THE CYBERCRIMES AND CYBERSECURITY BILL – THE RATIONALE BEHIND IT AND WHY YOU SHOULD COMMENT

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by PPM Attorneys | July 10, 2017

The enacting of legislation undergoes a consultative process; the Promotion of Administrative Justice Act 3 of 2000 ("**PAJA**") provides that where an administrative action materially affects the rights of the public, the public must be consulted. The principle behind public participation is that all the stakeholders affected by a piece of legislation have a right to be consulted and contribute to such a decision. For this reason, when a bill is published for comment, it is important to take a proactive approach and make submissions.

The Cybercrimes and Cybersecurity Bill ("**the Bill**") plays an important role in regulating the technologically driven space. It seeks, among other things, to criminalise unlawful and intentional conduct relating to accessing, acquiring, using, possessing data and data messages, computer systems and programs, networks and passwords. While it is a positive move towards twenty first century challenges, there is room for improvement. Those in the media, internet, health, education and finance industries have a vested interest as this extensive piece of legislation will materially affect these industries and how they conduct their business activities. The Portfolio Committee has invited interested parties and stakeholders to submit their comments on the proposed Bill by 10 August 2017. We have provided a brief outline of the provisions that impact the aforementioned industries.

Chapter 2 of the proposed Bill makes it an offence to unlawfully and intentionally acquire data. If you consider the nature of democracy and the media's role, this provision will largely impact journalists and whistleblowers because damning information on issues such as corruption are usually brought to light by whistleblowers and published by journalists. In terms of the bill, the act of accessing, storing and using such information is considered a criminal offence, and no such exceptions are provided for. So, take the example of the recent #GuptaLeaks, some of the implicated government officials have referred to the manner in which the leaked emails were obtained as a cybercrime.

Another issue of relevance is the issue of jurisdiction, which is covered in Chapter 4. This is a complex issue as the cyber landscape is vast, and is not confined to national borders. For example, South African websites, with a South African audience may not be hosted in the Republic. Again,

using the #GuptaLeaks as an example, some sites containing information which has infringed the privacy of South African journalists, are hosted in other countries. How do we deal with this?

The Bill, in Chapter 9, further places certain obligations on electronic communications service providers and financial institutions: if such entities become aware that their computer system are involved in the commission of any offence, they must report the offence to the South African Police Service within 72 hours and preserve any offence which may be of assistance. This, however, does not mean that the abovementioned entities will need to actively seek facts or circumstances indicating any unlawful activity. So, for clarity, what measures should be taken regarding the monitoring and reporting process to comply with the provisions of Chapter 9?

Additionally, the Bill affords the South African Police Service considerable powers regarding investigating, searching, accessing and seizing computer data storage mediums and any part of a computer system. From a legal standpoint, there are very real privacy and information security concerns if a police officer may search and seize your computer system without a warrant.

The Bill also establishes a Cyber Response Committee. The Committee is tasked with implementing Government policy relating to cybersecurity and consists of the Heads of the Department of Defence; Department of Home Affairs; Department of International Relations and Cooperation; Department of Justice and Constitutional Development; Department of Science and Technology; Department of Telecommunications and Postal Services; the Financial Intelligence Centre; the National Prosecuting Authority; the National Treasury; the South African Police Service; the South African Reserve Bank; the South African Revenue Service; and the State Security Agency. The Cabinet member responsible for the administration of justice is empowered and obliged to make regulations to regulate information sharing regarding cyber security incidents and the detection, prevention, investigation or mitigation of cybercrime. The wide representation clearly emphasizes that cyber security and cyber security is not to be viewed in isolation, it impacts every industry.

When a new Bill is proposed to be passed as legislation, it needs to be clear and provide certainty; be applied to practical situations; strike a balance between the rights of all affected parties, and have clearly defined sanctions and remedies. Does the Cybercrime and Cybersecurity Bill meet these standards?

Making submissions at this stage provides interested parties with an opportunity to ensure that their concerns are addressed. Don’t miss the opportunity to help craft a better piece of legislation.

By Sasha Beharilal