ENSafrica webinar
Cybercrimes Bill
THU 18 FEB 2021
agenda

- cybercrime defined
- interesting facts and stats
- status of the Cybercrimes Bill
- overview of the Cybercrimes Bill
- practical considerations

Ridwaan Boda  
Rakhee Dullabh  
Jessica Steele
cybercrime defined

National Cybersecurity Policy Framework for South Africa, 2012 (7 March 2012) states:

“Cybercrime” means illegal acts, the commission of which involves the use of information and communication technologies.

The Cybercrimes Bill, does not provide a definition for “cybercrime” but rather creates a number of offences which we can refer to collectively as “cybercrimes”.

interesting facts and stats

• In 2020, 80% of organisations saw a rise in cyberattacks
  o there is an attempted cyberattack every **28 seconds**
    (https://www.fireeye.com/cyber-map/threat-map.html)
  o the damage related to cybercrime is projected to hit **$6trillion** annually by 2021
  o **Phishing attempts** have increased by **more than 660%** since March 1, 2020
  o **Ransomware attacks** rose **148%** in March 2020

• South Africa has the **third** highest number of cyber crime victims worldwide, resulting in a loss of about 2.2 billion Rand each year to cyber attacks, according to the South African Banking Risk Information Center (SABRIC). While we are rated as the 31st worst country when it comes to cybersecurity
  (https://www.itweb.co.za/content/5yONPvEg2YkMXWr6)

• The rise of **Crime-as-a-Service**.
status of the Cybercrimes Bill [B6 D – 2017]

21 February 2017

National Assembly

National Council of Provinces

Presidential Signature

Approved by Parliament. Waiting to be signed into law.
an overview of the Cybercrimes Bill
chapters in the Bill

- Chapter 1 – definitions
- Chapter 2 – cybercrimes
- Chapter 3 – jurisdiction
- Chapter 4 – powers to investigate, search and access or seize
- Chapter 5 – mutual assistance
- Chapter 6 – designated point of contact
- Chapter 7 – evidence
- Chapter 8 – reporting obligations and capacity building
- Chapter 9 – general provisions
objects of the Bill

- Create cybercrime offences
- Criminalise distribution of harmful data messages
- Prescribe penalties for cybercrimes
- Provide interim protection orders
- Regulate the jurisdiction for cybercrimes
- Regulate aspects of mutual legal assistance
- Regulate the power to investigate
- Establish 24/7 point of contact
- Provide for proof of certain facts by affidavit
- Impose obligations to report cybercrimes
- Provide that the Executive may enter into agreements with foreign states to promote cyber security
cybercrimes

S 2 – unlawful access  
S 3 – unlawful interception of data (acquisition, viewing, capturing, copying)  
S 4 – unlawful acts in respect of software and hardware tools (use or possess)  
S 5 – unlawful interference with data or a computer program  
S 6 – unlawful interference – computer storage medium or computer system  
S 7 – unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices (purpose)  
S 8 – cyber fraud  
S 9 – cyber forgery and uttering  
s 10 – cyber extortion  
S 11 – aggravated offences  
S 12 – theft of incorporeal property (patent)
malicious communications

S 14 – data message which **incites** damage to property or violence
S 15 – data message which **threatens** persons with damage to property or violence
S 16 – data message of **intimate image**
Penalties for conviction of cybercrimes contained in Chapter 2 of the Bill can range from 1 year to 15 years as well as a fine or both, depending on the cybercrime.

**protection order**

- Prohibit disclosure or further disclosure
- Order an **electronic communication service provider** whose electronic communications service is used to host or disclose the data message – **remove or disable access**
obligations placed on Electronic Communications Service Providers and Financial Institutions

An ECSP or Financial Institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Part I Chapter 2, must:

(a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and

(b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

Failure to do so can lead to imposition of a fine not exceeding R50,000.
jurisdiction

South African courts have jurisdiction to try offences in the following instances:

• person is arrested or offence is committed in SA or on board a vessel, ship, installation, fixed platform, aircraft registered in SA

• person is citizen, resident, incorporated or registered in SA

• actions in preparation of/necessary to commit offence occurs in SA or on board a vessel, ship, installation, fixed platform, aircraft registered in SA

• offence affects a person, restricted computer system in public body or business in SA

• offence committed outside of SA but against citizen, resident, incorporated or registered in SA, restricted computer system or government facility in SA

• other basis
designated point of contact

- National Commissioner must:
  - establish / designate an office within existing structures of SAPS
  - equip and maintain the designated Point of Contact
- Purpose of Designated Point of Contact is to provide immediate expedited assistance for proceedings and investigations related to cybercrimes.
concluding remarks

EXCELLENCE
NOVEL SOLUTIONS
SYNERGY
Concluding remarks

- Cybercrimes Bill can only be seen in isolation – other pieces of legislation such as POPIA, various regulatory codes (e.g. banking industry etc) also deal with the subject.

- Questions arise as to how effectively will the state be able to respond to crimes reported, especially if local SAPS is tasked with policing the Bill.

- Once promulgated, the Bill will likely affect certain types of employee behavior in companies e.g. dealing with marketing lists given prohibitions against unlawful “interception” of data.
how can we assist

• Critical for companies to ensure that polices factor in all applicable legislation such as POPIA, Regulatory codes, Cybercrimes Bill etc as well as common sense and best practises
• Also essential for companies to ensure that ALL staff are given cybersecurity training – the weakest link remains people!
• When faced with cybercrimes, essential to have a strong legal team as part of your overall incident management plans – also to benefit from legal privilege
• ENSafrica services include:
  • Contracting for cybersecurity services
  • Drafting and vetting of policies and procedures
  • Cybersecurity training and POPIA training
  • Breach Response services
  • Forensics and investigations
  • Liaison with regulatory bodies and SAPS
  • Litigation including obtaining Court Orders
thank you for joining us

Africa’s largest law firm
ENSafrica.com

No information provided herein may in any way be construed as legal advice from ENSafrica and/or any of its personnel. Professional advice must be sought from ENSafrica before any action is taken based on the information provided herein, and consent must be obtained from ENSafrica before the information provided herein is reproduced in any way. ENSafrica disclaims any responsibility for positions taken without due consultation and/or information reproduced without due consent, and no person shall have any claim of any nature whatsoever arising out of, or in connection with, the information provided herein against ENSafrica and/or any of its personnel. Any values, such as currency (and their indicators), and/or dates provided herein are indicative and for information purposes only, and ENSafrica does not warrant the correctness, completeness or accuracy of the information provided herein in any way.