New Bill offers robust game plan against cybercrime in South Africa

12 Jun 2019 |Hanneke van der Westhuizen - SAIIA Programme, Economic Diplomacy

Source - https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/

A significant increase in internet access combined with a growing reliance on e-governance, commercial services, social networks, and the Internet of Things has increased the vulnerability of both citizens and governments to cyber criminals.

Conventional crimes normally leave a trail of evidence that can be tracked to solve the crime, however, crimes that takes place in cyberspace are much more complex to trace and therefore to solve. South Africa, like other countries, is not immune to this phenomenon.

According to the South African Banking Risk Information Centre (SABRIC), 16,296 acts of cybercrime in the banking sector were reported to SABRIC between January and August 2018. Since the early 2000s, the government has introduced various forms of legislation to address the ever-evolving threat of cybercrime. However, despite all its efforts, the implementation of legislation to counter cybercrime and ensure data protection remains challenging.

The newly drafted Cybercrimes Bill, expected to come into effect later this year, introduces a more proactive focus on the various forms of cybercrime and brings current data protection laws under its ambit. The implementation of data protection laws in tandem with a cybercrimes policy could be a powerful tool to reduce cyber threats and narrow the space for cybercrime.

The Cybercrimes Bill’s main objective is to deal with offences relating to cybercrimes, jurisdiction of courts, powers of investigation, search, seizure, access, evidence gathering, the establishment of a designated point of contact, reporting obligations and penalties.

The following timeline for the development of the Cybercrimes Bill and privacy and data protection laws in South Africa is instructive on how policy thinking has evolved to deal with this challenge.

Timeline: South Africa in the battle against cybercrime

In order to create the first legislative framework against cybercrime, government initiated a cybercrime section into the Electronic Communications and Transactions Act (ECT) in November 2002. The purpose of the Act was to establish a structure that defines, develops, regulates and governs e-commerce in South Africa.

As cybercrime became a more prominent threat, the Regulation of Interception of Communications Act (RICA), introduced in 2005, was created to complement the ECT Act. It governs the seizure of paper-based and electronic communications. RICA focuses on how monitoring of communication takes place – meaning that all forms of monitoring and interception of communications are unlawful unless monitoring and interception takes place within the RICA framework. RICA would, therefore, not prevent an employer from monitoring data of an employee unless it falls within the RICA framework.

Critics argued that the cybercrime section in the ECT Act was too broad and that it did not adequately legislate the codification of cybercrimes and the related penalties, which ultimately restricted the prosecution of cybercriminals. The main concern with RICA is that it serves as an infringement of the Constitutional right to privacy.

According to the Norwegian Institute of International Affairs (NUPI), developing countries are not paying enough attention to legislation on cybercrime, making them more attractive to criminals. The ECT Act and RICA have not created a scope and consequence for liability, making South Africa more vulnerable to cyber-attacks and prompting a need for a legislative framework that establishes a cyber security infrastructure.

In 2017 the draft Cybercrimes and Cybersecurity Bill, initiated by the Ministry of Justice and Correctional Services, was submitted to Parliament. The Cybercrimes Bill differs quite substantially from previous versions. Previously, it consisted of two sections namely (i) cybercrimes and (ii) cybersecurity. The cybersecurity section raised various concerns around freedom of expression and internet censorship. As a result, the section pertaining to cybersecurity was removed and the focus shifted to cybercrime alone.

According to the World Economic Forum, cybercrime caused losses to the South African business sector worth approximately R5.8 billion in 2015. South Africa’s banking sector is the biggest target of cybercrime operations and banks have to invest three times more on cybersecurity than other non-financial organisations of a similar size. To support the Cybercrimes Bill, the Payments Association of South Africa introduced DebiCheck in August 2018, which enables clients to authorise electronic debit orders before a payment is processed.

Once the Cybercrimes Bill is finalised, the South African Police Service (SAPS) will be empowered to act against such crimes, enabling cybercrime specialists to better track unlawful activity. However, the capability of the SAPS to implement the legislation given the lack of cybercrime skills development training remains a challenge.

In the UK every police force now has a dedicated cybercrime unit to investigate and pursue offenders, assist businesses and victims to protect themselves from attack and to prevent vulnerable individuals from being hacked. In order to be able to provide such protection, each unit receives coordination and support from both the Regional Organised Crime Units and the National Cybercrime Units. It is too soon to say if cybercrime is decreasing in the UK, but South Africa can learn from the UK's capacity building efforts to fight cybercrime.

Privacy and data protection

Privacy and data protection are vital in generating secure cyber infrastructure. According to IBM, the average cost of a data breach in South Africa has escalated from R32 million in 2017 to R36.5 million in 2018. Data has become a valuable currency. Companies such as Facebook, Twitter and Uber have built their businesses and revenue models on personal data and how online customer behaviour could be utilised to serve its clients and owners. We live in an era where information means power and electronic assets such as software, websites, databases, intranets, accounting records, customer lists and other data are an integral part of how business is conducted. Since the increase in the value of data, cyber criminals have gone to great lengths to access data.

In November 2013, South Africa's Protection of Personal Information (POPI) Act was signed into law in response to the accumulation of personal information without the data subject's permission. The core purpose of the POPI Act is to enable data subjects to act against organisations for data breaches. However, the Act is still not fully operational because an implementation date has not yet been set. Once set, South African companies will have one year to adjust to the new rules set by the Act. Penalties for non-compliance could range from R10 million in fines to 10 years' imprisonment.

Developed countries are well ahead of developing countries in the fight against cybercrime. Acknowledging that data protection is an important human right, the European Union (EU) is leading with its binding law that protects the usage of data of EU citizens. The General Data Protection Regulation (GDPR) came into effect in May 2018 with the aim of regulating information management including permitting internet users to manage the use of personal or institutional data. When GDPR is disregarded, fines are imposed in line with the scope of the criminal act.

EU regulators have devised a methodology for assessing the risk value of data in order to resolve which data protection procedures to use. Although the GDPR could be instructive in strengthening the POPI

Act, it is important to recognise the uneven developmental challenges that the POPI Act has to consider. Some South African companies have taken an initiative to adopt GDPR consumer protection measures to enforce stronger security measures against cybercrime.

Conclusion

Earlier South African legislation did not fully respond to the challenges involved in combatting cybercrime. The newly proposed Cybercrimes Bill is very different in this respect. The new responsibilities imposed on institutions (including banks, electronic service providers and financial institutions) to comply with far more stringent security requirements in managing the data of citizens will play a key role in protecting South Africa against cybercrimes. The Bill will require an alignment with the established data protection Acts, namely RICA and the POPI Act to build “a wall” against intruders. Cybercrime presents complex problems that requires a more profound skills set. The skills of the SAPS to prevent and investigate cybercrime remains a concern. The successful implementation of the POPI Act and the Cybercrimes Bill, once it is enacted, will therefore require private sector institutions and governmental agencies to jointly strengthen their counter cybercrime efforts.