Commentary on the Cybercrime and Cybersecurity Bill

Definitions of Terms Part II

Following the brief 2017 year end break, we return with this fourth instalment of the commentary series on the draft Cybercrime and Cybersecurity Bill.

As a follow up to the Third instalment that focussed on the Definition of Terms for Computer Device and Remote Forensic Tool, this edition examines the definition of the term Computer Data Storage Medium. This edition highlights how the wide definition of the term in the current draft bill may lead to the violation of fundamental human rights such as the right to privacy.

Computer Data Storage Medium

Computer data storage medium is defined in Section 3 of the draft Bill that contains a host of other terms used throughout the Bill.

It is defined as:

> *"Any device or location from which data is capable of being reproduced or on which data[1] is capable of being stored, by a computer device, irrespective of whether the device is physically attached to or connected with the computer device."*

Simply put, any device that can either produce data, or be used to store data is considered a computer data storage medium. This wide definition includes traditional data storage devices such as external hard drives, but most importantly, it is broad enough to also include cellphones.

[1] Data is defined in section 3 of the Bill as "any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data."

The possibility of the inclusion of mobile phones in this definition is based on the fact that mobile phones, by their nature, can *reproduce* data.

The unauthorised access to data on computer data storage mediums is criminalised in terms of Section 6 (1) of the Bill. Section 9, on the other hand, criminalises the unlawful interference of data kept on a computer data storage medium.

Such unlawful interference can be in the form of altering, damaging, or deleting the data without lawful consent. These are all welcome safeguards meant to ensure the integrity of data stored on all forms of computer data storage mediums.

It must be noted, however, that the wide net cast in this definition causes potential problems when viewed against Section 33 of the Bill which regulates search and seizure procedures for the process of investigating cyber crime. In Section 33 (1)(b), computer data storage mediums are listed as equipment that can be seized in terms of the Act.

This means that while investigating a cyber crime, investigating authorities can seize computer devices, including mobile phones, even if there is no evidence that the mobile phones have been plugged into any computer devices belonging to the person(s) under investigation.

There are already, instances where the Zimbabwe Republic Police (ZRP) Criminal Investigations Department, has seized mobile devices during investigations. For example, during investigations in the Martha O'Donovan case in November 2017, investigating officers seized her mobile phone along with her laptop.

A wide definition of computer data storage mediums will make it possible for investigating officers to seize any electronic equipment, including equipment which is not directly involved in the criminal activity being investigated.

This is a major privacy concern because investigating officers will have the discretion to decide which electronic equipment to grab during cyber criminal investigations.

Summary

- The definition of computer data storage medium is too wide. It gives room for the seizure of personal equipment, which might not fall in the category of traditional data storage devices and equipment.
- The current definition of computer data storage medium exposes personal devices such as mobile phones to search and seizure during cyber crime investigations.
- The current definition will entrench and legitimise the illegal practice by investigating officers of seizing electronic equipment that is not linked to a cybercrime.

End