BIZCOMMUNITY

World's largest crime zone... cyberspace

By Simone Gill and Bilal Bokhari

18 May 2016

It is essential for South Africa to establish and implement cybersecurity measures and legislation, as cyberspace becomes the world's largest crime zone.

The rapid evolution and widespread deployment of ICTs has tremendously increased accessibility to the internet in developing nations, where cyber security laws are either non-existent or still in their infancy.

Rights such as freedom of expression, freedom of trade and access to information apply equally in cyberspace and need to be both recognised and protected.

While the revolutionary socio-economic benefits of Internet accessibility are undeniable, the ease of access facilitated by ICTs poses immense dangers to the security of the electronic information society. The grave magnitude of the increasing threat of cybercrimes has validated the necessity for comprehensive and effective national cyber security laws.

Current cyber security law in South Africa

Cyber security is currently regulated in South Africa through provisions contained in the Electronic Communications and Transactions Act (ECTA). Furthermore, South Africa is signatory to international treaties, such as the Southern African Development Community (SADC) Model and the Budapest Convention. These treaties recognise that the Internet, being a global phenomenon, requires an internationally harmonised legislative approach to cyber security and international cooperation in order to combat cybercrimes efficiently.

Over the past few years, the South African government took a number of measures and steps in respect of cybersecurity.

These include the publication of the National Cyber Security Policy Framework (which was approved by the Cabinet in March 2012), which outlined policy positions regarding cybercrime, national security threats in cyberspace, combatting cyber warfare and developing and updating applicable existing laws to ensure alignment. The Framework aimed to coordinate state activities on cybersecurity and required co-operation between government, the private sector and civil society.

In October 2013, South Africa's first National Cyber Security Advisory Council was inaugurated and mandated to advise government on cyber security issues.

Also, the ECTA Amendment Bill (gazetted in October 2012) proposed the establishment of a 'cybersecurity hub' by the Minister of Communications in consultation with the Justice, Crime Prevention and Security ministries (JCPS Cluster). The cybersecurity hub was assigned responsibility for creating awareness of cybercrime, responding timeously to incidents or threats of cybercrime, detecting and preventing cybercrime and fostering co-operation between government, the private sector, civil society and international businesses and communities in implementing guidelines or standards for cyber security requirements.

The National Integrated ICT Policy Green Paper, published in January 2014, identified numerous hurdles including fragmented systems and non-alignment of laws and policies, which need to be overcome prior to implementation of an effective national cyber security strategy.

Although the majority of the provisions of the Protection of Personal Information Act (POPI Act), which was assented to in November 2013, are yet to come into force, its implementation appears to be imminent. This represents a significant advancement in data security standards in South Africa by imposing stringent requirements pertaining to the lawful processing of personal information and requiring data processors to implement security measures aimed at protecting personal data from breach or compromise. The POPI Act further imposes administrative as well as punitive penalties for infringements of its provisions.

Draft Cybercrimes and Cybersecurity Bill, 2015

The steps taken by Government as indicated above appear to have culminated in the draft Cybercrimes and Cybersecurity Bill, published for public comment in August 2015, which embodies the legislature's most comprehensive cybersecurity framework to date.

To this end, the Bill provides for the criminalisation of a broad range of cybercrimes, including:

- using personal information (as defined in POPI and including addresses, phone numbers, dates of birth and identity numbers) and financial information (any information or data which can be used to facilitate a financial transaction including information regarding credit cards, savings accounts and financial planning information) to commit offences;
- unlawfully accessing and intercepting data;
- using software, hardware and computer systems to commit offences;
- prohibited financial transactions such as money laundering;

- possession and distribution of malware such as viruses, worms, logic bombs and Trojan horses;
- computer related fraud such as online auction fraud where perpetrators offer non-existent goods for sale and request unsuspecting buyers to pay prior to delivery;
- computer related forgery and uttering such as the manipulation of digital documents or the usage of phishing by perpetrators to obtain sensitive information from victims;
- computer related appropriation, which entails the intentional and unlawful appropriation of ownership or rights in property such as money, credit, any information that can be used to facilitate a financial transaction, or any movable, immovable, corporeal or incorporeal thing that has commercial value;
- computer related extortion, which occurs for example in instances where a person threatens another person by means of a data message to disclose unflattering personal information of the person unless the demands of the extortionist are met or where the extortionist threatens to install malware onto another's servers if his or her demands are not met;
- computer related terrorist activity such as the propagation of terrorist activities to recruit new members, disseminating information on how to make bombs or weapons, online coordination of terrorist attacks and any activity aimed at causing destruction, destabilisation or threating national or international security;
- computer related espionage which includes the usage of hacking, social engineering and specialised software and hardware to gain unauthorised access to critical data or a critical database or National Critical information infrastructure;
- a prohibition on the dissemination of data messages which advocates, promotes or incites hate, discrimination or violence by making available, broadcasting or distributing a data message representing ideas or theories, which advocate, promote or incite hatred, discrimination or violence, against a person or group of persons, based on race, origin, ethnicity, religious beliefs, gender, sexual orientation or mental or physical disability. Accordingly, the recent flurry of racist social media posts would constitute a specific crime in terms of the Bill; and
- Infringement of copyright and notably the criminalisation of infringing copyright using peer-to-peer file sharing.

Assisting, attempting, inciting or procuring any of the above also constitutes an offence in terms of the Bill and penalties on conviction include fines of between R5 million and R10 million or imprisonment of up to 25 years. Importantly, the offences created in terms of the Bill are not technology specific and will remain relevant in an ever-changing technology landscape.

Also worth noting is that the provisions of the Bill do not affect criminal liability in terms of the common law or other legislation which means that the penalties may be interpreted to be additional to any penalties which may be imposed under other existing law.

Powers relating to investigation, search and seizure

The Bill establishes procedures, which cater specifically for the investigation of cybercrime. The current legislative provisions applicable to investigating aspects relating to cybercrimes, such as those contained in the ECTA, the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) and the Criminal Procedure Act, are deemed inadequate measures for the investigation of cybercrimes and the Bill confers extensive powers to law enforcement authorities and other investigators in respect of access, search and seizure procedures.

Impact on electronic communications services providers, including financial institutions

The Bill imposes a number of obligations on electronic communications service providers, defined widely under the Bill to include not only persons or entities providing electronic communications services but also persons and entities which transmit, receive, process or store data and also, interestingly, 'financial institutions' as defined in the Financial Services Board Act, which includes:

- any pension fund organisation registered in terms of the Pension Funds Act;
- any 'exchange', 'authorised user', 'stock -broker', 'settling party', 'clearing house', 'central securities depository', 'participant' or 'nominee' as defined in s1 of the Securities Services Act;
- any 'long-term insurer' as defined in the Long-term Insurance Act;

- any ‘short-term insurer’ as defined in the Short-term Insurance Act and the Regulations under the Long-term Insurance Act;
- any authorised financial services provider’ or ‘representative’ as defined in the Financial Advisory and Intermediary Services Act; and
- A bank as defined in the Banks Act.

The Bill accordingly has a far-reaching impact and compels electronic communications service providers to:

1. take reasonable steps to inform clients of cybercrime trends which can affect them;
2. establish procedures for clients to report cybercrime; and
3. Inform clients of measures to take to protect themselves against cybercrime.

In addition, an electronic communications service provider, which becomes aware that its electronic communications network is being used to commit cybercrime must:

4. immediately report matter to the National Cybercrime Centre; and

5. Preserve all information that will be relevant to the investigation of the cybercrime committed.

Failure to comply with the above provisions will cause the service provider to be guilty of an offence and liable upon conviction to a fine of R10,000 for each day in which it failed to comply.

Agreements with foreign states

The Bill provides that the President of the Republic of South Africa may enter into agreements with any foreign state regarding:

1. the provision of mutual assistance and co-operation relating to an investigation and prosecution of an offence cited in Chapter 2 of the Bill; and
2. An offence in terms of substantially similar laws to the laws of the Republic, which was committed by use of an article in that foreign state.
3. the implementation of cyber threat response activities;
4. the research of information on cyber security related matters;
5. the security of National Critical Information Infrastructures;
6. establishment of contact points;
7. establishment of emergency cross-border response mechanisms; and
8. the establishments of emergency centres to deal with cybercrime related matters.

Jurisdiction

The Bill has extensive jurisdiction related provisions, which have a broad scope. In summary, South African courts assume jurisdiction where:

1. the offence or any part thereof (including its preparation) was committed in South Africa or where such offence has an effect in South Africa;
2. the offence was committed by a South African citizen, permanent resident or a person carrying on business in South Africa; or
3. The offence was committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time the offence was committed.

Where an offence occurred outside of South Africa, regardless of whether such an act or omission is recognised as an offence in the place of commission, a South African court has jurisdiction if the person charged:

1. is a citizen or ordinary resident of South Africa;
2. was arrested in South Africa or in its territorial waters or on board a vessel registered or required to be registered in South Africa;
3. is a company, incorporated or registered in South Africa; or
4. is a body of persons, corporate or incorporate in South Africa.

An offence shall be deemed to have also been committed in South Africa if that:

1. act or omission affects or is intended to effect any person in South Africa;
2. person is found to be in South Africa; or
3. Person is not extradited by South Africa or there is no application to extradite that person.

Powers to investigate, search and access or seize and international cooperation and structures to deal with cybersecurity

The Bill establishes procedures, which cater specifically to the investigation of cybercrimes. The measures set out in existing legislation are considered not to adequately provide for the investigation of cybercrimes, which, by their very nature, require more technology specific, specialist, focussed investigative measures. The Bill allows extensive powers to be afforded to law enforcement members and other investigators (likely to be experts such as computer forensic specialists) in respect of access, search and seizure procedures.

The Bill establishes a 24/7 point of contact, (which is required to be available on a 24 hour, 7 days a week basis in order to ensure the availability of immediate assistance for the purposes of proceedings or investigations regarding commission of offences in terms of the Bill). It includes the following fora, (comprised of both private and public bodies, including the South African Police Service, the South African Defence Force, State Security Agency and private sector security incident response teams) to assist and facilitate with enforcement and/or compliance issues:

1. Cyber Response Committee
2. Cyber Security Centre
3. Government Security Incident Response Teams
4. National Cybercrime Centre
5. Cyber Command
6. Cyber Security Hub
7. Private Sector Security Incident Response Teams

National critical information infrastructure protection

The Bill deals with the designation of National Critical Information Infrastructures and the mechanisms established to deal exclusively with the protection of such critical infrastructure.

Information infrastructure/s will be declared as National Critical Information Infrastructure/s if it appears that the information is of such a strategic nature that the interference, damage or loss thereof may:

1. prejudice state security;
2. prejudice public health;
3. prejudice rendering of essential services;
4. prejudice economic stability; and
5. Create public emergency.

There are procedures which the Minister of Security must follow (including consultation with certain fora) before information infrastructure/s can be declared as critical.

Conclusion

The value of data in a digital era cannot be understated and it is crucial that businesses and individuals implement stringent data security measures and policies to mitigate against the potential risk of becoming victims of cybercrimes. The Bill serves to create further awareness of the importance of security measures and the impact of cybercrime, although its practical implementation will be costly and is likely to take some time. As South Africa can still be considered to be in its infancy in respect of cybersecurity legislation, we suspect that we will need to look to foreign jurisdictions for guidance on steps to be taken, particularly as cybercrime is a global phenomenon and one that is not restricted to any particular borders.

ABOUT THE AUTHOR

Simone Gill is a director and Bilal Bokhari, an associate designate, in Cliffe Dekker Hofmeyr's Technology and Sourcing Practice.