COMMENTS BY LEGAL AID SA ON THE CYBERCRIMES

AND CYBERSECURITY BILL [B6-2017]

AUGUST 2017

1. INTRODUCTION

The Portfolio Committee on Justice and Correctional Services has called for comments on the Cybercrimes and Cybersecurity Bill [B6-2017]. Legal Aid SA wishes to comment by providing a brief overview of the Bill and by referring to a number of concerns with the Bill.

2. COMMENTS BY LEGAL AID SA

With the advent of new technology, new types of crime have surfaced and traditional crimes such as fraud are now being perpetrated by means of sophisticated *technology (Unpublished: S. Maat, 'Cybercrime: A comparative law analysis", unpublished LLM dissertation, University of South Africa (2009 on page 3).*

The Concept "Cybercrime" and "Cybersecurity" needs no introduction. Cybercrime is rapidly evolving and thriving worldwide. Cyber criminals are using sophisticated techniques to steal data and peoples identities, to defraud mobile phone users and perform and execute corporate espionage, among other criminal activities (*G. Gordon "The hidden economy of cyber-crime Sunday Times 12 February 2012).*

Cyber-attacks are particularly intended to disrupt the proper functioning of the target such as computer systems, servers or underlying infrastructure, especially if the systems are part of critical information infrastructure of a country, among others by means of unlawful access, a computer virus or malware (*F. Cassim 'Addressing the spectre of terrorism: a comparative perspective' (2012) (15) PER 381*).

Over the last decade great strides have been made in South African legislation to address issues regarding cybercrime and cybersecurity. From the common law, to the promulgation of the Regulation of Interception of Communications and Provision of Communications Related information Act (Act 70 of 2002), to the Electronic Communications and Transactions Act (Act 25 of 2002) to the most recent development,

the Cybercrime and Cyber Security Bill ('the Bill), which attempts to address shortcomings which have been identified in the current legislation which deals with cybercrimes. The Cybercrimes and Cybersecurity Bill was introduced as B6-2017 in February 2017 and is currently under consideration by the National Assembly. In terms of the Medium-Term Strategic Framework for Government 2014-2019 the Bill must be enacted and implemented by 2018/2019.

2.1 An overview of the Bill

Currently there is no coherent and organised approach in South Africa to deal with cybercrime and cybersecurity. There is inadequate capacity to deal with cybercrimes and cybersecurity. Information sharing about cyber incidents is limited. Critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The Electronic Communications and Transactions Act, 2002 narrowly caters only for the protection of databases and not for other information structures which need to be protected. No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with such structures.

The Bill aims to rationalise the laws of South Africa which deal with cybercrime and cyber security into a single Bill and to the extent, the Bill among other things:

1. creates new offences (unlawful accessing (hacking) and securing (ransomware) of data; cyberforgery and cyber extortion; aiding and abetting; theft of incorporeals and cyberharassment and bullying) and imposes penalties which have a bearing on cybercrime;
2. criminalises the distribution of malicious communications and provides for interim protection measures;
3. regulates jurisdiction to provide for the transnational dimension of cybercrimes;
4. regulates the powers to investigate cybercrimes;
5. regulates mutual assistance to deal with cross-border investigation of cybercrimes;
6. provides for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime;
7. regulates the proof of certain facts by affidavit;
8. imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes;
9. provides for the establishment structures to promote cybersecurity and capacity building;
10. provides for the identification and declaration of critical information infrastructures and implementation of measures to protect critical information infrastructures;

11. provides that the Executive may enter into agreements with foreign States to promote cybersecurity;
12. provides for the repeal and amendments of certain laws.

With the above said, the Bill creates fifteen new categories of 59 new crimes. These crimes include: offences against the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems (*Section 3-7 of the Bill*); offences committed or facilitated by means of data, computer programs and computer systems (*Section 8-10 of the Bill*); aggravated offences (*Section 11-14 of the Bill)* and malicious communications. The Bill further repeals or amends 13 other laws in the country. A number of structures will also be created by the new Bill, namely a Cybercrime Unit, a Cyber Response Committee; a Computer Security Incident Response Team; a Cybersecurity Hub; a Critical Information Infrastructure and a CyberCrimes Hub.

2.2 Concerns with the Bill

Legal Aid SA raises the following concerns with regards to this Bill.

2.2.1 The Bill threatens digital rights in significant ways, especially the freedom of expression and association and the right to privacy.
2.2.2 The Bill lacks important checks and balances and increases state power over the internet in concerning ways.
2.2.3 The Bill provides for significant state involvement in the monitoring of business and private cyber activity.
2.2.4 It appears that no social impact assessment was done for the Bill.
2.2.5 This legislation will inevitably have a major impact on other legislation such as POPI and PAIA, it also seems that the Bill requires people to act contrary to their rights in terms of other legislation.
2.2.6 The Bill gives the police greater powers of arrest.

The following issues also raises concern for Legal Aid SA and requires intervention by the legislature drafters.

- **Hacking and unlawful securing of data**
  The danger of the current Bill is that if you put data behind a password that should be open access (merely to protect the data and not for any malicious reason), you may be liable to a 10 year sentence, for instance if a journalist leaks information to the press, they may be liable for firstly obtaining information illegally and then for distributing the information. There is no public interest defence under this Bill.

- **Cyber harassment, bullying and revenge pornography**
  It seems that there was an attempt to deal with cyber harassment, bullying and revenge pornography in the Films and Publications Act and so sections are merely copied and pasted from them.

- **Cybersecurity and cyberwarfare**
  Worryingly, it is increasingly possible for people to be spied upon through their own devices.

- **Search warrants**
  To be valid, a search warrant must state the statutory provision in terms of which it is issued, identify the searcher, clearly mention the authority it confers upon the searcher, describe the person, container or premises to be searched, describe the article to be searched for and seized, with sufficient particularity, and specify the offence which triggered the criminal investigation and names of the suspected offender (see Minister of Safety and Security v Van der Merwe 2011 (2) SACR 301 CC par 55-56). Thus, if a search warrant specifies articles to be seized in broad and general terms, then such a warrant lacks particularity (Smith, Tabata and van Heerden v Minister of Law and Order 1989 (3) SA 627 E. It follows that a valid search warrant is one that outlines the ambit of the search it authorises both the searcher and the searched.
  Section 29(2)(e) of the Cybercrimes and Cybersecurity Bill provides the investigator or member of a law-enforcement agency with the right to access and search any data, computer device, computer network, database, critical database, electronic-communications network, or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant.
  Section 29(2)(f) further provides that the investigator or member of the law enforcement agency may obtain and use any instrument, device, equipment, password, decryption key, data or other information that is believed, on reasonable grounds, to be necessary to access or use any part of any data, computer device, computer network database, critical database, electronic-communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant.

  The Cybercrimes and Cybersecurity Bill clearly fails to outline the particularity expected in a search warrant. There is no obligation on the

investigator or peace officer to know the exact location of the evidence within a computer device or computer network. This means that investigators can search through a person's emails, social-networking profiles, messages and computer files in search for evidence. There is no actual limit for the search, which leaves individuals vulnerable and violated.

This amounts to the state exceeding the bounds of a search and infringing a person's right to privacy.

The definition of article under section 26 part (a) and (c) of the Cybercrimes and Cybersecurity Bill requires the investigator to show that there were reasonable grounds that the article was connected with the commission of the offence, or intended to be used in the commission of the offence. The requirement for reasonable grounds is absent in part (b) of section 26. The Cybercrimes and Cybersecurity Bill provides that an article may be searched if it may provide evidence for the commission of a crime. This provision empowers investigators to search any article without the need to prove that there are reasonable grounds that it will provide evidence for the commission of a crime. This provision gives the State unnecessary powers to pry into people's privacy as long as the investigator is of the opinion that the information will provide evidence of the crime.

3. Conclusion

At present, South Africa does not have a co-ordinated approach in dealing with cybercrime and does not have a comprehensive cyber defence strategy in place. The complexities of cyber space and the dynamic nature of technological innovations require a holistic cyber defence framework. The structures that have been established to deal with cyber security issues and the current legal system is inadequate to holistically deal with these issues.

It is recommended that cybercrime laws should encompass more than merely criminalizing unlawful conduct but also need to deal with procedures in the prevention, detection and investigation of crime and collection of evidence for subsequent prosecution.

It is recommended that the Cybercrimes and Cybersecurity Bill must ensure that investigators have reasonable belief that every article searched is linked to, affords evidence and intended to be used in the commission of a crime in order to avoid unnecessary intrusion into an individual's privacy.