Cyber Crimes Act

19 of 2020

EUGENÈ JOUBERT

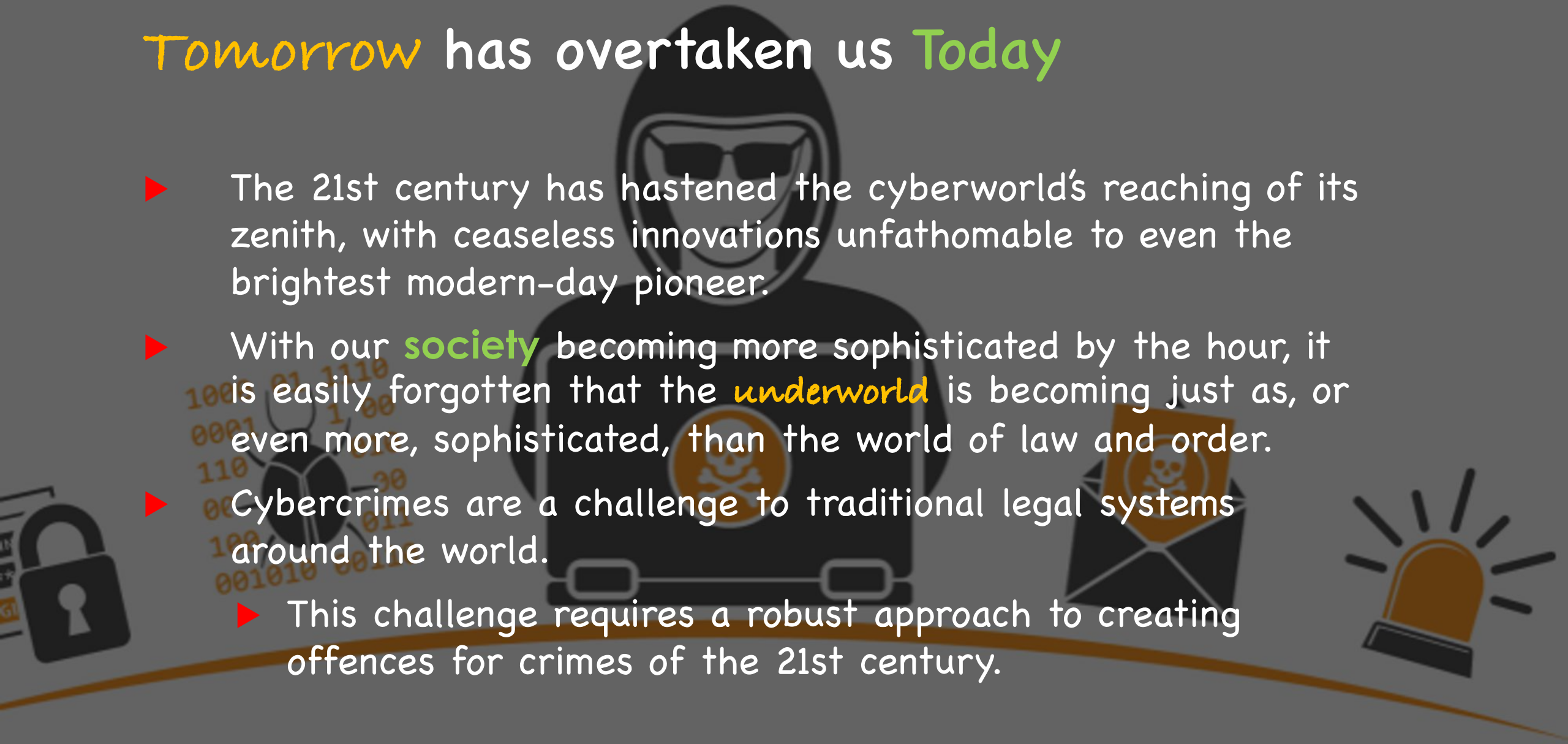
CHAIRMAN

CR GROUP OF COMPANIES

Do you know the stats ?

- The Norton Cyber Safety Insights Report of 2021 indicates that **477 million people** globally have been the **victim of a cybercrime** in their lifetime.
- **328 million** of the **477 million** taking place in the **12 months** prior to May 2021.
- South Africa has the **third highest** number of cybercrime victims worldwide, and it's estimated that it costs us **R2.2 billion a year**.

Tomorrow has overtaken us Today



- The 21st century has hastened the cyberworld's reaching of its zenith, with ceaseless innovations unfathomable to even the brightest modern-day pioneer.
- With our **society** becoming more sophisticated by the hour, it is easily forgotten that the *underworld* is becoming just as, or even more, sophisticated, than the world of law and order.
- Cybercrimes are a challenge to traditional legal systems around the world.
  - This challenge requires a robust approach to creating offences for crimes of the 21st century.

The main purpose of the Cybercrimes Act

- the **criminalisation** of the **disclosure of harmful data messages**
- the **creation** of **new cyber** and **data related offences**
- the imposition of **penalties**
- the **reporting obligations** of **financial institutions**

Definitions in the Cyber Crimes Act

- **"data"** means electronic representations of information in any form
- "data" elektroniese voorstellings van inligting in enige format.
- **"data message"** means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form.
- "databoodskap" data gegenereer, gestuur, ontvang of geberg by wyse van elektroniese middele, waar enige uitset van die data in 'n verstaanbare vorm is.
- **"person"** means a natural or a juristic person.
- "persoon" 'n natuurlike of regspersoon.

Definitions in the Cyber Crimes Act

- **"interception of data"** means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4(2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data, and includes the -
  - **examination** or **inspection** of the contents of the data; and
  - **diversion** of the data or any part thereof from its intended destination to any other destination.

Definition of Financial Institution > Financial Sector Regulation Act

- **'financial institution' means any of the following, other than a representative**
  - a financial product provider
  - a financial service provider
  - a market infrastructure;
  - a holding company of a financial conglomerate; or
  - a person licensed or required to be licensed in terms of a financial sector law
- **Conduct of Financial Institutions Bill**
  - Payment service (financial service)
  - Licensing – payment institutions

The Cyber Crimes Act provides, among others, for …

- acts which **constitute cybercrimes** and **malicious communication offences**;
- the power afforded to any police official to **search** for, **access** or **seize** any article within South Africa; and
- the responsibility of the National Commissioner to establish or designate an office within the existing structures of the South African Police Service, to be the **Designated Point of Contact**.

Unlawful access and unlawful interception of data

Sections 2 and 3

- Any person who **unlawfully and intentionally** performs an act in respect of a computer system or computer data storage medium, which **places the person** who performed the act or any other person **in a position to commit an offence**.

- Any person who **unlawfully and intentionally**:

  - **intercepts data** within or which is transmitted to or from a computer system; and
  - **possesses data** or the output of data **with knowledge** that such data was **intercepted unlawfully**.

- Any person will also be found guilty of an offence if such **person is found in possession of data** or **output of data** and there is a **reasonable suspicion** that such **data was intercepted unlawfully**.

Not defined – Common Law Interpretation …..

- **"unlawfully"** when used in a narrow sense, may refer only to conduct that is criminally punishable – other times it may refer only to actions that violate statutory law.

- **"intentionally"** means that a person acts intentionally with respect to the nature of the conduct, or to a result of the conduct, when it is the person's conscious objective, or desire to engage in the conduct or cause the result.

Unlawful acts in respect of software or hardware tool and unlawful interference with data or computer program or computer storage medium or computer system

Sections 4 to 6

- **Section 4** any person who **unlawfully** and **intentionally** uses or possesses any software or hardware tool that is in contravention of certain provisions listed (access, interception, interference, access codes) is guilty of an offence.
- **Section 5** any person who **unlawfully** and **intentionally** interferes with data or a data program (deletes, alters, damage or deteriorate data or a computer program) is guilty of an offence.
- **Section 6** any person who **unlawfully** and **intentionally** interferes with a computer data storage medium or a computer system (alter any resource or interrupt or impair the functioning or integrity of a computer data storage medium or a computer system) is guilty of an offence.

Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device

Section 7

- Any person who unlawfully and intentionally acquires, possesses, provides to another person, or uses a password, an access code or similar data or device to contravene certain provisions is guilty of an offence.

- **"Password, access codes or similar data or device" means without limitation –**

  - a secret code or pin; an image; a security token; an access card; any device; biometric data; or a word or a string of characters or numbers, used for –

    - financial transactions; or
    - user authentication in order to access or use data, a computer program, a
    - computer data storage medium or a computer system.

Cyber extortion and aggravated offences

Section 10 and 11

- Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in certain sections (3(1), 5(1), 6(1) of 7 (1) (a) or (d) in order to obtain any advantage from another person or to compel another person to perform or to obtain from performing an act, is guilty of cyber extortion
- Any person who commits an offence in terms of sections 3 (1), 5 (1), 6(1) or 7 in respect of or relating to a **restricted computer system**, and who knows or ought reasonably to have known or suspected that it is a restricted computer is guilty of an aggravated offence.
  - A **'restricted computer system'** means any data, computer program, computer data storage medium or computer system under the control of, or exclusively used by –
    - a financial institution; or
    - an organ of state as set out in section 239 of the Constitution, including a court; and
    - which is protected by security measures against unauthorised access or use.

Disclosure is broadly defined

Section 13

- sending the data message to the intended recipient or any other person
- storing the data message on an electronic communications network (such as WhatsApp), where the data message can be viewed, copied or downloaded
- sending or making available a link to the data message that has been stored on an electronic communication network.

Data message which incites damage to property or violence

Section 14

- Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite the causing of any damage to property belonging to; or violence against, a person or a group of persons, is guilty of an offence.

Data message which threatens persons with damage to property or violence

Section 15

- A person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a data message, which threatens a person with damage to property belonging to that person or a related person; or violence against that person or a related person; or
- threatens a group of persons or any person forming part of, or associated with, that group of persons with damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or violence against the group of persons or any person forming part of, or associated with, that group of persons,
- and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated above.

Disclosure of data message of intimate image

Section 16

- Any person ('A') who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person (**'B'**), without the consent of 'B,' is guilty of an offence.
  - **'B'** means
    - the person who can be identified as being displayed in the data message;
    - any person who is described as being displayed in the data message, irrespective of the fact that the person cannot be identified as being displayed in the data message; or
    - any person who can be identified from other information as being displayed in the data message.

Reporting obligations

- An electronic communications service provider or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 must –
  - 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
  - preserve any information which may be of assistance to the South African Police Service in investigating the offence.
- financial institutions who fail to report such offences are guilty of an offence and are liable to a fine not exceeding R50 000.

Reporting Overlap and Penalties

- POPIA imposes an obligation on responsible parties to notify the Information Regulator and affected data subjects where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

- The Cyber Crimes Act prescribes penalties that offenders will be liable for on conviction of the cybercrimes created by the Act. These penalties include fines and/or imprisonment ranging up to 15 years of imprisonment.

Criminals are finding new ways to commit cybercrimes

Hacking

- unlawful and intentional access to data, a computer program, a computer data storage medium or a computer system.

Unlawful interception of data

- acquiring, viewing, capturing or copying of data of a non-public nature through the use of hardware or software tools

Malicious communications

- the distribution of data messages with the intention to incite the causing of damage to any property belonging to, or to incite violence against, or to threaten a person or group.

Cyber fraud

- fraud committed by means of data or a computer program or through any interference with data, a computer program, a computer data storage medium or a computer system.

Cyber forgery

- the unlawful and intentional creation of false data or a false computer program with the intention to defraud.

Cyber uttering

- the unlawful and intentional passing-off of false data or a false computer program with the intention to defraud, or to incite violence against, or to threaten a person or group of persons.

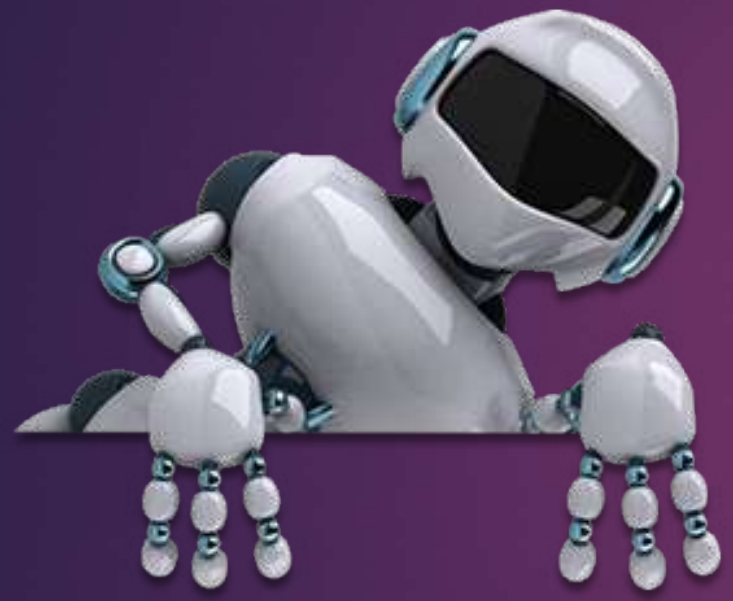
Conclusion

The Cyber Crimes Act will impact everyone in South Africa and the way in which we interact with data or use electronic devices.

With the advent of the age of remote working emanating from the Covid-19 pandemic, cybercrime is rapidly becoming the latest "cyberdemic".

It takes a global and legal effort to curb the spread of cybercrime and breaches of cybersecurity.

QUESTIONS



OPINIONS

(OPINIONS IN THE ALTERNATIVE)

EUGENÈ JOUBERT

082 926 0251