Cybercrimes and Cybersecurity Bill

South Africa

Data Governance

Definitions of Data:

''data'' means electronic representations of information in any form

Main Focus of Document:

Creates offences and imposes penalties as it relates to cybercrime

Target Beneficiaries or Sectors:

n/a

Key Elements:

Unlawful securing of access 2. (1) Any person who unlawfully and intentionally secures access to (a) data; (b) a computer program; (c) a computer data storage medium; or (d) a computer system, is guilty of an offence. (2) For the purposes of this section a person secures access to (a) data when the person is in a position to (i) alter, modify or delete the data; (ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium; (iii) obtain its output data; or (iv) otherwise use the data; (b) a computer program when the person is in a position to (i) alter, modify or delete the computer program; (ii) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium; (iii) cause the computer program to perform any function; (iv) obtain its output; or (v) otherwise use the computer program; (c) a computer data storage medium when the person is in a position to (i) access data as contemplated in paragraph (a) or access a computer program as contemplated in paragraph (b), stored on the computer data storage medium; (ii) store data or a computer program on a computer data storage medium;or (iii) otherwise use the computer data storage medium; or (d) a computer system when the person is in a position to (i) use any resources of; (ii) instruct; or (iii) communicate with, a computer system, and the access contemplated in paragraph (a), (b), (c) or (d) which the person secures is unauthorised.

Unlawful acquiring of data 3. (1) Any person who unlawfully and intentionally (a) overcomes any protection measure which is intended to prevent access to data; and (b) acquires data, within or which is transmitted to or from a computer system, is guilty of an offence. (2) Any person who unlawfully and intentionally possesses data, with the knowledge that such data was acquired unlawfully as contemplated in subsection (1), is guilty of an offence. (3) Any person who is found in possession of data, in regard to which there is a reasonable suspicion that such data was acquired unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. (4) For purposes of this section, ''acquire'' means (a) use; (b) examine or capture data or any output thereof; (c) copy data; (d) move data to (i) a different location in a computer system in which it is held; or (ii) any other location; or (e) divert data from its intended destination to any other destination.

Cyber fraud 8. Any person who unlawfully and with the intention to defraud, makes a misrepresentation (a) by means of data or a computer program; or (b) through any interference with data or a computer program as contemplated in subsection 5(2) or interference with a computer data storage medium or a computer system as contemplated in section 6(2), which (i) causes actual prejudice; or (ii) is potentially prejudicial, to another person, is guilty of the offence of cyber fraud.

Obligations of electronic communications service providers and financial institutions 52. (1) An electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Chapter2 and which is determined in terms of subsection (2), must— (a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and (b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

Government structures supporting cybersecurity 54. (1) (a) The Cabinet member responsible for State security must— (i) establish, equip, operate and maintain a computer security incident response team for Government; (ii) establish and maintain sufficient human and operational capacity to— (aa) give effect to cybersecurity measures falling within the Constitutional mandate of the State SecurityAgency; and (bb) effectively deal with critical information infrastructure protection; and (iii) in cooperation with any institution of higher learning, in the Republic or elsewhere,develop and implement accredited training programs for members of the State Security Agency in order to give effect to subparagraphs (i) and (ii). (b) The Cabinet member responsible for State security may make regulations to further regulate any aspect referred to in paragraph (a).

Protection of critical information infrastructure 57. (1) The State Security Agency— (a) in consultation with the Cyber Response Committee; and (b) after consultation with the owner or the person in control of any information infrastructure which is identified as a potential critical information infrastructure, must within 12 months of the fixed date, submit to the Cabinet member responsible for State security, information and recommendations regarding information infrastructures which need to be declared as critical information infrastructures. (2)The Cabinet member

responsible for State security may, subject to subsection(3), after considering any information and recommendations made to him or her in terms of subsection (1), by notice in the Gazette, declare any information infrastructure, or category or class of information infrastructure or any part thereof, as critical information infrastructure if such information infrastructure or information infrastructures are of such a strategic nature that any interference with them or their loss,damage, disruption or immobilisation may— (a) substantially prejudice the security, defence, law enforcement or international relations of the Republic; (b) substantially prejudice the health or safety of the public; (c) cause a major interference with or disruption of an essential service; (d) cause any major economic loss; (e) cause destabilisation of the economy of the Republic; or (f) create a major public emergency situation.

Data Data storage Digital infrastructure Electronic communication

Policy/regulation mirrored:

Countries: