Speech of
Honourable Deepak Balgobin,
Minister of Information Technology, Communication and Innovation

Cybersecurity and Cybercrime Bill
(Second reading)

National Assembly
Republic of Mauritius

Tuesday, 9th November 2021

Mr Deputy-Speaker, Sir,

I beg to move that the **Cybersecurity and Cybercrime Bill (No. XV of 2021)** be read a second time.

1. INTRODUCTION

Monsieur le Vice-Président,

Le débat que nous entamons aujourd'hui dépasse les limites de la politique partisane. Notre objectif est de défendre et de protéger chaque enfant, chaque personne âgée, chaque individu, chaque entreprise, de notre République.

Nous sommes conscients que les cybercriminels, de manière très claire, ciblent le maillon le plus vulnérable et qui prennent avantage sur la méconnaissance des gens.

La révolution numérique n'a pas seulement bouleversé les économies et le bon fonctionnement du monde entier, elle a, malheureusement, aussi accru la cyber délinquance. Cette délinquance est menée par des gens mal intentionnés. A part des délits qui ont toujours existé, de nouveaux délits ont surgi qui menacent autant les particuliers que les entreprises, surtout depuis le début de la pandémie de la COVID-19.

Au cours des dernières années, le développement très rapide de l'Internet a entraîné dans son sillage des abus et aussi des infractions de toutes sortes par des personnes ayant des motifs sinistres.

La toile, monde sans frontières, est devenue aujourd'hui un lieu de prédilection pour le crime organisé pour certains, pour faire des déclarations incendiaires ou pour déstabiliser le bon fonctionnement de la société.

Ces personnes, malveillantes se cachent souvent derrière de faux profils ou prennent avantage de l'absence de contrôle ou de réglementation juste. Je suis sûr que, dans cette auguste Assemblée, chacun de nous a une histoire d'un ou d'une proche qui a été, d'une façon ou une autre, victime d'un délit en ligne. Pire, chaque citoyen lambda, responsable et respectueux, vit dans une crainte perpétuelle d'être une victime de la cybercriminalité.

Il est donc essentiel, et c'est le rôle d'un Gouvernement responsable, de protéger ses concitoyens ainsi que les entreprises, le secteur privé et les services publics contre des cyber attaques dont les conséquences sont souvent désastreuses sur tous les plans - personnel, social ou financier.

Il est donc impératif de mettre en place un écosystème robuste qui répond aux enjeux du jour, surtout que le monde virtuel est si dynamique.

Monsieur le Vice-Président,

Nous avons, comme à notre habitude, assumé notre responsabilité en proposant une nouvelle loi, plus moderne que celle existante, soit le **Computer Misuse and Cybercrime Act de 2003,** qui je dois dire, a fait son temps. Ce nouveau projet de loi est mieux adapté à la situation actuelle qui prévaut sur le cyber-espace et le rendra plus résilient et sécurisé pour être utilisé par les internautes.

Monsieur, le Vice-Président,

Contrairement aux démagogies, faussetés et les campagnes mensongèresque veulent faire croire les détracteurs de ce projet de loi ce document met en exergue trois priorités fondamentales :

- **Mieux combattre la cybercriminalité**
- **Renforcer notre cyber-résilience**
- **Renforcer la coopération internationale**

Mr Deputy-Speaker, Sir,

Today, at a time when we are facing unprecedented threats from rogue hackers and all sorts of cybercriminals, this Government is unveiling and proposing a new piece of legislation to take urgent actions, to give the Government and the private sector the tools we need to combat cyber threats and to protect each and every citizen of our country.

It is with a great sense of responsibility, for me, to present this piece of legislation, the Cybersecurity and Cybercrime Bill, of utmost importance for the future of our people, of our economy and of our Republic. It goes in line with Late Sir Anerood Jugnauth's Vision 2030 for the country. A vision which will transform Mauritius into a high income, inclusive and green economy, including a safe and secure cyberspace in our jurisdiction.

The noble motive behind devising this Bill is to protect everyone, including our children and youngsters from cyberthreats. The finalisation of the Bill has been based on a comprehensive desk review and the analysis of different legislations.

2. STATISTICS AROUND THE WORLD

Mr Deputy-Speaker, Sir,

In this new era of advanced technology, world economies are harnessing the benefits of digitalisation and state of the art solutions, particularly, in critical sectors such as Health, Finance, Industry and Commerce. As a result, ever greater resilience and security of these infrastructures have become a priority for any Government.

Cybercriminals are becoming more and more sophisticated and are perfecting their methodologies in the quest to attack critical information infrastructure. They can operate from anywhere in the world, targeting individuals, large numbers of people or businesses across boundaries, making it more challenging for cyber defenders.

We are now on the eve of 2022 and the Computer Misuse and Cybercrime Act dates back to 2003. In these 18 years, the cyber threat landscape has changed drastically. Therefore, we need to keep pace to address these threats so that we can better protect ourselves and our people.

I wish to draw the attention of the House on how our citizens, irrespective of their social status, are becoming victims to cybercrimes on a daily basis. Even our children, youngsters and senior citizens are not spared by unscrupulous persons.

The statistics gathered for the last four years, through the Mauritian Cybercrime Online Reporting System (MAUCORS) are alarming. Cases reported in 2021 are around 5 times more than those in 2018.

In 2021, January to date, 2320 cases have been reported as compared to 426 cases in 2018!

We are witnessing the trauma and anxiety which our people are experiencing through as a result of fake profiles, cyber scams, phishing, revenge pornography, electronic frauds, amongst others. The trend shows no sign of slowing down.

Not later than this year, one of the heart-breaking incidents was of the mobile application “Telegram”, issue, where intimate pictures of young Mauritian girls were circulating on different groups. Another most recent case was the circulation of a humiliating video targeting disabled persons on Tiktok or disgusting hate speech videos on Facebook. We should also not forget the incident where our children in Rodrigues fell victim to the heinous acts of pedophiles through WhatsApp.

Mr Deputy-Speaker, Sir,

Allow me to elaborate on the threats which institutions are facing such as malware infections, social engineering, denial-of-service attacks, bot-nets, ransomware, website defacement, compromised accounts, amongst others. These words may seem unfamiliar to many of us, but these are real threats happening in our beautiful country.

On the regional front, due to the growth of digital transformation across Africa, the continent has become an attractive target for cyber criminals. According to a report released by a global cybersecurity and digital privacy company, Kaspersky, in August 2021, four countries accounted for 85 million cyberattacks in all its forms in the span of six months, with South

Africa being the most targeted with 32 million attacks; followed by Kenya, 28.3 million; Nigeria, 16.7 million; while Ethiopia had 8 million cyberattacks.

In Europe, the Middle East and Africa, organizations experienced a 36% increase in cyber-attacks since the beginning of the year. The United States has observed a 17% increase in cyber-attacks, while the Asia Pacific region recorded a 13% increase.

In the United States, the Colonial Pipeline, a major fuel company fell victim to a ransomware attack this year, which led to its entire fuel distribution pipeline being shut down, causing shortages across the US East Coast and influencing oil prices globally.

Last year, hackers stole the personal data of around 1.4 million people who took COVID-19 tests in the Paris region.

Mr Deputy-Speaker, Sir,

These are not just mere figures for computation purposes only, but reflect the dangers hiding around in the digital and cyber world. Cyber-attacks are indeed causing severe financial losses to organisations in Mauritius and worldwide.

According to the World Economic Forum Global Risks Report 2020, cyber-attacks rank first among global human caused risks. A report from the popular cybersecurity firm, McAfee, estimated that global losses from cybercrime topped 1 trillion US Dollars in 2020.

Cybersecurity Ventures, one of the world's leading researcher for the global cyber economy, predicts that this year, cybercrime will cost the world 11.4 million US Dollars every minute. It also predicts that global cybercrime costs will grow by 15 percent per year over the next five years, reaching 10.5 trillion US Dollars annually by 2025, compared to 3 trillion US Dollars in 2015.

3. GAPS OF THE EXISTING LAW

Mr Deputy-Speaker, Sir,

Law enforcement capabilities are critical to safeguard and secure cyberspace as they perform an essential role in investigating cybercrimes and prosecuting those responsible. Cybercrime is borderless by nature and this makes criminal investigations more complicated for law enforcement authorities.

Adequate cross–border provisions are required and international cooperation as well as mutual assistance between law enforcement agencies need to be enhanced to effectively address cybercrime.

The importance of the fight against cybercrime in the whole world is also growing. In order to allow the ICT sector and the digital economy to significantly grow, appropriate measures need to be implemented to tackle cybercrime. This includes mechanisms for harmonising legislation on cybercrime and electronic evidence.

The Computer Misuse and Cybercrime Act 2003 is the existing legislation in force on cybercrime and contains several provisions of substantive

criminal law, which allow for the identification of the main cybercrime actions as illegal activities.

Although the Act provides the possibility to investigate and prosecute criminal activities in cyberspace, it has its limitations in the face of growing cyber attacks, especially those which are new and more harmful in nature.

The Computer Misuse and Cybercrime Act 2003 does not cater for emerging cyber threats occurring due to the fast development in Information Technology. Moreover, it does not have any governance framework for the coordination of cybersecurity and cybercrime at national level.

One of the important aspects of international cooperation, which is essential for resolution of cybercrime occurring at cross border level, is missing and needs to be addressed. And most importantly, the existing law is not harmonised with the international and regional conventions that Mauritius is a signatory to, such as the Budapest Convention on Cybercrime and the African Union - Malabo Convention on Cybersecurity and Personal Data Protection.

4. NEED FOR A NEW LAW

Mr Deputy-Speaker, Sir,

Mauritius has proudly maintained its 1st position in Africa for the last 7 years in the International Telecommunication Union's (ITU) Global Cybersecurity Index and is currently placed 17th globally. This has been possible because of lots of initiatives that have been taken.

These initiatives include:

- Implementation of National Cybersecurity Strategy (2014) and Cybercrime Strategy (2017)
- Finalisation of the National Cyber Incident Response Plan (2020)
- Development of the Critical Information Infrastructure Policy (2021)
- Establishment and operationalisation of the Mauritian Cybercrime Online Reporting System (MAUCORS) (2018)
- Establishment and operationalisation of the ITU Centre of Excellence in the field of Cybersecurity (2020)
- Setting up of the Security Operations Centre for the Government (2020)
- Amongst others.

Mr. Deputy-Speaker, Sir,

Cybersecurity is attracting more attention than ever, given its increasing importance in the digitalised world. Not just in the headlines, but among industry leaders, academics, and the public. Successful cyberattacks are becoming more frequent and threatening as adversaries become more determined, organised and sophisticated.

This is why this Government is aiming to position Mauritius among the top secure nations by introducing a forward-looking and pro-active legislation, capable of addressing issues arising from evolving threats.

It is against this backdrop that I am privileged today to pilot as Minister of Information Technology, Communication and Innovation, the **Cybersecurity and Cybercrime Bill** in this august Assembly.

Mahatma Gandhi said, and I quote :

"The future depends on what you do today". **End quote.**

Today, Mr Deputy-Speaker, Sir, we have come up with this Bill to provide a new and comprehensive legal instrument for the country's cyber future. One that is secure, resilient, collaborative and adaptable. All these will help to make the Information Technologies a good servant, not a bad master.

As I mentioned before, the new Bill has been drafted taking into consideration the commitments taken by our country as a party to international conventions: the Budapest Convention on Cybercrime signed in November 2013 and ratified in March 2014 and the African Union - Malabo Convention on Cybersecurity and Personal Data Protection ratified in March 2018.

It includes measures to criminalise offences related to computer crime and to harmonise penalties with international practices while ensuring that core values and human rights enshrined in our constitution, are respected.

The Bill also aims at developing a more robust framework for the protection of the Mauritian cyberspace:

- by providing new criminal offences related to cybersecurity and cybercrime,
- reinforced provisions for protection of critical information infrastructure and implementation of a policy in that regard,
- improved investigation techniques and international cooperation,

- as well as mutual legal assistance in cybercrime matters and setting up of a National Cybersecurity Committee.

5. FORMULATION OF THE NEW LAW

Mr. Deputy-Speaker, Sir,

This piece of legislation is not the product of a haphazard approach. A dedicated and specialised team was constituted to work out this upgraded and modern piece of legislation, together with relevant stakeholders. Moreover, a comparative analysis of various legislations in different jurisdictions such as Singapore, Australia, UK, USA, Estonia, India and Kenya was carried out.

To ensure that this law is benchmarked with the highest of international standards in the sector and that every clause in this Bill is in line with the principles of preservation of fundamental liberties, the **Council of Europe** was consulted at various stages of the drafting and finalisation of this Bill.

Mr Deputy-Speaker, Sir,

I wish to stress on the fact that the Council of Europe, which is Europe's leading Human Rights organisation, democracy and rule of law, has provided its valuable inputs and has vetted the law, through the Attorney General's Office. Here, I would like to thank my colleague the Honorable Attorney General and his team for their valuable assistance. We can safely say that the clauses of this Bill are in line with principles of human rights, democracy and Rule of Law.

We have heard lots of irrational comments from a few irresponsible persons, who were claiming that this Bill is violating human rights, freedom of expression and according to them is anticonstitutional. I say it again, the very fact that the vetting of the Bill has been done by the Council of Europe is enough testimony of respect of democratic rights.

7. WHAT IS IN THE NEW LAW

Mr Deputy-Speaker, Sir,

Now, allow me to elaborate on the different sections of the new law.

(a) THE NATIONAL CYBERSECURITY COMMITTEE

The Bill makes provision for the setting up of a National Cybersecurity Committee which will comprise a Chairperson, to be appointed by the Prime Minister and representatives from competent bodies.

One of the main roles of this apex committee will be to drive the implementation of Government policy relating to cybersecurity and cybercrime as well as coordinate and facilitate the implementation of a Critical Information Infrastructure framework.

Mr Deputy-Speaker, Sir,

Let me say it loud and clear, **at no point in time**, will this Committee indulge in the investigation and prosecution of cybercrime. The Police and the Judiciary will, as always, act independently.

I firmly reiterate that the Committee will not be concerned at all with the day to day operations of the cybersecurity machinery. It will only ensure policy oversight and strategy implementation at the highest level.

OFFENCES

Mr Deputy-Speaker, Sir,

Let me now elaborate on the offences that have been catered for under this Bill. There are nineteen (19) offences in total. Among these, there are 7 existing offences from the Computer Misuse and Cybercrime Act 2003 which have been aligned with the Budapest Convention on Cybercrime. 12 new offences have been introduced in order to deal with new and emerging cyber threats. These have been conceptualised in the Mauritian context.

Members from both sides of the House will appreciate that the law has been toughened to increase the penalties and the terms of imprisonment . The offenders shall be punished by a fine ranging from 100,000 rupees to 2 million rupees and penal servitude ranging from 2 years to 25 years, depending on the gravity of the offence.

We have to think of damages suffered by victims of cybercrimes and we cannot tolerate perpetrators. The severe penalties will act as a deterrent for the latter who will think twice before acting.

As mentioned, 7 existing sections of the Computer Misuse and Cybercrime Act have been maintained and enhanced in order to clearly reflect the malicious intention of perpetrators in committing a crime. I

would like to highlight that the Council of Europe has played a crucial role here in adapting these clauses with the Convention.

The Budapest Convention stipulates that offences which involve unauthorised access such as hacking, intrusion, data tampering and degradation of service constitute a crime only if they are committed “intentionally” and “without right”. In the existing law, there is insufficient language to express the element of intent. Therefore, the new law aligns the existing provisions with Articles 2 to 10 of Budapest Convention to include those elements of intent and without right.

Today, with the latest technologies, it is very easy for a cybercriminal to hack someone’s password, to create viruses for the purpose of stealing personal information and to launch phishing attacks to defraud people. That is why we deemed it crucial to keep clauses such as unauthorised disclosure of passwords, unlawful possession of devices and computer data and electronic fraud.

Mr Deputy-Speaker, Sir,

Now, allow me to elaborate on the new offences that have been introduced in the new legislation.

Cyber-attacks such as Denial of Service or Distributed Denial of Service are very common nowadays. These types of attacks can shut down a machine or network, making it inaccessible to its intended users. Clause 9 on unauthorised interference caters for such cyber-attacks that hinder the functioning of computer systems and cause data loss.

Forgery using computer systems is very rampant and involves illegal alteration of computer data for wrongful gain and loss to innocent people. Therefore, Clause 15 on Computer-related forgery will act as a deterrent.

We are witnessing an increasing abuse of social media fake accounts on platforms such as Facebook, WhatsApp, Telegram, Instagram and TikTok, amongst others in Mauritius. This type of abuse has the sole purpose of causing harm to individuals, especially vulnerable children.

That is why we have introduced clause 16 on Misuse of fake profile.

This provision, however, Mr. Deputy-Speaker, Sir, has elicited quite some comments from the Opposition and this reflects the vibrancy of our democracy. I have no issues with that. However, we should not try to manipulate public opinion or instill fear in the mind of the people just for the sake of criticising. There is clearly a deliberate attempt to mislead people on the Government's intention and this is not new.

We on this side of the House, we will not accept that fake profiles are being used to cause harm to people, because we care for our people!

The misuse of fake profiles can in fact lead to any form of harm, ranging from emotional stress, physical injury and financial disaster to even suicide.

I would like to remind Members of the Opposition that the element of "harm" is causing a lot of controversies.

Let me clarify: Here, we are talking about a Cybersecurity and Cybercrime Bill and it is clear that we are referring to cyber harm which is understood as the damaging consequences resulting from cyber events, which can originate from malicious, accidental or natural phenomena, manifesting itself within or outside of the Internet. We cannot allow these harmful behaviours and content to undermine the significant benefits that the digital revolution can offer.

Mr Deputy-Speaker, Sir,

Another form of crime which is on the rise amongst school-aged children is cyberbullying. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is a repeated behaviour, aimed at scaring, angering or shaming those who are targeted. If this continues, we will also be facing similar situations as other countries such as UK, US, Australia and India, where cases of cyberbullying have led to suicide. We want to protect our children and youngsters unlike the members of the opposition who are against this bill. The clause 17 on Cyberbullying has been added to address this specific issue.

Another common problem being noted in the country these days is “drop-by shipping”. Abusers are using this technique to extract money from people. That is the reason why we have included clause 18 on Cyber extortion to minimise this fraudulent act of extorting money from individuals or groups of people, including organisations using digital technology.

Revenge Pornography is one of the most recurring incident on social media platforms and causes distress and anxiety amongst people. It

involves the sharing of private images or videos of partners, peers or others for revenge purposes. Clause 19 on Revenge Pornography has been introduced to tackle this particular problem.

The Internet can be used for the purpose of spreading extremist propaganda and execution of terrorist attacks. This type of attack is becoming very prevalent in big countries such as the US, Russia, UK, India and China. With the Government's vision of preventing acts of terrorist, clause 20 on Cyber Terrorism will aid in circumventing such types of attacks in the country.

The illegal downloading of movies, music or pirated software for commercial purposes is of concern in the country at the moment. Currently, there are challenges to address this issue. Therefore, clause 21 on Infringement of copyright and related rights has been included in the Bill, to deal with the scourge.

Critical sectors such as Government, Health, Telecommunications and Financial sectors are imperative for providing essential services to the population. A massive cyber-attack on such critical infrastructures can have a debilitating effect on people's lives and the damage to the economy will be inestimable.

This is why we, as a responsible Government, need to ensure protection of critical information infrastructures, on which most essential services rely upon. That is why clause 22 on Increased penalty for offences involving critical information and infrastructure is necessary.

Mr Deputy-Speaker, Sir,

Now, let me come to clause 23 of the Bill, that is, Failure to moderate undesirable content

I have taken cognizance of some unfounded comments that this clause of the Bill will be an impediment to freedom of expression, especially to the Press. This is yet again a misinformation campaign conducted by some twisted minds just to create confusion and to instigate the Press against us.

Clause 23(3) clearly defines “undesirable content” as an online content that is being used with the intent to threaten, defame, and mislead the public. But, more importantly, when it comes to promoting hate speech and racism, it threatens National Security or Public Health and Safety of the country.

Mr Deputy-Speaker, Sir,

Let me give an example of what exactly this clause is all about.

Let’s say for instance, I am the administrator of a public page on social media, where there is a large number of members and followers and there is an ill-intentioned person who posts a content on my wall, saying that we should have a racial war in the country or that one section of the population should fight against another one or still, burn all places of worship of a particular community.

This heinous post is accessible not only to the members and followers of the page, but also to the public in general. One can only imagine the disastrous effect of such an inflammatory post when it goes viral.

Now, this provision of the Bill will be applied only when somebody reports the matter to the Police and after the Police have conducted their investigation and found that the online post constitutes an undesirable content, the Police informs the Administrator to remove that content.

It is, if and only when the Administrator fails to remove that undesirable content, then this clause will apply.

Mr Deputy-Speaker, Sir,

During the course of an investigation by the Police, confidentiality has to be maintained at all times. Should there be any breach, clause 24 on Disclosure of details of an investigation would apply.

Moreover, clause 25 pertaining to Obstruction of investigation has also been included to take legal action against those who obstruct or delay an investigation intentionally and illegally.

We are very much open to constructive criticism with regards to fines which, according to some people, are deemed to be very severe. However, we have to think of damages suffered by victims of cybercrimes and we cannot tolerate perpetrators. The severe penalties will act as a deterrent for the latter who will think twice before acting.

As published in the local newspapers, we see that legal experts are also in support of the high penalties and penal servitude because they feel that it will act as a preventive measure.

Mr. Deputy-Speaker Sir,

Now let me come to Part IV of the Bill which deals with the Investigation Procedures. The legislation enhances the systematic way in which the Police conducts investigations in relation to cybercrimes.

The systematic manner in which the Police will have to mandatorily conduct their investigation as per this legislation reflects not only respect for human rights but also ensures fairness. It will authorise the Police to execute set procedural measures for the purpose of collection or production of evidence with respect to specific cybercriminal investigations or proceedings.

108. This process will involve expedited preservation of evidence, disclosure of information with regard to traffic and content data, powers of access, search and seizure of devices and data for investigation purposes. It also caters for the deletion of unlawful contents from devices. This ensures that there won't be any arbitrary manner in which the Police could conduct their investigation. It will also ensure transparency, certainty and trust.

Mr. Deputy-Speaker Sir,

I would like to draw the attention of the House on provision 29 which is the Real-time collection of traffic data and provision 30, that is, the Interception of content data.

These two clauses have been provided for in order to ensure a thorough investigation and prosecution of a cybercrime case. When a case is reported to the Police, the latter will have to start an investigation. If the investigation requires specific information requiring a Judge's Order, they will have to follow the legal procedures as laid down in this legislation.

Much has been said by members of the Opposition and also taken up by the Press that this clause is being purposely introduced to be able to do content filtering and data monitoring on various social media platforms.

It has also unjustly been stated that this provision is a camouflage of the ICTA Consultation paper on social media content filtering.

I state it, in no uncertain terms, that at no point in time will content filtering and data monitoring be carried out under this clause. This clause is an existing section in the Computer Misuse and Cybercrime Act which dates back to 2003. During the past 18 years when the Computer Misuse and Cybercrime Act was in force, no one challenged this provision. Now that the same provision has been subsumed in this new legislation, some people are shouting on all rooftops that this provision is violating Human Rights.

But let me remind some Honourable Members on the other side of the House, they were the ones who signed the Budapest Convention on Cybercrime in November 2013, and rightly so. Now that our legislation is being aligned with the provisions of this same Convention to enhance our cybersecurity ecosystem as well as to simultaneously respect Human Rights, there is suddenly an uproar. This is pure demagogy and hypocrisy. I leave it to the population to draw its own conclusion.

Mr Deputy-Speaker, Sir,

There are so many lawyers on the other side of the House. Based on what they have stated in the press regarding the Bill, I wonder how they didn't know that this clause was already present in the Computer Misuse and Cybercrime Act of 2003 !

Mr Deputy-Speaker, Sir,

Let me give an example to clarify how this clause can help authorities in their investigation process.

For instance, in a case where there has been online financial fraud.

A person receives an email supposedly from a bank, which looks genuine. The email contains a link on which he is prompted to click and to provide his banking details. The person provides his details thinking that the request is genuine from the bank. After a few days, the person discovers that he has been victim to phishing and that all his money has disappeared in thin air.

The person reports the matter to the Bank and the Police. As part of the investigation, the Police will have to determine the source of the message.

Following the initial investigation, the Police analyses the incident and determines that additional information is required from the Internet Service Provider (ISP) in order to identify the email source.

For the purpose of obtaining some additional information, the Police has to apply for a Judge's Order because it cannot on its own get the information from the ISP as it is bound by the Data Protection legislation.

Once this is obtained, the Police sends a request for information to the ISP along with the Judge's order. The request for information pertains to collection and recording of traffic and content data in real time for that particular email.

Now, here I would like to clarify the proper meaning of "real-time" that is being used in this Bill, as I notice that there are lots of politicians outside this Parliament who have suddenly become cybersecurity experts giving all sorts of interpretations.

Here, "real-time collection of data" - *is a technical jargon and should not at all be confused with live content filtering or monitoring as they are presuming*. "Real-time" refers to a specific time frame for which the Judge, depending on the merits of the case, will give the necessary permission to have access to the required traffic and/or content data at that material time and in this case, the time when the email was sent.

The information required from the ISP include the time, date, source and destination IP address and content of the email amongst others, which will constitute evidence in this case.

Mr Deputy-Speaker, Sir,

As I have explained, this is a routine investigation technique that is being used by all countries around the world for cybercrime cases. I want to stress again that this is by no means Content Filtering and Data Monitoring.

I hope that I have been very clear on that scope and the population can rest assured of the seriousness of this Government to combat cybercrime in all its forms. The whole intent and purpose of this legislation is to shield our people against cybercriminals, contrary to what some gossip mongers are trying to make people believe.

"Critical information infrastructure" are critical information systems meant to operate essential services such as Health, Finance and Government.

The rapid digitalisation and connectivity of Critical Information Infrastructure have led to new vulnerabilities and broadened the categories of risks threatening the resilience of critical sectors. It is therefore crucial to keep pace with technological advancement and anticipate actions against any cyber threats. Part V of the bill caters for measures for the protection of critical information infrastructures.

The Computer Emergency Response Team of Mauritius (CERT-MU) is the focal point for addressing cybersecurity issues at the national level. It

is also the leading Computer Emergency Response Team in the region and has gained a strong international reputation over the years.

It also assists and provides capacity building to different CERTs and incident response teams in the region and worldwide. Part VI of the bill provides legal mandate to allow CERT-MU to operate under the aegis of my Ministry and perform its functions as laid down in the bill.

With information technology, the world is now a global village. A coordinated approach to track cybercrime across borders would not be possible with as many jurisdictions as the number of states that exist. In fact, a silo approach would be a boon for cybercriminals. To effectively deal with such cybercriminals, Part VII on International Cooperation has been introduced.

The main elements of this provision is the mutual legal assistance and the expedited preservation of data as well as the proper functioning of 24/7 point of contact. As it has been aligned with the Budapest Convention on Cybercrime, this provision will also address the lack of a harmonised legal framework with respect to transborder cybercriminal activities.

Mr Deputy-Speaker, Sir,

Gone are the days when cybersecurity was a mere IT issue. In today's interconnected world, the whole functioning of a modern society depends on a robust and resilient cybersecurity ecosystem.

The **Cybersecurity and Cybercrime Bill** is part of this Government's duty and responsibility to strengthen the nation's cybersecurity posture.

With cyber threats growing globally, this Bill is timely to empower the authorities to safeguard essential services from disruptions by cyber-attacks, prevent and respond to cybersecurity threats and incidents to improve the credibility of cybersecurity services in Mauritius. This ensures that our people continue to live, learn, play and work in a trusted and secured cyberspace.

All Members of this august Assembly will therefore fully agree with me on the pertinence and importance of securing the Mauritian cyber territory in order to nurture the different growth vectors of our economy.

With this Bill, we are all set towards our smart nation journey.

It is above politics.

It's about public safety and national security.

As we know, the virtual world is going viral.

And we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine.

To quote the famous American Computer Scientist, Newton Lee :

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

End quote.

This is our Moment ! I firmly believe that with the support of our Prime Minister, Honourable Pravind Kumar Jugnauth, Mauritius will shine as a leading digital country for decades to come and will establish itself as a model not only for the region, but also for the whole world.

Mr Deputy-Speaker, Sir,

I am convinced that this Bill will be a breakthrough for a secure, resilient and progressive Mauritius. I therefore commend the **Cybersecurity and Cybercrime Bill** to the House.

END