

Assessing the proposed amendments to the ICT Act to regulate social media in democratic Mauritius

Analytical paper by:

Christina Chan-Meetoo

Senior Lecturer in Media and Communication

University of Mauritius

chanssc@uom.ac.mu

19 May 2021

Foreword

On 14 April 2021, the Information and Communication Technologies Authority (ICTA) released a Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius.

Members of the public were invited to submit their comments on the proposal by email to a dedicated email address (socialmediaconsultation@icta.mu) by a first deadline of 5th May 2021 which was then extended to the 20th May 2021 further to requests from the public. This process is a positive one as it gives the opportunity for anyone who wishes to react and reflect on the proposed amendments.

Below is a paper which analyses the proposed amendments and associated mechanism for regulating social media in Mauritius as presented by the ICTA Consultation Paper.

What are the justifications provided for the proposed amendments?

There is a perceived need for regulation of social media in Mauritius. The stated objective is to combat illegal and harmful content (and comment) in a way that is not dependent on international social media companies. These platforms are deemed to be not sufficiently responsive to requests from the authorities in terms of:

- time taken to respond,
- community standards which are not as strict as nor necessarily compliant with our domestic laws, and
- the Creole language which the platform moderators do not necessarily understand.

The paper states that a “*minority of individuals or organised groups*” are at fault and that “*The issue at hand is when these abuses, even though perpetrated by few individuals/groups, go viral, the damage created is very far reaching.*”

Preliminary comment about the justifications provided for the proposed amendments

A first comment is that a list of concrete examples is needed here to gauge the extent of the problem at the national level. Before proposing any solution, the exact nature of an existing problem needs to be examined in detail. This should include detailed information about the “*very far reaching damage*” created. The consultation paper does include a table listing the number of incidents reported to the Mauritian Cybercrime Online Reporting System (MAUCORS). But, this is barely sufficient to really gauge the real extent of the issue.

We would thus need more details on the following aspects (inter alia):

- the investigation process for all of the incidents reported in the table,
- the actions taken by the authorities in all of these cases,
- whether these incidents were dealt with locally by law or reported to the social media platforms,
- and the results obtained by local authorities and final outcomes achieved.

An in-depth analysis of all of the above would be needed. This would enable an objective evaluation of the proportionality of the proposed mechanism with respect to the extent of the problem to be addressed. In a nutshell, the question is: **How big is the problem of misuse and abuse of social media really in the country that warrants such far-reaching measures as those being proposed by the ICTA in its consultation paper?**

What are the proposed amendments to the ICT Act?

To summarise, the ICTA is proposing the creation of:

- a National Digital Ethics Committee (NDEC) as the decision-making body on the contents. The key mandate of the NDEC would be to: *"investigate on illegal and harmful content on its own or through interaction with other stakeholders already involved in national security, crime investigation, detection and prevention or through complaints received;"*
- a Technical Enforcement Unit to enforce the technical measures as directed by the NDEC.
- a technical toolset to be deployed whereby internet users in Mauritius will have to use a local proxy server as intermediary and will be asked to install a self-signed digital certificate allowing them to be accepted as intermediary by the browser or the app, thereby bypassing the https protocol. The stated objective is to allow the proxy server to:
 - segregate traffic to and from social media sites,
 - decrypt such information
 - analyse and store data for investigations purposes

Comment about the underlying philosophy for the proposal

The adjective *"harmful"* needs to be defined clearly with a list of all types of content and the criteria which will be used to classify such content as harmful. Otherwise, this will inevitably lead to questions in the public's mind about what is allowed and what is not allowed. In other words, the "rules of the game" should be clearly spelt out in advance.

There is an inherent risk of potential abuse and misuse by authorities and any parties involved in the mechanism if the term *"harmful"* is not clearly defined. An important matter such as this cannot be open to interpretation, bearing in mind that the principle of potential "alternance" of parties in power is still valid in Mauritius and that there is always a risk of petty power games as a result.

Assuming that the intention of the current appointees of the ICTA with this proposal is genuinely to create a safe online public sphere in Mauritius and to work for the greater good rather than for vested interests, there is no guarantee that subsequent appointees would follow suit. The adjective *"harmful"* which leaves the door open to interpretation is thus highly risky, including for those who currently occupy positions of authority. The adjective *"illegal"* is clearer as this relates to the laws of the country, which are enacted by parliament, interpreted by courts of justice and implemented by policy-makers.

More importantly, the main issue with this proposal is a potential conflict with Section 12 of the Constitution as highlighted in the paper itself.

What does Section 12 of the Constitution say?

As a reminder, Section 12 of the Constitution of Mauritius¹ states that:

"12. Protection of freedom of expression

(1) Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision— (a) in the interests of defence, public safety, public order, public morality or public health;

(b) for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the Courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting, television, public exhibitions or public entertainments; or

(c) for the imposition of restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society."

¹ The Constitution of Mauritius, available at:

<https://attorneygeneral.govmu.org/Documents/Laws%20of%20Mauritius/A-Z%20Acts/C/Co/Constitution.%20GN%2054%20of%201968.pdf>

12. Protection of freedom of expression

(1) Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision—

(a) in the interests of defence, public safety, public order, public morality or public health;

[Issue 1]

CON – 14

(b) for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the Courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting, television, public exhibitions or public entertainments; or

(c) for the imposition of restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.

Extract of the Constitution of Mauritius

This section states that there can be no interference in our communications except with our consent and except for specific provisions involving public defence, safety, order, morality and health, reputation, privacy, courts authority, technical administration of telecoms and civil service restrictions. BUT, the last line puts everything in perspective as the provisions should be “*justifiably reasonable in a democratic society*”. Unfortunately, the proposed amendments to the ICT Act do not seem “justifiably reasonable in a democratic society”.

The proposal is tantamount to blanket surveillance on the citizens of Mauritius without judicial oversight. No warrant would be needed to spy on specific individuals. ALL citizens’ communication would be interfered with in a blanket manner. The proportionality test is here crucial to determine whether such a surveillance system is really warranted in a democratic society like ours. Does this pass the balance of risks/benefits? Fundamentally, this proposal seems to contradict the philosophy of the Data Protection Act which aims to protect citizens’ private data and which was adopted in 2017 (and modelled on the EU GDPR).

What are other democratic states doing or proposing to address abuse and misuse of social media?

We do not know of any other democratic state which is using such a system as the one proposed by the ICTA. This would be a first in the world, in the negative sense of the word. As a result, there is a high probability that Mauritius will tumble down in world freedom rankings.

In all the democratic states cited in the consultation paper, the responsibility for moderation and removal of illegal content remains vested with the social media platforms.

In Germany, the Network Enforcement Act has forced platforms such as Facebook to employ many more moderators for the country and the law provides that the data should be stored by the platforms for only up to 10 weeks.

In the UK, Ofcom has been tasked with the regulation of social media and the Chief Executive states on the official website that *“We won’t censor the web or social media. Free expression is the lifeblood of the internet and it’s central to our democracy, values and modern society.”* and *“We won’t be responsible for regulating or moderating individual pieces of online content. The Government’s intention is that online platforms should have appropriate systems and processes in place to protect users; and that Ofcom should take action against them if they fall short. We’ll focus particular attention on tackling the most serious harms, including illegal content and harms affecting children.”*

India has recently introduced new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules which require “significant” social media intermediaries (based on the number of users) to have a local representation with a Chief Compliance Officer, a Nodal Contact Person and a Resident Grievance Officer and the platforms would need to publish regular reports about compliance with a Code of Ethics.

There have also been intense debates in all cases and some parts of legislations proposed had to be reviewed or are still being reviewed with no successful model emerging for the time being. For instance, large sections of the French Loi Avia were deemed anti-constitutional by the Senate and had to be reviewed.

The key takeaway here is that State agencies in democratic countries are not endowing themselves with any technical capacity to interfere, intercept and remove any content on social media in comparison with the Mauritian ICTA proposal.

Despite not being an expert in technology, I can assume that the mechanism for intercepting, decrypting and re-encrypting social media traffic requires enormous technical capabilities given the enormous amounts of data (photos, videos, livestreams, etc.) generated daily. It is also very much a moving target because nothing can prevent any social media network from changing some implementation details which might make the system ineffective. Anyway, anyone can bypass the system just by using a Virtual Private Network (VPN), .

Other key questions posed by the proposed amendments

- Will all social media be concerned? Will there be a list which will be published and updated?
- Would the filtering, analysis and classification be done by humans or by a software? If so, would the code be transparent and open to scrutiny?
- What about the potential risk for middleware to be tampered with? (by subcontractors for example)?
- What will be the composition of the National Digital Ethics Committee? What criteria will be used to designate the chairperson and the members?
- What will be their expected volume of work (given that there are enormous amounts of content being created everyday)?
- What criteria will be used for assessing content?
- Will there be hearings in case an individual or group is suspected of creating and disseminating “illegal and harmful content”? Will there be an appeal system?
- What will be the safeguards against misuse and abuse of the mechanism?
- Is there sufficient technical capacity to handle the volume of data generated and shared on social media on the national level? What about potential issues with quality of service on the network which may affect the digital sector of the economy as well as all operations of non-digital firms which use digital tools to effect transactions, promote their products and services, handle internal processes and information?
- Will the digital certificate installation be compulsory? How? What if people refuse? What if people resort to VPNs?
- Have other solutions been explored? How far? Could the analysis be made public? How about strengthening local investigation capacity?

- The issue of monetisation of news content and payments to be made by platforms to local media in the case of Australia is also cited. How is this related to the proposed amendments?
- According to the press communiqué issued by the ICTA, private messaging apps will not be concerned by the amendments. Why is the example of killings following false rumours of child kidnapping spread through WhatsApp in India cited in the proposal?

What are potential alternatives to the proposed amendments?

- The last question in the consultation paper asks citizens if they think that local courts of justice should be empowered to “*impose sentences (which include banning use of social media) on persons convicted of offences relating to misuse of social media tools*”. This may indeed be explored.
- Preventive measures such as education, sensitisation and digital literacy remain crucial to create a more civic space online.
- We could also explore the use of our diplomatic connections at the regional level to enter into negotiation with the social media platforms in order to improve their responsiveness to requests from local authorities (eg. AU, SADC).

Conclusion

It is a positive sign that this paper is the subject of public consultation, thus requiring inputs from Mauritian citizens as individuals or groups, hopefully shaping the outcome of the final decision to amend legislation or not. In the same spirit, the next phase of the process should be transparent, that is, it is expected that there be a public report about inputs received and how these inputs are tackled by the ICTA and any other authority involved in the process. We welcome the statement in the Consultation paper that *"The comments will then be compiled as well as the way forward on this issue will be posted on ICT Authority's website, www.icta.mu."* and hope that this will be indeed the case.

On the basis of information provided so far, the present proposed amendments do not seem reasonable at all in terms of the proportionality of the measures with respect to the problem to be tackled. Rather, they represent a significant threat to our democratic setup and may have far-reaching repercussions not only on the social and political but also on the economic fronts.

Summary of questions being released for public consultation

14.1 What are your views on the present approach of self-regulation of social networks by social media administrators themselves where they decide to remove an online content or not based on their own usage policy and irrespective of your domestic law?

Countries around the world face issues concerning circulation of posts which are potentially in breach of their domestic laws on social media platforms. There is, at present, no fully satisfactory response which is proposed or effectively deployed in any democratic country. Only non-democratic countries have recourse to drastic measures aiming to block and/or intercept all of their own citizens' online communications and social media traffic in an attempt to regulate the same. As a democratic country, Mauritius cannot use methods which would be more suitable for non-democratic regimes.

It is true that the content being circulated online which either targets or is created by Mauritian citizens on social media may be in breach of domestic laws. However, an objective assessment of the extent of such illicit content being circulated needs to be conducted to determine the extent of abuse and/or misuse as already specified in the above paper,

It should also be recalled that social media platforms offer various levels of privacy, meaning that one may categorise the online communication sphere created by these into multiple sub-categories, which can tentatively be broadly listed as follows:

1. **Online national public sphere** created by public personalities (prominent members of society such as politicians, leaders of big organisations, community and religious leaders, opinion leaders, etc.) and organisations (whether public or private bodies) who decide to publish their posts on the full "public mode" level. Their content becomes accessible to anyone without the need to be directly connected as "friends" or "friends of friends". They generally have a large number of followers/friends and their posts can be shared, thereby enabling them to become viral.
2. **Targeted public circles** created by specific individuals and bodies who wish to communicate within a semi-restricted sphere, upon invitation.

3. **Private circles** whereby an individual or entity communicates only with their friends and whose posts cannot be shared outside of the network of friends.

There are obviously more levels of control which are generally available on some social media platforms in between those three broad categories. Suffice to say that the first level (online national public sphere) is the one which should command the most attention, followed by the second level (targeted public circles) whereas the third level (private circles) may be considered the equivalent of private conversations between private individuals.

Individuals and entities who have large follower bases in the online national public sphere and targeted public circles are the ones who should be more subject to scrutiny as they have the potential for virality and their speech is tantamount to public speech, which may be evaluated against prevailing domestic laws.

As it is, the responsibility for regulating content rests primarily on the social media platforms themselves, the most popular of which are based overseas, thus not directly subjected to domestic laws. These platforms use their own terms of use or community standards to evaluate content (1) when prompted by other users who flag potential issues or (2) when their internal algorithms detect highly sensitive content requiring intervention by the platform.

Intense debates have taken place after the occurrence of major incidents linked to social media accounts of public figures such as former US President Donald Trump. The latter's account was shut down on platforms such as Twitter and Facebook after the Capitol invasion in January 2021 when he lost elections. Despite multiple posts which contained fake news and racist comments during his presidency, he was only banned from social media platforms when he lost the last elections, thus sparking debates about whether all major public figures around the world would henceforth be liable to similar treatment by the platforms. This was one of the most prominent cases entrusted by Facebook to its own Oversight Board² for review. The Facebook Oversight Board published its ruling on 5th May 2021 and upheld the decision but requested that Facebook

² The Oversight Board's website is accessible at: <https://oversightboard.com/>

review the decision within the next six months and also develop clear, necessary, and proportionate policies that promote public safety and respect freedom of expression³.

Thus, it can be deduced that platforms are not monolithic organisations and they are prone to debates both on the internal and external fronts. All parties involved still fray with the delicate issue of regulation and remain open to reviews and possible disruption of their moderation policies and mechanisms.

These mechanisms remain unsatisfactory and will probably never ever be satisfactory due to the complexity involved whereby the very same platforms can be used:

- to mobilise for good causes or incite bad mass behaviour,
- to communicate on different levels such as one-to-one, one-to-few, few-to-few, one-to-many or many-to-many.

Regulating social media is not an easy task and a simple one-size-fits-all solution will simply not work without creating bigger prejudices.

14.2 Do you think that the damage caused by the excesses and abuses of social networks to social cohesion warrants a different approach from the self-regulatory regime presently being enforced by social media administrators themselves?

There is not enough data which has been made available about the damage caused by the excesses and abuses of social networks to social cohesion in Mauritius to be able to formulate an informed reply to this question. The data remains impressionistic rather than scientific. For instance, how many such cases have there been over the last years and months that have not been detected and tackled through the current investigation and legal system? What have been the trends in the number of such cases? What is the exact breakdown? What have been the actions taken by authorities? In what way have they been insufficient? To date, we have no knowledge of massive excesses that have created havoc in the social tissue of our country. There have been no major riots nor major ethnic conflicts which have been reported by the Mauritian police over the past few days that we know of.

³ Case decision 2021-001-FB-FBR accessible at: <https://oversightboard.com/decision/FB-691QAMHJ/>

14.3 What are your views on the overall proposed operational framework in terms of the

- **National Digital Ethics Committee (NDEC)**
- **Enforcement Division**

which is intended to bring more clarity to section 18 (m) of the ICT Act, where the ICTA is mandated to take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services.

Please refer to comments made in the paper submitted above.

14.4 What are your views on the proposed legal amendments to the ICT Act to give legal sanctity and enforcement power to the NDEC?

This is a risky proposal as the composition of such a committee will inevitably be reviewed each time a new political party or coalition gains majority in the National Assembly to constitute government. Such powers should rest only within the justice system to ensure impartiality and independence from political power games.

14.5 What are your views on the proposed modus operandi of the NDEC?

There is scant information provided in the consultation paper about the modus operandi of the proposed NDEC. It merely stipulates that *"it is proposed that the Chairperson and members of the NDEC be independent, and persons of high calibre and good repute."*

There are no indications whatsoever about the following:

- Number of members
- Composition of the committee (profiles of members)
- Process for nomination of members
- Duration of mandate for members
- Process for evaluating complaints
- Existence of a review or appeal systems (as opposed to the justice system where the different appeal levels are clearly defined by law)
- Proposed stages of penalty or fines (as opposed to the justice system where maximum sentences and fines are clearly defined by law)

14.6 What are your suggestions on the safeguard measures to be placed for the NDEC?

No specific safeguard measures for the NDEC have been proposed in the consultation paper. The paper merely stipulates that:

"Before start of operations, the NDEC will also be tasked to come up with sufficient and effective safeguards to be published in order to ensure complete operational transparency and avoidance of any abusive use and misuse of this operational framework."

First and foremost, the nature of the committee itself is problematic and one cannot expect the committee to define its own safeguards, which would be the equivalent of a watchdog being asked to watch over itself.

14.7 What are your views on the use of the technical toolset, especially with respect to its privacy and confidentiality implications when enforcing the mandatory need to decrypt social media traffic?

As stated by major browsers namely Google and Mozilla in their joint submission⁴, the proposed technical toolset is very dangerous as it would undermine the privacy of Mauritian citizens and put them at risk of attacks by third parties if it does work. Browser makers may decide to block the system. The proxy server may be clogged down by the volume of traffic to be handled and may even be targeted by cyber attacks. As a result, access to the internet may be slowed down or even paralysed for all in Mauritius. This would not only impact citizens but also foreigners communicating and transacting with people based in Mauritius as well as local and international corporate entities.

This toolset can set us back completely as an aspiring tech hub. We may lose business and partnership opportunities, incoming FDI, inbound tourists, and existing foreign companies may prefer to move their branches or headquarters to other countries.

If this toolset is implemented, Mauritius will also undoubtedly be downgraded in international indices such as Freedom House, Reporters Without Borders, the ITU ICT Development Index, the Global Innovation Index or even the Ease of Doing Business index, inter alia. The repercussions for the economy may be far-reaching. Many international organisations have already expressed their concern and opposed the proposed amendments to the ICT Act⁵.

⁴ Joint submission by Mozilla and Google available at:
<https://blog.mozilla.org/netpolicy/files/2021/05/Mozillas-Response-to-the-Mauritian-ICT-Authoritys-Consultation.pdf>

⁵ See public statements at:
<https://www.accessnow.org/cms/assets/uploads/2021/05/Mauritius-ICT-Act-Submission.pdf>
<https://www.eff.org/deeplinks/2021/04/proposed-new-internet-law-mauritius-raises-serious-human-rights-concerns>

14.8 Can you propose an alternative technical toolset of a less intrusive nature which will enable the proposed operational framework to operate in an expeditious, autonomous and independent manner from the need to request technical data from social media administrators?

No technical toolset can be proposed at the local level. Solutions should preferably be sought in consultation with the social media platforms and the legal and judiciary should be better equipped to deal with complaints related to social media.

In the first case, diplomatic negotiations should be leveraged with regional organisations such as the African Union, SADC and COMESA or international partnerships such as with fellow Commonwealth and Francophone allies and SIDS (Small Island Developing States).

When reinforcing our legal capacity to tackle infringements to domestic laws on social media, the investigative teams within the police force also need to be provided with regular training as technological products and services evolve quickly.

More importantly, if abuse and misuse of social media in breach of domestic laws are to be tackled in a sustainable manner, it is very important to invest in nation-wide as well as targeted campaigns for:

- digital literacy,
- media and information literacy,
- civic education.

14.9 Should the Courts be empowered to impose sentences (which include banning use of social media) on persons convicted of offences relating to misuse of social media tools?

The responsibility of adjudicating sentences should indeed remain within the judiciary system of Courts as learned magistrates and judges are trained professionals for adjudicating sentences.

The investigative teams within police departments concerned should also be reinforced through capacity building.