Submissions on Proposed Amendments to the ICT Act of Mauritius

May 2021

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) welcomes this opportunity to present submissions on the proposed amendments to the ICT Act of Mauritius. These submissions arise from the call by the Information & Communication Technologies Authority for comments to the "Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius".

For any questions on this submissions, please contact wakabi@cipesa.org and programmes@cipesa.org

---

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?

This "self-regulation" approach described above is not a universal practice. As it was rightly pointed out in the consultation document, many countries have laws that regulate social media, especially with regards to content takedown. In the case of Mauritius, the issue as stated is the "non-responsiveness" or slow rate of response by social media administrators to content takedown requests. Moreover, under the "self-regulation" scenario above, social media platform administrators and other intermediaries do not stand outside the reach of national judicial processes. Under the platforms' guidelines or "Community Standards", the social media platforms implement content moderation strategies that prescribe mechanisms for reporting illegal and objectionable content, as well as the remedial actions, and they have increasingly issued transparency reports that detail their moderation activities and requests for content takedown. For example, Facebook has recently put in place a policy to restrict access to content that is illegal under local laws once it is reported to them. The company also has a portal for use by law enforcement to request records from Facebook.

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?

Governments have a legitimate interest in tackling disinformation, hate speech and other forms of objectionable content, particularly that which can cause offline or online harm. It is essential therefore that platforms work with governments and other actors (such as private companies and civil society organisations and the media) in controlling the spread of harmful content.

While a different approach or modification to current approaches could boost efforts to forestall potential damage caused by harmful content, the approach proposed in the consultation paper is neither necessary nor proportionate and does not measure up to international human rights standards. Indeed, there is no clear evidence as to the actual damage caused by the presumed abuse of social media networks in

Mauritius (since the consultation paper points to none), which could then have informed and justified the remedial regulatory or other measures.

However, any government requests to platforms to take down content, shut down accounts, or reveal users' identifying information, need to be backed by an order issued by impartial judicial authorities. Moreover, where any such measure is to be implemented, it needs to be provided for under the laws, it should serve a legitimate aim, and should be necessary in a free and democratic society. The proposed measures fall short of these requirements.

14.3 What are your views on the overall proposed operational framework in terms of the National Digital Ethics Committee (NDEC) and the 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.

It is important to appropriately flag and quickly remove illegal and harmful content from social media platforms. However, an entity involved in this, unlike the NDEC as proposed, should be a completely independent and transparent body whose objectives would be to assist the application of national policies and also act as an arbitrator between social media platforms and the government in case of arbitrary content takedown.

The appointment of personnel for this body should be inclusive, with multi-stakeholder representation. Whereas the consultation paper indicates that the Chairperson and members of NDEC would be "independent, and persons of high calibre and good repute" in order to ensure transparency and public confidence in its functions, the selection criteria and appointing authority are not specified, nor are recourse mechanisms for fair hearing and appeals against the decisions of the proposed entity. For its part, the proposed set up of the Enforcement Unit by the ICTA (Para 10.1) could potentially affect its independence as there might be no guarantees as to who actually is appointed to manage the unit and whether such appointed persons are independent of political or other external influence.

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?

We find it problematic that the proposed NDEC will be a decision making body and come along with "a Technical Enforcement Unit to enforce the technical measures as directed by the NDEC" (Para 7.2), with its work extending to taking "steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services" (para 8.1). The NDEC as indicated in (para 8.2) will have excessive powers with no checks and balances. Given that the NDEC will be run under a government entity, it might be used as a political weapon for arbitrary content takedown and persecution. The NDEC could thus - through unrestricted surveillance and interception - limit freedom of expression, the right to privacy, and access to information. Accordingly, we view the proposed amendments to the ICT Act as unwarranted, as they go against international human rights standards and best practices in protecting human rights online and are counter to the spirit of a free, open, and secure internet.

According to section 18(m) of Mauritius' Information and Communication Technologies Act, the ICT Authority shall "take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services". The Authority states that it has not fulfilled the mandate of curtailing illegal content as it is not currently vested with investigative powers under the Act and that social media platforms are often non-responsive to its requests. It therefore proposes revisions to the law, including the creation of the controversial entity.

However, the Authority's claims of powerlessness appear unfounded. According to Facebook's Transparency report, Mauritius made two requests for preservation of five user accounts pending receipt of formal legal processes in 2017. In 2019, Mauritius made one request to Facebook for preservation of two accounts. Similarly, the country has barely made any requests for content take down to Google, with only a total of 13 since 2009. The country has never made a user information or content takedown request to Twitter.

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

Through a technical toolset (a proxy server), proposed under section 11, the regulator will be able to identify social media traffic which will then be automatically decrypted, archived, and analysed. The regulator expects that once a complaint regarding social media is received, they will be able to block the implicated web page or profile without necessarily needing the intervention of social media platforms. Additionally, the Authority expects social media users to accept installation of a one-time digital certificate on their internet-enabled devices to facilitate the re-encryption of traffic before it is transferred to the social networking sites. In other words, the Authority wants internet users in Mauritius to replace their own padlocks used for their *home* security with ones given to them by the Authority, which it has open and unfettered access to.

The technical toolset would undermine HTTPS in order to inspect internet traffic. This means that information of all social media users pertaining to device specifics, content type, location, among others, would be available to the authorities. In this regard the measures proposed under para 11 would gravely affect the privacy and security of individuals, freedom of expression and access to information online. Indeed, individuals, particularly those critical of the government and political leaders, may be forced to regress into self-censorship in fear of arbitrary arrests, detention and prosecution.

We note that neither the existing Act nor the consultation paper define what constitutes "illegal content". Moreover, while para 9.1 and 9.2 mention recruitment of the Committee's members and cites the need for safeguards in operations, they fail to provide for competence-based and independent appointment of members of the envisaged entity, nor do they mention judicial oversight mechanisms and the high levels of transparency and accountability measures that such an entity would require.

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

We do not support the establishment of the NDEC as proposed. That said, any efforts by Mauritius authorities to investigate illegal and harmful content and to pursue their takedown must be guided by established regional and international human rights instruments to which Mauritius is party. There should be clear investigative processes that are in line with the principle of rule of law. These entail clear definitions of the offences or illegal content, effective complaints mechanisms, clear appeal and remedial mechanisms, judicial/independent oversight. Such processes should also adhere to the country's Data Protection Act (DPA), 2017, and the Constitution. For reference purposes, the African Commission in its declaration has called upon States and Intermediaries to mainstream human rights safeguards when moderating or filtering online content. Likewise, Santa Clara principles, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and the Manila principles of intermediary liability have proposed best practices to foster internet freedom.

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?

The technical toolset is flawed not least because there is no mention in the document as to how confidentiality of other sensitive information will be protected, for instance financial transactions. Mauritius has in the past demonstrated commitment to internationally recognised best practices including the DPA's alignment to European Union's General Data Protection Regulation and more recently, the signing and ratification of the Council of Europe's Convention for the Protection of individuals with regard to automatic processing of personal data. Therefore, proceeding with the technical toolset in its current fashion would amount to a breach of the country's afore-mentioned progressive legacy.

The proposed actions under the consultation paper do not address the fact that interception and decryption may involve access to personal usernames and passwords. There is no acknowledgement that the ICTA could access such personal credentials which not only interferes with individual autonomy but also with personal privacy. Hence, personal logins and passwords of internet users are at risk of exposure to cyber criminality and also with unscrupulous individuals who could use such credentials for fraud and blackmail in social, economic and political fields.

There is a guarantee that information transiting through the proxy server will not be modified. Neither is it guaranteed that only social media traffic will be monitored. We are further concerned that the toolset can easily be extended for any type of traffic such as device specifics, content type, location, among others, would be available to the authorities thus potentially interfering with individual rights to privacy and security. Moreover, it could facilitate usage beyond the intended/prescribed scope.

The proposed approach to decrypting traffic will break certain core HTTPS functionalities, including encryption authentication if enabled by social media websites. For instance, it is probable that major web browsers might not agree to install and trust the one-time *Mauritius_MITM_certificate* (digital certificate), which might expose users to security vulnerabilities and poor user experiences.

Ultimately, the proposed amendments to the ICT Act go against Mauritius' commitments to respecting and promoting freedom of expression, assembly and association, data protection and privacy, the right to access information, under its constitution, and national, regional and international law. In particular, Mauritius' GDPR-aligned Data Protection Act (2017) requires informed consent of users, prohibits disproportionate collection of user data, and mandates fair and lawful processing of user data. In March 2018, Mauritius also ratified the African Union Convention on Cybersecurity and Personal Data Protection, although the Convention is yet to come into force. Moreover, in September 2020, Mauritius signed and ratified the Council of Europe's Convention for the Protection of individuals with regard to automatic processing of personal data.

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?

There is no such thing as a "technical toolset" which is not intrusive. There is no silver bullet for social media content regulation but a range of measures and safeguards would be helpful, including educating the population on the roles and responsibilities of individuals online, and having independent, multistakeholder, and rights-respecting national mechanisms that work hand-in-hand with platforms in combating harmful content.

Mauritius has already proved that aligning domestic and international laws and practices is necessary by fashioning its data protection law along the lines of the GDPR. Additionally, Mauritius could leverage existing partnerships with other countries of regional economic blocs such as The Common Market for Eastern and Southern Africa (COMESA) to form a coalition of fact-checkers that have direct access to social media platforms. Similarly, the Authority could collaborate with technology platforms such as Facebook to support Creole language human moderators. This could be a necessary step to enhancing content moderation through automated decisions and more so for "low resource" groups of languages including Mauritian Creole.

The ICTA may also want to evaluate the reputation loss that Mauritius is likely to suffer if it implemented the suggested measures. The country is likely to lose foreign direct investment, with big social media companies such as Twitter, Facebook, Google being among those unlikely to consider setting up business in Mauritius. European companies and other companies that have operations in Europe and which are bound by the GDPR would equally be disinclined to invest in Mauritius.

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?

Mauritius has adequate civil laws to protect citizens - laws for instance on defamation, impersonation, cybercrime and computer misuse. It is also to be recalled that as recently as October 2018, there was a contentious amendment to Section 46 of the ICT Act, which criminalised content perceived to cause "annoyance, humiliation, inconvenience, distress or anxiety to any person," and established penalties of up to 10 years in prison.