# Council of Europe Octopus Conference

Workshop 5: The Global State Of Cybercrime Legislation

South African Overview

**17 November 2021** 

Presented by Adv Jacqueline Fick
B luris LLB MBA CFE FP(SA)

CEO VizStrat Solutions Pty Ltd



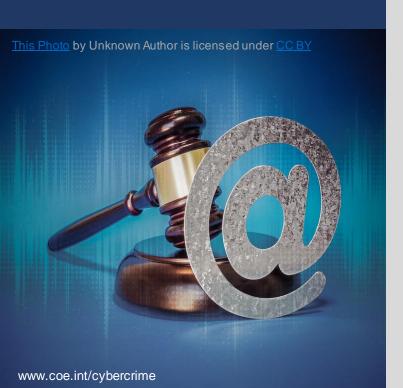


## **Relevant Legislation**



- Various legislation that impact on cybersecurity and cybercrime.
   Includes but not limited to the following:
  - □ National Cyber Security Policy Framework
    - https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000
  - ☐ Electronic Communications and Transactions Act, No 25 of 2002
    - Providing for measures dealing with electronic evidence
    - Cyber offences, which will be repealed by the new Cybercrimes Act, No 19 of 2020)
    - https://www.gov.za/documents/electronic-communications-and-transactionsact
  - ☐ Cybercrimes Act, No 19 of 2020
    - https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000
  - ☐ Protection of Personal Information Act, No 4 of 2013
    - https://www.gov.za/documents/protection-personal-information-act
  - ☐ Cybersecurity Bill still being drafted
  - ☐ Constitution of the Republic of South Africa
    - https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-1

# Key Areas of the Cybercrimes Act





#### **Definitions**

Important to lay foundation for understanding Act



#### **Chapter 2: Cybercrimes**

Cybercrimes, malicious communications inciting violence/damage to property, threatening messages, distribution of intimate images (real and simulated), sentencing and orders to protect complainants from harmful effect of malicious communications.



#### **Chapter 3: Jurisdiction**

Offences committed inside and outside the borders of South Africa



#### Chapter 4: Powers to Investigate, Search, Seize and Access

Standard Operating Procedures, rules on search, seize, access procedures



#### **Chapter 5: Mutual Assistance**

Spontaneous Information, requests for assistance (in addition to MLA processes)



#### **Chapter 6: Designated Point of Contact**

Within existing structures of SAPS, rendering assistance local/international



#### **Chapter 7: Evidence**

Proof of facts



#### **Chapter 8: Reporting Obligations and Capacity Building**

Obligations of electronic communications service providers and financial institutions, capacity building to detect, prevent and investigate cybercrime



#### **Chapter 9: General Provisions**

National Executive and new agreements, several Acts amended/repealed by the Cybercrimes Act, commencement date to be announced





## Roadmap



- Comprehensive legislation to assist in addressing a borderless crime
- Training and awareness imperative: this includes investigators, prosecutors and the judiciary
- Word of thanks to Council of Europe for assistance with reviewing draft Standard Operating Procedures

# Contact



#### **Adv Jacqueline Fick**



jacky@vizstratsolutions.com



https://www.linkedin.com/in/jackyfick/

