The Cybersecurity and Cybercrime Bill 2021
New law not without difficulties and concerns

The Cybersecurity and Cybercrime Bill 2021 ("CC Bill") replaces the existing cybercrime legislation, the Computer Misuse and Cybercrime Act 2003. The CC Bill comes at the right moment after the FATF has taken Mauritius off the grey list. There is a clear link between technological innovation and financial crime. One of the first cases surrounding the illegal use of crypto assets was "Silk Road" used by criminals, including terrorists. The Bill also aims to protect personal integrity from harmful use of a computer system, including the internet, but the broad outlay of the investigative and penal provisions triggers the question of potential misuse.

In this legal update, we set out the main provisions of the CC Bill.

The CC Bill creates the following new offences:

- **Misuse of fake profile:** making use of a fake profile to cause harm. A 'fake profile' is defined as an untrue online representation, existent or non-existent.

- **Cyberbullying:** any behaviour using information and communication technologies which are, for example, repetitive, persistent and intentionally harmful.

- **Cyber extortion:** using the internet to demand money or other goods or behaviour from another person by threatening to inflict harm to his person, reputation, or property.

- **Revenge pornography:** using a computer system to disclose or publish a sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing distress to that person.

- **Cyberterrorism:** accessing or causing to be accessed a computer system or network for carrying out an act of terrorism.

- **Infringement of copyright and relates rights:** using a computer system to, for example, publish or distribute another person's work for commercial purposes without the person's consent, or downloading movies, music files or pirated software applications for gain or against remuneration, or posting a copyrighted work online for gain or against remuneration.

- **Failure to moderate undesirable content:** failure by the administrator of an online account to moderate and control undesirable content that has been brought to the administrator's attention by the authority. An undesirable content includes an online content that is inaccurate and which is posted with intent to defame, or a content that threatens public health or national security or promotes racism.

- **Unlawful disclosure of details of an investigation:** except if the person disclosing the details of an investigation of an offence under the CC law does so by virtue of a statutory power or in the performance of is lawful duties or contractual obligation or pursuant to a legal obligation, the investigation must be kept confidential.

- **Obstruction of investigation:** destroying, deleting, altering, concealing, modifying or rendering a computer data meaningless, ineffective or useless with intent to obstruct or delay an investigation.

The CC Bill investigation procedures which existed in the Computer Misuse and Cybercrime Act 2003

are reproduced in the CC Bill and in some instances have been enhanced.

- **Expedited preservation and partial disclosure of traffic data:** the investigatory authority may serve a notice on a person who is in possession or control of traffic data stored in a computer system or device, which is required for investigation if the investigatory authority has reasonable grounds to believe that there is a risk that the traffic data may be modified, lost, destroyed, or rendered inaccessible. The integrity of the data must be maintained for a period not exceeding 90 days. However, this period of 90 days may be extended pursuant to a judicial order.

- **Production order:** a person may be compelled, under the authority of a judicial order, to submit specified data to an investigatory authority.

- **Powers of access, search and seizure for purposes of investigation:** a computer data storage medium or a computer system or part of the computer system, may be accessed, searched and seized for the purpose of an investigation or prosecution of an offence under the authority of a judicial order.

- **Real-time collection of traffic data:** the collection or recording of traffic data (e.g., date, time and route of a communication) on the Mauritian territory and compelling a service provider, within its technical capabilities, to collect and record such traffic data, under the authority of a judicial order.

- **Interception of content data:** the collection and recording of content data (e.g., the message that is being transmitted) in the territory of Mauritius in real-time, and, within the technical capabilities of the service provider, to cooperate and assist the investigatory authority in such collection and recording.

- **Deletion order:** the deletion of data that is unlawful which is found in a computer system or on a device, or disactivating access to unlawful activity which is made available through a computer system.

- **International cooperation:** In addition to the Extradition Act and the Mutual Assistance in Criminal and Related Matters Act, the Attorney-General who is the Central Authority, may make a request for mutual legal assistance in any criminal matter to a foreign State, for example, for the collection of evidence in electronic form of any criminal offence. The types of criminal offences for which this power is exercised is not limited to offences under the CC Bill. The Attorney-General may also grant legal assistance in the same manner to a foreign State. Furthermore, subject to the provisions of the CC Bill and any other relevant law, the Attorney-General may forward to a foreign State information obtained in a Mauritian investigation if he considers that the disclosure of such information may assist the foreign State in initiating an investigation or proceedings concerning offences relating to cybercrime and cybersecurity. The Attorney-General may require that the information is kept confidential and if disclosed only subject to conditions that he may imposed. The mutual assistance extends to the real-time collection of traffic data and the interception of content data.

- **24/7 point of contact:** For the purposes of investigations or proceedings concerning criminal offences related to computer systems and computer data, or for the collection of electronic evidence of a criminal offence, the Commissioner of Police shall designate a 24/7 point of contact available on twenty-four-hour, seven-day-a-week basis to provide immediate assistance to the point of contact of another Party on an expedited basis.

Critical information infrastructure

In addition to the provisions which create the offences and the procedural provisions mentioned above, the CC Bill also provides that the National Cybersecurity Committee may, after consultation with the regulatory authority in control of an information infrastructure, identity information structures which need to be declared critical information structures. A critical information infrastructure is an asset, facility, system network or process, whose incapacity, destruction, or modification would, for example, have a devastating effect on the availability, integrity or delivery of essential services, or a significant impact on the national security, national defence, of the functioning of the State.

Computer Emergency Response Team of Mauritius (CERT-MU)

The CERT-MU which already exists and operates under the aegis of the National Computer Board since 2008 and which itself is under the Ministry for Information Technology, Communication and Innovation, is transferred under the direct supervision of the Ministry: the CERT-MU is now set up within the Ministry. Like the National Cybersecurity Committee, which is established under the CC Bill, one of the functions of the CERT-MU is to advise and assist the Government on the development and implementation of cybersecurity.

Comments

It is not proposed to critically examine the provisions of the CC Bill in this legal update. We shall address a few points only.

- **International cooperation:** The international cooperation regime which is contained in the CC Bill is a significant improvement on the existing regime. In addition, it will be possible for the investigatory authority to serve a notice on a person (including a service provider) who is in possession or control of traffic data, requiring that person to expeditiously preserve the traffic data or disclose the required traffic data to identify the service providers and the path through which communication was transmitted. Requiring the preservation of traffic data is not intrusive as opposed to, for example, the disclosure of content data for which a judicial order is required.

- **Internet content monitoring:** The CC Bill does not impose a general monitoring obligation of internet content: to impose a general obligation of monitoring could disproportionately limit users' freedom of expression and freedom to receive information, and in addition, could be considered as an undue interference on the conduct of their business. However, the precise offence which is created in clause 23(2) is unclear. Besides, the CC Bill does not define who is an administrator of an online account. Surprisingly, the expression "online account" is defined in an unconventional manner. An "online account" as defined, includes pages on search engine service. A search engine allows users to search the internet for content using keywords. Google, Yahoo, Baidu and Bing are popular search engines. As drafted, clause 23(1) of the CC Bill allows a Mauritian investigatory authority to require a search engine service provider to moderate and control undesirable content, such content that, according to the investigatory authority, is for example, deceptive or inaccurate and posted with intent to defame. Whether this may or may not have been the intention of the Government, this provision may have unintended.

- **Absence of proportionality in the sentences:** It is undisputed that the National Assembly has the power to make laws for the peace, order and good governance of the country. This power to make laws also include the power to set the sentence for criminal offences. On the other hand, due respect must be given to the necessity of upkeeping a proportionality with the seriousness of the

offence. In *Reyes v. The Queen* [2002] UKPC 11, the Judicial Committee reiterated that it is and has always been considered a vital precept of just penal laws that the punishment should fit the crime. This case has been cited with approval by the Supreme Court of Mauritius on numerous occasions. Whilst 'proportionality' is an issue at the stage of sentencing, however, the sentencing provisions ought to give an indication about the severity of the offences. This is however not the case with the sentencing provisions which are contained in the CC Bill. As an example, clause 9 which creates the offence of unauthorised hindrance of a computer system provides as sentence, a fine not exceeding one million rupees and penal servitude for a term not exceeding 10 years. Such hindrance may be caused by the alteration or deletion of computer data. However, clause 11 which makes it an offence the intentional and unauthorised modification of computer data provides as sentence, a fine not exceeding one million rupees and penal servitude for a term not exceeding 20 years. The nature of the two offences is not so different: in both cases, computer data are deleted without authority and intentionally. Clause 23 of the Bill which concerns the failure to moderate undesirable content provides for a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years. It appears that failure to moderate undesirable content must be treated more severely than the unauthorised hindrance of a computer system.

Written by

Ammar Oozeer

Senior Associate at BLC Robert

Counsel and Head of Compliance