

Weak Legal And Institutional Framework;

A Hindrance To Justice For Survivors Of Online Violence Against Women And Girls In Uganda

December 2020

Implemented by:









Weak Legal And Institutional Framework;

A Hindrance To Justice For Survivors Of Online Violence Against Women And Girls In Uganda

December 2020

Implemented by:







Table of Contents

	Executive summary	2
	List of acronyms	3
	List of tables	3
	List of figures	3
	List of appendices	3
1.0	Introduction	4
2.0	General Objective	5
2.1	Specific Objectives	5
3.0	Problem Statement	5
4.0	Literature Review	6
5.0	Methodology	10
5.1	Scope of the research	10
6.0	Principle findings	11
6.1	Legislators and key informants	11
6.1.1	Technology-related violence – awareness and manifestation	11
6.1.2	Rationale for the occurrence of technology-related violence against women and girls	12
6.1.3	Existence of legal frameworks to provide effective justice to victims of online violence against women.	12
6.1.4	Legal remedies against online violence	13
6.1.5	Recommendations	14
6.2	General Public report	15
6.2.1	Demographics	16
6.2.2	Understanding of what technology-related violence against women and girls is all about	16
6.2.3	Experience with forms of technology-related violence	16
6.2.4	Recency of experience	17
6.2.5	Means of access to victims	18
6.2.6	Relationship with the offender	18
6.2.7	Social and psychological Impact of online violence	20
6.2.8	Reporting of cybercrimes and online violence to law enforcers	21
7.0	Recommendations	27
8.0	Appendices	28



Executive summary

The Internet is a unique space and is crucial for women to participate in given its importance for work, politics and social engagement therefore it's imperative that we advocate for the freedom to communicate and create safe online spaces.

Technology-related violence is just as damaging to women and girls as physical violence and it is estimated that 73% of women have endured cyber violence, with women being 27 times more likely than men to be harassed online. Existing laws, in several instances, are essentially no longer being enforced. The excessive time taken to file charges, delays in investigations, and the number of years that go by before a case is properly considered are some of the factors that make women survivors of technology-related violence desist from filing complaints.

This research sought to examine existing domestic legal remedies for survivors of technology-related violence against women to access to justice in Uganda. It was carried out between September and November 2020, and it involved conducting a comprehensive literature review to map out domestic legal remedies and adoption of a survey design, thus employing a multi-method approach.

More than half of the respondents interviewed knew that they could report the online violations they were experiencing, yet none of them reported the matter to police or even sought legal intervention. More than half of the respondents did not report because of fear and also confessed to not knowing who to report to.

The need for improved digital literacy among more women in Uganda and Africa is fundamental and should be supported with a thorough understanding of the online and offline social structures that could influence their willingness to actively participate in the online arena. Women should be aware of the options available to them in case they have been violated online. Massive awareness on online violence against women should be promoted in society so as to overcome the challenge of society's attitude of trivializing violence that happens in the online spaces.

Unwanted Witness would like to acknowledge the precious contributions made by the researchers in compiling this report. The organization is highly indebted to the respondents that survived online violence, officials from Uganda's Parliament, Uganda Police Force, the Judiciary and those from the Directorate of Public Prosecution who provided this important information. The organization is also indebted to its development partners, DW Akademie for their support in having this research undertaken.



List of acronyms

CEDAW	Committee on the Elimination of Discrimination against Women		
	Convention on the Elimination of All Forms of Discrimination against Women		
CID	Criminal Investigation Directorate		
GBV	Gender-based violence		
ICT	Information and communication technology		
Tech	Technology		
UPF	Uganda Police Force		
UN	United Nations		
UNESCO	United Nations Educational, Scientific and Cultural Organization		
VAW	Violence against Women		
VAWG	Violence against women and girls		

List of tables

Table		Page
Table 1:	Respondents' mention of legal remedies against online violence	13
Table 2:	Perceptions on best way to handle the issue of online violence against women	14
Table 3:	Age-groups under which respondents fell	15
Table 4:	Level of education of respondents	15
Table 5:	Respondents' experience of any form of technology-related violence	15
Table 6:	Form of technology-related violence experienced by respondents	16
Table 7:	Form of technology-related violence against women and girls experienced and the Internet platform used	16
Table 8:	Length of respondents' experience with technology-related violence	17
Table 9:	Ways in which offenders gained access to someone's online space	17
Table 10:	Victims' relationship with offender	18
Table 11:	Suspected reasons for online violence	18
Table 12:	Summary of relationship with offender, means of access to online space and possible reason	19
Table 13:	How online violence impacted the victims socially and psychologically	20
Table 14:	Reporting of online violence	21
Table 15:	Why survivors did not report online violence	22
Table 16:	Breakdown of Cybercrime Offences	

List of figures

Figure	Page
Figure 1: Legislators' level of awareness of technology-related violence	10
Figure 2: Legislators' knowledge of the existence of legal frameworks for victims of On	line 12
violence against women	
Figure 3: Public's level of awareness to report cybercrimes and online violence	21

List of appendices

Appendix		Page
Appendix A:	Questionnaire for members of the judiciary	23
Appendix B:	Questionnaire for survivors/ victims of online abuse	24



1. Introduction

Technology has enabled us to manage our daily lives with ease, especially when it comes to communication. With technology, we can efficiently communicate with our friends, families and others. ICT provides a fertile terrain that amplifies reach of transmission. With the help of new technologies, women around the world have benefited from outstanding possibilities on the Internet, both in terms of power and visibility and in terms of access and opportunities!

In May 2013, the UN Broadband Commission agreed to an ambitious new target designed to increase female access to ICT, calling for gender equality in broadband access by the year 2020. The goal was to use ICT to transform the lives of millions of women by giving them access to information and services in line with health, education, opportunities for income-generation, access to services, avenues for political participation and mobilization. In addition, it was noted that ICT could also be used to prevent and respond to violence against women, which depended on the Internet serving as a safe and welcome place for women. In line with that, this report addresses a critical issue in providing redress to victims/ survivors of violence against women.

According to UNESCO, violence against women and girls is already a problem of pandemic proportion, and it is manifested in forms such as domestic violence and technology-related violence. Research shows that one in three women will experience some form of violence in her lifetime. According to the Ministry of Gender, Labour and Social Development, a total of 3,280 cases of gender-based violence were reported to the Police between March 30 and April 28, 2020. Now, the new problem of tech-related VAWG could significantly increase this staggering number since we are seeing an increase in the usage of the Internet and technology in the COVID-19 period. UNESCO research shows that 73% of women have been exposed to or have experienced some form of online violence. With an upsurge of different social networks, this is a problem that urgently needs to be addressed if the Internet is to remain an open and empowering space for all².

³Technology-related violence against women involves acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of ICTs, such as phones, the Internet, social media platforms, and email. It can be broken down into three categories, ie, Pornography, Cyberstalking and Sexual harassment⁴. It has similar manifestations with the other existing forms of gender-based violence.

While gender-based violence is not a new phenomenon, the technology dimension adds elements of searchability, persistence, replicability and scalability which facilitate aggressors' access to women they are targeting and can escalate and exacerbate harm⁵.

Numerous international human rights instruments and documents state clearly and unequivocally that all forms of gender-based violence amount to discrimination, and seriously inhibit women's ability to enjoy their human rights and fundamental freedoms. There is no exception for violence against women perpetrated through the use of ICTs.

International law mandates states to exercise due diligence to promote, protect and fulfil human rights. This includes the obligation to prevent violations, protect victims/survivors of human rights abuses,

¹ Policy Department for Citizen's Rights and Constitutional Affairs (2018), *Cyber violence and hate speech online against women*, http://www.europarl.europa.eu/supporting-analyses.

² Final report of the Broadband Commission Working Group on Gender(2015), **Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call,** https://en.unes-co.org/sites/default/files/highlightdocumentenglish.pdf

 $^{3 \\ \}qquad \text{https://mglsd.go.ug/ministerial-press-statement-on-the-effects-of-covid-19-on-employment-and-gender-relations/} \\$

⁴ Women of Uganda Network (WOUGNET)[2018], Investigating Tech-Related Violence Against Women in Peri-Urban Areas of Uganda, https://www.apc.org/en/pubs/tech-re-lated-violence-against-women-peri-urban-areas-uganda

Association for Progressive Communications (APC) (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*, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf



prosecute violations, punish perpetrators, and provide redress and reparation for victims/survivors⁶. Research has shown that despite the existence of laws that can be applied in cases of technology-related VAW, the incompetence of duty bearers presents a significant barrier to women's access to justice. ⁷Law enforcement typically trivializes technology-related VAW and victim blaming is common among police personnel. This attitude results in a culture of silence, where survivors are inhibited from speaking out for fear of being blamed for the violence they have experienced.

2.0 General Objective

To examine how existing domestic legal remedies determine access to justice for survivors of technology-related violence against women in Uganda

2.1 Specific Objectives

- i) To identify available domestic remedies in case of technology-related violence against women in Uganda
- ii) To analyze the strengths and limitations of available domestic legal remedies in relation to women's experiences
- iii) To highlight the voices and experiences of survivors who have sought legal remedy and to identify insights from their experience

3.0 Problem Statement

⁸A United Nations report indicates that cyber violence is just as damaging to women and girls as physical violence; and estimates that women, of whom 73% have endured cyber violence, are 27 times more likely than men to be harassed online. Efforts to minimize and eradicate technology-related violence against women are on a largescale globally, although the issue remains an extensive and widely underrecognized form of human rights violation in African countries.

Research done globally on domestic legal remedies for cases of technology-related violence against women exposed a prevailing culture of impunity around these human rights violations. Some studies illustrated the superficial impression of a comprehensive breakdown in the criminal justice system, comprising the investigation, prosecution and adjudication of cases involving violence against women. The inefficiencies of the laws and the lack of government action were aggravated by gender insensitivity on the part of enforcers and service providers, which served to silence women instead of encouraging them to assert their rights.

Relevant laws, in several instances, were essentially dead letter legislation, i.e. laws that were no longer being enforced. The excessive time taken to file charges, delays in the investigations, and the number of years that passed before a case was properly considered were all factors that made women survivors desist from filing a complaint?

G Zarizana Abdul Aziz(2017), **Due Diligence and Accountability for Online Violence against Women**, APC. https://www.apc.org/en/pubs/due-diligence-and-accountability-online-violence-against-women

Association for Progressive Communications (APC) (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, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

⁸ Donald Flywell Malanga(2020), **Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic,** https://www.apc.org/en/pubs/tackling-gender-based-cyber-violence-against-women-and-girls-malawi-amidst-covid-19-pandemic

⁹ APC Women's Rights Programme(2015), Briefing paper on Violence Against Women. https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20 paper_FINAL_June%202015.pdf



4.0 Literature Review

Violence against women is a form of discrimination against women and a human rights violation highlighted in the Convention on the Elimination of All Forms of Discrimination against Women and other international and regional instruments, according to which violence against women includes gender-based violence, that is, violence directed against a woman because she is a woman and/or that affects women disproportionately¹⁰.

Article 1 of the Declaration on the Elimination of Violence against Women further specifies that violence against women is 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.

The definition of online violence against women, therefore, extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of 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.

The Sustainable Development Goals (SDGs), which established the global development priorities, include a goal on gender equality, which places women's access to technology for their empowerment as one of the core¹² indicators for progress. For this to be realized, all stakeholders must take accelerated actions to ensure a safer, more secure Internet for present and future generations. Increased prevalence of techrelated violence against women, the lack of effective measures to prevent and contain it, and the ensuing impunity must be addressed as part of the struggle for victims and survivors to access justice. The state has an obligation to promote, protect and fulfil human rights. This includes the obligation to prevent violations, protect victims/survivors of human rights abuses, prosecute violations, punish perpetrators and provide redress and reparation for victims/survivors. This also includes the obligation to remove impunity and provide for certainty of punishment of perpetrators of violence against women¹³.

Domestic legal remedies for technology-related violence against women in Uganda

Existing policy, legal and institutional framework

This part assesses the existing institutional, legal and policy frameworks on technology-related violence against women and establishes whether they have effectively contributed to accountability and redress for survivors. Uganda has a zero-tolerance standard towards gender-based violence in its domestic laws, policies, regional and international commitments. Technology-related violence against women, women's online participation and representation and domestic legal remedies for survivors' digital rights are provided for through these instruments. This section highlights some of the key provisions.

International laws

¹⁰ Convention on the Elimination of All Forms of Discrimination against Women (2017), General recommendation No. 35on gender-based violence against women, updating general recommendation No. 19, file:///C:/Users/Advocacy/AppData/Local/Temp/N1723154.pdf

Human Rights Council (2018), Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, https://digitallibrary.un.org/record/1641160?ln=en

¹² The 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, https://en.unesco.org/sites/default/files/genderreport2015final.pdf

Association for Progressive Communications (APC) (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, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf



Access to justice is a fundamental right guaranteed under Article 8 of the Universal Declaration of Human Rights: "Everyone has the right to an effective remedy by competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law." ¹⁴The right to access to justice is established and guaranteed as well by other international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

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 officials do not themselves engage in gender-based violence against women, but also that they take appropriate measures to prevent the infliction of violence by private actors, to investigate and sanction such actions and to provide protection and support for the survivors of violence. Increased prevalence of online violence against women, the lack of effective measures to prevent and contain it, and the ensuing impunity must be addressed as part of the struggle to eliminate all forms of gender-based violence.

At the UN level, the Committee on the Elimination of Discrimination against Women (the CEDAW Committee) articulated the obligations of states party to the Convention on the Elimination of All Forms of Discrimination against Women (the CEDAW Convention) to eliminate violence against women.

Other UN human rights treaty bodies, such as the Human Rights Committee and the Committee against Torture, have also made clear that states' obligations under the International Covenant on Civil and Political Rights 1966 (ICCPR) and the Convention against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment 1984 (CAT) include eliminating public and private violence against women. Regional human rights bodies have reached similar conclusions under their general human rights conventions.

Violence against women is perpetrated by both state and non-state actors. By making the state accountable for violence committed by both state and non-state actors, public international law recognizes that violence against women, regardless of who commits it, constitutes human rights violation. Uganda has not yet ratified the Optional Protocol to CEDAW. 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 that gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including in the contexts of the family, the community, public spaces, the workplace, leisure, politics, sport, health services and ¹⁶educational settings, and the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments.

Uganda ratified the Convention on the Elimination of Discrimination Against Women (CEDAW), therefore, it is only imperative to note that as digital spaces morph and develop, so too must the application and implementation of human rights norms.

Uganda has also ratified the African Charter on Human and Peoples' Rights (ACHPR) and, in July 2010, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol). ¹⁷Uganda is also a signatory to the African Union Solemn Declaration on Gender

Women's Legal and Human Rights Bureau for the End violence: Women's rights and safety online (EndVAW) project(2014), Domestic legal remedies for technology related violence against women: Review of related studies and literature, APC

The State of the State of Stat

¹⁶ Convention on the Elimination of All Forms of Discrimination against Women (2017), General recommendation No. 35on gender-based violence against women, updating general recommendation No. 19, file:///C:/Users/Advocacy/AppData/Local/Temp/N1723154.pdf

¹⁷ International Federation for Human Rights(2012), Women's rights in Uganda: gaps between policy and practice, https://www.fidh.org/IMG/pdf/uganda582afinal.pdf



Equality in Africa.

General gender equality laws

Uganda's Constitution (1995) states that all persons are equal before and under the law in all spheres of political, economic, social and cultural life and in every other respect and shall enjoy equal protection of the law (Article 21; Clauses 1&2). The Constitution goes ahead to prohibit discrimination on the ground of sex, race, colour, ethnic origin, tribe, birth, creed or religion, social or economic standing, political opinion or disability. ¹⁸Article 29 (1; a) highlights the rights of freedom of speech and expression; and says that the state has a constitutional duty to protect and promote all people more especially women and their freedom of expression. Similarly Article 33 (5) provides that women shall have the right to affirmative action for ¹⁹the purpose of redressing the imbalances created by history, tradition or custom.

Criminal laws

The Penal Code Act is an ²⁰act to establish a code of criminal law. ²¹An Act is a Bill which has passed through the various legislative steps required for it and which has become law. Under the Penal Code, any act of defamation, which is likely to²² injure the reputation of a person by exposing them to hatred, contempt or ridicule or likely to damage any person in his/her profession or trade by an injury to his or her reputation, is contrary to section 180 of the Penal Code Act.

Section 83 of the Penal Code²³ Act observes threatening violence as an offence and the perpetrator is liable to imprisonment for a period not exceeding four years. The Penal Code Act further states that it is an offence to incite violence ²⁴ on the basis of, among other grounds, sex, traffic in obscene publications for the purpose of trade, cause another to die by suicide due to threats of violence, or attempt extortion by threats. ²⁵Libel is also a crime in Uganda, and it applies to content which "exposes a person to hatred, contempt, or ridicule."

Although these offences do not target technology-related violence against women 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 Code²⁶.

Any act associated with non-consensual accessing, using, manipulating, disseminating or sharing of private data, information and/or ²⁷content, photographs and/or videos, including sexualized images, audio clips and/or video clips or photoshopped images is an act of technology-related violence against women. Under the Anti-Pornography Act Section 13(1), ²⁸it is an act of offence to produce, traffic in, publish, broadcast, procure, import, sell or abet any form of pornography. Anti-Pornography Act was put in place to define and create the offence of pornography; to provide for the prohibition of pornography; to

- 18 Constitution of the Republic of Uganda (2005), Article 29(1)
- 19 Article 33(5)
- 20 The Penal Code Act Cap. 20 (1950)
- Women of Uganda Network (WOUGNET)[2018], Investigating Tech-Related Violence Against Women in Peri-Urban Areas of Uganda, https://www.apc.org/en/pubs/tech-related-violence-against-women-peri-urban-areas-uganda
- 22 The Penal Code Act Cap. 20 (1950), Section 180
- 23 Section 81
- 24 Section 83
- 25 Section 179
- Chioma Nwaodike and Nerissa Naidoo (2020), Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda, https://ogbv.pollicy.org/legal_analysis.pdf
- Human Rights Council (2018), Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, https://digitallibrary.un.org/record/1641160?ln=en
- 28 The Anti-Pornography Act 2014, Section 13(1)



establish the Pornography Control Committee and prescribe its functions; and for other related matters.

The Computer Misuse Act (2011) is aimed at making provision for the safety and security of electronic transactions and information systems, to prevent unlawful access, abuse or misuse of information systems (including computers) and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters. The Computer Misuse Act (2011) prohibits cyber harassment, ²⁹which 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. Definitions of obscene, lewd, lascivious, and indecent are not provided³⁰.

Any act of offensive communication is contrary to section 25 of the Computer Misuse Act, which states that any person who willfully and repeatedly uses electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication, whether or not a conversation ensues, commits a misdemeanor and is liable on conviction to a fine not exceeding twenty-four currency points or imprisonment not exceeding one year, or both. ³¹ The act states that any person who willfully, maliciously, ³²and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyberstalking and is liable on conviction.

The Data Protection And Privacy Act (2019) aims at protecting the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters. ³³The Act elaborates Article 27(1)(2) of the Constitution (1995) that guarantees the right to privacy. This act can be used to charge some of the cyberbullying tactics such as sharing of private conversations, private photos, and the collection of personal information without consent. The Data Protection Act was passed in 2019. However, the government is yet to establish the office of the data protection commissioner for its full administration.

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 survivor. Survivors of online technology-related violence may bring a civil suit for defamation under the common law.

While gender-based violence needs to be eliminated both offline and online, and much of the law, policies, processes and procedures may be equally applicable to technology-related violence and other forms of violence against women. ³⁴The specificity of information communication technology for example, its reach, its speed, the participation of secondary perpetrators, the aggregated harm, the anonymity and the disinhibition that accompanies communications, all require some level of re-thinking and re-training.

²⁹ The Computer Misuse Act 2011, Section 24(2)

³⁰ Chioma Nwaodike and Nerissa Naidoo (2020), Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda, https://ogbv.pollicy.org/legal_analysis.pdf

³¹ The Computer Misuse Act 2011, Section 25.

The Computer Misuse Act 2011, Section 26

³³ Constitution of the Republic of Uganda (2005), Article 27(1)(2)

Zarizana Aziz(2018), Due Diligence Project: Eliminating Online Violence against Women, https://www.sistersforchange.org.uk/wp-content/uploads/2020/docs/01-SFC-DB-FILES/672-Due-Diligence-to-Eliminate-Online-Violence-against-Women-The-State-Intermediaries-and-Engendering-Universal-Access-to-the-Internet.pdf



Uganda Police

The Uganda Police Force was established in 1906 by the British Colonial government as a Para-military Force called the Uganda Armed Constabulary. Like in colonial days, the police force largely remains an authoritarian instrument of state control of the public, taming perceived opponents of the state and for enforcing law and public order³⁵.

As a state institution, Uganda Police Force (UPF) was established under Article 211 of the 1995 Constitution of the Republic of Uganda; ³⁶there shall be a police force known as Uganda Police Force and such other police forces as parliament may by law prescribe. ³⁷Article 212 of the Constitution grants the UPF specific mandate of protecting life and property and protecting law and order as well as detecting and preventing crime.

In addition to the above mandate, the UPF has a wide range of powers also prescribed under the Police Act; ³⁸Powers to detect crime in society and ensure public safety and order, ³⁹Powers to investigate, search, arrest, and detain and powers to use lethal force. In the execution of their mandate, however, ⁴⁰Article 211 of the constitution mandates UPF to be professional, disciplined, and competent and to exercise restraint in carrying out their duties.

Criminal Investigation Directorate (CID)

The Ugandan legal system being a common law country is comprised of two very different types of cases civil and criminal. Crimes are generally offenses against the state and are accordingly prosecuted by the state. Civil cases on the other hand are typically disputes between individuals regarding the legal duties and responsibilities they owe one another.

In Uganda's criminal justice system, the police perform investigation on their own authority under the Criminal Investigation Directorate (CID) in order to execute their functions as enshrined in the 1995 Constitution of The Republic of Uganda. CID whose headquarters are in Kibuli Kampala has a major responsibility of detecting, preventing and investigating crime, compiling information on criminals and gathering evidence for use in criminal prosecutions. However the handling of criminal related complaints by Uganda Police Force (UPF) has been question of contention among academicians and police actors.

5.0 Methodology

5.1 Scope of the research

The research was conducted over a period of three months, from September to November 2020 and it involved conducting a comprehensive literature review to map out domestic legal remedies and adoption of a survey design employing a multi-method approach.

A total of 21 women and girls, aged between 23 to 50 years, responded to an online survey questionnaire.

- 35 https://www.upf.go.ug/history-of-upf/
- 36 The Constitution of The Republic of Uganda, Article 211(1)
- 37 Article 212
- 38 The Police Act Section 4
- 39 The Police Act Section 24-33
- 40 The 1995 Constitution of the Republic of Uganda Art. 211(3)



Women and girls who participated in this report owned and/or had access to various online/digital platforms such as social media, laptops, smartphones, basic phones, online personal accounts and the Internet, among others.

In addition, semi-structured interviews were distributed to 40 legislators and key informant interviews were conducted with officials from Uganda Police Force, judiciary and office of the Directorate of Public Prosecution.

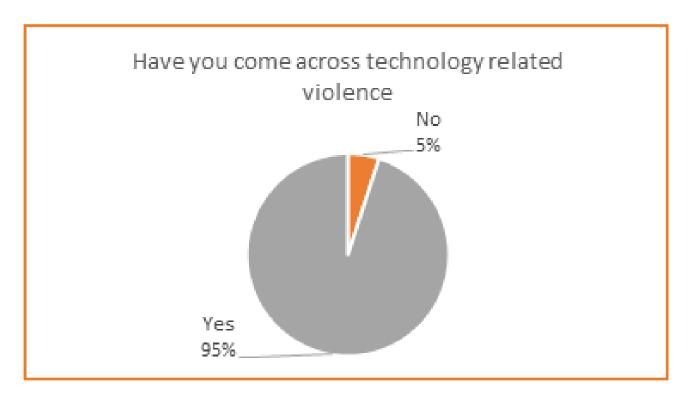
6.0 Principle findings

6.1 Legislators and key informants

6.1.1 Technology-related violence – Awareness and manifestation

An overwhelming majority (95%) of the legislators have come across technology-related violence. The subsequent section spells out their understanding of how online violence is said to be manifested and how each of them has interacted with it.

Figure 1: Legislators' level of awareness of technology-related violence



Results from the legislators further show that online violence, commonly being referred to as cyberattack, against women is considered to manifest in different forms, but not confined to women being harassed, bullied, defamed, and abused. In some instances, it was mentioned that stalking on phone and social media was also a common manifestation.

"Someone insulting a woman on phone calls and messages to belittle her," noted a legislator Other ways in which legislators believe victims have experienced online violence were mentioned as being subjected to hate speech and exploitation.



Exposure, as well as non-consensual sharing of photos, videos and messages with pornographic content to cause shame to the victims were singled out as being a common online vice. The latter being further defined as "content, be it in form of a text, graphics i.e. videos, photos aimed at relating women to what they are not".

They further mentioned that the use of derogatory language against women with intent of eroding their dignity also connotes violence against women.

6.1.2. Rationale for the occurrence of technology-related violence against women and girls

There are a number of things that legislators saw that perpetuate or amplify violence against women using technology. These are:

- Existing imbalances in marriage relations, perceived as effects of marital failures, are seen to raise moments of conflict which are not easily resolved
- Weak laws
- Ignorance of the masses
- Moral decadence
- Means of extortion
- Acts of revenge
- A means to cause fear and intimidation
- Random incitement of violence

They reported that documentation of how laws have been used to curb online violence against women has not been done, and so, there is lack of any precedence to alert victims or cause the offenders to fear.

As such, the likelihood of apprehension, prosecution and conviction was inevitably seen to affect the behavior of potential perpetrators, as well as reporting.

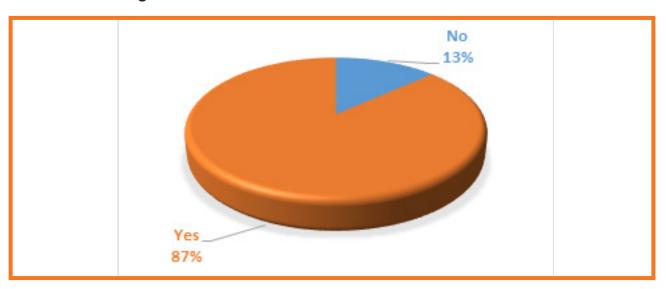
They further indicated that victims reporting would be a factor of attitudes and norms around violence. Reporting, for example, was seen not to be easy and many have not reported.

6.1.3. Existence of legal frameworks to provide effective justice to victims of online violence against women

Majority of the legislators (87%) recognize that there are legal frameworks to provide justice to victims of online violence against women. This means that they agreed that there are specific laws addressing online GBV.



Figure 2: Legislators' knowledge of the existence of legal frameworks for victims of online violence against women



However, some respondents indicated that they did not know how effective the laws are, while others observed and argued that there has not been sufficient sensitization on these laws, and that only a few precedencies exist while the courts have not publicized any cases. That alone shrouds the mind of the legislators with lots of uncertainties. Below are what some of the legislators said:

- Legislator 1: 'Not very effective laws"
- Legislator 2: "There are a few precedencies"
- Legislator 3: "We have not seen publication of any cases"

Others noted that in many cases, the would-be law enforcers were failing to take adequate action in response to acts of online gender-based violence

6.1.4. Legal remedies against online violence

Participants indicated that there is a diversity of remedies that includes both the formal and informal social domains for addressing online gender-based violence.

They further indicated that the elimination of online violence against women has been said to be recognized by the Government of Uganda and that the country has legislations that criminalize such acts. Notable remedies/legislations are;

- Computer Misuse Act, 2011
- Anti- Pornography Act
- Data protection & privacy Act, 2020



Table 1: Respondents mention of legal remedies against online violence

Legal remedies	Number of mentions
Computer Misuse Act, 2011	20
Data Protection & Privacy Act ,2020	12
Anti-Pornography Act	9
Penal Code (Defamation, libel, serious publication)	4
Police Cybercrime Investigation Act	3
Laws on impersonation & falsification	2
Media Act & Practitioners Act	2
Sexual Assault Act	2
Award in damages	1
Criminal sanctions in law e.g. imprisonment, sanction	1
Cybercrime unit in police	1
DPP, Police (Judiciary)- Provides legal advice- lodge a complaint	1
Orders of seizures	1
Police arresting perpetrators	1
Protection orders	1
Responding to the police, Go to court of law, getting the evidence	1
The Cyber Act	1
To restore morals in churches	1

It was further observed that interventions to change attitudes and behaviors are also seen to play a pivotal role in minimizing online gender-based violence.

We also see from the findings where legislators and key informants imply that dealing with only the consequences of violence is not enough, because a lot of online violence may go unnoticed, as such, some legislators opt for additional non-legal or informal remedies such as restoring morals in church that deal with character, values, and practices to influence positive change, though the extent to which such interventions have played out in changing behavior and keeping victims safe is not mentioned.

6.1.5. Recommendations

While legislators believe that there is legislation on online violence, there is a feeling that not so many people are aware of the existence of these laws and perhaps their interpretation. It is clear from the legislators' recommendations that government's focus should be in the areas of training, ensuring prevention before occurrence, enacting strong laws that ensure that victims are protected and offenders punished.

The participants agreed that this is a moral question and that there is need for public awareness, in addition to training women and girls to protect themselves because they are the most vulnerable group online.

Some participants noted that the laws on online violence were weak, and urged government to take reasonable action to address and eliminate online violence against women. They noted that the lack of



effective measures to prevent and contain online violence against women creates impunity, adding that government has been slow in addressing the problem.

Because of the perception that the laws are weak, it was noted that there are several major obstacles to their effectiveness. There is, thus, a call to government to effectively implement and review legislation to ensure that it is effective in eliminating online violence against women, especially in the areas of prevention and the prosecution of offenders.

To some, police should do a lot more in following up related cases to instill confidence in the victims, but also to alert the perpetuators of the seriousness of the offences.

Table 2: Perceptions on best way to handle the issue of online violence against women

What do you think is the best way to handle the issue of online violence against women?

Moral rehabilitation (Posting, Traffic making & dissemination awareness/Education /Sensitisation Cautious update of law

Girls shouldn't seduce people into those kinds of violence

Law enforcement should be active

Legislation is weak because it is a new area

Men need to be addressed in the ease of harassment

Need to protect both genders

No romancing the problem. Sanctions must e levied. Strong penalties

Offender isn't aware of the violence

Punish the culprits/ punishments should be harsh enough to deter others from doing the same

Strengthen legal frameworks and upgrade technology for evidences to implicate the offenders.

Strengthen the laws with stringent penalties for culprits

Try to have a sense of security

Well regulated FOE

Women (victims) should not be frustrated by the police when following up on the cases

Women need to be aware of security

6.2 General public report

A total of 21 women and girls, aged between 23 and 50 years, responded to an online survey questionnaire. Women and girls who participated in this report owned and/or had access to various online/digital platforms such as social media, laptops, smartphones, basic phones, online personal accounts and the Internet.



6.2.1 Demographics

Majority of the members of the general public who were sampled were 35 years and below (72%). Most of them had attained relative education, the majority having attained university education (76%) and the others tertiary education (19%).

Table 3: Age groups under which respondents fell

Age group	No. of respondents	%
Less than 25 years	2	10%
25-30 years	8	38%
31-35 years	5	24%
36-40 years	4	19%
41-45 years	1	5%
46-50 years	1	5%
Total	21	100

Table 4: Level of education of the respondents

Level of education	No. of respondents	%
Secondary	1	5%
Tertiary	4	19%
University	16	76%
Total	21	100

6.2.2 Understanding of technology-related violence against women and girls

All respondents in the general public category indicated that they had an understanding of what technology-related violence against women and girls was, without delving into the depth of their knowledge on the subject as this was not a requirement at this point of the survey.

6.2.3 Experience with forms of technology-related violence

When respondents were probed further on their experience with technology-related violence, majority (71%) indicated that they had experienced some form of technology-related violence.

Table 5: Respondents' experience of any form of technology-related violence

Answer	Number of respondents	Percentage
No	6	29
Yes	15	71
Total	21	100

Those that had indicated having had an experience with technology-related violence were further



probed on the nature of violence experienced. Results indicate that most had encountered predominantly online hate speech and non-consensual pornography.

Table 6: Form of technology-related violence experienced by respondents

Form of technology-related violence experienced	Number	Percentage
Online hate speech	4	24%
Non-consensual pornography	4	24%
Cyber harassment/ Cyber bullying	2	12%
Online defamation	2	12%
Online sexual exploitation	2	12%
Other	2	12%
Cyberstalking (e.g. false accusations, threats, etc.)	1	6%
Total	17	100

Table 7: Social media is evidently the biggest vehicle that the perpetuators have used to reach out to their victims. And this is seen to cut across the different forms of violence.

Form of technology-related violence against women and girls experienced and the Internet platform used				
	e-mail	High school	A mixture of several platforms	Social media
Cyber harassment/ Cyber bullying				2
Cyberstalking (e.g. false accusations, threats)				1
Non-consensual pornography				4
Online defamation	1			1
Online hate speech			1	3
Online sexual exploitation				2
Other		1		
Total	1	1	1	13

6.2.4 Recency of experience

On how long ago the technology-related violence had been experienced, most respondents indicated that they had experienced it as far back as a month, with some noting that they had experienced the violence as recently as a few minutes ago or even the previous day before the interview.

In some cases, the victims had had multiple experiences with online violence. Perhaps signifying that such is not a one-off but continues to be perpetuated in different forms, multiple times.



Table 8: Length of respondents' experience with technology-related violence

What form of technology related Violence against women and girls did you experience?	How long did the violence last?
Cyber harassment/ Cyber bullying	Different people, different situations, different days buy at least once a month
Cyber harassment/ Cyber bullying	2 months
Cyber stalking (e.g. false accusations, threats, etc.)	1 month
Non-consensual pornography	Week
Non-consensual pornography	Not longer than a week
Non-consensual pornography	2 days
Non-consensual pornography	2 days
Online defamation	One day
Online defamation	4 months
Online hate speech	1month
Online hate speech	3 months
Online hate speech	1 month
Online hate speech	Weeks
Online sexual exploitation	2mins
Online sexual exploitation	One day

6.2.5 Means of access to victims

In respect to how the offenders gained access to the victim's online space, results show that creation of fake accounts is a more common means. Gender trolling and hacking are the other avenues that have been utilised by the offenders.

Table 9: Ways in which offenders gained access to someone's online space

Means of gaining access	Number of times	Percentage
Fake Accounts	5	31%
Gender trolling	3	19%
Hacking	3	19%
Communication threats	1	6%
Direct chats	1	6%
Had my contact already	1	6%
The offenders commented on a post I had written	1	6%
Through my step mum and my diary.	1	6%
Total	16	100%

6.2.6 Relationship with the offender

While it seems like online violence typically begins with a relationship between the perpetrator and the victim, to many of the victims interviewed, there is indication that there was no relationship, but rather just random people on social media.



In majority of incidences, the victims said that they did not know the offenders, meaning that they had no relationship with the perpetuators of the online violence. Only in a few instances did they mention that they knew the perpetuators, and that they were either friends or acquaintances on social media.

Table 10: Victims' relationship with offender

Relationship with offender	Frequency of response
I didn't know him/Stranger/No relationship	11
Friend	3
Ex-workmate	1
Facebook friend	1
Husband	1

Further probing on the reasons the victims could have been targets for technology-based violence, majority of them indicated that they did not know.

Table 11: Suspected reason for online violence

Suspected reason	Frequency
I don't know	9
Assignments competition. He felt threatened because I was chosen over him for an assignment	1
Being a woman, he misinterpret friendship and wanted to take advantage	1
Just to blackmail me and to try and make me be hated by everyone.	1
Not happy because I had moved on	1
Suspected cheating	1
That is his style	1
They were abusing me for standing up for a cause that was not even for women. But I was abused as a woman, for example, things like "you look like a slut. They	
must have thought you were a whore"	1
When someone they like or love comments on pictures	1
Total	17

However, looking at the data further, and trying to compare relationships between victims and the offenders, a few hints were established. Jilted lovers, workplace competition, stalking of persons are some reasons for the possible violence.



Table 12: Summary of relationship with offender, means of access to online space and possible reason

Relationship with offender	How offender gained access to victim's online space	Possible reason for the violence
Husband	Hacking	suspected cheating
Friend	Had my contact already	Not happy because I had moved on
Friend	Gender trolling	Being a woman, he had misinterpreted my friendship and wanted to take advantage
None	Hacking	l don't know
I don't even know them.	Communication threats	When someone they like or love comments on pictures
Facebook friend	Hacking	l don't know because I do not know this person in person
Former workmate	Direct chats	Assignments competition. He felt threatened because I was chosen for an assignment over him
Friend	Fake Accounts	l have no idea
They were people I studied with and family.	Through my step mum and my diary.	Just to blackmail me and make me hated by everyone.
Stranger	Gender trolling	l don't know
Stranger	Fake accounts	l dont know
Stranger	Fake accounts	That is his style
Stranger	Gender trolling	l don't know
There is no relationship	Fake accounts	I have no idea
There is no relationship	Fake accounts	l have no idea
Strangers on social media	The offenders commented on a post I had written	They were abusing me for standing up for a cause that was not even for women. But I was abused as a woman, e.g. "you look like a slut. They must have thought I was a whore"

6.2.7 Social and psychological Impact of online violence

The violence had evidently taken a toll on the women who were interviewed. Results show that many felt tortured psychologically. Almost all the women respondents felt the negative effect of online violence and abuse on their offline lives, which ultimately impacted their attitude and use of the Internet.

For example, one participant noted:

"I still cry up to today when I remember the blackmail I experienced in school and out of school. I lost my self-esteem, confidence, and trust in people. Up to date I fear opening up about my life because I trust no one and I feel that even if I tell someone anything small, they will twist it and spread it differently"



Another respondent said the abuse took a toll on her confidence and self-esteem.

"It totally made me feel useless, unwanted, a failure"

The social and psychological consequences are seen to vary from one woman to another. Results show that while some women respondents felt stressed, lost self-esteem and confidence, felt psychologically tortured and anxious, others reacted by shunning or shelving their online activities.

Table 13: How online violence impacted the victims socially and psychologically

Emotionally stressed

I felt intimidated and went offline for some time

I hated it and got stressed

I just stopped confirming friend requests

I left social media for some time

I still cry up to today when I remember the blackmail I suffered while still in school and out of it. I lost my self-esteem, confidence, and trust in people. Up to date, I fear opening up about my life because I have no one to trust and I feel even if I tell someone anything, however small, they will twist it and spread it differently.

I was affected emotionally and reported him to a close mutual friend. He stopped and apologized. GBV online is a very common thing even with so-called male allies

I was humiliated

I went through a lot of psychological torture

It made me angrier and determined with my activism even more.

It totally made me feel useless, unwanted, a failure

It was really disgusting and traumatizing

It is mental abuse.

My relationship with family and friends was affected

None (no impact)

Pornography is not my style, and he was vulgar

6.2.8 Reporting of cybercrimes and online violence to law enforcers

Results show low awareness (47%) for reporting cybercrimes and violence. Less than half of the members of the general public who were interviewed indicated that they were not aware that they can report cybercrimes and online violence.



No 53%

Yes 47%

Figure 3: Public's level of awareness to report cybercrimes and online violence

Further probing showed that most feared and, in many cases, did not know anybody they could report to. A few of them indicated reporting to their peers (friends) and relatives.

Table 14: Reporting of online violence

To whom victims of online violence reported	Frequency
Mother	1
A friend	1
Close and mutual friend.	1
At the time, I didn't know any reporting options	1
A few people, I asked the people in question	1
I feared to report/ had no one to report to	11
Total	16

It is, therefore, of paramount importance that much of the effort should go into educating the masses, victims and the law enforcement on the seriousness of such crimes and how they should be able to handle them.

It is also a pointer to the fact that raising public awareness and sensitization through educating women and girls of their rights and how to exercise them is important, while also emphasizing the consequences of such crimes to the general public.



Table 15: Why survivors did not report online violence

Reason	Frequency
Because I felt like nothing will be done about it	2
Because he stopped	1
Because I got what I wanted anyway, without public support, and justice was served	1
I felt it was not necessary	1
I did not know where to go	1
I did not have the information of who I could speak to	1
I did not know that there was a law against such	1
I do not trust Uganda's police	1
I felt that it was my faulty; I was misled with excuses	1
I thought it would escalate issues and require more discussion, which I wanted to	
avoid	1
I was no aware such could be reported.	2
I Just blocked him and rested my case	1
I thought it would be more embarrassing on social media	1
Grand Total	16

6.3 CID – GBV Department

Under the UPF's constitutional mandate of "protecting law and order, detecting and preventing crime," UPF established the GBV Department in 2012 with a main purpose of solving the escalating cases sexual and child related offences and the effects caused by gender based violence. The department is under the Criminal Investigations Directorate and handles and investigates cases of sexual nature and child abuse including cases of Human Trafficking addressing young and old, male and female. Among the cases investigated include: Rape, Defilement, Abduction, Human Trafficking, Domestic violence among others.

The unit has desks with trained personnel throughout the Police Districts handling cases involving violence against women and girls. The desks work on a referral mechanism and this helps address the accessibility challenge when it comes to reporting crimes committed against women and girls. The department works hand in hand with other departments with in Uganda Police to prevent and respond to cases and these include; The Children And Families Protection Unit, The Cyber Department, The Organised Crime Unit, The Training Department, General Crimes Department And Crime Data Department.

6.3.1 Investigation

When a case comes in, the first thing is to have the case registered, then interview victim with psychosocial sessions and continuous monitoring of the case is followed closely while collecting the evidence and witness testimony about the reported case. This process however applies for the cases that have happened offline. The department has got a challenge of officers not being familiar with the advancement in technology hence the offences that are groomed online and then the crime is committed offline, are often registered as offline cases. The other challenge is that Online Child Sexual abuse is not



an offence according to the Ugandan law so cases are investigated and recorded as the exact act that took place. Cases involving online sexual offenses, the department works hand in hand with the Cyber Unit and Forensic Department are treated as offline.

However the GBV department further discloses that crimes related to Online Sexual offences are investigated using the Computer Misuse Act. Cases that were groomed online and turned out to be physical like defilement or Rape are investigated using the penal code Act.

GBV Department doesn't have any data on online violence against women or online offences and the only source of data in relation to cybercrime and online violations is the Annual Crime Report of 2019.

Table 16: Breakdown of Cyber offences

	Offences Number of Cases Reporte		f Cases Reported
		2019	2018
1.	Electronic Fraud	68	76
2.	Threatening Violence	33	28
3.	Unauthorized Access	27	10
4.	Defamation	22	25
5.	Obtaining Money by False pretense	20	08
6.	Personation	19	12
7.	Offensive Communication	19	19
8.	Theft	06	03
9.	Money Laundering	06	00
10.	Obtaining Goods by False Pretense	05	00
11.	Cyber HarassmentW	04	07
12.	Cyber Stalking	02	01
13.	Unauthorised Disclosure of Information	02	02
14.	Soliciting Bribe	02	00
15.	Disappearance	02	00
16.	Possession of Suspected Stolen Property	02	00
17.	Sectarianism	02	00
18.	Stealing Motor Vehicle	01	00
19.	Subversion	01	00
20.	Unlawful Obtaining of Data	01	00
21.	Embezzlement	01	00
22.	Incitement to Violence	01	01
23.	Forgery	01	01
24.	Conspiracy to Defeat Justice	01	00
25.	Unauthorised Modification of Computer Material	00	02
26.	Pornography	00	02
	TOTAL	248	198



Uganda Police Force, Annual Crime Report 201941

According to the Annual Crime report 2019, by the end of the year, out of 248 reported cases, 188 cases were still under inquiry, 30 cases were taken to court, 08 cases secured convictions, and 18 cases were still pending in court. The police report noted that the number of cases reported on Cyber harassment and defamation decreased and there was no reported case of pornography and Unauthorised Modification of Computer Material reported in 2019.

The Annual Crime Report 2018 indicates that total of 198 cases were reported in 2018 compared to 158 cases in 2017. By the end of 2018, 142 cases were still under inquiry, 16 cases were taken to court, 06 cases secured convictions, 02 cases were dismissed and 08 cases were still pending in court.

6.3.2 Observation.

- It important to note that for the past three years, online violence cases have been increasing by an average of 25%.
- From the Annual Crime Reports one is not able to know how many women and girls were victims to the enlisted cybercrime cases reported.
- The Annual Crime Reports don't give an accountability of status of the pending court cases from the previous years.
- From the table above one can note that the cases that are more inclined to women and girls like
 cyber harassment, cyberstalking and pornography are not held in high regard as compared to the
 cases that are inclined to finances like Electronic fraud. This is confirmed by the statement in the
 Annual crime report that endorses the ⁴²recovery of Ugx. 51,890,000 and doesn't account for how
 many of the gender sensitive cases or victims actually got justice.
- The Annual Crime Report 2019 doesn't indicate what happened to the 30 cases that didn't make it to court and didn't make it to the list of cases still under inquiry.
- Reporting of the gender sensitive cases is really low as compared to the financial related cases. In Annual Crime Report 2019, financial related cases like Electronic fraud, money laundering, and theft contributed 32% of the total reported cases while the gender sensitive cases contributed 2.4%.
- According to the Annual Crime Report 2019, Cybercrimes led to a loss of Ugx. 11,446,603,500 in 2019 in which Ugx. 51,890,000 was recovered which implies that most of the cyber cases that reached court were finance related cases.

6.3.3 Why most victims don't report cases

From the Annual Crime Report one is able to access and know that very few cases are reported when it comes to online violence. The Crime Investigator interviewed attributed this to the following

Victim Blaming – Victims are afraid of the victim blaming and name calling that will come along when they report anything to the police. Society has a way of causing stigma to the victim with a special brand names that detail what happened or the crime that was committed to the victim. ⁴³Even when the perpetrators are apprehended or punished, life is never the same for the victims.

Bureaucracy-The whole process from reporting all the way to prosecution is very long and psychologically

⁴¹ https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801

⁴² https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801

⁴³ https://observer.ug/businessnews/67815-careless-data-collection-propagates-violence-against-women-online



exhausts the victim. This is further catalyzed by the judicial system at hand that requires a victim to testify in court in front of everybody including the offender/perpetrator.

Cultural and social norms that are a basis for stereotyping. This is also enhanced by the upbringing where by women and girls prefer to keep silent of the violations that happen to them.

6.3.4 Challenges of the crime Investigators

- The time it takes to retrieve incriminating information from the victim's gadget or hand held device. This job is done by the Uganda Police's forensic department, one unit handling and analyzing all cybercrime and technology- related cases for the whole country including cases of online violence against women. 44According to UPF, Cybercrime is on the increase and Police Forensic Laboratory is overwhelmed with request for forensic analysis from Criminal investigations and other Ministries, Departments and Agencies
- The cyber unit and forensic department also has got a challenge with keeping up with the technology advancement of some gadgets especially those gadgets with the iphone Operating System. They tend to take a longer time retrieving evidence from such gadgets.
- The ever changing tactics used by the perpetrators reaching an extent of using simcards for the deceased to commit technology-related crimes against women and girls. In the Uganda Police Annual Crime Report 2019, indicates that fraudulent simcard swapping and registration from some scrupulous telephone company agents aids a number of online violence cases.

 45These telephone company agents fraudulently obtain the biometrics of unsuspecting persons more than once, and make more copies of the National Identity card of unsuspecting persons and later register more than one SIM card in the names of the unsuspecting persons whose biometrics have been taken more than once and more copies of National Identity cards have been made behind their backs.
- Most of the officers at the different GBV desks around the country don't know what to do
 when it comes to technology-related cases and they are not familiar with the advancement
 in technology more especially online violence against women and girls. Capacity building is
 needed especially in the area of digital detection and investigation of online violence against
 women.
- The investigating officers in the GBV Unit and the cyber forensic departments have little or no internet available to them as they carry on with the investigations. The officer interviewed highlighted that some of the cases have social media and internet as point of entry into investigations, then the investigator starts working backwards until the victim is got. This process requires adequate internet access. The cyber forensic department needs adequate internet to get to the infrequently accessed data also known as cold data from the gadgets of the victims, a process that requires adequate internet access.
- Witness withdrawal-Some Witnesses tend to withdrawal from cases when they find out that
 their testimony involves going to court. This is attributed to the lack of laws in areas like
 witness protection.

44

https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801

⁴⁵ https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801



- UPF has a challenge the positioning of the cybercrimes is both national and transnational.
- According to the Annual Crime Report 2019, UPF has a challenge of not having enough staff to handle the cases. The current strength of CID personnel is only 5,292 instead of the approved 19,843 leading to work overload⁴⁶. The UN standard is 1:12 cases per detective per year. The current workload stands at 45 case files per detective.
- ⁴⁷There is lack of vital equipment to facilitate investigations especially technology-related investigations like recorders, spy cameras, telephone tracking equipment which should be able to direct/point/locate suspects/victims being traced.

7.0 Recommendations

From the research, most legislators recommend the use of existing laws that address violation of rights (such as the Computer Misuse Act, the Anti-Pornography Act and the Data Protection and Privacy Act) to address online abuse and violence against women. It is ideal to have women-centered legislation that specifically targets online violence against women and protects women's freedom of expression, including consensual sexual expression. It should also include defined parameters to promote swift access to justice for victims/survivors while prioritizing reparation and redress, over criminalization.

Amendment of the Computer Misuse Act to include stronger and biting sanctions.

Civil Society Organizations to work alongside government to create awareness of existing laws that can deal with online violence against women.

The State should fulfill its obligation to promote and protect human rights. This includes the obligation to prevent violations, protect victims/survivors of human rights abuses, prosecute violations, punish perpetrators and provide redress and reparation for victims/survivors. The State needs to review all laws that regulate online activity to ensure that they are consistent and support the elimination of violence against women.

Women should be empowered to make decisions to protect their online safety and there is need to raise awareness among women on the options available to them to ensure their safety and privacy online. The information communicated to the women, including those with added vulnerabilities, should clearly state what constitutes violence in addition to enabling the validation of their experiences.

Mass education and sensitization campaigns are needed to promote community awareness of consent and the applicability of consent to actions done through social media as well as to challenge notions of victim-blaming and shaming of girls and women.

There is need to target prevention programs at the youth and even take a step further of engaging them in the creation of such programs because research shows that online violence against women is prevalent among the youth, ie, those below 35 years.

There is need to change society's attitude about on online violence against women. Society trivializes technology-related violence against women and victim blaming is common. This attitude often results in a culture of silence, where survivors are inhibited from speaking out for fear of being blamed for the

⁴⁶ https://www.upf.go.uq/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801

⁴⁷ https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801



violence they have experienced.

Uganda Police

In discussing women's access to legal recourse, we must also acknowledge the role police play as women's first contact with the criminal justice system. Therefore, any legal approach to make online spaces safer for women must include policies to build police's capacity in the field of online violence and police's ability to keep up with the advancement in technology.

Uganda Police to develop a more elaborate Annual Crime Report that clearly shows the gender of the victims. The crime report should be in position to show the status of the pending court cases and cases under investigation from the previous crime report.

The Uganda Police's forensic department, one unit handling and analyzing all cybercrime and technology- related cases for the whole country including cases of online violence against women. Cybercrime is on the increase and Police Forensic Laboratory is overwhelmed with request for forensic analysis from Criminal investigations and other Ministries, Departments and Agencies. Establishment of regional Police Forensic Laboratory is needed to shorten the time it takes police to investigate cases related to online violence against women.

The Annual Crime Report clearly documents the amount of money recovered by police from Cybercrimes. This implies that most cases that went to trial were financial related and attention was paid to their documentation. We recommend that the same treatment is given to all cybercrime cases especially those that violate the usage of internet space.

8.0 Appendices

Appendix A: Questionnaire for members of the Judiciary

Legislation Questionnaire

The growing reach of the Internet, the rapid spread of mobile information and communications technologies (ICTs) and the wide diffusion of social media have presented new opportunities and enabled various efforts to address violence against women and girls. However, they are also being used as tools to inflict harm on women and girls. This study examines the existing domestic legal remedies for survivors of technology related violence against women to access to justice in Uganda.

No	me		
Ge	nder		
1. Have you come across technology related violence?			
	● Yes		
2.	. In your opinion, what do you consider to be online violence against women?		



3.	3. What is the rationale for the occurrence of technology related Violence against women and girl			
4.	Are there legal frameworks used to provide effective justice to victims of online violence against women?			
	2Yes 2No			
5.	If yes, what legal remedies exist to handle such kinds of violence?			
6.	What do you think is the best way to handle the issue of online violence against women?			
	opendix B uestionnaire for survivors/ victims of online abuse			
Sı	ırvivors/Victims Questionnaire			
ted en as	e growing reach of the Internet, the rapid spread of mobile information and communications chnologies (ICTs) and the wide diffusion of social media have presented new opportunities and abled various efforts to address violence against women and girls. However, they are also being used tools to inflict harm on women and girls. This study examines the existing domestic legal remedies for rvivors of technology related violence against women to access to justice in Uganda.			
Ag	e			
Ge	nder			
Ed	ucation			
Oc	ccupation			
1.	How often do you use social media? ◆Daily ◆Weekly ◆Every fortnight ◆Monthly ◆Don't Know			
2.	Do you understand what technology-related violence against women and girls is all about? •Yes •No			
3.	Have you experienced any form of technology-related violence? ●Yes ●No			
4.	What form of technology-related violence against women and girls did you experience? • Cyber harassment/ Cyber bullying			

Cyber stalking (e.g. false accusations, threats, etc.)

Online hate speech Online sexual exploitation Non-consensual pornography



	Online defanOther	nation		
5.	How long did the viol	ence last?		
6.	When did you realise	you were being violated onlir	ne?	
7.	What internet platfor	m did the offender use to co	mmit the violent behaviors?	
	•Social Media	•Online Accounts	•Entertainment Sites	
	Dating Sites	•Other		
8.	How did the offender	gain access to your online s	pace?	
	Hacking	Gender Trolling	•Fake Accounts	Doxing
	•Communication T	hreats		
9.	What is your relations	ship/connection with the offe	ender?	
10.	Why did the offender	do what they did?		
11.	How did this attack in	mpact you socially and psych	nologically?	
12.	Are you aware that or •Yes	ne can report cybercrimes ar	nd violence to law enforcement? •No	
13.	Who did you report th	nis offense to?		
14.	Did you seek legal su •Yes	pport services?	•No	
15.	If yes, who did you red	ach out to?		
16.	If no, why?			
17.	Did you pay any mon	ey to access any legal servic	es?	
	•Yes		•No	

18. How much did you pay to access the legal services?



Block 381, Plot No. 26, Nsibambi Village P.O. Box 71314 Clock Tower K'la Tel: +256 414 697635

Email: info@unwantedwitness.org Website: www.unwantedwitness.org

- **1** Unwantedwitness-Uganda
 - Qunwantedwitness
 - unwantedwitness