7 JULY 2020

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS **ALERT**

IN THIS ISSUE >

The Cybercrimes Bill is one step away from becoming law

On 1 July 2020, the National Council of Provinces (NCOP) passed the Cybercrimes Bill, which now awaits President Cyril Ramaphosa's assent.

FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

CLICK HERE

CDH
CLIFFE DEKKER HOFMEYR

The Cybercrimes Bill is one step away from becoming law

The Cybercrimes Bill arrives on the President's desk after a significant Parliamentary process involving numerous deliberations, proposed amendments and an extensive public participation process.

On 1 July 2020, the National Council of Provinces (NCOP) passed the Cybercrimes Bill, which now awaits President Cyril Ramaphosa's assent.

The Cybercrimes Bill arrives on the President's desk after a significant Parliamentary process involving numerous deliberations, proposed amendments and an extensive public participation process. In terms of section 79(1) of the Constitution, the President is required to assent to the Bill (i.e. sign the Bill into law) or refer it back to the National Assembly for reconsideration if he has reservations about its constitutionality. If the President assents to the Bill, the Bill will become a law of the Republic of South Africa.

The controversial 'Cybercrimes and Cybersecurity Bill'

The Cybercrimes Bill is the product of an interesting legislative process where the 'Cybercrimes and Cybersecurity Bill (B6–2017)' (the Old Bill) was subjected to a great deal of scrutiny. The Old Bill was broadly divided into two parts, namely a "*cybercrimes*" section and a "*cybersecurity*" section. The criticism against the Old Bill was primarily aimed at the cybersecurity section, which raised various concerns about the government's extensive powers, including the concern that it violated the right to freedom of expression entrenched in section 16 of the Constitution. This resulted in the clauses in the Old Bill pertaining to cybersecurity being completely removed and its name being changed to the 'Cybercrimes Bill' – which now only deals with cybercrimes.

Cybercrimes under the Cybercrimes Bill

The Cybercrimes Bill criminalises, *inter alia*, the following types of cybercrimes:

- unlawful access – which includes the unlawful and intentional access to data, a computer program, a computer data storage medium or a computer system (commonly referred to as "*hacking*");
- unlawful interception of data – which includes the acquisition, viewing, capturing or copying of data of a non-public nature through the use of hardware or software tools;
- unlawful acts in respect of software and hardware tools – being the unlawful and intentional use or possession of software and hardware tools that are used in the commission of cybercrimes (such as hacking and unlawful interception);
- unlawful interference with data, computer programs, storage mediums and computer systems – being the unlawful and intentional interference with data, a computer program, a computer data storage medium or computer system;
- cyber fraud – being fraud committed by means of data or a computer program or through any interference with data, a computer program, a computer data storage medium or a computer system;
- cyber forgery – being the creation of false data or a false computer program with the intention to defraud;

The Cybercrimes Bill is one step away from becoming law...*continued*

Businesses who may fall victim to a cybercrime or who, for example, have an employee who commits a cybercrime, are required to offer cooperation and assist law enforcement officials in any investigations they may conduct.

- cyber uttering – being the passing-off of false data or a false computer program with the intention to defraud; and
- malicious communications – being the distribution of data messages with the intention to incite the causing of damage to any property belonging to, or to incite violence against, or to threaten a person or group of persons, including the distribution of *"revenge porn"*.

Penalties

The Cybercrimes Bill prescribes the sentences that offenders will be liable to on conviction of the cybercrimes created by the Bill, which entail fines and/or imprisonment ranging from five to 10 years, with aggravated offences attracting imprisonment of up to 15 years. In the case of the offences of cyber fraud, cyber forgery and uttering, the Bill provides for broad penalties that could be imposed for anyone found guilty of any of these cybercrimes where a court will have a discretion to impose a penalty that it deems appropriate under section 276 of the Criminal Procedure Act 51 of 1977. Such penalties may include a fine (unspecified), imprisonment, a declaration as a habitual criminal and correctional supervision.

Obligations under the Cybercrimes Bill for businesses in South Africa

The Cybercrimes Bill does not simply prescribe offences and penalties to regulate criminal conduct. The Bill also imposes obligations on businesses in general and on electronic communications service providers (ECSPs) and financial institutions in relation to the commission of cybercrimes. ECSPs and financial institutions will have obligations in relation to (i) the reporting of cybercrimes and (ii) the preservation of evidence in relation to the commission of cybercrimes. Any ECSPs or financial institutions that fail to comply with such obligations could be found guilty of an offence and be liable on conviction to a fine not exceeding R50,000.

Businesses who may fall victim to a cybercrime or who, for example, have an employee who commits a cybercrime, are required to offer cooperation and assist law enforcement officials in any investigations they may conduct. Such businesses may be required to comply with search warrants and/or may be called to comply with directions issued by the court to furnish particulars to the court relating to the computer systems involved in a cybercrime and/or may be requested to comply with court directions to preserve data or evidence relevant in a cybercrime investigation.

Preeta Bhagattjee, Aphindile Govuza and Liam Sebanz

OUR TEAM

For more information about our Technology, Media & Telecommunications practice and services, please contact:

Christoff Pienaar
National Practice Head
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Fatima Ameer-Mia
Director
T +27 (0)11 562 1837
E fatima.ameermia@cdhlegal.com

Preeta Bhagattjee
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

Simone Dickson
Director
T +27 (0)11 562 1249
E simone.dickson@cdhlegal.com

Aphindile Govuza
Senior Associate
T +27 (0)11 562 1090
E aphindile.govuza@cdhlegal.com

Nikita Kekana
Associate
T +27 (0)21 481 6334
E nikita.kekana@cdhlegal.com

Liam Sebanz
Associate
T +27 (0)11 562 1625
E liam.sebanz@cdhlegal.com

BBBEE STATUS: LEVEL TWO CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com