Information & Communication Technologies Authority

Consultation Paper on
proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius

Publication date: 14 April 2021

Deadline for submission of comments: 05 May 2021

Table of Contents

Part I

1. Executive Summary

By enabling end users to publish online content and share it with other users, social media networks have indeed revolutionised the communication industry by offering everyone a direct channel for expressing their views. Nevertheless, the possibilities offered by social networking services can also lead to unacceptable abuse of those same freedoms. Moreover, in Mauritius, when offensive and abusive online content is posted in the native creole language, in the majority of cases, complaints made by local authorities to the social media administrators remain unattended or are not addressed in a timely manner.

Legal provisions prove to be relatively effective only in countries where social media platforms have regional offices. Such is not the case for Mauritius. The only practical solution in the local context would be the implementation of a regulatory and operational framework which not only provides for a legal solution to the problem of harmful and illegal online content but also provides for the necessary technical enforcement measures required to handle this issue effectively in a fair, expeditious, autonomous and independent manner.

Under section 18 (m) of the Information and Communication Technologies (ICT) Act, the Authority is mandated to take steps to regulate or curtail the harmful and illegal contents on the Internet and other information and communication services. Given the generic nature of this function, the idea is to bring more clarity under this mandate by

- **completely separating the need to first properly identify whether the online content is an illegal and harmful content; and**

- **putting in place technical enforcement measures to curtail the identified illegal and harmful content.**

The amendments to the ICT Act will define a two-pronged operational framework with the setting up of:

- **a National Digital Ethics Committee (NDEC) as the decision-making body regarding the harmful and illegal content; and**
- **a Technical Enforcement Unit to enforce the technical enforcement measures as directed by the NDEC.**

The composition and mode of operation of the NDEC are instrumental not only for the smooth operation of the proposed framework, but also for the prevention of any attempt to make an abusive use of this operational framework.

In order to regulate the use of social media and to operationalise the above, the deployment of a new technical toolset is mandatory and requires the decryption of encrypted traffic on social media platforms. To make this happen, it is important to **segregate from all incoming and outgoing Internet traffic in Mauritius, social media traffic, which will then need to be decrypted, re-encrypted and archived for inspection purposes as and when required.**

While respecting our constitutional provisions, the amendments to the ICT Act have been proposed to effectively address any inappropriate use of social media platforms in our local context, while at the same time avoiding any possible abuse of this enforcement measure by putting into place the required safeguards.

2. Introduction

2.1 The communication industry has been revolutionised by social media networks. Nevertheless, the possibilities offered by social networking services also give rise to unacceptable abuses by a minority of individuals or organised groups, to which social media administrators are not providing sufficient and timely responses. The issue at hand is when these abuses, even though perpetrated by few individuals/groups, go viral, the damage created is very far reaching. In the early 2000s, social media firms argued that they simply created tools that enable distribution of information. They did not regulate the content on their platforms, and people were able to share their thoughts and opinions freely. This has remained the practice for a long time and often to the detriment of people around the world.

3. Impact of Social Media Platforms

3.1 In July 2018, at least 17 persons were killed over false child kidnapping rumours being spread through Facebook's subsidiary WhatsApp in India. In November 2018, Facebook was used to spread hate speech and incitement that led to violence against the Rohingya minority within the country in Myanmar which led to some 700,000 members of the Rohingya community fleeing the country amid a military crackdown and ethnic violence. In recent years, these companies have come under a lot of scrutiny. For e.g. Facebook's involvement in the Cambridge Analytica scandal (data leak on potentially over 87 million users, with 70.6 million of those people from the United States) in early 2018 and also YouTube's involvement in the dissemination of the Christchurch live stream (gunman killed 50 people and injuring 50 more in a mosque in New Zealand) in March 2019, these figures demonstrate

that people are becoming increasingly concerned with the amount of power held by social media companies.

3.2 These events have prompted a shift in the mindset of both regulators and social media companies that social media companies are much more than mere technical platforms. Currently, social media platforms are applying self-regulating measures. However, the current approach of self-regulation of social media platforms by their own administrators is exclusively based on their own acceptable usage policies irrespective of the domestic laws of individual countries, and are still evolving. Several jurisdictions around the world are also coming up with legislative frameworks to make social media companies accountable for their online content and impose sanctions on them in case of non-compliance with their respective domestic laws. Regulators around the world are scrambling to deal with this growing problem and the big challenge for them is to create regulatory solutions that curb their power in a way that promote competitiveness, innovation and openness online.

3.3 In Mauritius, we face the added difficulty of the language barrier. In this self-regulatory regime, when offensive and abusive online contents are posted in the native creole language, social media administrators need to first translate and properly understand the meaning of these posts in the local context. In the majority of cases, complaints made by local authorities to the social media administrators remain unattended or are not addressed in a timely manner.

4. Measures taken at the international level

4.1 Germany

4.1.1 **In January 2018, the Network Enforcement Act, NEA was promulgated to prompt social media companies to quickly remove "illegal content" within 24 hours of it being uploaded online. Under this Act, illegal content has been defined as content that ranges from insults of public office to threats of violence. Offenders under the Act could face large fines exceeding €50 million.**

4.2 United Kingdom

4.2.1 **In April 2019, the U.K. government announced that it would create legislations to make the U.K. the safest place in the world to use the internet. The British government intends to establish a new statutory duty of care to make social media companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. Compliance with this duty of care will according to the British government be overseen and enforced by an independent regulator.**

4.2.2 **It is expected that the UK regulator will have a suite of powers to take effective enforcement action against companies that have breached their statutory duty of care which may include the powers to issue substantial fines and to impose liability on individual members of senior management.**

4.3 France

4.3.1 **In May 2020, the French Parliament passed a hate speech law (Avia law, Loi No. 2020-766 du 24 juin 2020) which punish social media companies for failing to remove certain types of illegal content within 24 hours with the most harmful content to be removed within an**

hour. This law allows companies like Facebook, Google, and Twitter to be fined if they fail to remove some illegal content (hate speech, abusive speech, sexual harassment, child pornography, and content provoking terrorist acts) within 24 hours of being flagged up by users. The most serious illegal content – the most explicit terrorist and paedophilic content – must be removed within just one hour of being flagged. Platforms could face fines up to €1.25m. However, in June 2020, French Court ('Conseil Constitutionnel', the highest constitutional authority) struck down some of the provisions of this law.

4.3.2 **However, in January 2021, the French National Assembly adopted a draft amendment to the draft bill "Consolidating the principles of the Republic". This amendment would have the consequence of modifying the French Law for Trust in the Digital Economy of 21 June 2004.**

4.3.3 **Under the proposed law, social media platform operators would be under heavier obligations in relation to online harmful content and their accountability mechanism will be monitored by the Conseil Supérieur de l'Audiovisuel, which is to be granted greater enforcement powers.**

4.4 European Union

4.4.1 **The EU is considering a clampdown, specifically on terror videos. Social media platforms will face fines if they do not delete extremist content within an hour. EU has also introduced the General Data Protection Regulation (GDPR) which set rules on how companies, including social media platforms, store and use people's data. It has also taken action on copyright issues. Its copyright directive puts the onus on social media platforms to make sure that copyright infringing**

content is not hosted on their sites. Previous legislations only required the platforms to remove such content if it was pointed out to them. Member states have until 2021 to implement the directive into their respective domestic laws.

4.5 Australia

4.5.1 **In April 2019, following the Christchurch massacre, Australia passed laws (Criminal Code Amendment [Sharing of Abhorrent Violent Material] Act 2019) that punish social media companies for violent posts. These posts must be removed expeditiously or companies could face fines up to 10% of their annual profit.**

4.5.2 **The Australian parliament also recently passed a landmark media law that would make Google and Facebook pay news publishers for displaying their content. The Australian Competition and Consumer Commission held an 18-month inquiry which found there was an imbalance in power between the platforms and the media companies that threatened the viability of the news businesses.**

4.5.3 **The legislation had been fiercely opposed by the US tech giants, with Facebook blocking all news content to Australians. Facebook agreed to reverse its decision after negotiations with the government, which led to changes to the law to address some of their concerns. This law is seen as a test case for similar regulation around the world.**

4.6 India

4.6.1 **In India, new regulations (The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021), for social media companies and digital streaming websites will soon be enforced to make them more accountable for the online content**

shared on their platforms and to give the government more power to police them.

4.6.2 **The regulations include a strict oversight mechanism that would allow the government to ban content affecting the sovereignty and integrity of India. These regulations would also require social media companies to assist investigations by India's law enforcement agencies. They will require social media companies to remove illegal content as quickly as possible, but within no more than 36 hours after they receive a government or legal order. Social media messaging sites must also disclose to the government the original source of any online content under investigation.**

4.6.3 **The new regulations would also require social media platforms to appoint chief compliance and grievance officers to handle complaints from law enforcement agencies. These officers should be Indian citizens and must send monthly compliance reports to the government.**

5. Would laws involving takedown notices or removal orders to social media companies be effective in the Mauritian context?

5.1 **Laws similar to those enacted in Germany, Australia and New Zealand to block or remove harmful and illegal online content could be enacted in Mauritius. Implementation of such statutory framework is possible only because social media platforms such as Facebook, YouTube, TikTok, Twitter and Instagram have a physical presence through their regional offices in these countries. However, such laws would be of**

no effect whatsoever in Mauritius as there are no representatives or offices of social media platforms in Mauritius.

6. The local scene

6.1 In light of the prevailing international trends, sitting on the fence is not an appropriate option for Mauritius albeit a universal silver bullet solution does not exist. The following number of incidents reported on the Mauritian Cybercrime Online Reporting System (MAUCORS) from January 2020 to January 2021 further reinforces the need for appropriate corrective measures to be undertaken in Mauritius:

Type of Incidents	No of Incidents Reported
Hacking	524
Online Harassment	480
Offensive Contents	379
Sextortion	63
Identity Theft	241
Cyberbullying	87
Cyber Stalking	20
Online Scams and Frauds	225
Phishing	27
Malware	5
Total	2051

6.2 Taking into consideration the local context, the real challenge is to strike the right balance between an effective solution and avoiding being perceived as a repressive measure.

6.3 Given that social media platforms have no representatives or local offices in Mauritius, the only logical and practical solution would be the implementation of a statutory framework that not only provides a legal solution to the problem of harmful and illegal online content but also provides the necessary technical enforcement measures

required to handle this issue in a fair, expeditious, autonomous and independent manner.

6.4 In the local context, not only legal but also technical enforcement measures would be required to be able to monitor this issue effectively. The value addition of this technical enforcement measure will also enable Mauritius to come up with operational measures in an autonomous and independent manner without the need to solely rely on social media administrators for actions. It is also imperative to do due diligence by building appropriate safeguards in this operational framework so as to avoid infringing the constitutional rights of the Mauritian citizens as to their freedom of expression and fundamental democratic values.

6.5 With the advent of the Internet and more specifically of online social media platforms where any Internet user can publish his/her own online contents at the click of the mouse, this aspect of the regulatory work of the ICTA has been projected to the forefront in the recent years. Undoubtedly, with such online facilities, the number of abusive online content and online fake news cases has also skyrocketed.

6.6 For the resolution of these offences, different stakeholders have different understanding of what needs to be done and what can be done by the ICTA to curtail this problem. This probably results from the very open-ended nature of section 18(1)(m) of the ICT Act of Mauritius, where it is stipulated that the ICTA has to *"take steps to regulate or curtail harmful and illegal content on Internet and other information and communication services"*.

6.7 The ICTA has so far enforced section 18(1)(m) of the ICT Act of Mauritius by addressing only the illegal content aspect of the problem. As a preventive measure, the ICTA has deployed a technical toolset only to block access to websites/webpages depicting child sexual abuse (CSA) material which is an offence under the Child Protection Act of Mauritius.

6.8 Harmful content is a more subjective matter on which the ICTA does not have an authoritative mandate as it is not presently vested with investigative powers under the ICT Act.

6.9 Presently, when the Police investigates a cybercrime issue where the identified offender is located in Mauritius, it generally makes use of sections:

46 (ga) of ICT Act:

'*uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to any person;'* and

46(ha) of ICT Act:

'uses an information and communication service, including telecommunication service, to impersonate, or by any other means impersonates, another person which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to that person;'

rather than the provisions of the Computer Misuse & Cybercrime Act (where digital forensic evidence is required) to impose charges on the offender.

6.10 However, in more complicated cybercrime cases such as impersonation where the Police requires technical data from the website administrator (e.g. Facebook) for the identification of the online offender, the tracing exercise becomes a complex and lengthy issue. Moreover, in all cases where the Police requests social media administrators to remove any offensive and abusive online content, the social media administrator will only assess the reported content with its own usage policy and act accordingly, irrespective of whether the reported content breaches the domestic law of the country.

6.11 For the above reason, even if tomorrow the ICTA is vested with power of investigation, it would not be able to do better that what is being done by the Police as it would face similar problems, unless it comes forward with a new modus operandi.

6.12 In this new operational framework, it will need to carry out investigations without the need to rely on the request for technical data from social media administrators. This is a tall order for which it must necessarily equip itself with a new technical toolset.

7. Proposed regulatory and operational framework

7.1 Under section 18 (m) of the ICT Act, the Authority is mandated to take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services. Given the generic nature of this function, the idea is to bring more clarity under this mandate by:

- **completely separating the need to first properly identify whether the online content is an illegal and harmful content and;**

- **putting up technical enforcement measures in place to curtail the identified illegal and harmful content.**

7.2 The amendments to the ICT Act will relate to defining a two-pronged operational framework with the setting up of:

- **a National Digital Ethics Committee (NDEC) as the decision-making body on the contents; and**
- **a Technical Enforcement Unit to enforce the technical measures as directed by the NDEC.**

8. Scope of work and structure of National Digital Ethics Committee

8.1 While it is possible to take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services under section 18 (m) of ICTA, given the potentially intrusive and invasive aspects of the legal and technical enforcement measures contemplated as regards privacy and confidentiality laws, the proposed statutory framework would ideally be incorporated as a distinct set of legal provisions within the ICT Act itself, rather than by way of regulations.

8.2 The NDEC will, therefore, need to be given legal sanctity by way of new provisions under the ICT Act in the same line as section 32(5) of the ICT Act which provides the public operator powers as follows:

(a) Nothing in this Act shall prevent a public operator or any of his employees or agents from intercepting, withholding or otherwise dealing with a message which he has reason to believe is-

(i) indecent or abusive;

(ii) in contravention of this Act;

(iii) of a nature likely to endanger or compromise State's defence, or public safety or public order.

8.3 The National Digital Ethics Committee shall –

8.3.1 **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;**

8.3.2 **decide whether, in its opinion, online content under investigation is harmful and illegal;**

8.3.3 **where it decides the online content under investigation is potentially harmful and illegal:**

- **act as the national focal point and first report the matter to the social media platform administrators for necessary action to remove at source the identified illegal and harmful content from the social media servers;**
- **as a timely preventive measure, order the Enforcement Unit to block that content on the internet and/or provide any relevant digital evidence; and**

8.3.4 **refer to the Police the required digital evidence collected by the Enforcement Unit through the use of the technical toolset.**

8.4 The modus operandi of the NDEC will also need to comply with the requirements of the Data Protection Act 2017 of Mauritius in terms of the handling of personal data. However, one important note to be highlighted in this respect is that breaches in terms of personal data

privacy committed by social media administrators themselves are outside the control of the NDEC. The Internet today is nothing like the World Wide Web initially envisioned and invented in 1989. While it continues to be a place where people can interact in a free exchange of ideas, a handful of giant monopolies are bent on collecting users' personal data. This is what we are seeing around the world and it explains why we have the so-called GAFAM – Google, Apple, Facebook, Amazon and Microsoft - in the U.S and the so-called BAT – Baidu, Alibaba and Tencent – in China. This is also the reason why personal data is viewed as the most valuable asset in this digital era. Personal data collection is done through the use of algorithms. Social media users experience algorithms every day, from insertion of sponsored content, to algorithms to moderate content contrary to the terms of use, friend suggestions, etc. Presently, at the international level, there is much concern about the lack of transparency in the use of algorithms by social media platforms for the collection of personal data from users. The importance they have gained on social networking platforms and the abuses they may cause (for example, promotion of hate speech, ineffective moderation, etc.) is the main source of this concern.

9. Composition and functions of the NDEC

9.1 The composition and mode of operation of the NDEC are instrumental not only for the smooth operation of the operational framework, but also for the prevention of any attempt to make an abusive use and misuse of this operational framework. For these reasons, with a view to making the NDEC transparent and creating public confidence in the functioning of the NDEC and keeping the confidentiality of the

information/data that it will come across, it is proposed that the Chairperson and members of the NDEC be independent, and persons of high calibre and good repute.

9.2 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.

10. Structure and scope of work of the Enforcement Unit

10.1 Whereas the NDEC will need to be given legal sanctity by way of new provisions under the ICT Act, the Enforcement Unit will be set up at the ICTA itself for legal and cost effectiveness reasons. The legal reason is that, to be able to deploy its proposed technical solution, the ICTA, as the national ICT regulator will need to connect its proposed technical toolset with all local Internet Service Providers' networks by again making use of Section 32(5) of the ICT Act.

11. The technical toolset

11.1 Mode of operation

The deployment of the new technical toolset mandatorily requires the resolution of a major technical difficulty due to the use of encrypted traffic on social media platforms. For example, in order to decrypt the "https" traffic between a local user's Internet device and a Facebook webpage, there is a need to first intercept this traffic, decrypt it, archive it and then inspect/block its content (as and when required). This, in turn, implies that all Facebook traffic (both incoming and outgoing for Mauritius) will need to be decrypted and archived. In the proposed technical model, only social media traffic will need to transit

via a filtering set up for decryption, archiving, inspection (as and when required) and re-encryption with the technical toolset self-signed digital certificate. It is to be noted that this technical approach is not specific to Mauritius. In fact, any other agency in any other country which needs to regulate encrypted online content will need to use the same technical approach.

11.2 Scope of work

11.2.1 **Incoming and outgoing Internet traffic in Mauritius will first need to be segregated, that is, only social media traffic will need to be routed to the technical toolset (proxy server). All social media traffic will be decrypted so that when a complaint regarding social media is received, the following actions can be effected:**

a. **Blocking of the incriminated social media web page without blocking the whole social media site;**

b. **Blocking of a fake profile page and determine who created the fake profile (without the need to contact social media administrator);**

c. **Regarding offensive comments posted, let's say on a newspaper social media webpage, blocking of its page is not envisaged. In this case, with the technical toolset, it will be possible to determine the originating IP address of the person who posted the offensive comment; and**

d. **Once decryption is done, copy and send decrypted traffic to the data analysis software with an advanced reporting feature to be able to drill into the decrypted traffic to search specific**

keywords, comments posted, etc and correlate with originating IP addresses.

11.3 Another important feature of the technical toolset is the need to re-encrypt the decrypted social media data with the self-signed digital certificate of the proxy server before reaching out to or originating from the social media servers. This is a one-off operation to be done by each user from Mauritius trying to access social media websites for the first time via the proxy server. The envisaged operational scenario is that the social media end user from Mauritius should be prompted for the automatic installation of this self-signed certificate on his workstation/device when he will try to access the social media website for the first time via the proxy server. He will also be informed in the prompt that it is only after having successfully installed the self-signed certificate of the proxy server on his workstation/smart phone, that he will be able to access his chosen social media platform.

12. Conclusion

12.1 Unregulated social and digital media can pose a threat to social harmony and national security. The challenges therein can be addressed by regulating social media efficiently in accordance with the provisions of our domestic laws and Constitution.

12.2 The principle that all social media platforms must abide by, therefore, is that any content on these platforms should pass the test of section 12 of our Constitution. The proposed statutory framework will undoubtedly interfere with the Mauritian people's fundamental rights

and liberties in particular their rights to privacy and confidentiality and freedom of expression.

12.3 Similarly, the take-down policies for these social media platforms should also be compliant with and not go beyond that section in order to avoid breaches in terms of freedom of expression and democratic values.

Part II

13. Consultation procedure

13.1 The present public consultation exercise is a major milestone in the inclusive process adopted for the elaboration of the social media regulatory and operational framework. This democratic consultative process also aims at dispelling the perception of the deployment of a repressive measure which, in turn, aims at mitigating the risk for social media platforms to threaten to shut down their operations in Mauritius on this basis as has been the case in Pakistan.

13.2 In this consultation paper, the ICT Authority would like to invite views and comments from the public and all other stakeholders on the issues raised herein. In order to facilitate this consultation process, questions have been asked for the public's careful consideration. Notwithstanding this, members of the public are not confined to these questions and are encouraged to raise any issues pertinent to them.

13.3 Members of the public are welcome to submit their comments on this consultation paper to socialmediaconsultation@icta.mu latest by 05 May 2021 at 16:00 hrs. The comments will be most useful if they are substantiated with rationale examples and alternative proposals. Kindly also include full contact particulars such as full name, designation and organisation name (if relevant), postal address, e-mail address and contact numbers. 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.

14. 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?

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?

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.

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?

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

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

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?

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?

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?