A comprehensive critique of: The Computer Misuse and Cybercrime Act (2018)

by Brian Kidiga

of P101/1400G/20

1. Abstract

The cybercrime act of 2018 was a significant milestone in laying down the regulations for cyber-activities. Even though the act being an influential draft of the other two international treaty instruments, it still has some provisions that provide definitions and sanctions that are inconsistent with international standards. With a defined abstraction level this article aims to provide a critique to the Cybercrime act that the author considers would have been stated otherwise.

KARATINA UNIVERSITY
Inspiring Innovation and Leadership

2. Introduction

Over the past recent Kenya has witnessed a vast of improvements in the technological space. The application and use of technology has led the world to be viewed as a ***global digital village.*** This dominance has led to the increase of cyber crimes which can be expressed in various forms including hacking, infrigment of intellectual property, phishing,cyber squatting, credit card theft, phishing, spamming, cyber-stalking, illegal access to data, misuse of computer devices for fraud, cyberterrorism among other forms.

The global nature of the internet makes it easy for an individual armed with a computer and the internet to victimise other individuals and businesses anywhere in the world from the comfort of there home. This has greatly increased the question of information security, the incident where biodata from the countrys' ministry of foreign affairs was leaked brought rise to the need for a legislation act to monitor cyber-activities.

3. Overview of the Kenyan cybercrime act

The act, in its power works "***to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes***".

The act can be broken down into the following sections if read in fully. Sections 1 through 3 of Part I contain the preamble, which defines the terms and purposes of the Act. Sections 4–13 of Part II outline the National Computer and Cybercrimes Coordination Committee's formation and operating procedures. Sections 14–46 of Part III list specific cybercrimes and their corresponding punishments, outlining substantial criminal offences. Sections 47–56 of Part IV delineate the pertinent investigative and procedural authorities that are applicable to offenses involving computers and cybercrimes. These powers encompass particular rules concerning the examination and confiscation of computer data, the interception and preservation of data, and the evidentiary value of this data.

The framework for international cooperation in the investigation and punishment of cybercrimes, which frequently contain transnational components, is outlined in Part V (sections 57–65). Sections 66–69 of Part VI address general provisions, which include consequential revisions and the priority clause. The delegation of legislative powers granted by this Act is outlined in Part VII, Section 70.

4. Objectives of the act

Generally, the act provides the following set of objectives:

1. To provide for offences related to computer crimes.
2. To enable timely effective and jurisdiction of cyber crimes
3. Facilitate international co-operation in matters related to cybercrime.

5. Criminal offenses in the act.

A number of crimes pertaining to computers and cybercrimes are outlined in the Cybercrime Act of 2018. In order to preserve digital security and integrity, these offenses are essential. Nevertheless, several features of these offenses have drawn criticism and attention despite their significance.

The Act's definitions' vagueness and broadness are among the main causes for concern. For example, although it lists crimes like hacking, phishing, and cyberterrorism, the definitions could not be precise enough or thorough enough. This ambiguity may cause problems for the interpretation and application of the law, which could lead to unfair results.

Furthermore, the Act imposes stringent penalties for various offenses, including hefty fines and lengthy prison sentences. While it is essential to deter cybercriminal activities, critics argue that some of these penalties may be disproportionately harsh, especially for individuals who may have committed offenses inadvertently or with minimal malicious intent.

Additionally, the Act's framework for international cooperation in cybercrime matters is vital given the transnational nature of many cybercrimes. However, there is a need for clarity and consistency in how such cooperation is facilitated to ensure that it aligns with international legal standards and respects sovereignty and jurisdictional boundaries.

In conclusion, even if the Cybercrime Act of 2018 is a big step in the right direction toward reducing cyberthreats and improving digital security, there are still some issues with it. Amendments or additional legislation must carefully analyze and resolve criticisms about the definitions' clarity, the proportionality of punishments, the protection of individual rights, and international cooperation procedures. The viability and legitimacy of the Act ultimately depend on finding a compromise between protecting individual rights and freedoms and effectively combating cybercrime.