The Cybercrime and Cybersecurity Bill and POPIA: Prioritising data protection

July 2017
Without Prejudice

On the tail of 12 May global "WannaCry" ransomware attack, arguably the most widespread cyber-attack in history which, according to Raconteur, affected more than 250 000 victims in approximately 150 countries, big business is left to question its vulnerability and exposure to cyber-attacks.

Locally, a reputable telecommunications service provider acknowledged that several of its customer service systems were offline as a result of "WannaCry" ransomware.

The Protection of Personal Information Act (POPIA) and the Cybercrime and Cybersecurity Bill (the Bill) are two pieces of legislation in the process of becoming effective, and introduce several provisions aimed at protecting data subjects from data breaches.

POPIA establishes the Information Regulator, and confers on the Information Regulator various powers, duties and functions, including monitoring and enforcing compliance by public and private bodies with POPIA and handling complaints in respect of contraventions of POPIA.

Of particular importance, the Information Regulator is empowered to investigate complaints about violations of the protection of personal information of data subjects, which includes summoning individuals to appear before the Information Regulator, receiving evidence, conducting private interviews and, upon issuing of a warrant, entering and searching any premises and seizing articles linked to the commission of an offence in terms of POPIA.

According to the Information Regulator, who was the keynote speaker at a recent Hogan Lovells seminar, the process of drafting regulations under POPIA is underway and those regulations can be expected later this year. It was further indicated that POPIA is likely to become fully effective in 2018.

POPIA establishes a comprehensive compliance framework, which regulates an organisation to increase the integrity and strength of its systems to prevent data breaches thereby reducing its vulnerability to malware such as "WannaCry".

POPIA includes several provisions relating to the obligations of responsible parties aimed at the protection of data, among others:

- Entrenchment of the rights of data subjects, including the right of data subjects to be notified that the data subjects' personal information has been accessed by an unauthorised person; and
- Placing an obligation on responsible parties to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to it.

In order to enhance the legal recourse available in the event of cyber-attack, the Bill addresses cybercrime and cybersecurity in South Africa. According to the Memorandum on the Bill, it is acknowledged that our cybercrime laws are not in line with those of the international community and, while the common law is used to prosecute certain offences, it needs to grapple with new concepts such as intangible data.
Further, different government departments have enacted legislation to protect their own interests creating a "silo-based approach", which fails to address various essential steps necessary for a comprehensive cybersecurity regulatory framework in South Africa.

The Bill, which was recently tabled in parliament, creates several offences relating specifically to the unlawful possession of data, in accordance with international guidelines. These include:

- The unlawful and intentional securing of access to data, a computer programme, a computer data storage medium or a computer system;
- The unlawful acquisition of access to data by overcoming any protection measure, which is intended to prevent access to data, and the unlawful possession of that data; and
- The unlawful acquisition, possession, provision, receipt or use of a password, access codes or similar data or devices to commit cyber offences in terms of the Bill.

The Bill also creates structures such as the 24/7 Point of Contact, the Cybersecurity Hub and nodal points, to promote the reporting, investigation and prosecution of incidents of cybercrime. The 24/7 Point of Contact will operate on a twenty-four-hour, seven-day-a-week basis to provide immediate expedited assistance to

investigate offences in terms of the Bill.
Each sector is tasked to establish a nodal point which will be responsible for reporting cyber incidents, receiving information about cyber incidents from the Cybersecurity Hub and receiving and distributing information about cyber security incidents with other sector nodal points.

Both pieces of legislation confer power to the South African Police Services to investigate, search and access or seize any article used in the commission of an offence, and create mechanisms for mutual assistance between foreign states in cross border investigations.
In collaboration, the Bill and POPIA broaden the South African legislative framework relating to data protection and privacy, to bring South Africa in line with international guidelines. They establish minimum requirements for the processing and protection of personal information thereby promoting the right to privacy enshrined in section 14 of the Constitution.

> Read the full article online