CYBER LAW

Cyber law is part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyberlaw covers a fairly broad area, encompassing several subtopics, including freedom of expression, Internet access to and usage, and online privacy. Generically, cyber law is called the Law of the Internet.

Cyber laws prevent or reduce damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices. Due to the various jurisdictions that cyber activities traverses, enforcement is difficult.

Cybercrime in South Africa has increased exponentially, and the Cybercrimes Act aims to keep people safe from criminals, terrorists, and other states. It also consolidates cybercrime laws and related regulations into the Cybercrimes Act. The law's primary goal is to improve data transmission over the internet whilst keeping it safe.

NB: **The South African Cybercrimes Act has severe consequences for non-compliance.**

Impact

- The Cybercrimes Act [the Act] impacts all organisations and all individuals. It now criminalises the perpetrators of cybercrimes and non-compliance in specific instances [punitive]. It should be noted that as this is a cross-border practice, South Africa has to comply with its international obligations. It impacts everyone who processes data or uses a computer, organisations and private individuals. Together with the Protection of Personal Information Act [POPiA] and the Electronic Communications Transaction Act [ECTA], this legislative regimen will impact the everyday lives of all South Africans. I

  The President signed the Bill into law on 26 May 2021. The proclamation date of **certain sections of** the Cybercrimes Act is 1 December 2021. The President may set different dates for different provisions of the Act.

The Act - Act No. 19 of 2020: Cybercrimes Act, 2020

The main objectives of the Cybercrimes Act are to deal with offences relating to cybercrimes, powers of investigation, criminalisation of the distribution of data messages which are harmful, provide for interim protection orders, evidence gathering, regulate the jurisdiction of courts, the establishment of a specified point of contact and the reporting of obligations and penalties.

The Cybercrimes Act criminalises various types of cybercrimes, including illegally accessing a computer system or intercepting data, cyber extortion, unlawfully acquiring a password, cyber fraud, and theft of incorporeal property. Any person who violates this Act could face a fine, imprisonment of up to 15 years or both. The broad scope of jurisdiction created by this Act

means that the South African courts will have the power to try persons that are non-SA citizens and persons that commit crimes in other countries, where this affects a person or business in South Africa. The South African Police Services ("SAPS") have been given extensive search and seizure powers under the Cybercrimes Act, including searching and seizing information held within a private database or network without a search warrant. This could potentially give rise to many Constitutional rights being infringed, such as the right to privacy and freedom of expression. Jurisprudence will develop as SA courts deal with these matters over time.

The act sets out the objectives of the legislation:

- ✓ to create offences which have a bearing on cybercrime;
- ✓ to criminalise the disclosure of data messages which are harmful and to provide for interim protection orders;
- ✓ to further regulate jurisdiction in respect of cybercrimes;
- ✓ to further regulate the powers to investigate cybercrimes;

- ✓ to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes;
- ✓ to provide for the establishment of a designated Point of Contact; to further provide for the proof of specific facts by affidavit;
- ✓ to impose obligations to report cybercrimes;
- ✓ to provide for capacity building;
- ✓ to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes;
- ✓ to delete and amend provisions of specific laws; and
- ✓ to provide for matters connected in addition to that.

The Cybercrimes Act has imposed new responsibilities on institutions and businesses to comply with far more stringent security requirements in managing the data of citizens and employees, which will play a key role in protecting South Africa against cybercrimes.

Sections of the Act that are now in operation:

- ✓ Chapter 1: Sets out the definitions of the Act.
- ✓ Chapter 2: This chapter sets out all the new cybercrimes created by the Act. The section deals with obtaining orders to protect the complainant pending finalising criminal proceedings that are not yet in operation.
  NB: [excludes Part VI]
- ✓ Chapter 3: This section refers to the jurisdiction of the Act.
  A South African court will have the authority to try any offence created in the Act if the violation affects any person or business in South Africa or if the crime was committed outside of South Africa against any citizen or ordinarily resident in South Africa.
- ✓ Chapter 4: This chapter deals with the authorities powers to investigate, search, access or seize. The excluded sections deal with the preservation of data directions.
  NB: [excludes 38(1)(d), (e) and (f), 40(3) and (4), 41, 42, 43 and 44].

- ✓ Chapters 5: This section is **not yet in operation.** This relates to mutual assistance with foreign requests and establishing a designated Point of Contact within the South African Police Services [SAPS].
- ✓ Chapter 6: This section is **not yet in operation** and
- ✓ Chapter 7: This section sets out the process to prove facts by submission of an affidavit by a suitably qualified individual.
- ✓ Chapter 8: deals with reporting obligations and capacity building to investigate and prosecute cybercrimes. **The reporting obligations for electronic communications service providers and financial institutions are not yet in operation.**
  NB: [excludes section 54]
- ✓ Chapter 9: This section deals with the general provisions and sets out which other rules are repealed or amended by this Act. The Act replaces sections of the Electronic Communications and Transactions Act, 25 of 2002, dealing with unlawful accessing, interception or interference with data messages. Several proposed amendments related to prosecuting harmful disclosure of pornography ("revenge porn") are not yet in operation. However, the offence of "revenge porn" is in process.
  NB: [excludes sections 11B, 11C, 11D, and 56A(3)(c), (d) and (e) of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, from the Schedule of laws repealed or amended in terms of section 58].

Cybercrime and Cybersecurity

Areas that are related to cyber law include cybercrime and cybersecurity. With proper cybersecurity, businesses and people can protect themselves from cybercrime. Cybersecurity looks to address weaknesses in computers and networks. The International Cybersecurity Standard is known as ISO 27001.

Cybersecurity policy is focused on guiding anyone that might be vulnerable to cybercrime. This includes businesses, individuals, and even the government.

Information and training are essential ways to improve cybersecurity.

Cybercrimes are committed against society, including governments, businesses, and people.

UNODC excerpt:

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters.

Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organisations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law.

Categories of Cyber Crime

Generally, there are three major categories of cybercrimes, including:

- **Crimes Against People.** While these crimes occur online, they affect the lives of ordinary people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online-related defamation etc.
- **Crimes Against Property.** Some online crimes attack property, such as a computer or server. These crimes include hacking, virus transmission, cyber, computer vandalism, and copyright infringement [including IP] violations. In many instances, the attackers lock users out of their systems and release access once the ransom is paid [usually in crypto currency] – referred to as 'ransomware.'
- **Crimes Against Government.** When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

Cyber Law Trends

Cyber law is increasing in importance every single year. This is because cybercrime is increasing. To fight these crimes, there have been recent trends in cyber law. These trends include the following:

- New and more stringent regulations.
- Reinforcing current laws.
- Increased awareness of privacy issues.
- Cloud computing.
- How virtual currency might be vulnerable to crime.
- Usage of data analytics.

Creating awareness of these issues will be a primary focus of governments and cyber law agencies.

Companies specialising in Cyber protection generally offer a holistic service, including specialist digital and internet tools [software including AI] and advisory services.
Many institutions provide free online guidance, registering to receive newsletters with updates etc.

NIST- National Institute of Standards and Technology - https://www.nist.go

CISA – Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov

Register to receive newsletters with updates etc.

Many ICT companies also have valuable website guidance [register for email advisories].

Cyber Law and Intellectual Property

An essential part of cyber law is intellectual property. Intellectual property includes art, literature, music, and businesses. IP rights related to cyber law generally fall into the following categories:

Copyright protects almost any piece of IP you can transmit over the internet. This includes books, music, movies, etc.

Patents are generally used to protect an invention. These include software and online business processes, including systems, etc.

Trademarks are used virtually as they are in the real world. Trademarks will be used for websites and special services provided online.

Trade Secrets. Online businesses can use trade secret protections, although these can be *reversed engineered* in the modern online world.

Domain Disputes are about who owns a web address.

Contracts. Any person accessing a website generally has to agree to the terms of service. - This is a contract.

Privacy. Online services and any electronic storage of client information are subject to data privacy laws, POPiA. The storage or retention of client information is prohibited unless there is an ongoing business relationship with the client.

Cyber Security Strategies

Besides understanding cyber law, organisations must build cybersecurity strategies. These, at a minimum, must cover the following areas:

Ecosystem. A robust ecosystem helps prevent cybercrime. Your ecosystem includes three areas—automation, interoperability[1], and authentication. A robust system can prevent cyberattacks like malware, attrition, hacking, insider attacks, and equipment theft.

Framework. An assurance framework is a strategy for complying with security standards. This allows updates to infrastructure. It also allows governments and businesses to work together in what's known as "enabling and endorsing'.

Open Standards. Open standards lead to improved security against cybercrime. They allow businesses and individuals to use proper protection easily. Open standards can also improve economic growth and new technology development.

It is strengthening Regulation. This speaks directly to cyber law. Governments can work to improve this legal area.

E-Governance. E-governance is the ability to provide services over the Internet. Developing this technology is an integral part of cyber law.

Infrastructure. Protecting infrastructure is one of the most critical parts of cybersecurity.

Refer to the LSSA website for guidance in this regard www.LSSA.org.za

Mitigating Risk

Cyberlaw aims to reduce the risk, including the protection of network security.

Cybersecurity should be treated as a business risk and mitigated [reduced]. The general rule is that *'it is not if but will you be hacked.'*

This requires a business continuity plan [to recover fast], with cloud computing being the preferred choice.

Cyber security practitioners have enhanced the simulation and scenario planning in risk mitigation.

Breach and Attack Simulations (BAS) are growing in popularity as a way of testing cyber resilience. The technology is used to automatically spot weaknesses in an organisation's cyber security, a little like automated, ongoing penetration testing.

For risk mitigation strategies, resources including cyber guidance, visit the LSSA website: www.LSSA.org.za

Cyber Law Business Consideration

A business's website is a significant asset. It is also highly vulnerable to cybercrime. Various agencies and organisations provide guidance; in many instances, these are ICT companies or State agencies.

Clients

Protecting your client's personal information is essential to comply with cyber law and POPiA. **This is true even if your business lacks a website or the client information is not digitally stored [hard copies].**

Regarding POPiA, your business's privacy and security policies must be available to your clients. This confirms your commitment to protecting their personal and financial information when they use your website.

Cyber Law Terms and Laws

There are three main terms that people need to know related to cyber law.:

1. **Information Technology Law.** These laws refer to digital information. It describes how this information is gathered, stored, and transmitted.- POPiA / ECTA
2. **Cyber Law/Internet Law.** These laws cover the usage of the internet. ECTA & Cybercrimes Act
3. **Computer Law.** This covers a sizeable legal area. It includes both the internet and laws related to computer IP. – ECTA
4. **Critical Infrastructure. T**he State's physical or virtual systems and assets are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.

5. **Cyber Infrastructure.** The communications, storage, and computing devices upon which information systems are built and operate.
6. **Cyber Operation.** The employment of cyber capabilities to achieve objectives in or through cyberspace.
7. **Cyberspace.** Physical and non-physical components form the environment to store, modify, and exchange data using computer networks.