Womxn's Rights and ICTs under the Law

A guide to navigating cyber laws in Uganda.

www.herinternet.org

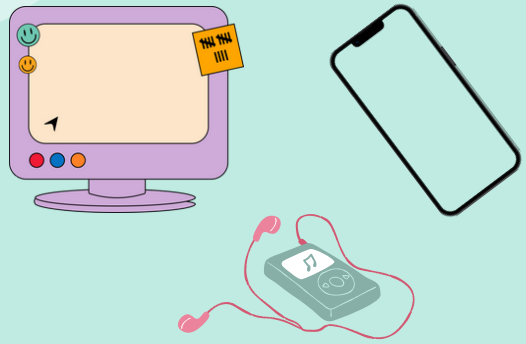
TABLE OF CONTENTS

Introduction

This guide summarises the key provisions in the law that affect the use of the internet and ICTs in Uganda, with a focus on the way communities of lesbian, bisexual and queer (LBQ) womxn and female sex workers (FSW) use the internet.

Important definitions

The law defines a *computer* as an electronic, magnetic, optical, electro-chemical or other data processing device or a group of such interconnected or related devices. These include devices with data storage or communications facilities. Therefore, smartphones, laptops, desktops and other such devices are computers.



Human rights are the basic freedoms that belong to every person in the world from time of birth until death. Despite the fact that they can never be taken away since they are defined and protected by law, human rights can sometimes be restricted. In Uganda, human rights are provided for under Chapter Four of the Constitution and can only be restricted if they affect the fundamental human rights and freedoms of other individuals or public interest.

All government ministries, departments and authorities have a responsibility to **respect**, **promote**, **protect** and **fulfil** human rights.

Did you know?

The use of the internet and ICTs is connected to constitutionally guaranteed rights including the right to privacy, access to information, and freedom of expression.

LBQ womxn and female sex workers can make use of the law to address harms that they face on the internet.

Producing, broadcasting, and sharing pornography is no longer illegal in Uganda. This means that victims of non-consensual distribution of intimate images (NCII) will no longer be prosecuted and sex workers can no longer be charged under this law.

The main laws governing the internet and ICTs in Uganda include:

-The Constitution of the Republic of Uganda of 1995 provides for the basis of enjoyment of human rights, including on the internet.

-The Computer Misuse Act of 2011 provides for the safety or security of electronic transactions and information systems by criminalizing unlawful access, abuse and misuse of computers.

-The Data Protection and Privacy Act of 2019 provides for protection of the privacy of individual and personal data by regulating the collection and processing of personal information.

-The Regulation of Interception of Communications Act of 2010 provides for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda.

-The Electronic Transactions Act of 2011 provides for the use, security, facilitation and regulation of electronic communications and transactions.

-The Electronic Signatures Act of 2011 provides for and regulates the use of signatures.

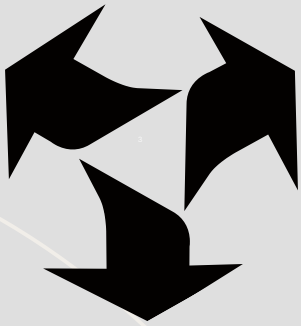
-The Anti-Pornography Act of 2014 was originally passed to define and create, as well as prohibit the offense of pornography.

Internationally, the Human Rights Council has emphasized that states should take all necessary steps to foster the independence of new media like the internet and ensure individuals' access to them as part of their mandate to guarantee freedom of expression and access to information.

Restrictions of freedom of expression must be:

Proportionate

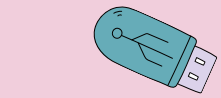
Provided by law

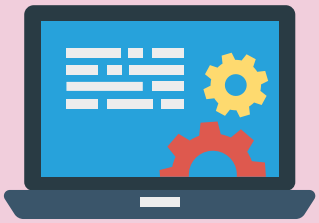


Necessary for the respect of the rights or reputations of others, protection of national security or public order and protection of public health or morals.

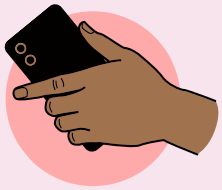
Regulations

The primary government body charged with internet-related matters is the *National Information Technology Authority of Uganda (NITA-U)*. The authority is responsible for, among other things, co-ordination, supervision and monitoring the utilisation of information technology in both the public and private sectors.





The *Uganda Communications Commission (UCC)* is an independent regulator within the communications sector that is mandated with monitoring, inspection, licensing, supervision, control and regulation of communications services as well as receiving, investigating, and arbitration of complaints relating to communications services, among other functions.

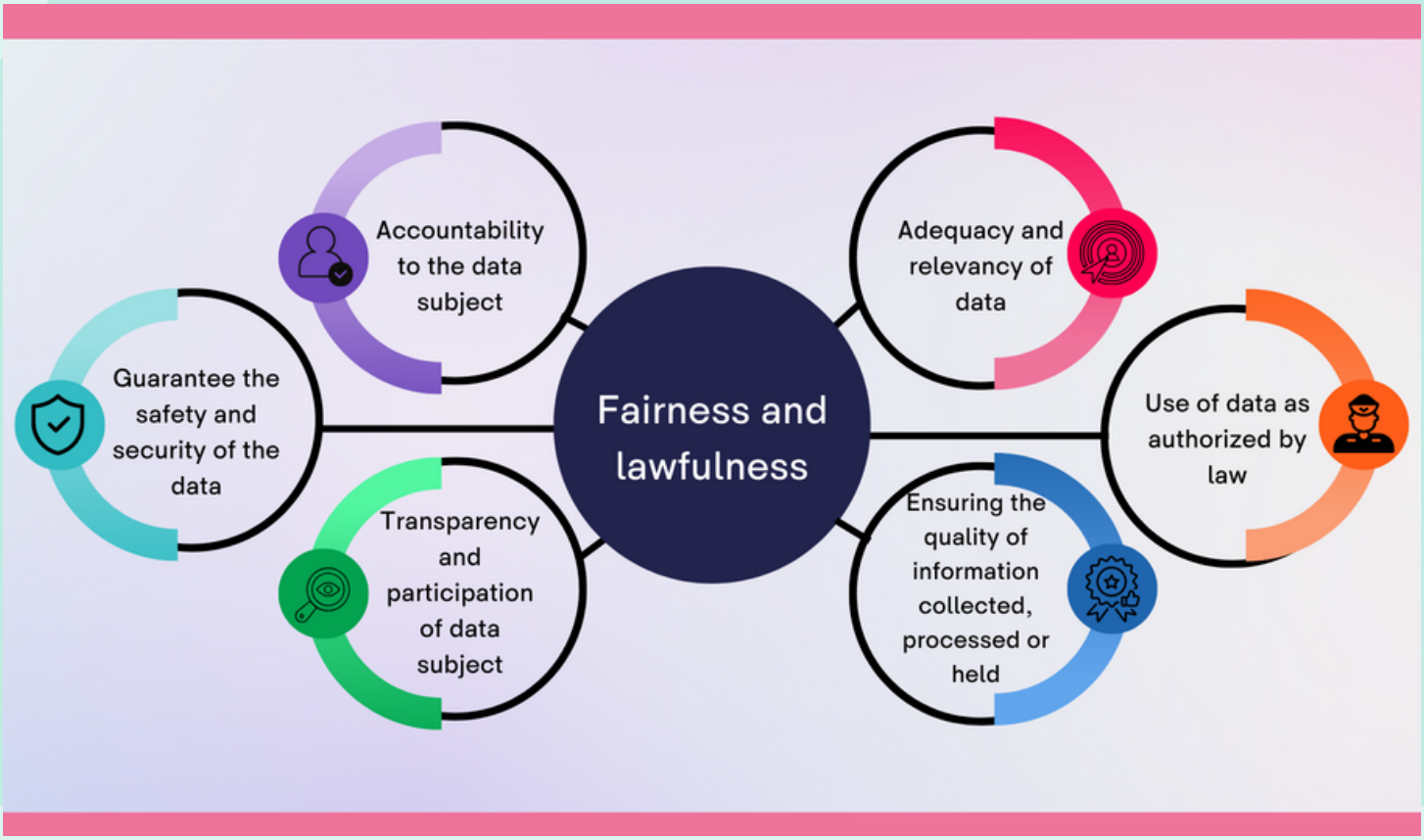


The *Uganda Police Force (UPF)* also has the Department of Electronic Counter Measures under the ICT Directorate to deal with cyber crimes including cyber-harassment and stalking, electronic fraud and email-related crimes among others.

Data Protection

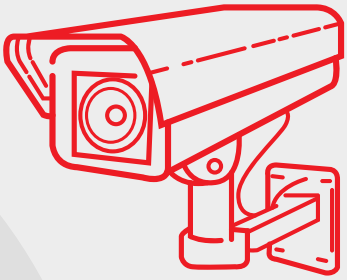
Data is defined as raw information which is processed by means of equipment operating automatically in response to instructions given for that purpose. Or it is information that is recorded with the intention to be used or processed.

The law provides for the following principles in handling data:



Surveillance

The African Declaration on Internet Rights and Freedoms states that everyone has the right to communicate anonymously on the Internet and to use appropriate technology to ensure security and privacy.



The Regulation of Interception of Communications Act and the Anti-Terrorism Act grant security agencies wide powers to intercept communications and collect information from service providers for purposes of guaranteeing national security.

However, international human rights standards call for the application of necessary and proportionate restrictions as well as due process, user notification, transparency, public oversight and the integrity of communications and systems. They also safeguard against illegitimate access, fosters international cooperation and right to effective remedy.

Penalties

The table below lists some of the penalties provided for in the Computer Misuse Act to counter common examples of cyber crime faced by queer womxn and female sex workers on the internet:

OFFENSE	MAXIMUM PENALTY
Cyber harassment	A fine of UGX 1,440,000 / 3 years / both
Offensive Communication	A fine of UGX 480,000 / 1 year / both
Cyber stalking	A fine of UGX 2,400,000 / 5 years / both
Child pornography	A fine of UGX 7, 200,000 / 15 years / both
Electronic fraud	A fine of UGX 7, 200,000 / 15 years / both

Cyber Laws and womxn in Uganda

Although the laws highlighted above seem neutral, the implementation of such laws often reflects discrimination against marginalised communities.

According to a 2021 research report on *The Trends And Impacts of Technology Assisted Violence Among LBQ Womxn and Female Sex Workers (FSW)* in Uganda released by HER Internet, many LBQ womxn and FSW are ignorant about the existence of these laws and their implementation. In addition, the existence cyber laws do not offer explicit protection of womxn online and thus redress is lacking.

Furthermore, the continuous criminalization of same sex relations and sex work discourages the meaningful participation and involvement of these communities of womxn within online spaces. There are also limited to no resources and information on cyber laws in relation to female gender and sexual minorities which could help raise awareness, prompt discourse and deeper discussions on the subject.

Many law enforcers and authorities perceive online violence as an illusion or fallacy and yet, they influence the establishment and implementation of laws within the constitution. Coupled with homophobia that is deeply ingrained in Uganda's society, LBQ womxn and FSW are further pushed into silence, fear and limited justice -if at all when they experience and become victims of technology-facilitated violence.

Recommendations

a. As part of its responsibility to protect, promote, respect and fulfill human rights, the government should:

- Include multiple communities in the conceptualization and debate of laws relating to ICTs. This will ensure that everyone's needs are reflected.
- Provide resources to marginalized communities which will enable them to access ICTs at subsidized prices.
- Include restorative sanctions such as compensation to survivors of online violence rather than simply prescribing prison time and government fines.
- Law enforcement officers and authorities need awareness about digital rights, internet freedoms and cyber laws in place which will equip them with knowledge they can rightfully utilize to enforce the law.

b. Given the spiralling cases of online violence against womxn which normally go unreported, it is important that online violence and cyber crimes against LBQ womxn and FSWs are reported, documented and investigated thoroughly so that the perpetrators can be brought to book.

CONTACT US

info@herinternet.org

www.herinternet.org

HER Internet