

THE JOURNEY TO CYBERCRIME LEGISLATION: A BOTSWANA PERSPECTIVE

Presented by:
Khursheed Rossenkhan
Attorney-General's Chambers
Botswana

**COE OCTOPUS CONFERENCE ON COOPERATION AGAINST CYBERCRIME
(2018)**

BOTSWANA




BRIEF FACTS

- ❖ Democratic country in Southern Africa
- ❖ Landlocked – Neighbours: South Africa, Namibia, Zimbabwe, Zambia
- ❖ Population: Approximately 2 million
- ❖ **Total area: 6, 300 000 km₂ (approx. size of France)**

BOTSWANA'S JOURNEY – THE BEGINNING


- ❖ 1997: The Botswana Government formulated the National ICT Policy Master Plan (Maitlamo)
- ❖ Maitlamo: An ICT Policy that provided Botswana with a clear and compelling roadmap to drive social, economic, cultural and political transformation through the effective use of ICTs

- 
- ❖ Comprehensive Legislative Gap Analysis conducted
 - ❖ Formulation of the Legislative Framework and Change Report
 - ❖ BUT, events overtook some of the report recommendations
 - ❖ Decision by Government = urgent drafting of the Cybercrime and Computer Related Crimes Act

CYBER CRIME AND COMPUTER RELATED CRIMES ACT

- ❖ 2006 : Cabinet approved drafting of a Cybercrime Bill
- ❖ Skepticism –
 - relevance and importance
 - Little access to internet/basic IT services – rural areas
 - “Bigger fish to fry”

- ❖ BUT because of being a soft target and the importance of addressing the growing int'l problem of cybercrime = such concerns overridden
- ❖ Due to urgent need, little by way of drafting instructions
- ❖ Desktop benchmarking, at the time, with Commonwealth Secretariat Model Law on Cybercrime and on the other few laws available online
- ❖ Cybercrime and Computer Related Crimes Act passed and commenced in 2007

- 
- ❖ Cybercrime is ever-changing and technology is ever-evolving
 - ❖ Decision was taken in 2015 to amend the Act
 - ❖ The Act was repealed and re-enacted through Bill No. 33 of 2017, published on 20th October, 2017

HOT OFF THE PRESS

- ❖ Cybercrime and Computer Crimes Act assented to by H. E. The President on 29th June, 2018 and published on the same day as Act No. 18 of 2018



OVERVIEW OF THE ACT

- ❖ Comprises of 36 sections and divided into 4 parts –

Part I – Preliminary

Part II – Offences

Part III - Procedural Powers

Part IV – Miscellaneous Provisions



❖ Some peculiarities –


- 1) Offences deliberately drafted in as general and widely-encompassing terms as possible e.g. s12, “”computer contaminant” instead of “virus” etc.;
- 2) The extension of jurisdiction clause, due to cybercrime being a global phenomenon;
- 3) Offences under the Act considered to be extraditable crimes for which extradition may be granted/obtained under the Extradition Act



PART II – HEART OF THE ACT

OFFENCES INCLUDE –

- ❖ Unauthorised access to a computer, computer system or computer service
- ❖ Unauthorised interference with data
- ❖ Critical national infrastructure
- ❖ Cyber extortion
- ❖ Cyber fraud

- 
- ❖ Cyber harassment
 - ❖ Cyber stalking
 - ❖ Offensive electronic communication
 - ❖ Pornographic or obscene material
 - ❖ Revenge pornography
 - ❖ Racist or xenophobic material or motivated insult
 - ❖ Unlawful disclosure by service providers

CHALLENGES

- ❖ Implementation
- ❖ Small and developing country
- ❖ Lack of resources and limited capacity for training
- ❖ Lack of sophisticated technology at our disposal
- ❖ Lack of manpower and lack of expertise (hands full with “traditional crimes”)
- ❖ Small Police IT Unit

POSITIVES AND WAY FORWARD

- ❖ Enactment of supporting legislation, such as –
 - Electronic Records (Evidence) Act
 - Data Protection Bill (currently in Parliament)
 - Electronic Communications and Transactions Act

CYBERCRIME ACT – WHAT NOW?

- ❖ Continuous review of the Act
- ❖ BUT instructions are a huge challenge
- ❖ Possible urgent interventions –
 - Soliciting of comments from regional/international experts in the field
 - Benchmarking with other laws, including model laws, regionally and internationally

THANK YOU FOR YOUR ATTENTION

