MAKERERE LAW JOURNAL AUGUST 2022

Volume 31 Issue 1

A COMMENTARY ON THE COMPUTER MISUSE (AMENDMENT) BILL, NO. 16 OF 2022

Dr. Anthony C.K. Kakooza

Recommended Citation: Anthony C.K Kakooza (2022); "A Commentary on the Computer Misuse (Amendment) Bill, No. 16 of 2022," Volume 31 Issue 1, Makerere Law Journal, pp. 243-249

A COMMENTARY ON THE COMPUTER MISUSE (AMENDMENT) BILL, NO. 16 OF 2022

Dr. Anthony C.K Kakooza*

1.0 INTRODUCTION

The Computer Misuse (Amendment) Bill, No. 16 of 2022 (the Bill), was tabled in Parliament for first reading by Honourable Mohammad Nsereko, as a Private Members' Bill, in July 2022 to amend the Computer Misuse Act No. 2 of 2011 (the Principal Act). Its general objective is not only to create tougher penalties for the use of cyberspace by inserting new provisions on crimes in the principal Act, it also proposes stringent penalties for existent offences and those introduced by the Bill.

In this commentary of each of the clauses in the Bill, I set out to show that much as there is a need to curb abuse in cyberspace triggered by the rapid advancement in computer-generated technology, the proposed clauses in the Bill, risk throwing the baby out with the bath water.

2.0 RESERVATIONS CONCERNING PROPOSED REVISIONS OF THE PRINCIPAL ACT

Clause 1: Amendment of Section 2

In its current form, Section 2 of the Principal Act has no explicit meaning attached to the word 'leader'.

The proposed amendment defines a leader as having the meaning assigned to it under the Leadership Code Act, 2002. This interpretation would encompass the various groups referred to in the Second Schedule of the Leadership Code Act, as per the interpretation in Section 2 of the Leadership Code Act.

An amendment of the interpretation section to include the word "leader" is not necessary, where such word only appears once in the Act and the Amendment Bill itself. In any case, the proposed amendment clause in which it appears provides for "a leader or public officer".

The necessity question being put aside, the interpretation of the word 'leader' given in the Bill appears to cast a net that is rather wide and encompasses leaders of national political parties. It

* The author is a Lecturer in the Commercial Department of the School of Law, Makerere University and a Partner in Byenkya, Kihika & Co. Advocates.

then becomes questionable, over the context or as to what the intention of the section in which the word 'leader' is mentioned and applied. Is it arguable that the section on restriction from holding office might be politically tainted?
As I will argue in detail at a later stage, if this clause were to remain in the Bill, the term "public officer" should be preferred, as it encompasses a "leader."

Clause 2: Amendment of Section 12

Both the current Section 12(1) in the Principal Act and its proposed amendment are problematic. Section 12(1) in the former incudes, as having committed an offence, a person who intentionally accesses or intercepts any program or data without authority or permission.

The proposed substitution goes against a number of principles in the Copyright and Neighbouring Rights Act, No. 13 of 2006 (CNRA), which provide for limitations and exceptions to access to copyright as well as fair use provisions.[1] By way of example, if a person is undertaking research for educational purposes, under Section 15 of the CNRA, he or she does not need to obtain permission from the owner of such information, inclusive of information that is sourced through a computer.

In the same context, the definition for "intercept", in the Principal Act is rather vague because it is perceived to lean more towards interfering with the functionality of a computer as opposed to unlawfully accessing data. This would, to an extent, justify the amendment proposed in the Bill.
On the other hand, however, Section 2 of the principal Act, defines "access" as "gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective". On the basis of the definition of "intercept", as it appears in the Principal Act, the words 'access' and 'intercept', thus cannot be used together as is proposed in the amendment of Section 12 under clause 2 of the Bill.
We should bear in mind that a person undertaking online research falls under the definition of 'gaining access'. In this case, the proposed clause 2 would conflict with the principles of fair use under Section 15 of the CNRA.
Clause 12(1) (b) and (c) which prohibit the voice and video recording or sharing of information that relates to other persons, can be interpreted to encapsulate the rights of a performer which are protected in Section 22 of the CNRA, which would render the proposed amendment irrelevant.

---

1 Section 15, Copyright and Neighbouring Rights Act, No. 13 of 2006. It is also important to consider the fact that data or information on any computer device can also be considered as work in which a copyright subsists.

It can also be argued that the proposed amendment to Section 12 of the Principal Act is already sufficiently addressed in Section 7(1) of the Data Protection and Privacy Act, 2019 (DPPA). If a question is posed as to what the mischief is behind the need to come up with an amendment to Section 12 of the Principal Act, it would probably be that a data subject needs to provide consent before his or her data is accessed or intercepted.

However, clause 2 (a)(c) of the Bill on the sharing of information about or that relates to another person, when contextualised in respect of personal data as defined in Section 2 of the DPPA, has its object already captured in Section 7(1) of the DPPA. It can be reasoned therefore that there is no need for clause 2 of the Bill.

On the flip side, justification for clause 2 of the Bill can stem from the argument that the DPPA is not clear as to reprisal for unlawfully obtaining personal data. Sections 31 and 32 of the DPPA provide, as a remedy, for the person who believes that his or her rights have been infringed in this regard, the filing of a complaint with the Authority.[2] An investigation of the complaint would then follow. Specifically, Section 35(1) of the DPPA provides for a situation where a person unlawfully obtains personal data from a *data collector*, and not necessarily directly from the *data subject*. This is confusing and thus leaves a gap over the issue of unlawfully obtaining data from a data subject, hence justifying the proposed amendment under the Bill. However, rather than solve this lacuna by placing the penalty within the Bill, it would probably be more viable to clear up the anomaly in the DPPA itself.

It is also noted that the DPPA, 2019[3] and the Principal Act[4] both provide for punishment liability. Under the DPPA, liability is for a non-excess of 240 currency points (4.8 million shillings) or imprisonment ***for*** ten years, while under the Computer Misuse Act, imprisonment is ***not to exceed*** 10 years.

The proposed amendment raises the bar to 750 currency points (15 million shillings). Although the length of jail time under the Bill is in line with the current legislation, the proposed fine is rather high. It is likely that most convicts will face jail time as opposed to paying such a hefty fine.

2 National Information Technology Authority – Uganda or NITA-U
3 Section 35(2)
4 Section 12(7)

3.0 PROPOSED ADDITIONS TO THE PRINCIPAL ACT

Clause 3: Insertion of Section 22A

This provision proposes an inclusion of Section 22A on prohibiting unauthorized sharing of information about children. It can be argued that such unauthorized sharing of information can also be regarded as *offensive communication* which is covered under Section 25 of the principal Act (on disturbing the peace or right of privacy of any person). However, we should bear in mind that Section 25 of the principal Act has been challenged before the Constitutional Court as being unconstitutional.[5]

Nonetheless, Section 8 of the DPPA, which provides for parental or guardianship consent prior to collection of personal data relating to children, appears to have the same coverage as the proposed Section 22 A, save for the sanction under Section 22A (2). As such, the proposed Section 22A is an unnecessary repetition of already existing law.

Clause 4: Insertion of Section 23A – Hate Speech

Clause 4 of the Bill proposes the criminalisation of hate speech.

Hate speech has no particular definition under international human rights. This complicates giving a perspective as to where to draw the line with freedom of expression. The Council of Europe explains that it is a term used to describe broad discourse that is extremely negative and constitutes a threat to social peace.[6]

One angle to render this proposed amendment inessential can be to refocus on Section 25 of the Principal Act on offensive communication. It can be argued that offensive communication sufficiently caters for hate speech, subject to the current ghosts of looming unconstitutionality hovering over this section.

The alternative argument would be to look at the ingredients of hate speech proposed under Section 23A to justify the proposed amendment. They include ridiculing, degrading, demeaning persons or groups of persons; creating divisions, and; promoting hostility among and against groups of persons, ethnicities, religions or genders. Under this proposed law, a conviction would thus only be raised if proof of intent (i.e., an element of mens rea) in that direction, is manifested

---

5 See: *Gwogyolonga S. Nsamba and 2 Others versus Attorney General*, (Constitutional Petition No. 15 of 2017) It should be noted, however, that the Constitutional Court is yet to pronounce itself on this petition as well as other similar petitions filed by other parties, such as the Uganda Law Society.

6 Council of Europe: 'Hate Speech', available at: <https://www.coe.int/en/web/>, accessed August 3 2022

in Court. To a great extent, it would so happen to be difficult to prove these intentions in court. Ultimately, this would protect acts of parody, academic discourse or innocent communication, which then falls back to protection under the freedom of expression principle.

Clause 5: Insertion of Section 24A – Unsolicited information

It is proposed in this clause that the sharing or sending of unsolicited information is to be criminalised.

This proposed section does not give due consideration to innocent or unintentional sharing of unsolicited information; freedom of expression[7]; or access to information.[8] These rights are many a time exercised by the expression, sharing or sending of unsolicited information.

By drafting this provision in such a broad manner, it is likely to be subjected to a number of constitutional petitions similar to Section 25 of principal Act. For instance, social groups, including WhatsApp groups comprising of family members, work colleagues, high school association groups and many others would be affected where a member of such a group posts something without the solicitation of any other member(s).

It would be advisable to rephrase it, if at all it is to remain, in a manner wherein exceptions can be provided, similar to Section 26 of the Electronic Transactions Act, No. 8 of 2011. The said section is restrictive to transactions or e-commerce communications and gives provision for someone who does not want any more unsolicited information to be sent to him or her, to notify the sender accordingly.

In its current form, clause 5 is thus a barrier to web-based social interactions as well as e-commerce and online businesses which gain traction through advertising on social platforms and groups. Many of these advertisements are unsolicited and these businesses risk unconsciously breaking the law or missing out on business opportunities or both.

Clause 6: Insertion of Section 26A – Misleading or Malicious Information

Clause 6 of the Bill prohibits the sending, sharing or transmitting of any misleading or malicious information about a person or relating to any person through a computer.

To an extent, this is already covered under Section 25 of the DPPA, which provides for the right to prevent processing of personal data. It can be argued that processing of personal data would include misleading personal data. However, the shortfall in relying on Section 25 of the DPPA, is

7 Article 29 of the 1995 Constitution of the Republic of Uganda
8 Article 41 of the 1995 Constitution of the Republic of Uganda

that the DPPA provision is restrictive to data controllers or data processors and not "a person", which would thus justify this proposed provision to fill in the gap.

In the alternative, it should also be considered that a tortious liability action, such as defamation, can be taken out against someone who posts misleading or malicious information. This would thus rule out the need to create a criminal sanction over the same, as is proposed in the Bill.

Clause 7: Insertion of Section 27A – Restriction on Holding Office

This clause introduces a restriction on the holding of office by a person who has been convicted under the principal Act for a period of ten years.

This proposed provision is reasonable, based on the general requirement of 'moral conduct' of someone holding a public office. However, the provision should also consider that, apart from being convicted, such person should also have been dismissed or removed from public office as is stipulated under the law.[9] It can also be argued that the phrase 'public officer' is wide enough in scope to cover a 'leader' and therefore dispels of the need to state 'leader or public officer' as is provided under the Bill.

Furthermore, denial of a convict under this law, from holding public office over a ten-year period, is very restrictive, considering that, ideally, the minimal term of holding public offices is between four and five years. This is a seemingly hefty punishment upon, say, a youthful person, who serves his or her punishment, goes through reconciliation and is ready to move on.[10] Such person would, however, be held back from progress in life, particularly through taking up a public office, because of a ten-year impediment to personal development. It is therefore preferable that such proposed restriction is limited downwards to a five-year period.

4.0 CONCLUSION

Cyberspace is always evolving and the law can never keep up with it. Unfortunately, although such developments in the Information, Communications and Technology (ICT) Sector ease our lifestyles, they also attract negative social tendencies that call for stringent regulation of ICT usage. As such, for sanity to prevail, regulation of cyberspace is a welcome endeavour. Nonetheless, as

9 This would be an action in line with Article 235 of the 1995 Constitution of the Republic of Uganda for breach of the Leadership Code.

10 It should be considered that the majority of persons likely to be charged under this proposed section of the law, would be youthful persons, since it is such category of persons that engage in cyber related activities.

we seek to regulate how we utilize the ICT sector, we should be mindful of the existing socio-economic rights around us, and the roles they play in easing social and economic interaction.

Stifling the rights associated with the freedom of expression; access to information; and the limitations and exceptions to copyright, among others, would be counterproductive. By proposing to use a sledgehammer to hit a mosquito that is biting one's arm, the Computer Misuse (Amendment) Bill may only end up decapitating the arm. Overall, it is an unnecessary amendment to the law, with already existing alternatives, which can be utilized in realizing what it seeks to enforce.