Presentation by Deputy Minister of Information, Publicity and Broadcasting Services, Hon K. Paradza to the Parliamentary for Global Action African Workshop on Engaging Female and Male Parliamentarians in Africa

April 3-4, 2023.

Lilongwe, Malawi

Cybercrime is not only a challenge in Zimbabwe but a global problem. Many nations around the world have since formulated Cyber Laws in order to fight numerous typologies of cybercrime. Zimbabwe started to feel the impact of cybercrimes around 2012. This led Business Against Crime Forum of Zimbabwe (BACFOZ), Criminal Investigations Department (CID), and the Commercial Crimes Division to establish a Cyber Laboratory in 2013 with a view to ease investigations of cybercrimes through digital evidence analysis. The Cyber Laboratory was later operationalized in September 2018. The more the nation turned to the use of plastic money, the more cybercrimes increased such as card cloning and identity theft.

In terms of technology since we are in the fourth industrial revolution it is of utmost importance to have in place model frameworks and instruments that can be applied to prevent, respond to and to prosecute Cybercrime. We live in a world where there is increased digitization which improves economic changes but may as a result cause cyber challenges. However, stringent and watertight measures have to be put in place in order to combat

criminals who may prey on citizens because of the availability and access to their personal data.

In response to this my country moved in and crafted the Cyber Security Bill which resulted in the birth of the hybrid Act called the Cyber and Data Protection Act (12:07), No.5 of November 2021. This law amended three pieces of legislation namely, the Criminal Law (Codification and Reform Act), the Criminal Procedure and Evidence Act and the Interception of Communications Act.

Legal Instruments to Fight Cybercrimes

We now have our Cyber and Data Protection Act whose object serves to curb the offences that relate to invasion of privacy, and those relating to electronic communications and material, transmission of messages inciting violence or damaged property and sending of threatening data messages. This Act criminalises these offences and combats Cybercrime.

The nation of Zimbabwe is yet to criminalise cybercrimes, currently there is no cyber law. The recently promulgated Cyber and Data Protection Act (12:07), which repealed and amended sections 162-166 of the Criminal Law Codification and Reform Act 9:23, does not clearly state the creation of offences that has a bearing on Cybercrimes. The Act has only criminalized one cybercrime offence,

which is "Hacking" and has left out various other known typologies of cybercrime which includes amongst others the following;-

- Cyber fraud
- Credit/debit Card fraud or Card Cloning
- Business E-mail Compromise (BEC)
- Phishing
- Identity Theft
- Cyber extortion
- Ransomware
- Intellectual Property Fraud (IPF)
- Cyber Terrorism
- Cyber Pornography
- Sextortion etc, which are currently crimes of concern in our nation.

In our call the Cyber and Data Protection Act is important as it also promotes a number of principles namely;

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy

5. Storage limitation

6. Integrity and confidentiality

7. Accountability

8. Increased trust and credibility

An Organization can gain trust and credibility from its Consumers if it can be demonstrated that it follows the above stated principles in making decisions regarding data protection. As Privacy and Security continue to converge, it means a high level of data security which is an object valued by almost every type of organization. Mature organizations have been protecting their confidential business data in a similar fashion to personal data thereby curbing the issues of infringement of data Privacy.

As it stands the Cyber and Data Protection Act, is more biased to Data Protection than dealing with cybercrimes. Some gaps in the Act are;

- The Act does not define cybercrime and there is no provision of essential elements of cybercrimes though the Act is cited as Cyber and Data Protection Act.
- The Act is silent on recognizable Data Sites where the majority of cybercrimes are committed e.g. Social Media Platforms (WhatApp, Facebook, Twitter, Instagram etc).

- Cybercrime has a transnational effect. Social Media e.g. Social Media Servers are domiciled outside Zimbabwe. The Act is not clear on issues to do with mutual legal assistance procedures, with respect to retrieval of evidence and presentation of evidence in a court of law.

The Cyber and Data Protection Act protects the citizenry and ensures that there is technological advancement in the country. The main purpose of this Act is to curb cybercrime and to ensure that the cyber security will protect the fundamental human rights of all citizens of the country that way promoting the right to Privacy.

The freedom of expression as clearly stated in our section 61 of the Zimbabwean Constitution provides that "**the right to every person to freedom of expression, which includes freedom to seek, receive and communicate ideas and other information…..”However there is a limitation to the right of freedom of expression and freedom of the media which is where now the Cyber and Data Protection Act criminalises offences like "incitement to violence, advocacy of hatred or hate speech, malicious injury to a person's reputation or dignity and malicious or unwarranted breach of a person's right to privacy..".**

There is an issue of abuse of social media which is a global menace. The issue around fake news is a global debate and this Act combats and criminalises these offences. Fake news, misinformation, disinformation and abuse of social media can now be regulated by this Act.

This law is of paramount importance in a data driven economy as we will be able to curb cybercrime and protect the fundamental human rights of all citizens. The provision of this Act ensures that there is no dehumanization with regard to cybercrimes and that the law is enforced reasonably and with due regard to fundamental human rights and freedoms.

As Government we have done the following to ensure implementation of the Act:

(i) Disseminating information on the Act by creating platforms for raising awareness;

(ii) Conscietising the public on issues to do with the Act;

iii) Facilitation of engagements with multi stakeholders and the citizenry in promoting the usage of the Act.

Other Legal Instruments

Zimbabwe also relies on other pieces of legislation in dealing with cybercrimes such as the Postal and Telecommunications Act, and the Censorship Act.

Initiatives to combat cybercrimes in Zimbabwe

Promulgation of the Cyber and Data Protection Act

Establishment of a Zimbabwe Republic Police (ZRP) Cyber Laboratory

Participation on Global Cybercrime Awareness Campaigns by Interpol NCB Zimbabwe

The Government has declared the month of October as the Cyber Awareness Month.

Cybercrime Awareness campaigns by the Ministry of Information, Communication and Technology.

Creation of a special Cybercrime Investigation section within CID CCD.

Community Outreach Programs by Postal & Telecommunications Regulatory Authority of Zimbabwe, Reserve Bank of Zimbabwe, Procurement Regulatory Authority of Zimbabwe, Consumer Council of Zimbabwe in partnership with the ZRP (CID CCD).

Capacity building programs for Cybercrime Investigations.

Zimbabwe participation in Southern Africa Regional Police Chiefs Corporation Organization (SARPCCO) strategic meetings on preventing cybercrimes in the Region.

The ZRP is currently making an input on the Cyber and Data Protection Act on identified shortcomings in the Act in addressing cybercrime.