

# REPUBLIC OF UGANDA



# PARLIAMENT OF UGANDA

REPORT OF THE SECTORAL COMMITTEE ON INFORMATION, COMMUNICATION TECHNOLOGY AND NATIONAL GUIDANCE ON THE COMPUTER MISUSE (AMENDMENT) BILL, 2022

OFFICE OF THE CLERK TO PARLIAMENT

PARLIAMENT BUILDING- KAMPALA

SEPTEMBER 2022

1

Atom

Huse Som

## 1.0. INTRODUCTION

The Computer Misuse (Amendment) Bill, 2022 was read for the first time on Tuesday 19th July, 2022 by Hon. Mohammad Nsereko, MP, Kampala Central. Pursuant to Rule 129(1) of the Rules of Procedure of Parliament, the Bill was referred to the Committee on Information, Communication Technology and National Guidance for scrutiny.

The Committee has examined the Bill in accordance with Rule 129 (2) of the Rules of Procedure of Parliament, and hereby presents its report.

## 2.0. BACKGROUND

The Computer Misuse Act, 2011 was enacted to protect electronic and cyber space users from crimes created or encountered online. It regulates access to a computer, modification of computer material and disclosure of access code, among others. The Act further creates offences, including for unauthorized access, modification of computer material, unauthorized disclosure of information, electronic fraud, child pornography, cyber harassment and cyber stalking. The Act, therefore facilitates the safety and security of information systems by preventing abuse or misuse of information systems, thereby securing the conduct of electronic transactions in a trustworthy electronic environment.

The Computer Misuse Act, 2011 defines a computer as an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices. In addition, according to section 2 of the Computer Misuse Act, 2011, a person is deemed to have accessed a computer when he or she gains entry to any electronic system or data held in an electronic system or causes the electronic system to perform any function to achieve that

ر ر

objective.

Arth

Amsa

Balani

The Computer Misuse (Amendment) Bill, 2022 is generally premised on the need to enhance the enjoyment of the right to privacy which is being affected by the abuse of online and social media platforms through unauthorized access, the sharing of unsolicited, malicious, hateful and unwarranted information and to address new and emerging threats to the enjoyment of the right to privacy which are not covered under the Computer Misuse Act, 2011.

The internet is a significant means for socio-economic transformation in Uganda because it plays the key role of transforming the nation into a digital economy, with ICT contributing 4.8% of Uganda's GDP. Relatedly, according to the Uganda Police Force, Uganda has over 13.92 million internet users, with Facebook alone estimated to have over 2.4 million users, contributing to 5.5% of the population.

It is further reported that 8% of these accounts are suspected to be fake user accounts used to commit social media related crimes. Organized criminal groups are equally on the rise using digital technologies to facilitate illegal activities such as theft, electronic fraud, attacks on computer hardware, software, hacking into emails and social media accounts, cyber bullying and cyber stalking, non-consensual sharing of intimate images, revenge pornography, ransomware, cyber terrorism, misinformation and disinformation, tech-facilitated radicalization and extremism.

## 2.1. THE RIGHT TO PRIVACY

The 1995 Constitution of the Republic of Uganda recognizes the right to privacy under Article 27(2). In the same spirit, Article 41 prohibits the release of information which is likely to interfere with the right to the privacy of any other person. Further, a number of laws have been enacted to strengthen the protection of the right to privacy. These include, the Computer Misuse Act, 2011, Data Protection and Privacy Act, 2019, the Regulation of Interception of Communications Act, 2010, the Access to Information Act, 2005, , the Uganda

Walnus Ruin

Die Bay

Hus &

Communications Act, 2013, the Children Act, Cap. 59, the Electronic Transactions Act, 2011 and the Penal Code Act, Cap. 120.

In addition, Uganda is a signatory to international conventions which provide for protection and preservation of the right to privacy. These include, Universal Declaration of Human Rights the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the Convention on the Rights of a Child, the African Charter on the Rights and Welfare of the Child.

Despite the existence of the legal framework on the right to privacy, the continued rapid advancement in computer-generated technology presents dynamic challenges to the enjoyment of this right. The enjoyment of the right to privacy is currently affected as the previously unimagined innovations in information technology continue to evolve, for example the abuse of online and social media platforms.

## 3.0. THE OBJECT OF THE BILL

The object of the Bill is to amend the Computer Misuse Act, 2011 to:

- (a) enhance the provisions on unauthorised access to information or data to strengthen the protection of the right to privacy;
- (b) prohibit the sharing of any information relating to a child without authorisation from a parent or guardian or any other person having authority to make decisions on behalf of a child;
- (c) prohibit the sending or sharing of information that promotes hatred; and
- (d) provide for the prohibition of sending or sharing of misleading, malicious and unsolicited information.
- (e) restrict persons convicted of any offence under the Computer Misuse Act, 2011 from holding public office for a period of ten years.

All wood

A.h.

Mani

your

Joly

The Convo

#### 4.0. METHODOLOGY

In the process of analyzing the Bill, the Committee:

- (a) interfaced with the following stakeholders:
  - (i) Hon. Mohammad Nsereko, MP, Kampala Central- Mover of the Bill;
  - (ii) Ministry of Information, Communication Technology and National Guidance;
  - (iii) Attorney General;
  - (iv) The Uganda Communications Commission;
  - (v) The National Information and Technology Authority-Uganda (NITA-U);
  - (vi) The Uganda Police Force;
  - (vii) The Uganda Law Society;
  - (viii) Centre for Policy Analysis (CEPA);
  - (ix) Independent Online Journalists Association Uganda;
  - (x) E-Trade Association and Start-up Association of Uganda;
  - (xi)Collaboration for International ICT Policy in East and Southern Africa (CIPESA);
  - (xii) Human Rights Network for Journalists-Uganda;
  - (xiii) Uganda Parliamentary Press Association;
  - (xiv) Mr. Michael Aboneka of Thomas & Michael Advocates;
  - (xv) Injeel Ministries
  - (xvi) Dr. Anthony C.K Kakooza; and
  - (xvii) Unwanted Witness-Uganda.
- (b) reviewed the following documents:

(i) The Constitution of the Republic of Uganda, 1995;

The Ha

in the

Thursdames

- (ii) The Computer Misuse Act, 2011;
- (iii) The Penal Code Act, Cap. 120;
- (iv) The Uganda Communications Act, 2013;
- (v) The Data Protection and Privacy Act, 2019;
- (vi) The Regulation of Interception of Communications Act, 2010;
- (vii) The Children Act, Cap. 59;
- (viii) The Electronic of Transactions Act;
- (ix) The Access to Information Act, 2005;
- (x) Copyright and Neighbouring Rights Act, 2006; and
- (xi) Written submissions from stakeholders.

## **OBSERVATIONS AND RECOMMENDATIONS**

The Committee has examined the proposed amendments contained in the Computer Misuse (Amendment) Bill, 2022 in light of the Constitution and other relevant laws and makes the following observations and recommendations.

## 5.1. Unauthorized access

Clause 2 of the Bill proposes to replace subsections (1) and (7) of section 12 of the Computer Misuse Act, 2011 to prohibit unauthorized access to or interception of any program or another person's data, unauthorized voice or video recording of another person and the sharing of any information about or that relates to another person. Clause 2 also seeks to increase the fines for the offence of unauthorized access under section 12 of the principal Act from two hundred forty currency points to seven hundred fifty currency points.

The provisions of the Computer Misuse Act, 2011 which clause 2 seeks to amend state:

"(1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence.

(7) A person who commits an offence under this section is liable, on conviction, to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both."

The Committee has examined the proposals under clause 2 and appreciates that although the advancement in technology especially the computer-generated technology has improved communication and led to economic development, the internet has become a platform for misuse and abuse which calls for the strengthening of the existing legal framework. The Committee noted that the proposals seek to strengthen the protection of the right to privacy by regulating the emerging abuses especially on social media platforms.

The Committee however, observed that the proposed subsection (1) of the Bill excludes the element of "intent", yet intention is an essential element in the commission of criminal acts. This makes the provision overly broad to cover legitimate and inadvertent disclosure of information.

The Committee further observed that the proposed section 12(1) does not expressly provide for circumstances under which a person is deemed to have been authorized to access, intercept or share information. For example, information which is accessed, intercepted or shared with the consent of the person to whom the information is about or relates or where the information is accessed, intercepted or shared in compliance with the law should be expressly exempted. This will enhance clarity and allow the flow of legitimate information and authorized disclosures under the law.

## Recommendation

The Committee recommends that clause 2 be adopted with amendments to include the element of "intent" and clearly provide for circumstances under which a person is deemed to have been authorized to access, intercept or

share information.

# 5.2. Unauthorised sharing of information about children.

Clause 3 seeks to prohibit the sending, sharing or transmitting of any information about or relating to a child through a computer unless the person obtains consent of the child's parent, guardian, or any other person having authority to make decisions on behalf of the child.

The Committee has examined the proposals under clause 2 and appreciated the intended objective of the proposal which is aimed at strengthening protection and preservation of the right to privacy of children in the digital age. The Committee noted that threats to children's privacy in the digital space are increasing at alarming rates. Much as parents have a role to play in protecting their children's right to privacy, there is need to safeguard children's rights through enhanced regulation.

The Committee however, noted that clause 3 is overly broad given that it prohibits the sharing of any information about or that relates to a child unless consent of a parent or guardian is obtained. The provision has an effect of discouraging the public from sharing information about or that relates to a child in danger or in need of help since in most cases it is not probable to obtain the consent of the child's parent or guardian. This will discourage 'Good Samaritans' from coming to the rescue of children, thereby disregarding the best interest of the child principle which should be the primary consideration in all matters involving or affecting children.

The Committee is therefore, of the considered opinion that there is need to provide for circumstances under which information about children may be shared, including taking cognizance of the existing laws that already permit such disclosures.

Status .

The Pair

Notes

ezzu

8

**A** 

## Recommendation

The Committee recommends that clause 3 be adopted with amendments to provide for additional circumstances under which information about or that relates to children may be shared.

## 5.3. Hate speech.

Clause 4 seeks to prohibit hate speech through writing, sending or sharing of any information through a computer, which is likely to—

- (a) ridicule, degrade or demean another person, group of persons, a tribe, an ethnicity, a religion or gender;
- (b) create divisions among persons, or against a tribe, an ethnicity, a religion or gender; or
- (c) promote hostility against a person, group of persons, a tribe, an ethnicity, a religion or gender.

The Committee recognises that clause 4 is well intended given that it enhances the promotion of respect of human dignity, social harmony, cohesion, maintenance of public order and protection of rights of others.

The Committee comparatively analyzed the regulation of hate speech in other jurisdictions and observed that hate speech is a permitted limitation to the freedom of expression in a number of jurisdictions. In Canada, its Criminal Procedure Code prohibits hate speech and this was well decided by its Supreme Court in R Vs James Keegstra [1990] 3SCR 698-9 where Court considered a case where a teacher had taught anti-Jews propaganda to his students. The Supreme Court was faced with the determination of the balance between the right to freedom of speech outlined in the Canadian Charter of Rights and Freedoms and the law's limits on hate speech stipulated in the Criminal Code. The Court ultimately ruled against Keegstra, the teacher, by deciding that Canada's hate laws imposed a "reasonable limit" on a person's freedom of expression.

The South Africa's Promotion of Equality and Prevention of Unfair Discrimination Act, 4 of 2000 provides for the prohibition of hate speech under section 10 through publication, propagation, advocating or communication of words that could reasonably be construed to demonstrate a clear intention to be hurtful, harmful or to incite harm, or promote or propagate hatred.

The Committee further noted that the 2010 Constitution of Kenya under Article 33 (1) provides for freedom of expression and expressly provides for a clear limitation to freedom of expression. Clause 2 of the same article states that the right to freedom of expression does not extend to hate speech. In the same spirit, during the consideration of the appeal of Onyango Obbo & Anor Vs Attorney General (Constitutional Appeal No. 2 of 2002), the Supreme Court of Uganda considered and accepted a proposition of the Supreme Court of India in the case of Rangarajan Vs Jagijivan Ram & others; and Union of India & others Vs Jagijivan Ram (1990) LRC) which was to the effect that freedom of expression ought not to be suppressed except where allowing its exercise endangers community interest.

The Committee took cognizance of the offence of promoting sectarianism under section 41 of the Penal Code Act which is a permitted limitation to the freedom of expression. However, the Committee noted that the provision is restrictive in as far it restricts the targeted groups to a religion, tribe, ethnic or regional origin. The Committee further noted that the penalty prescribed does not match the gravity of the offence.

Therefore, the Committee supports the proposal under clause 4 that seeks to provide for the prohibition of hate speech.

Recommendation

The Committee recommends that clause 4 be adopted.

Jano

. Joé 6

Jan Co

H

## 5.4. Unsolicited information.

Clause 5 prohibits the sending or sharing of unsolicited information through a computer to or with another person. The proposal seeks to strengthen the protection of the right to privacy by fighting spam. The Committee appreciates that advancement in information technology offers users a massive range of new products and services. However, some users of online media platforms misuse or abuse the platform through sharing of unsolicited messages.

The Committee examined the proposal under clause 5 and observed that the Uganda Communications Act, 2013 and the Electronic Transactions Act, 2011 regulate the sharing of unsolicited SMS/MMS and unsolicited commercial communication respectively. The Committee however, noted that the regulation of unsolicited messages under the Uganda Communications (Text and Multimedia Messaging) Regulations, 2019 is restricted to short messaging service (SMS) and multimedia messaging service (MMS) and therefore, do not apply to unsolicited information/messages shared or transmitted over the internet such as WhatsApp etc. On the other hand, the Electronic Transactions Act, 2011regulates unsolicited commercial communication.

The Committee therefore, noted that clause 5 is overly broad since it impliedly includes unsolicited information already regulated under Uganda Communications Act, 2013 and the Electronic Transactions Act, 2011. The Committee is of the opinion that clause 5 should be restricted to the regulation of information shared or transmitted over the internet, with the exception of unsolicited commercial communication and unsolicited information in public interest.

## Recommendation

The Committee recommends that clause 5 be adopted with an amendment to clearly define the scope of unsolicited information to be regulated.

Aldrina St. tr

10

Husa H

# 5.5. Misleading or malicious information.

Clause 6 proposes to prohibit the sending, sharing or transmitting of any misleading or malicious information about or relating to any person through a computer. Clause 6 also seeks to create an offence for breach of the provision and provides for a penalty of a fine not exceeding seven hundred fifty currency points or a term of imprisonment not exceeding seven years, or both.

The Committee examined clause 6 and observed that, in the case of Charles Onyango Obbo and Another Vs Attorney General, Constitutional Appeal No. 2 of 2002, the Supreme Court declared section 50 of the Penal Code Act which provided for criminalization of publication of false news, unconstitutional. The proposal to criminalize sending, sharing or transmitting of misleading information has an effect of reintroducing the outlawed offence. The Committee is therefore, of the opinion that reference to misleading information under Clause 6 should be deleted.

### Recommendation

The Committee recommends that clause 6 should be amended to remove reference to the criminalization of misleading information.

## 5.6. Restriction on holding office.

Clause 7 seeks to introduce a new provision in the Computer Misuse Act to restrict leaders and public officers who commit any offence under the Computer Misuse Act from holding any public office for a period of ten years.

The Committee noted that the offences prescribed under the Computer Misuse Act, 2011 carry penalties which include fines and imprisonment sentences. Clause 7 therefore, seeks to impose an additional penalty on leaders and public officers, a proposal that is not only extreme and not commensurate to the offence, but also discriminatory since it targets a single category of the likely offenders and leaves out others. Given that the existing laws adequately provide

At

for the grounds for disqualifying or removal of leaders and also provide for grounds under which public officers may vacate or be dismissed from office, the clause should therefore, be deleted.

## Recommendation

The Committee recommends that clause 7 should be deleted.

## 5.7. Social Media

In the undertaking of the consideration of the Bill, the Committee observed that the information technology evolution has created a new medium of communication called Social Media that is not fully regulated in the existing laws.

The Committee further observed that Social Media is the commonest platform of Computer Misuse and noted the need to regulate the use of social media.

#### Recommendation

The Committee recommends that provisions be included in the Bill to regulate social media and clearly define social media.

## 6.0. CONCLUSION

Rt. Hon. Speaker and Honourable Members, the Committee has examined the Computer Misuse (Amendment) Bill, 2022 and recommends that it is passed into law, subject to the proposed amendments.

I beg to report.

12

Rose -

your De

# PROPOSED AMENDMENTS TO THE COMPUTER MISUSE (AMENDMENT) BILL, 2022

# CLAUSE 1: AMENDMENT OF COMPUTER MISUSE ACT, 2011

Delete clause 1.

## Justification

It is a consequential amendment arising from the deletion of clause 7.

## CLAUSE 2 AMENDMENT OF SECTION 12 OF PRINCIPAL ACT

Clause 2 is amended—

- (a) in the proposed subsection (1), by inserting the words "intentionally and" immediately after the word "who"; and
- (b) by inserting immediately after the proposed subsection (1), the following—
  - "(1a) A person shall be deemed to have obtained authorisation under subsection (1) where the person—
  - (a) obtains consent from the person to whom the information is about or relates; or
  - (b) is authorised by law."

## Justification

- The element of "intent" is an essential element in the commission of criminal acts. At common law, a mental element of a person's intention to commit a crime is paramount to secure a conviction.
- To achieve clarity by specifying the circumstances under which a person would be deemed to have been authorized under the proposed subsection (1).

## CLAUSE 3: INSERTION OF SECTION 22A IN PRINCIPAL ACT

Clause 3 is amended by substituting for the proposed subsection (1), the following—

- "(1) A person shall not send, share or transmit any information about or that relates to a child through a computer unless—
  - (a) the person obtains consent of the child's parent, guardian, or any other person having authority to make decisions on behalf of the child;
  - (b) the person is authorized by law; or
  - (c) the sending, sharing or transmitting of the information is in the best interest of the child."

## **Justification**

To enhance the protection of children by providing for additional circumstances under which information about or that relates to children may be shared.

## **CLAUSE 5: INSERTION OF SECTION 24A IN PRINCIPAL ACT**

Clause 5 is amended in the proposed section 24A—

- (a) in the proposed subsection (1) by inserting immediately after the word "computer" the words "unless the sending or sharing of the unsolicited information is in public interest."
- (b) by inserting immediately after the proposed subsection (2), the following—
  "For the purposes of this section, "unsolicited information" means information transmitted to a person using the internet without the person's consent, but does not include an unsolicited commercial communication."

## Justification

• The insertion in subsection (1) is to allow the sharing of legitimate unsolicited information in public interest.

M

Marke

14

Jun Je

- The insertion of the definition of the phrase "unsolicited information" is to achieve clarity.
- The exclusion of unsolicited commercial communication in the definition of "unsolicited information" is to ensure consistency since unsolicited commercial communication is already regulated under section 26 of the Electronic Transactions Act, 2011.

#### CLAUSE 6: INSERTION OF SECTION 26A IN PRINCIPAL ACT

Clause 6 is amended in the proposed section 26A (1) by deleting the words "any misleading or".

## Justification

To avoid contradiction with the Supreme Court decision in Charles Onyango Obbo and Another Vs Attorney General, CA No. 2 of 2002 which declared section 50 of the Penal Code Act that provided for the criminalization of publication of false news unconstitutional.

## CLAUSE 7: INSERTION OF SECTION 27A IN PRINCIPAL ACT

Delete clause 7

## Justification

- The additional penalty instituted on leaders and public officer on top of the criminal sanctions created under the Computer Misuse Act is excessive and discriminatory.
- The existing laws provide for sufficient grounds under which a leader ceases to hold office or may be disqualified from holding office.

#### **INSERTION OF NEW CLAUSE**

Insert a new clause immediately after clause 6 as follows—

## "Misuse of social media

(1) A person who uses social media to publish, distribute or share information, prohibited under the laws of Uganda or using disguised or false identity, commits an offence.

- (2) Where the information under subsection (1) is published, shared or distributed on a social media account of an organization, the person who manages the social media account of the organization, shall be held personally liable for the commission of the offence.
- (3) For the purposes of this section, "social media" means a set of technologies, sites, and practices which are used to share opinions, experiences and perspectives, and includes YouTube, WhatsApp, Facebook, Instagram, Twitter, WeChat, TikTok, Sina Weibo, QQ, Telegram, Snapchat, Kuaishou, Qzone, Reddit, Quora, Skype, Microsoft Team and Linkedin.
- (4) A person who contravenes subsection (1) is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding five years or both.
- (5) For the purposes of prosecution under this section, it shall be presumed, until the contrary is proved that the information published, distributed or shared on a social media account-
  - (a) which is verified by a social media operator has been published by a legal or natural person;
  - (b) is published, distributed or shared by the person or organization in whose name the telephone contact is registered;
  - (c) which is registered using an email address which has been used or submitted as data by any data collecting entity, is published by the person or organization in whose name the email address is registered."

#### Justification

To provide for the regulation of social media.

#### INSERTION OF NEW CLAUSE

Insert a new clause immediately after clause 7 as follows—

## "Amendment of section 30 of principal Act

The principal Act is amended in section 30 by repealing subsection (3)."

Justification

Subsection (3) of section 30 contradicts subsection (2) of the same provision which allows for the prosecution of a person who commits an offence under this Act, outside the territorial jurisdiction of Uganda.

Athing the state of the state o

# MEMBER SIGNATURE SHEET

NO	NAME	CONSTITUENCY	SIGNATURE
1	Hon. Magogo Moses Hassim	Budiope East	14116
	C/P	County	AMETO
2	Hon. Igeme Nathan Nabeta	Jinja South	
	D/CP	Division East	
3	Hon. Elotu Cosmas	Dakabela County	
4		Buyaga West	
	Hon. Tinkasiimire Barnabas	County	
5		PWDs	.00
	Hon. Ndeezi Alex	Representative	Mosi
6	Hon. Chemutai Phyllis	DWR Kapchorwa	
7	Hon. Acon Julius Bua	Otuke County	
8		Kasese	
	Hon. Kambale Ferico	Municipality	
9	Hon. Lolem Micah Akasile	Upe County	
10	·	Bunyole West	An to
	Hon. Mutiwa Geoffrey	County	th.m
11	Hon. Chelangat Alinga		Dille -
	Solomon	T'oo County	Milolomo
12	Hon. Nebanda Florence	DWR Butaleja	
13	Hon. Kamusiime Caroline	DWR Rukiga	
14	Hon. Kinobere Herbert	Kibuku County	<u> </u>
15	Hon. Ojok Andrew Oulanyah	Omoro County	TARRE
16	Hon. Feta Geofrey	Ayivu Division East	T, C

17	Hon. Afoyochan Esther	DWR Zombo	
18	Hon. Tumwine Anna Mary	DWR Ntoroko	Auri
19	Hon. Bainomugisha Jane Kabajungu	DWR Ibanda	
20	Hon. Bagala Joyce Ntwatwa	DWR Mityana	
21	Hon. Namugga Gorreth	Mawogola South	
22	Hon. Kazibwe Bashir Mbazira	Kawempe South	Allino
23	Hon. Isabirye Aga David	Jinja City North	
24	Hon. Kabugho Florence	DWR Kasese	Husa
25	Hon.	UPDF	
26	Hon. Mpindi Bumali	PWDs Representative	Lani
27	Hon. Abeja Susan Jolly	DWR Otuke	<b>A</b> ·
28	Hon. Musa Noah	Koboko County North	Muni
29	Hon. Kiiza Kenneth Nyendwoha	Bujenje County	