CYBERCRIME AND THE LEGAL AND REGULATORY FRAMEWORK

By JULIET WANGUI MAINA
INTRODUCTION AND BACKGROUND
WHAT IS CYBERCRIME?

Cyber-crime is broadly defined as criminal activity in which computers or computer networks are a tool, a target or place of criminal activity and include everything from electronic cracking to denial of service attacks.

Cybercrime also includes traditional crimes in which computers or networks are used to enable illicit activity.

However, there is currently no definition of cybercrime in our law.

Cybersecurity is defined in the *Kenya Information and Communications Act (2013)* as "the collection of tools, policies, security concepts, security safeguards, guidelines, actions, training, best practices that can be used to protect the cyber environment"
CYBERCRIME OFFENCES

Cyber offences can be classed into four key categories:
• Computer related offences
• Content related offences
• Offences relating to the Confidentiality, Integrity and Availability of Information
• Offences relating to the infringement of Intellectual property rights
COST OF CYBERCRIME

Loss of personal identity information

Reputational damage to the organization

The loss of intellectual property

Opportunity costs: Service disruption

Indirect implications of cybercrime
LEGAL AND REGULATORY FRAMEWORK FOR CYBERCRIME
Penal Code
• KICA (Amendment) amended Section 267 of Penal Code to include information as part of things capable of being stolen
• Forgery of an electronic record
• Unauthorised electronic records
• Use of a cancelled or expired electronic record
• Defamation

Kenya Information and Communications Act Cap 411A
Copyright Act (2012)
Sexual Offences Act (2006)
CHALLENGES OF FIGHTING CYBERCRIME
CHALLENGES

Over-reliance of ICTs
Increased number of users
Availability of Information
Technological developments
Access and Availability of devices
International dimensions
Jurisdictional barriers – crime scene
Anonymity
Failure of traditional investigation instruments
LEGAL CHALLENGES

Challenges in drafting National Criminal law
Non-appreciation of gaps
New offences
New approach to Investigation
Procedures for digital evidence
Lack of technical capacity amongst the Law Enforcement Agents
Challenges in Investigation and Prosecution of Cybercrimes
CHALLENGES WITH THE CURRENT FRAMEWORK

- Some of the existing laws were enacted long before we adopted new technologies such as mobile money, mobile internet and Wi-Fi.

- Mobile payment channels on a daily basis now process millions of transactions valued at over Billions of Kenya Shillings per day;

- The Kenya Electronic Payment and Settlement System (KEPSS) (a banking and electronics payments system) transacts billions per day

- These systems are open to national and international vulnerabilities.
Although the **Evidence Act (Cap 80)** and the **Penal Code (Cap 63)** were amended to provide for electronic evidence and offences using electronic methods, there have been no amendments with regard to procedure and investigation methods that are required.

The current laws are not aligned to the advanced forensic investigation methods adopted by the police. These include the laws relating to extraction, collection and analysis of digital evidence, the scope of warrants, recognition of acceptable tools of trade, preservation of digital evidence and matters of jurisdiction among other challenges.
PROPOSED LEGAL AND REGULATORY FRAMEWORK
<table>
<thead>
<tr>
<th>PROPOSED POLICY, BILLS AND REGULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Bill (2013)</td>
</tr>
<tr>
<td>Critical Infrastructure Protection Bill (2015)</td>
</tr>
<tr>
<td>National ICT Policy (2016)</td>
</tr>
<tr>
<td>Computer and Cybercrime Bill (2017)</td>
</tr>
<tr>
<td>KICA (Cybersecurity Regulations) (2016)</td>
</tr>
</tbody>
</table>
SHORT TITLE: An Act of Parliament to provide for offences relating to computer systems; to enable timely and effective collection of forensic material for use as evidence, and facilitate international cooperation in dealing with cybercrime matters; and for connected purposes.

PROPOSED COMPUTER AND CYBERCRIMES BILL 2017
Offences and Liability

Jurisdiction

Yes, we have “general” jurisdiction.

International cooperation

Investigative Procedures
PART II

OFFENCES

The Bill stipulates wide ranging offences relating to aspects such as:

✓ Unauthorized access, interception and interference
✓ Offences Access with intent to commit further offences committed through use of computer systems
✓ Unauthorized disclosure of a password or access code
✓ Offences involving protected computer systems
✓ Child pornography
✓ Cyber bullying and stalking
✓ Computer fraud, etc
✓ Cyber Espionage
✓ False Publications
Traditional offences committed through use of computer systems have also been captured/ well elaborated under section 21 of the Bill. For example, terrorism is provided for under the Prevention of Terrorism Act.

An offence under this section is therefore punishable under that Act and when propagated through computer systems will also in addition be punishable under the Bill.

Proportionality in sentencing has been taken into consideration in line with the magnitude of the crimes we see today. Additionally, the Bill has sought to incorporate human rights best practices.
The Bill provides for previously lacking investigation procedures necessary for effective prosecution.

This includes criteria for obtaining search warrants for seizure of computer equipment and applications for subscriber information, content and traffic data from private and public entities.

It empowers specific authorized parties, as well as the police by providing grounds through which access to information may be provided.

This is done through application to the court for issue of warrant and thus also provides safeguards and conditions for the use of these investigative powers in order to prevent their abuse.
BALANCING OLD AND NEW LEGAL FRAMEWORKS

SEARCH AND SEIZURE WARRANT

REAL TIME COLLECTION OF DATA

EXPEDITED PRESERVATION

INTERCEPTION OF CONTENT DATA

PRESERVATION ORDER

DISCLOSURE OF TRAFFIC DATA

REAL TIME COLLECTION OF DATA
Part IV of the Bill is necessary to ensure that the Republic will be in a position to obtain cross-border computer and cybercrime assistance.

This applies to investigations, collection of evidence and obtaining expeditious preservation as well as collection of traffic data and spontaneous information. It is to be read with the already existing Mutual Legal Assistance Act (2011).

This Bill also provides for a Point of Contact which will operate 24/7 and which will have the authority to coordinate and enable access to international mutual assistance under the proposed Bill.

This is in accordance with international best practice which is set out in the Council of Europe Convention of Cybercrime (2001)
The Bill provides for jurisdiction that will accommodate the cross border nature of cybercrime.

Therefore, an act or omission will constitute an offence under this Act is deemed to have been committed in Kenya if—

(a) the person committing the act/omission is a
   i. citizen of Kenya or
   ii. is ordinarily resident in Kenya
(b) the act/omission is committed
   i. against a citizen of Kenya;
   ii. against property belonging to the Government of Kenya outside Kenya; or
   iii. to compel the Government of Kenya to do or refrain from doing any act.
(c) Person who commits the act/omission is, after the act/omission, present in Kenya

The Bill also has a **prevailing clause** at s.44 which states that in conflict, the Bill will supersede any such other law
CHALLENGES WITH THE PROPOSED FRAMEWORK

✓ There are no mandatory data breach notification obligations.

✓ The framework does not provide for information sharing mechanisms between private entities, or between the public sector and the private sector.

✓ No network security standards have been imposed on institutions or individuals.

✓ The framework does not account for the severe lack of capacity that is currently found in our Law Enforcement Agents, as well as the Judiciary.

✓ There is need to differentiate between civil and criminal offences.

✓ Some offences such as cyberstalking and cyberbullying may be difficult to gauge and prove. No clear standards.
CASE STUDIES
Cybersecurity Information Sharing Act (2015)

Forensic tools and procedures for collection of evidence

Introducing new provisions for mandatory data breach reporting

Global guidelines for international cooperation framework – CERTs and Point of contact

Minimum security requirements for network operators
ROLE OF LEGAL AND COMPLIANCE PROFESSIONALS

✓ Develop cyber compliance frameworks, to enable clients to assess their compliance with laws.

✓ Develop internal policies and incident response plans.

✓ Respond post breach, including advising the board on internal and external actions, coordinating investigation of the breach and liaising with regulators and third parties.

✓ Advise on International best practices that will cater for existing gaps in our legal and regulatory framework.

✓ Understand the meaning of contracts for technology, including services, software and outsourcing, and their impact on cyber risk.

✓ Anticipate legal risks and approach them appropriately.
THANK YOU

www.tripleoklaw.com
jmaina@tripleoklaw.com