



OCTOPUS CONFERENCE

KENYAN CASE STUDY (PART I)

KENYA LAW REFORM COMMISSION

17 NOVEMBER, 2016—COUNCIL OF EUROPE,
STRASBOURG

A. BRIEF COUNTRY PROFILE

- Internet penetration: 16 million (Communication Authority of Kenya, third quarter sector statistics, 2014)
- Estimated mobile banking users (mpesa, airtel): 26.2 million
- Monetary loss to cybercrime: 2 billion shillings annually

Kenyan secondary students learning how to use computers (access to education)



Kenyan youths using computers: Social-Economic development (employment, ihubs)



Kenya Vision 2030

ICT integral factor to achieve KV 2030

(middle income country status) **ACHIEVED**



- ICTs have taken a priority role in the development of the Kenyan economy
- Estimates indicate that ICT spending in Kenya has surged considerably over the past five years, growing from 8.9% of gross domestic product (GDP) in 2006 to an **estimated 12.1% of GDP in 2013**

B. Legislative Frameworks

- The key legislation dealing with matters of cyber crime and cyber security is the **Kenya Information Communication Act**, Chapter 411A, Laws of Kenya. The Act was substantially amended in the year 2009 and matters relating to cybercrime and computer related crimes including mobile transactions are covered in the legislation. (offences against confidentiality, integrity and availability of computer data and systems)

Contd. KICA

Offences created under KICA include; access with intent to commit offences; unauthorized disclosure of password; Electronic fraud; Tampering with computer source documents; Publishing of obscene information in electronic form and publication for fraudulent purposes, among others.

The Evidence Act, Cap 80, Laws of Kenya

- Recognizing the fact that crimes may involve electronic evidence on a computer or storage device, the Kenya Evidence Act, Cap 80, Laws of Kenya provides elaborately on electronic evidence, admissibility of such evidence and even proper chain of custody (preservation, analysis and presentation of such electronic evidence).

D. Institutions responsible for cyber related issues

I. The Ministry of Information, Communication and Technology

- This is the parent ministry in the national government that deals with matters relating to information, communication and technology. Noting that ICT is a national government function, therefore ICT ministry is in charge of developing and implementing Kenya's ICT policies.

II. Communication Authority of Kenya

- Established in 1999 under the Kenya Information Communication Act, 1998, it is the regulatory body for the communications sector in Kenya. The Authority's functions on include combatting cybercrime and developing frameworks to this end

IV. Kenya Incident Response Team Coordination Centre (Ke- CIRT/CC)

- The Kenya Information and Communication Act, 1998 required the Communication Authority of Kenya set up the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) whose **responsibility is to coordinate response and manage cyber security incidents nationally and to collaborate with relevant actors nationally, regionally and internationally.**

E. Cyber Needs: KENYAN CASE STUDY

a) Law reform

- Whilst the Kenya Information and Communication Act, Cap 411A provides for substantive criminal law, it is deficient on procedural law and matters of mutual legal assistance. A CLARION CALL FOR REVIEW AND AMENDMENT OF KICA FROM A RANGE OF STAKEHOLDERS INCLUDING MY FAVOURITE WANJIKU
- **Recommendation;** Development of a comprehensive legislation to cater for substantive criminal law, procedural law and mutual legal assistance.