South Africa: New Cyber Crimes Legislation

By Michael-James Currie and Camilla Warring

1 October 2020

The new Cybercrimes Bill (B 6B – 2017) has been the subject of much debate. It has been passed by the National Council of Provinces and now awaits assent by President Ramaphosa. If it passes into law it will create a number of new crimes, including the crime of "cyber fraud".

Data is defined as electronic representations of information in any form. Unlawful accessing of data is a crime under the Electronic Communications and Transactions Act 25 of 2002, the Bill broadens the scope of the crime. "Unlawful access" occurs when any person who unlawfully and intentionally accesses data, a computer program, a computer data storage system or a computer system is guilty of an offence.

A new crime contained in the Bill is "cyber fraud", whereby any person who unlawfully and with the intention to defraud makes a misrepresentation by means of data or a computer program or by way of interference with data or a computer program which causes actual or potential prejudice, commits the offence of cyber fraud. This definition contains the elements of the common law offence of fraud with which we are familiar, that is; the unlawful and intentional misrepresentation which causes actual or potential prejudice. However, it adds the element of "defrauding" and the mode of misrepresentation, being by means of data or a computer program or interference with data or a computer program. "Defrauding" is not defined in the Bill. Accordingly, this element of the definition is somewhat circular. If this creates any interpretive difficulty, prosecutors may opt to continue charging offenders under the common law crime of fraud.

John Oxenham

Director
South Africa

j.oxenham@primerio.international

Cell +27 (0)83 233 0484

Michael-James Currie

Director
South Africa

m.currie@primerio.international

Cell +27 (0)84 506 7610

Contact details

Johannesburg, South Africa
John Oxenham, Michael-James Currie
j.oxenham@primerio.international
m.currie@primerio.international
135 Daisy Street Sandton, Johannesburg, 2031

Nairobi, Kenya
Ruth Mosoti, Fidel Mwaki
r.mosoti@primerio.international
f.mwaki@primerio.international
Kalson Towers, 2nd Floor, The Crescent,
Off Parklands Road, Nairobi

Port Louis, Mauritius
Gilbert Noël
g.noel@primerio.international
Suite 401, St James Court, St Denis Street, Port Louis

Email: info@primerio.international
Tel: +27 (0) 11 083 2411

The common law crime of fraud presents its own difficulties, which are also present in the definition of cyber fraud. Namely, the element of causing “actual or potential prejudice” can make drawing the line between a completed “commission” of the crime and an “attempt” difficult. As in the common law, in terms of the Bill attempted fraud is a punishable offence. If one can be convicted for the completed crime of fraud without causing prejudice, as the definition makes room for “potential prejudice”, then presumably the distinction between an attempt to commit a crime and a completed crime is academic. In terms of the Bill the penalties for committing attempted cyber fraud are the same as if the crime was completed.

The common law crime of fraud presents its own difficulties, which are also present in the definition of cyber fraud. Namely, the element of causing “actual or potential prejudice” can make drawing the line between a completed “commission” of the crime and an “attempt” difficult. As in the common law, in terms of the Bill attempted fraud is a punishable offence. If one can be convicted for the completed crime of fraud without causing prejudice, as the definition makes room for “potential prejudice”, then presumably the distinction between an attempt to commit a crime and a completed crime is academic. In terms of the Bill the penalties for committing attempted cyber fraud are the same as if the crime was completed.

The Bill goes on to state that this obligation should not be construed as creating an obligation on financial institutions and electronic communications providers to monitor data or actively seek out information relating to unlawful activities. Nonetheless, in their clients’ interests it is best to be vigilant and ensure that systems are secure. More generally, firms should be mindful of how they interact with their clients’ data.

Coupled with the recently effective Protection of Personal Information Act, companies will be required to ensure that their internal collection, processing and monitoring obligations are adequate to ensure compliance with personal data laws as well as ensure that potential offences in terms of the Cyber Bill are quickly identified and reported.

[Michael-James Currie is a director at Primerio and specialises in anti-bribery and corruption laws and antitrust across Africa and can be contacted at m.currie@primerio.international]

About Primerio

Our team operates on a global scale, ensuring full compliance with African, European, and U.S./North-American Laws. Our business advisory practice has over 60 years of combined legal and commercial expertise. It includes regulatory compliance, litigation and arbitration, M&A, cartel counselling, antitrust / competition law, anti-money-laundering, anti-corruption / FCPA and fraud investigations.

Visit our website

Subscribe to our newsletter