020) *Alternate realities, alternate internets: African feminist research for a feminist internet*.

<sup>6</sup>International Covenant on Civil and Political Rights (1996), Article 3.

<sup>7</sup>Ibid, Article 17.

<sup>8</sup>African Charter on Human and People's Rights (1981), Article 2.

<sup>9</sup>UN Committee on the Elimination of Discrimination against Women (2017) *CEDAW General recommendation No.35 on gender-based violence against women, updating general recommendation No.19*, Article 20.

<sup>10</sup>The Constitution of the Federal Democratic Republic of Ethiopia (1995), Article 25.

<sup>11</sup>Ibid, Article 35(3).

<sup>12</sup>Ibid, Article 35(4).

<sup>13</sup>The Criminal Code of the Federal Democratic Republic of Ethiopia No. 414/2004, Article 553.

<sup>14</sup>Ibid, Article 580.

<sup>15</sup>Ibid, Article 581.

<sup>16</sup>Ibid, Article 582.

<sup>17</sup>Ibid, Article 613.

<sup>18</sup>Ibid, Article 713.

<sup>19</sup>Ibid, Article 714.

<sup>20</sup>Ibid, Article 580.

- <sup>21</sup>Ibid, Article 710.
- <sup>22</sup>Computer Crime Proclamation No. 958/2016, Article 13(1).
- <sup>23</sup>Ibid, Article 13(2).
- <sup>24</sup>Ibid, Article 13(3).
- <sup>25</sup>Ibid, Article 16.
- <sup>26</sup>Hate Speech and Disinformation Prevention and Suppression Proclamation No. 1185/2020, Article 4.
- <sup>27</sup>Ibid, Article 6(1).
- <sup>28</sup>Ibid, Article 7(4).
- <sup>29</sup>Ibid, Article 8(1).
- <sup>30</sup>The Constitution of Kenya (2010), Article 21(3).
- <sup>31</sup>Ibid, Article 27(3).
- <sup>32</sup>Ibid, Article 27(5).
- <sup>33</sup>Ibid, Article 27(6).
- <sup>34</sup>Kenya Penal Code Cap. 63 (2009), Article 96.
- <sup>35</sup>Ibid, Article 223.
- <sup>36</sup>Ibid, Article 238.
- <sup>37</sup>Ibid, Article 244.
- <sup>38</sup>Computer Misuse and Cybercrimes Act No. 5 of 2018, Article 37.
- <sup>39</sup>*Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR.
- <sup>40</sup>Computer Misuse and Cybercrimes Act No. 5 of 2018, Article 22.
- <sup>41</sup>Ibid, Article 23.
- <sup>42</sup>Ibid, Article 27.
- <sup>43</sup>Ibid, Article 27(2).
- <sup>44</sup>Ibid, Article 27(7).
- <sup>45</sup>The Sexual Offences Act No. 3 of 2006, Article 23.
- <sup>46</sup>Computer Misuse and Cybercrimes Act No. 5 of 2018, Article 27(3).
- <sup>47</sup>Constitution of the Republic of Senegal (Law No. 2001-03), Article 1.
- <sup>48</sup>Code Penal (Basic Law No. 65-60), Article 258.
- <sup>49</sup>Ibid, Articles 290-293.
- <sup>50</sup>Ibid, Article 256.
- <sup>51</sup>Law Amending the Criminal Code (Law No. 2016-29), Article 431.60.
- <sup>52</sup>Ibid, Article 431.61.
- <sup>53</sup>Cybercrime Law (Law No. 2008-11), Article 431.59.
- <sup>54</sup>Decree on Electronic Communications (Law No. 2008-08), Article 2(2).
- <sup>55</sup>Cybercrime Law (Law No. 2008-11), Article 431.38.
- <sup>56</sup>Cybercrime Law (Law No. 2008-11), Article 431.39.
- <sup>57</sup>Cybercrime Law (Law No. 2008-11), Article 431.40.

- <sup>58</sup>Law Amending the Criminal Code (Law No. 2016-29), Articles 431.42-43.
- <sup>59</sup>Ibid, Article 323bis.
- <sup>60</sup>The Constitution of the Republic of South Africa (1996), Section 1(b).
- <sup>61</sup>Ibid, Section 9(1).
- <sup>62</sup>Ibid, Sections 9(3)-(4).
- <sup>63</sup>The Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000, Section 3.
- <sup>64</sup>Ibid, Section 4(2)(a).
- <sup>65</sup>Ibid, Section 8(a).
- <sup>66</sup>Ibid, Section 11.
- <sup>67</sup>Ibid, Section 10.
- <sup>68</sup>Ibid, Section 21(2)(e).
- <sup>69</sup>Ibid, Section 21(2)(f).
- <sup>70</sup>Ibid, Section 21(2)(j).
- <sup>71</sup>Ibid, Section 21(4).
- <sup>72</sup>National Strategic Plan on Gender-Based Violence & Femicide 2020-2030 (2020), Page 12.
- <sup>73</sup>The Cybercrimes Bill (B6-2017), Section 14.
- <sup>74</sup>Ibid, Section 15.
- <sup>75</sup>Ibid, Section 16.
- <sup>76</sup>Ibid, Section 16(2)(a)(i).
- <sup>77</sup>Ibid, Section 16(2)(a)(ii).
- <sup>78</sup>Ibid, Section 16(2)(a)(iii).
- <sup>79</sup>Ibid, Section 16(b)(i).
- <sup>80</sup>Ibid, Section 16(2)(b)(i)(bb).
- <sup>81</sup>Ibid, Section 16(2)(b)(ii).
- <sup>82</sup>Ibid, Section 17.
- <sup>83</sup>Ibid, Section 19(7).
- <sup>84</sup>Ibid, Section 22(2).
- <sup>85</sup>Ibid, Section 22(2)(c).
- <sup>86</sup>Ibid, Section 22(1).
- <sup>87</sup>Ibid, Section 20.
- <sup>88</sup>Ibid, Section 23.
- <sup>89</sup>Ibid, Section 58.
- <sup>90</sup>Film and Publications Amendment Act 11 of 2019, Section 18F.
- <sup>91</sup>Protection from Harassment Act 17 of 2011, Section 2(1).
- <sup>92</sup>Ibid, Section 10(1)(a).
- <sup>93</sup>Ibid, Section 10(1)(b).
- <sup>94</sup>Ibid, Section 10(1)(c).
- <sup>95</sup>Ibid, Section 4(1).
- <sup>96</sup>Constitution of the Republic of Uganda (2005), Article 21(1).

- <sup>97</sup>Ibid, Article 21(2).
- <sup>98</sup>Ibid, Article 33(3).
- <sup>99</sup>Ibid, Article 33(6).
- <sup>100</sup>Ibid, Article 50(1).
- <sup>101</sup>The Penal Code Act Cap. 20 (1950), Article 81.
- <sup>102</sup>Ibid, Article 83.
- <sup>103</sup>Ibid, Article 166.
- <sup>104</sup>Ibid, Article 196.
- <sup>105</sup>Ibid, Article 291.
- <sup>106</sup>Ibid, Article 179.
- <sup>107</sup>The Computer Misuse Act 2011, Article 24.
- <sup>108</sup>Ibid, Article 25.
- <sup>109</sup>Ibid, Article 26.
- <sup>110</sup>The Anti-Pornography Act 2014, Article 13.
- <sup>111</sup>The Computer Misuse Act 2011, Article 27.
- <sup>112</sup>Association for Progressive Communications (2017) *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations special rapporteur on violence against women, its causes and consequences*. Available at: [https://www.apc.org/sites/default/files/APCSubmission\\_UNSR\\_VAW\\_GBV\\_0\\_0.pdf](https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf)
- <sup>113</sup>Pollicy (2020) *Alternate realities, alternate internets: African feminist research for a feminist internet*.
- <sup>114</sup>Ibid.
- <sup>115</sup>Association for Progressive Communications (2015) *From impunity to justice: Domestic legal remedies for cases of technology-related violence against women*. Available at: [https://www.genderit.org/sites/default/files/flow\\_domestic\\_legal\\_remedies\\_0.pdf](https://www.genderit.org/sites/default/files/flow_domestic_legal_remedies_0.pdf)
- <sup>116</sup>Pollicy (2020) *Alternate realities, alternate internets: African feminist research for a feminist internet*.
- <sup>117</sup>'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' in Daily Maverick on 24 July 2020. Available at: <https://www.dailymaverick.co.za/article/2020-07-24-anonymously-threatened-with-gang-rape-and-murder-sa-teenager-takes-facebook-inc-to-court-to-disclose-perpetrator/#gsc.tab=0>
- <sup>118</sup>Amnesty International (2017) *Analysis of the laws amending the criminal code and the code of criminal procedure*. Available at: <https://www.amnesty.org/download/Documents/AFR4960062017ENGLISH.PDF>
- <sup>119</sup>A/HRC/WGAD/2017/57 Opinion No. 57/2017 concerning Stella Nyanzi (Uganda).
- <sup>120</sup>Ibid.
- <sup>121</sup>World Wide Web Foundation (2015) *Women's rights online: Translating access into empowerment*. Available at: <http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf>