Proposed Changes to Uganda's Computer Misuse Law a Blow to Civil Liberties

Introduction

The Uganda Computer Misuse Act was enacted in 2011 to enhance safety and security in the increasingly digitised environment, including through the prevention of unlawful access, abuse or misuse of information systems including computers and securing the conduct of electronic transactions.

However, over the years this law has variously been used to suppress digital rights including free expression and access to information. For instance, academic and social critic Dr. Stella Nyanzi was arrested for insulting the president in a social media post. In 2019, she was convicted of cyber harassment contrary to section 24 of the Act but acquitted of offensive communications, which is proscribed under section 25. She was sentenced to 18 months imprisonment although the Court of Appeal acquitted her after determining that the prosecution's evidence was insufficient and the trial magistrate had no jurisdiction to convict her of cyber harassment.

Other individuals who have suffered the wrath of the same law include former presidential aspirant Henry Tumukunde who was arrested over alleged treasonable utterances in radio and television interviews, the Bizonto comedy group who were arrested over alleged offensive and sectarian posts, and author Kakwenza Rukirabashaija who was arrested, detained and prosecuted over offensive communication against the president and his son.

The Computer Misuse (Amendment) Bill, 2022, a private member's bill, was presented to Parliament in July 2022 before being referred to the Parliamentary Committee on Information and Communications Technology for scrutiny and collection of views from the public. The Bill's promoters argue that existing laws "do not specifically address regulation of information sharing on social media" or are "not adequate to deter the vice". Stated objectives of the amendment include to enhance the provisions on unauthorised access to information or data; prohibit the sharing of any information relating to a child without authorisation from a parent or guardian; prohibit the sending or sharing of information that promotes hate speech; prohibit the sending or sharing of false, malicious and unsolicited information; and to restrict persons convicted of any offence under the Computer Misuse law from holding public office for a period of 10 years.

There is a need to amend the Computer Misuse Act, 2011 due to advances in technology, upsurge in cybercrime, and controversial provisions that have rendered the law a tool for suppressing dissent. However, the proposed changes present fundamental concerns that should be addressed prior to the enactment of the Bill. The concerns are explained below.

Key Positives

- Given the advancement in technology and the upsurge in cybercrime, it is imperative that the Computer Misuse Act is amended to reflect the new technological dynamics and the evolving and increasingly sophisticated nature of cybercrime.
- The Bill makes strides to introduce a specific provision on hate speech under clause 4 which seeks to introduce section 23A in the Act. This provision will remove the uncertainties

presented by section 41 of the Penal Code Act Cap 120, which only provides for the prohibition of the promotion of sectarianism. Hate speech has previously been categorised under this provision.

- The Bill attempts to tackle disinformation, whose prevalence is hijacking political discourse and undermining civic participation. Clause 6, which seeks to introduce section 26A, provides that (1) that, "A person shall not send, share or transmit any misleading or malicious information about or relating to any person through a computer."

Emerging Concerns

Undermining Freedom of Expression and Access to Information

The proposed Bill greatly undermines the enjoyment of digital rights and freedoms including freedom of expression and access to information which are guaranteed by national, regional and international laws. The right to freedom of expression and access to information are guaranteed by various international and regional instruments, including the Universal Declaration of Human Rights (Article 19), the International Covenant on Civil and Political Rights or ICCPR (Article 19) as well as the African Charter on Human and Peoples' Rights (Article 9).

Article 19(2) of the ICCPR specifically provides that; "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. Although article 19(3) provides for certain limitations, these limitations shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Clause 5 of the Bill introducing section 24A prohibits the sending or sharing of unsolicited information through a computer. Unfortunately, the definitions of "unsolicited" and "solicited" are not provided. This presents uncertainties as to the scope of, and meaning of unsolicited information. Other jurisdictions have shown the difficulties of defining unsolicited information and how proscribing unsolicited information without offering clear definitions can unduly limit information access and sharing and free expression.

Since all information coming into possession of an individual or entity could potentially be categorised as 'solicited' or 'unsolicited', clause 5 could be misused and abused by the government and its agencies to curtail sharing and dissemination of information, which would limit freedom of expression and access to information.

Recommendation

i. Delete the entire clause 5.

ii. In the alternative, a clear definition and scope of the terms "unsolicited" and "solicited" should be provided.

Clause 6 on prohibition of sharing malicious or misleading information also undermines freedom of expression and access to information. This clause seeks to introduce section 26A to the effect that (1)

A person shall not send, share or transmit any misleading or malicious information about or relating to any person through a computer.

The publication of misleading or false and malicious information has become a major concern in society. However, the provision in its current state could be potentially used to limit freedom of expression and access to information since it limits sharing and dissemination of information and may promote malicious prosecution of individuals, particularly those who are critical of powerful individuals and groups. Moreover, Uganda's Supreme Court in Charles Onyango Obbo and Another v Attorney General has held that the penalisation of the publication of false news under Section 50 of the Penal Code is unconstitutional.

In April 2022, the United Nations Human Rights Council adopted a resolution on disinformation that called upon member states to ensure that their responses to the spread of disinformation comply with international human rights law and that their efforts to counter disinformation promote, protect and respect individuals' freedom of expression and freedom to seek, receive and impart information, as well as other human rights.

Thus, clause 6 presents vagueness and does not clearly relate to well-defined disinformation. It could as a result be potentially utilised to criminalise legitimate speech, including what state officials often term "false news".

Recommendation

Delete clause 6 of the Bill.

Duplication of the Data Protection law and the Regulation of Interception of Communications law.

Clause 2 of the proposed Bill aims to amend section 12 of the Computer Misuse Act to provide as follows:

> "(1) A person who, without authorisation, (a) accesses or intercepts any program or another person's data or information; (b) voice or video records another person; or (c) shares any information about or that relates to another person, commits an offence."; and
>
> (b)(7) A person who commits an offence under this section is liable, on conviction, to a fine not exceeding seven hundred fifty currency points or imprisonment not exceeding 10 years, or both.

The above proposals duplicate the law regulating interception of communication and the data protection and privacy law. They could potentially cause conflicts in enforcement if enacted, as indicated below.

Duplication of the Interception of Communications Law

The information and data which clause 2 relates to is already protected by the Regulation of Interception of Communications Act, 2010, which in section 2 prohibits the unlawful interception of communications.

Duplication of the Data Protection Law

Clause 2 is filled with issues and concerns which are already addressed by the Data Protection and Privacy Act that provides for the protection of personal data, data protection principles and the rights of the data subject. While clause 2 (a)(1)(a) of the proposed Bill prohibits access to another person's data and (c) sharing of information relating to another person, the Data Protection and Privacy Act in section 7 requires consent of the data subject before their personal data is collected or processed. Furthermore, the data protection law is emphatic on the need to seek and get consent of the data subject before sharing such data with a third party as stipulated in section 9(3)(c)(iii), section 13(2), and 19(b) on processing of personal data outside Uganda.

Clause 3 of the Bill seeks to prohibit unauthorised sharing of information about children. It provides that a person shall not send, share or transmit 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 proposed clause is redundant since section 8 of the Data Protection Act addresses unauthorised sharing of personal data relating to children.

Section 8 of the Data Protection and Privacy Act provides that a person shall not collect or process personal data relating to a child unless such collection or processing is (a) carried out with the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child; (b) necessary to comply with the law; or (c) for research or statistical purposes.

Recommendation
Delete clause 2 and 3 of the Bill.

Highly Punitive Provisions

The penalties which are prescribed by the proposed amendment, including Clause 2 on unauthorised access, interception, recording or sharing of information, clause 3 on unauthorised sharing of information about children, clause 4 on hate speech and clause 5 on unsolicited information, are high and excessive. The penalties proposed for these offences extend to fines not exceeding UGX 15 million (USD 3,900), imprisonment not exceeding 10 years, or both for unauthorised access, interception, voice or voice recording and sharing of information under clause 2. On the other hand, sharing information related to children (clause 3), hate speech (clause 4), unsolicited information (clause 5) and misleading or malicious information (clause 6) are punished with imprisonment not exceeding seven years.

The penalties in respect to punishing those who share information regarding children without the consent of their parents and guardians would be a good stride towards protecting children against unauthorised sharing of their personal data. However, the penalties for unauthorised sharing of personal data not relating to children in clause 2 are excessive and would limit freedom of expression, publication and sharing of information concerning errant individuals especially leaders.

Recommendation

Delete clause 2 and 3 of the Bill since they provide for highly punitive penalties and are redundant.

Undermining Accountable Leadership

Section 27A proposed for introduction by clause 7 of the Bill seeks to bar persons convicted under the Computer Misuse Act from holding public office for a period of 10 years, and to further dismiss

convicted public leaders from public offices that they were holding. According to the proposed Bill, a leader is defined under section 2 of the Leadership Code Act, 2002. The Leadership Code Act in the second schedule to section 2 provides a list of who political leaders include. Under the Leadership Code Act section 20(7), a person who is dismissed, removed from office, or convicted for breach of the Code as a result of the decision of the Tribunal, shall not hold any other public office whether appointive or elective for a period of five years from the date of dismissal, removal from office or conviction. This sanction is also lower than that prescribed under clause 7 of the Bill and has the potential to cause conflict in enforcement.

The adaptation of the definition of leaders to apply under the Computer Misuse Act seems to be facilitated by ill-motives to restrict and gag political leaders from being transparent and accountable, and exercising their rights, including to freedom of expression and access to information. In turn, the proposed section 27A (2) could be utilised to discourage whistleblowing by persons holding leadership positions where such disclosure would be necessary for enforcing transparency and accountability. Public officials in Uganda are already gagged under the Official Secrets Act which bars them from disseminating what may be considered "official" secrets of the government.

Recommendation

Delete the entire proposed clause 7.

Conclusion

The Computer Misuse Act 2011 requires amendment to ensure that it is up-to-date with the evolving nature of technology and fully protects digital rights. However, the amendments which are currently proposed are limited, do not address emerging technological challenges, have unfounded and redundant provisions, and stipulate highly punitive penalties. They potentially have adverse effects on digital rights including freedom of expression and access to information.

The provisions also fail to address some of the retrogressive provisions in the current law. For instance, the ambiguities presented by section 24 on cyber harassment and section 25 on offensive communication, which have been used to criminalise freedom of expression and are the subject of a Constitutional Court petition seeking to declare them unconstitutional, do not feature in the proposed Bill.

Moreover, the current proposals do not address some key cybercrimes that are currently affecting vulnerable communities such as women, for instance trolling, cyber harassment, unauthorised sharing of intimate images, and other forms of online violence against women and girls. A justifiable amendment should be comprehensive, addressing concerns that have emerged since the Computer Misuse Act was enacted.