The Regulation and Use of Artificial Intelligence and 5G Technology to Combat Cybercrime and Financial Crime in South African Banks

H Chitimira* and P Ncube**

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed, open access online law publications

Authors

Howard Chitimira
Princess Ncube

Affiliation

North-West University, South Africa
University of Pretoria, South Africa

Email

Howard.Chitimira@nwu.ac.za
princess.ncube@up.ac.za

Date Submission

28 October 2020

Date Revised

26 May 2021

Date Accepted

24 May 2021

Date published

30 June 2021

Editor Dr TV Warikandwa

How to cite this article

Chitimira H and Ncube P "The Regulation and Use of Artificial Intelligence and 5G Technology to Combat Cybercrime and Financial Crime in South African Banks" *PER / PELJ* 2021(24) - DOI http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10742

DOI
http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10742

Abstract

Artificial intelligence (AI) and fifth generation network technology (5G) are now being utilised by some companies and financial institutions such as banks to enhance their competitiveness and expand their businesses. The general types of AI include functional AI, interactive AI, text AI, visual AI and analytic AI. The key components of AI include machine learning, fast Internet connectivity, deep learning, neural networks and advanced data analysis. These components may be complemented by the adoption and use of standard 5G cellular networks. 5G utilises broadband Internet access and Internet connection, and is now employed by some banking institutions, especially in developed countries. It is not clear whether South African banking institutions have adopted 5G for their Internet connectivity and operations. AI and 5G may be used to detect and combat cybercrimes in banking institutions. On the other hand, AI and 5G may also be abused by cybercriminals to commit financial crimes such as money laundering and insider trading. In this regard it is submitted that South African policy makers should carefully revise the Cybercrimes Bill B6-2017 (Cybercrimes Bill) to embrace the use of AI and 5G to detect and combat cybercrimes in South African banks. Accordingly, this article examines the adequacy of the Cybercrimes Bill. It also explores the regulation and use of 5G and AI to detect, prevent and combat cybercrimes in banks and other financial institutions in South Africa.

Keywords

Cybercrimes; cyber security; financial markets; artificial intelligence; financial institutions.

.....

1 Introductory remarks

Cybercrime is carried out by means of computers and/or via the Internet. Cybercrime involves criminal activities that are carried out through the Internet, a computer system and/or computer technology. There are various types of cybercrimes, such as phishing, which is the use of fake email messages to get personal information from Internet users, the misuse of personal information (identity theft), hacking or the misuse of websites and computer networks, spreading hate, inciting terrorism, distributing child pornography and grooming. Owing to technological developments, cybercrimes are increasingly being perpetrated through the Internet and artificial intelligence (AI) against companies, banks and other financial institutions in many countries including South Africa.[1]

AI may empower devices or machines to learn and act in response to certain patterns and/or transactions in banks and other financial institutions in order to detect and combat cybercrimes and financial crimes.[2] AI and fifth generation network technology (5G) are now utilised by some companies and financial institutions such as banks to enhance their competitiveness and to expand their businesses.[3] The general types of AI include functional AI, interactive AI, text AI, visual AI and analytic AI. Examples of AI includes automation, machine learning (deep learning, supervised and unsupervised learning, reinforcement learning), machine vision, natural language processing, robotics and self-driving cars.[4] AI could be used to plan, search and interpret knowledge, solve problems and move objects. The key components of AI include machine learning, fast Internet connectivity, deep learning, neural networks and advanced data analysis.[5] These components may be complemented by the adoption and use of 5G for standard cellular

* Howard Chitimira. LLB (*cum laude*) LLM (UFH) LLD (NMMU). Research Professor and Professor of Securities and Financial Markets Law, Faculty of Law, North-West University, South Africa. E-mail: Howard.Chitimira@nwu.ac.za. Orcid: https://orcid.org/0000-0003-1881-1242.

** Princess Ncube. LLB LLM LLD candidate (North-West University). Lecturer, Faculty of Law, University of Pretoria, South Africa. E-mail: princess.ncube@up.ac.za. Orcid: https://orcid.org/0000-0001-5582-9017.This article was initially presented at the 2nd Annual Colloquium on Corporate and Financial Markets Law at North-West University, Faculty of Law, on 29-30 October 2020. In this regard, the author wishes to acknowledge the expert input of Prof H Chitimira.

1 Mbelli and Dwolatzky "Cyber Security" 1-6.

2 Goldfarb and Prince 2008 *Information Economics and Policy* 2-15.

3 Cassim 2010 *JICLT* 118-123.

4 Goldfarb and Prince 2008 *Information Economics and Policy* 2-15; Chitimira 2020 *Acta Universitatis Danubius Juridica* 28-43.

5 Smith *et al* 2006 https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf 1-27.

networks. 5G utilises broadband Internet access and Internet connection and is now employed by some banking institutions, especially in developed countries.[6] It is not clear whether South African banking institutions have adopted 5G for their Internet connectivity and business operations since its inception in 2019.[7] AI and 5G may be used to detect and combat cybercrimes in banking institutions. On the other hand, AI and 5G may also be abused by criminals to commit cybercrime and other financial crimes such as fraud, money laundering and insider trading.[8] In this regard, it is submitted that the South African policy makers should carefully revise the Cybercrimes Bill B6-2017 (Cybercrimes Bill) to embrace the use of AI and 5G to detect and combat cybercrimes in South African banks and other financial institutions. Accordingly, this article examines the adequacy of the Cybercrimes Bill in relation to the effective combating of cybercrimes in South Africa. The article also explores the regulation and use of 5G and AI to detect, prevent and combat cybercrimes in banks and other financial institutions in South Africa.[9]

The article also discusses the statutory and common law regulation of cybercrime in South Africa. Prior to the enactment of the *Electronic Communications and Transactions Act* (ECTA),[10] cybercrimes such as indecency (child pornography) and cyber fraud[11] were only prohibited under common law in South Africa. In addition, malicious communications, hacking, the unlawful interception of data, cyber forgery, cyber smearing and cyber uttering were not statutorily prohibited under the ECTA prior to 2002.[12] It is noteworthy that the United States of America's Federal Bureau of Investigation (FBI) regards South Africa as the sixth most active cybercrime country in the world.[13] While the increased reliance on the Internet offers many benefits to both human beings and banking institutions, it also provides new opportunities for unscrupulous persons to exploit both the common law and statutory regulatory gaps and commit cybercrimes. For instance, a criminal syndicate reportedly created and employed a malware known as "Dexter" to attack a number of South African retailers, and stole

6 Smith *et al* 2006 https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf 1-27.
7 Cassim 2010 *JICLT* 118-123; Cassim 2011 *CILSA* 123-138.
8 Cassim 2012 *PELJ* 381-415; Cassim 2010 *JICLT* 118-123.
9 Cassim 2009 *PELJ* 36-79.
10 *Electronic Communications and Transactions Act* 25 of 2002 (ECTA) ss 85-89.
11 Cassim 2010 *JICLT* 118; Cassim 2012 *PELJ* 381-415.
12 Cassim 2009 *PELJ* 36-79; Thomas *et al Cybercrime and Digital Forensics* 20-284.
13 Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime.

millions of rands.[14] This malware intercepted the payment details of ignorant customers from the point-of-sale terminals of retailers, created fraudulent duplicate bank cards, and stole money from the retailers and from their customers.[15] The Wolfpack Information Risk (Pty) Limited held in 2014 that about R2.65 billion is annually lost to cybercrime in South Africa.[16] Perhaps this could be related to the lack of statutory AI measures to curb cybercrimes in South African banking and related financial institutions,[17] or it could be that the policy makers adopted a flawed and fragmented approach by enacting different pieces of legislation to curb cybercrimes in South Africa. Such legislation includes the ECTA,[18] the *Regulation of Interception of Communications and Provision of Communication-Related Information Act* (RICA),[19] and the *Protection of Personal Information Act* (POPIA).[20] Furthermore, the National Cybersecurity Policy Framework was introduced in 2015 in a bid to curb cybercrimes in South African banks and other financial institutions, *inter alia.* Given this background, it is important to explore the adequacy of the statutory and other regulatory measures that are employed in South Africa to detect, prevent and combat cybercrimes in the South African banking and related financial institutions. This follows the fact that the Fourth Industrial Revolution (4IR) and the introduction of new technology such as AI and 5G have made it easier to commit new financial crimes and cybercrimes such as the online theft of financial data, the online theft of card payment data, cyber theft, the sale of corporate data, and cyber extortion in the financial institutions and financial markets in South Africa and other countries globally.[21] The authors of this article argue that AI and 5G measures could be an effective tool for the detection and prevention of cybercrimes and financial crimes in the South African banks and related

14 Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime; see further Dawson and Omar *New Threats and Countermeasures* 10-298.

15 Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime; see further Dawson and Omar *New Threats and Countermeasures* 10-298.

16 Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime.

17 Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime; see further Dawson and Omar *New Threats and Countermeasures* 10-298.

18 See ss 85-89 of the ECTA.

19 *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002 (RICA) ss 2-57; see the related discussion by Ziska *Handbook of Research on Information* 27-566, Brenner *Threats from Cyberspace* 36-200.

20 *Protection of Personal Information Act* 4 of 2013 (POPIA) ss 8-109; see the related discussion by Ziska *Handbook of Research on Information* 388-566.

21 Kovacich and Jones *Crime Investigator's Handbook* 100-400; Cassim 2009 *PELJ* 36-79.

financial institutions. Therefore, the Cybercrimes Bill and the ECTA should be amended to introduce provisions that specifically oblige banks and related financial institutions to adopt 5G and AI measures to curb cybercrimes and financial crimes in South Africa.[22] AI measures such as machine learning, big data analytics, neural networks and pattern recognition could play an important role in the detection and prevention of such crime.

South African policy makers should seriously consider enacting a comprehensive and specific anti-cybercrime statute to effectively protect financial consumers, banks and other financial institutions from cybercrime and financial crime. The current use of sensors and elementary detectors in banks and related financial institutions is not robust enough to monitor and prevent cybercrimes in South African banks and related financial institutions. The statutory introduction of 5G and AI measures such as machine learning and big data analytics could enhance the detection, investigation and prevention and of such crimes.[23] Furthermore, the role and functions of the Independent Communications Authority of South Africa (ICASA), the South African Police Services (SAPS), the 24/7 Point of Contact and other relevant enforcement authorities are discussed. This is done to recommend measures that could possibly be employed by the relevant enforcement bodies to enhance the combating of such crimes.

2 Historical background and definitional aspects

2.1 Brief historical background

The *Convention on Cybercrime of the Council of Europe*[24] was adopted on 23 November 2001 and it entered into force on 01 July 2004. The *Budapest Convention* is currently the only binding international instrument on the regulation and combating of cybercrime. It provides some guidelines on the basis of which member states may develop their own national legislation on cybercrime. It provides a general anti-cybercrime framework for international cooperation between member states. The *Budapest Convention* is the first international treaty that was adopted to deal with Internet and computer-related crime by drafting and recommending the

22 Galal and O'Halloran 2020 http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf 6-20; Abawajy *et al Internet and Distributed Computing Advancements* 100-300.

23 Paula *et al* "Deep Learning Anomaly Detection" 954-960; Abawajy *et al Internet and Distributed Computing Advancements* 100-300.

24 *Council of Europe Convention on Cybercrime* ETS No 185 (2001) (*Budapest Convention*).

enactment of adequate national laws, by improving investigative techniques and increasing co-operation among member states. This was done to develop and encourage all member states to adopt a common criminal policy against cybercrime – a policy that could be applicable globally. Forty-six member states have ratified the *Budapest Convention*, while eight other member states, including South Africa, signed it on 23 November 2001. Although South Africa adopted the *Budapest Convention* it has not yet ratified the treaty.[25] This means that South Africa is not bound by or obliged to comply with its provisions.

The *Budapest Convention* outlaws a number of practices such as illegal access, illegal interception, data interference, system interference, the misuse of devices, computer-related forgery, computer-related fraud, copyright and related rights offences, child pornography and any attempt to aid or abet another person to commit cybercrimes.[26] Cybercrime is outlawed under common law in South Africa. Moreover, in a bid to comply with the *Budapest Convention*, the ECTA was enacted in South Africa and came into force in 2002.[27] Online offences such as child pornography, cyber fraud and *crimen injuria* (cyber-smearing) are prohibited under both common law and statutory law in South Africa.[28] Nevertheless, the South African common law prohibition on cybercrimes such as extortion, spamming and phishing is still inadequate and flawed. Therefore, although South Africa has taken commendable steps to regulate and combat various forms of cybercrimes, its common law regulatory efforts have not been effective and robust enough to combat cybercrime in banks and other related financial institutions. This culminated in the enactment of the ECTA, as indicated above, but the provisions of the ECTA are also flawed. For instance, only unauthorised access to or the interception of or interference with data and computer-related extortion, fraud and forgery activities are prohibited under the ECTA.[29] Moreover, the criminal sanctions that are provided under section 89 of the ECTA are too minimal and not sufficiently deterrent.[30] No specific amount of fine is provided and the imprisonment terms for most cybercrimes under the ECTA do not exceed five years.[31]

---

25 Council of Europe 2021 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=L3MN1W5t?.

26 Articles 2-12 of the *Budapest Convention*.

27 Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123.

28 Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123; *S v Mashiyi* 2002 2 SACR 387 (Tk); *Narlis v South African Bank of Athens* 1976 2 SA 573 (A).

29 Sections 86-87 of the ECTA.

30 Section 89 read with ss 86-88 of the ECTA.

31 Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123.

Furthermore, although the RICA deals with unlawful communication and interception-related offences, it does not expressly prohibit cybercrime and financial crime in South African banks and related financial institutions.[32] The RICA is also mainly focussed on criminal sanctions, while other measures such as civil sanctions and administrative sanctions are not provided.[33] The maximum criminal penalties of a fine between R2 million and R5 million or imprisonment for a period between two years and ten years are not sufficiently deterrent.[34]

Consequent on the flaws noted above, cybercrime is reportedly rife and increasing rapidly in South Africa.[35] South African banks, financial institutions and other companies are largely affected by cybercrime activities such as phishing schemes, the online theft of Internet users' identities and online fraud.[36] This position is further exacerbated by jurisdictional challenges, lack of adequate resources and the poor prosecution of cyber criminals in South Africa. Owing to these gaps and flaws, the Cybercrimes Bill was recently introduced in South Africa. It prohibits any unlawful and intentional securing of access to data, a computer programme, a computer data storage medium or a computer system by any person.[37] This indicates that hacking and other related illegal computer practices are prohibited under the Cybercrimes Bill.

Any unlawful acquiring and interception of data, including the acquisition, use, viewing, examining, moving, diverting, capturing or copying of data of a non-public nature through the use of hardware or software tools to overcome any protection measure which is intended to prevent access to such data is outlawed under the Cybercrimes Bill.[38] Moreover, all unlawful acts in respect of software and hardware tools including unlawful and intentional use, manufacturing, assembling, obtaining, selling, purchasing, making, advertising or possession of software and hardware tools that are used in the commission of cybercrimes such as hacking and unlawful interception are prohibited under the Cybercrimes Bill.[39]

32 Sections 2-57 of the RICA.
33 Sections 47-57 of the RICA.
34 Section 51 of the RICA.
35 Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123.
36 Cassim 2010 *JICLT* 118-123.
37 Section 2 of the Cybercrimes Bill B6-2017 (the Cybercrimes Bill).
38 Section 3 of the Cybercrimes Bill.
39 Section 4 of the Cybercrimes Bill.

Unlawful interference with data or computer programmes is prohibited under the Cybercrimes Bill.[40] Therefore, any unlawful and intentional interference with computer programmes and/or computer data systems is outlawed in the Cybercrimes Bill.[41] Likewise, any unlawful and intentional interference with computer storage mediums, computer systems and/or computer data storage mediums is outlawed in the Cybercrimes Bill.[42] Any unlawful and intentional acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices is prohibited under Cybercrimes Bill.[43] Furthermore, cyber fraud by means of any unlawful and intentional misrepresentation of computer data or a computer programme or any interference with data or a computer data storage medium and/or a computer system is outlawed in the Cybercrimes Bill.[44] Cyber forgery through the creation of false data or a false computer programme with the intention to defraud other persons is outlawed in the Cybercrimes Bill.[45] Similarly, cyber uttering and/or the passing-off of false data or a false computer programme with the intention to defraud other persons is prohibited in the Cybercrimes Bill.[46] Cyber extortion and other aggravated offences are prohibited in the Cybercrimes Bill.[47]

Any person that commits any of the offences stated above will be liable to unspecified monetary fines and/or imprisonment terms ranging between five and ten years under the Cybercrimes Bill.[48] In this regard, aggravated offences will give rise to unspecified monetary offences and/or imprisonment terms for up to 15 years under the Cybercrimes Bill.[49] The provision of unspecified monetary fines for cybercrimes could suggest that the courts have discretion to impose monetary fines which they deem appropriate in terms of section 276 of the *Criminal Procedure Act* 51 of 1977. This approach is too broad and less dissuasive for the purposes of deterrence. Additionally, civil sanctions and administrative sanctions are not provided under the Cybercrimes Bill.[50] Over and above, the prohibition of cybercrime in the Cybercrimes Bill does not specifically apply to juristic persons such as companies, banks and other related financial institutions.

40 Section 5 of the Cybercrimes Bill.
41 Section 5 of the Cybercrimes Bill.
42 Section 6 of the Cybercrimes Bill.
43 Section 7 of the Cybercrimes Bill.
44 Section 8 of the Cybercrimes Bill.
45 Section 9(1) of the Cybercrimes Bill.
46 Section 9(2) of the Cybercrimes Bill.
47 Sections 10 and 11 of the Cybercrimes Bill.
48 Section 14 of the Cybercrimes Bill.
49 Section 14(3) of the Cybercrimes Bill.
50 Section 14 of the Cybercrimes Bill.

2.2 Definitional aspects

Cybercrime refers to any unlawful activity or practice that is facilitated or committed through a computer, network, or hardware device, where a computer or device may be an agent of the crime, a facilitator of the crime and/or the target of the crime.[51] The terms "cybercrime" and "financial crime" are not expressly defined in the POPIA, the RICA, the ECTA and the Cybercrimes Bill. Notably, for the purposes of this article, financial crimes include fraud (point of sale fraud, bank fraud, insurance fraud, cheque fraud, credit card fraud, mortgage fraud, medical fraud, corporate fraud), insider trading, market manipulation, corporate scams, tax evasion, bribery, embezzlement, money laundering, forgery and counterfeiting.

AI refers *inter alia* to the computer simulation of human intelligence processes so as to learn certain information, reasoning and related rules, and/or apply such rules to reach approximate or definite conclusions, and to self-correction in relation to certain aspects and/or different situations in life.[52] AI further refers to the creation of intelligent devices or machines that function like human beings in respect of all and/or most aspects of life.[53]

Analytic AI is an advanced deep learning technique that relies on machine learning. Analytic AI is employed to scan data to check dependencies and patterns which are used to produce recommendations or to provide business insights and/or assist in data-driven decision-making.[54] Examples of analytic AI include sentiment analysis and supplier risk assessment.

Functional AI is also employed by the enforcement authorities and/or regulatory bodies to scan data and search for patterns and relevant dependencies in order for such authorities and/or bodies to take appropriate actions.[55] For instance, functional AI may identify a machine-breakdown pattern in the sensor data received from a certain machine and trigger a

---

51 Gordon and Ford 2006 *Journal in Computer Virology* 13-20; Brenner 2006 *Crime Law Soc Change* 192-193; Brenner *Threats from Cyberspace* 9-200; Brenner "Cybercrime" 12-29.

52 Kelemen, Romportl and Zackova Beyond *Artificial Intelligence* 3-41; Brynjolfsson and Mcafee 2017 *HBR* 3-11; Chitimira 2020 *Acta Universitatis Danubius Juridica* 28-43.

53 Goldfarb and Prince 2008 *Information Economics and Policy* 2-15; Dilek, Çakır and Aydın 2015 *IJAIA* 21-34.

54 Ezrachi and Stucke 2017 *U Ill L Rev* 1775-1809.

55 Kelemen, Romportl and Zackova Beyond *Artificial Intelligence* 3-41; Brynjolfsson and Mcafee 2017 *HBR* 3-11.

command to turn that machine off. Examples of functional AI include robotics, machine learning and supplier risk assessment.

Interactive AI is a sub-type of AI that enables companies and financial institutions to send automated and interactive communications to their consumers. Examples of interactive AI include chatbots and smart personal assistants that may answer pre-built questions and understand the context of some conversations.[56]

Text AI is computer-related technology that includes text recognition, speech-to-text conversion, machine translation and content generation capabilities.[57] For instance, text AI may be utilised in corporate research and to deliver company-related information to both internal and external consumers.

Visual AI includes computer vision and related computer systems that can identify, recognise, classify and sort objects, and convert images and videos into insights.[58] Visual AI helps companies to grade certain functions and project the profitability of their businesses on the basis of the relevant past and/or current trends in respect thereof.

In terms of the Cybercrimes Bill, the term "access" refers to the use of data, a computer programme, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an article.[59] No similar definition is found in the POPIA, the RICA and the ECTA.

The Cybercrimes Bill provides that the term "computer data storage medium" refers to any device or location from which data or a computer programme is capable of being reproduced or on which data or a computer programme is capable of being stored by a computer system, irrespective of whether the device is physically attached to or connected with the computer system.[60] Moreover, "computer programme" means data representing instructions or statements that, when executed in a computer

---

56 Kelemen, Romportl and Zackova Beyond *Artificial Intelligence* 3-41; Brynjolfsson and Mcafee 2017 *HBR* 3-11; Chitimira 2020 *Acta Universitatis Danubius Juridica* 28-43.

57 Kelemen, Romportl and Zackova Beyond *Artificial Intelligence* 3-41; Chitimira 2020 *Acta Universitatis Danubius Juridica* 28-43.

58 Kelemen, Romportl and Zackova Beyond *Artificial Intelligence* 3-41; Brynjolfsson and Mcafee 2017 *HBR* 3-11.

59 Section 1 of the Cybercrimes Bill.

60 Section 1 of the Cybercrimes Bill.

system, cause the computer system to perform a function.[61] The term "computer system" refers to one computer or two or more inter-connected or related computers, which allow these inter-connected or related computers to exchange data or any other function with one another, or to exchange data or any other function with another computer or a computer system.[62] No similar definitions are found in the POPIA, the RICA and the ECTA. The term "data" means the electronic representations of information in any form, while the term "data message" refers to data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form under the Cybercrimes Bill.[63] Furthermore, the term "public available data" refers to data which is accessible in the public domain without restriction under the Cybercrimes Bill.[64]

In terms of the ECTA, "automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties is not reviewed by a natural person in the ordinary course of such a natural person's business or employment.[65] The term "consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier, under the ECTA.[66] No similar definitions are found in the POPIA, the RICA and the Cybercrimes Bill.

The ECTA provides that "data" means electronic representations of information in any form while "data controller" refers to any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.[67] The ECTA defines "data message" as data generated, sent, received or stored by electronic means and includes a voice that is used in an automated transaction and/or stored records.[68] The term "data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of the ECTA.[69]

61 Section 1 of the Cybercrimes Bill.
62 Section 1 of the Cybercrimes Bill.
63 Section 1 of the Cybercrimes Bill.
64 Section 1 of the Cybercrimes Bill.
65 Section 1 of the ECTA.
66 Section 1 of the ECTA.
67 Section 1 of the ECTA.
68 Section 1 of the ECTA.
69 Section 1 of the ECTA.

The ECTA defines the term "electronic communication" as a communication by means of data messages while the term "transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services.[70] The term "universal access" entails access by all South African citizens to Internet connectivity and electronic transactions under the ECTA.[71]

Cybersecurity refers to measures that are employed by the banks and other enforcement authorities to safeguard and prevent incidents of cybercrimes in South Africa.[72] Cybersecurity also refers to technologies, processes and practices that are designed to protect networks, devices, programmes and data from attack, damage, or unauthorised access from any persons.[73] Consequently, cybersecurity measures are generally employed by companies and financial institutions to defend computers, servers, mobile devices, electronic systems, networks and data from malicious activities and related digital, technological and/or electronic attacks.[74] However, cybersecurity is not defined in the POPIA, the Cybercrimes Bill, the RICA or the ECTA.

Cybersecurity is a growing concern for banks and other companies in South Africa because it harms the integrity of and public confidence in the financial markets.[75] Cybercrime includes computer crime which violates the relevant criminal laws in relation to the knowledge of and/or the illicit use of computer technology by the offenders.[76] Computer crime includes criminal acts that are perpetrated through computers, electronic communication networks, information systems and/or through the publication of illegal content over electronic media.[77] Cybercrimes usually take place on computer-related platforms and they rely primarily on computer-related technologies for their

70 Section 1 of the ECTA; also see Orji 2019 *Tilburg L Rev* 105-124; Orji *Cybersecurity Law and Regulation* 95-591.

71 Section 1 of the ECTA; also see Madhusanka *et al Comprehensive Guide* 102-400; Siegel and Mirakovits *Forensic Science* 169-500; Osterburg, Ward and Miller *Criminal Investigation* 162-500.

72 Cassim 2010 *JICLT* 118-123; Savona *Crime and Technology* 18-149; Moore *Cybercrime* 3-260.

73 Easy *Steps to Managing Cybersecurity* 24-100; Joshi *Digital Finance* 131-200.

74 Johnson *Forensic Computer Crime Investigation* 100-290.

75 Buys *Cyberlaw* 111-423; Liang and Lu 2010 *J Contemp Crim Justice* 103-120.

76 Franklin *Investigator's Guide* 50-302.

77 Franklin *Investigator's Guide* 50-302.

successful execution.[78] Examples of computer-related cybercrimes include cyberwarfare, cyber espionage, industrial espionage and cyber fraud.[79]

3 Overview of the regulation of cybercrimes in South Africa

3.1 The common law position on cybercrimes

It is submitted that cybercrime became more prevalent in South African banks and related financial institutions in the early 1990's when the Internet started to be widely used in South Africa and other countries.[80] During this period the common law was most often used to prohibit, prosecute and combat cybercrime in South Africa. Accordingly, cybercrimes such as online defamation, online child pornography, the dissemination of child porn online, cyber-smearing, cyber fraud, the online publication of any court proceedings without the courts' permission, and forgery were prohibited under common law in South Africa.[81] However, any unlawful interception of data which included the acquisition, viewing, capturing or copying of data of a non-public nature through the use of hardware or software tools, cyber fraud, cyber forgery or cyber uttering was not prohibited under the South African common law.[82] Notably, South African banks were more vulnerable to phishing, data loss, identity theft and online scams in the early 1990s.[83] This suggests that the common law was not effectively able to curb cybercrimes in South Africa in the early 1990s.[84] Its enforcement was impeded by physical court jurisdictional challenges since most cybercrime offences are perpetrated online.[85]

---

78 Axelrod *Violence Goes to the Internet* 5-299; Bidgoll *Internet Encyclopedia* 200-500.

79 Rajput *Cyber Economic Crime* 8-260; Cruz-Cunha and Portela *Handbook of Research on Digital Crime* 67-600; Ericsson, Monserrat and Nokia *5G Mobile* 100-398; Vishnevsky and Kozyrev *Distributed Computer and Communication Networks* 171-300.

80 Thornton *et al Telecommunications Law* 16-332.

81 Cassim 2010 *JICLT* 118-123; Thornton *et al Telecommunications Law* 16-332; Van der Merwe *et al Information and Communications Technology Law* 70-74.

82 Smith, Grabosky and Urbas *Cyber Criminals* 65-200, Wells *Internet Fraud Casebook* 105-300; Tillman *Global Pirates* 50-1654.

83 Cassim 2010 *JICLT* 118-123; Van der Merwe *et al Information and Communications Technology Law* 70-74; Burgmann *Globalization* 15-243; Ennew and Waite *Financial Services Marketing* 23-381.

84 Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123; *S v Mashiyi* 2002 2 SACR 387 (Tk); *Narlis v South African Bank of Athens* 1976 2 SA 573 (A); Thornton *et al Telecommunications Law* 16-332; Carlan, Nored and Downey *Introduction to Criminal Law* 40-195.

85 Snail 2009 *JILT* 3-13.

3.2 The statutory regulation of cybercrimes in South Africa

After many years of legal uncertainty regarding the regulation of cybercrime, the ECTA has been enacted *inter alia* to curb cybercrime in South Africa. The ECTA is the first statute to directly outlaw cybercrime in South Africa.[86] Although it does not expressly define the term "cybercrime", it defines "access" to include the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.[87] Any unauthorised access to or interception of or interference with data is outlawed under the ECTA.[88] Thus, any person who knowingly and intentionally accesses or intercepts any data without authority or permission from the relevant authorities or owners of such data is liable for an offence.[89] Likewise, any person who knowingly and intentionally interferes with data or causes such data to be modified, destroyed or rendered ineffective is liable for an offence.[90] The ECTA also prohibits all persons from unlawfully producing, selling, offering to sell, procuring for use, designing, adapting for use, distributing and/or possessing any device or computer programme in order to overcome data protection security measures or gain unlawful access to any data.[91] These provisions are probably aimed at combating cyber-related offences involving unlawful interference with data by any persons. Moreover, all computer-related extortion, fraud and forgery practices are prohibited under the ECTA.[92] For instance, any person who performs or threatens to perform cybercrimes or interfere with any data in order to obtain any unlawful proprietary advantage over other persons will be liable for an offence under the ECTA.[93] Any person who attempts to commit any cybercrime activities is liable for an offence under the ECTA.[94] Furthermore, any person who aids or abets, or attempts to aid and/or abet someone to commit any cybercrime activities is liable for an offence under the ECTA.[95] Nonetheless, as earlier stated, the unspecified amount of fine and the imprisonment terms for cybercrimes under the ECTA are not robust and deterrent enough.[96] Moreover, the ECTA does not expressly provide for the use of AI and 5G to

86 Sections 85-89 of the ECTA.
87 Section 85 of the ECTA.
88 Section 86 of the ECTA.
89 Section 86(1) of the ECTA.
90 Section 86(2) of the ECTA.
91 Section 86(3) of the ECTA.
92 Section 87 of the ECTA.
93 Section 87(1) of the ECTA.
94 Section 88(1) of the ECTA.
95 Section 88(2) of the ECTA.
96 Section 89 of the ECTA; Cassim 2009 *PELJ* 36-79; Cassim 2010 *JICLT* 118-123.

detect and curb cybercrime in South African banks and related financial institutions, and it does not expressly prohibit cybercrimes such as cyber warfare and cyber fraud in the South African banking institutions.[97] However, it is generally expected that the ECTA will curb hacking and the selling, designing and/or production of anti-security and circumventer technology in South African banks and other financial institutions.[98]

The RICA prohibits any unlawful interception of communication by any authorised persons in South Africa.[99] It also prohibits any person from the unlawful provision of real-time information and/or any archived communication-related information to other persons.[100] Therefore, the RICA regulates the application and authorisation of directions regarding the interception of communications and communication-related information. However, the RICA does not prevent an employer from monitoring the work-related data of employees in the workplace as long as such monitoring does not violate the relevant provisions of this Act. The RICA enables the relevant regulatory bodies and enforcement authorities to identify illicit mobile phone users and track cybercriminals who use mobile phone numbers for illegal activities.[101] Nonetheless, as indicated before, the RICA does not expressly prohibit cybercrime and financial crime in South African banks and related financial institutions.[102] Moreover, the RICA does not expressly provide for the use of AI and 5G to detect and curb cybercrime in South African banks and related financial institutions.

The POPIA seeks to protect all persons and/or data subjects from data breaches on their personal and private information.[103] The POPIA establishes the Information Regulator which is inter alia responsible for monitoring and enforcing compliance with the provisions of the POPIA by all persons including public and private bodies to curb personal information violations for all data subjects in South Africa.[104] Notably, the Information Regulator is empowered to investigate complaints about violations of the

97 Section 875 of the ECTA; see the related discussion by Sharma *E-Governance* 19-323; Van der Merwe *et al Information and Communications Technology Law* 70-74.

98 Section 86 of the ECTA; Pitts *Cyber Crimes* 52-90; Armstrong *et al Access to Knowledge* 20-304; Bhateja *et al Intelligent Computing* 102-400.

99 Section 49 read with ss 2-15 of the RICA; see further Armstrong *et al Access to Knowledge* 20-304.

100 Section 50 read with ss 2-15 of the RICA; see further Armstrong *et al Access to Knowledge* 20-304.

101 Sections 10 and 11 of the RICA.

102 Sections 2-57 of the RICA.

103 Sections 5-35 of the POPIA; Solove *Digital Person* 74-200; Richardson *Cyber Crime* 63-300.

104 Sections 39 and 40 read with ss 4, 5, 49 and 50 of the POPIA.

protection of the personal information of data subjects and it may summon individuals to appear before it to receive evidence, conduct private interviews and enter and search any premises with a search warrant to seize articles linked to the commission of an offence in terms of the POPIA.[105] The POPIA imposes a statutory obligation on all relevant persons to protect and promote the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to such information.[106] Despite these positive measures, cybercrime is still rife in South Africa. For instance, it is reported that the Amalgamated Banks of South Africa (ABSA) lost about R500 000 after its accounts were hacked in 2003. Hackers also attacked the First National Bank (FNB), the Standard Bank and the Amalgamated Banks of South Africa (ABSA -again) in 2006 and transferred cash from bank accounts into prepaid accounts that were held by mobile operators.[107] In 2020 Experian (a credit bureau) reported that the personal information details of about 24 million people and about 800 000 businesses had been compromised after they were hacked by a fraudster in South Africa.[108] This could have been aggravated by the fact the relevant statutes such as the POPIA do not expressly provide for the use of AI and 5G to detect and curb cybercrime in South African banks and related financial institutions.[109] In this regard, it is submitted that the statutory introduction and use of AI and 5G could enable enforcement authorities to timeously detect, prevent and combat cybercrimes in the South African banks and related financial institutions.

Given the statutory gaps and flaws enumerated above, the Cybercrimes Bill was introduced in South Africa. This Bill is *inter alia* aimed at protecting all persons, including companies, banks and financial institutions, from cyber criminals, terrorists and other unscrupulous persons that rely on computers, the Internet and recent technology to perpetrate cybercrimes in South Africa. As stated earlier in paragraph 2.1 above, any unlawful securing of access to data and/or unlawful acquiring of data by any person is prohibited under the Cybercrimes Bill.[110] Likewise, any unlawful acts in respect of

105 Sections 40 and 73-99 of the POPIA; Waschke *Personal Cybersecurity* 29-231.

106 Sections 57-59 of the POPIA; Waschke *Personal Cybersecurity* 29-231.

107 Van Niekerk and Chandarman 2017 *AJIC* 133-155.

108 Bottomley 2020 https://www.businessinsider.co.za/the-personal-details-of-millions-of-south-africans-have-just-been-hacked-2020-8.

109 Bottomley 2020 https://www.businessinsider.co.za/the-personal-details-of-millions-of-south-africans-have-just-been-hacked-2020-8.

110 Sections 2 and 3 of the Cybercrimes Bill; also see Casey *Digital Evidence* 35-187; Bottomley 2020 https://www.businessinsider.co.za/the-personal-details-of-millions-of-south-africans-have-just-been-hacked-2020-8.

software or hardware tool and illegal interference with data or a computer programme by any person are outlawed under the Cybercrimes Bill.[111] Unlawful interference with a computer data storage medium or computer system as well as any illegal acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices by any person is prohibited in the Cybercrimes Bill.[112] Cyber fraud, cyber forgery, cyber uttering and cyber extortion activities are prohibited in the Cybercrimes Bill.[113] Cyber-related aggravated offences are further prohibited in the Cybercrimes Bill.[114] Any person who attempts, conspires, aids, abets, induces, incites, instigates, instructs, commands or procures another person to commit cyber-related offences will be liable for an offence under the Cybercrimes Bill.[115] The common law offence of theft includes the theft of incorporeal things through cybercrimes under the Cybercrimes Bill.[116] Any person that distributes a data message with intimate images without consent from the affected person or posts or sends a harmful and unlawful data message which incites damage to property and/or violence will also incur criminal liability under the Cybercrimes Bill.[117] As indicated in paragraph 2.1 above, any person that commits any of the aforementioned cybercrimes will only incur criminal penalties under the Cybercrimes Bill.[118] The Cyber Response Committee (CRC) and the 24/7 Point of Contact are also established under the Cybercrimes Bill in a bid to enhance the combating of cybercrimes in South Africa.[119]

The Cybercrimes Bill obliges financial institutions such as banks and electronic communications service providers to report cybercrimes and preserve any evidence which could be utilised by the law enforcement agencies when investigating and/or prosecuting cybercrimes in South Africa.[120] Banking institutions should exercise their statutory obligation to keep, monitor, disclose and produce customer information in the event of the commission of cybercrimes by illicit perpetrators carefully to avoid violating their customers' right to privacy and the right to dignity as enshrined in the *Constitution of the Republic of South Africa*, 1996 (Constitution).[121]

111 Sections 4 and 5 of the Cybercrimes Bill.
112 Sections 6 and 7 of the Cybercrimes Bill.
113 Sections 8-10 of the Cybercrimes Bill.
114 Section 11 of the Cybercrimes Bill.
115 Section 12 of the Cybercrimes Bill.
116 Section 13 of the Cybercrimes Bill.
117 Sections 16-18 read with s 22 of the Cybercrimes Bill.
118 Section 14 of the Cybercrimes Bill.
119 See ss 53 and 50 of the Cybercrimes Bill respectively.
120 Section 52 of the Cybercrimes Bill.
121 Pollicino and Graziella *Internet and Constitutional Law* 100-220; Robinson and Baker *Artificial Intelligence* 104-250.

Consequently, any financial institutions and electronic communications service providers that fail to report cybercrimes and/or preserve any relevant evidence in respect thereof will be liable for criminal penalties under the Cybercrimes Bill.[122] Nevertheless, the Cybercrimes Bill does not expressly provide for the use of AI and 5G to detect and curb cybercrime in the South African banks and related financial institutions.[123]

4 Available anti-cybercrime enforcement role-players in South Africa

4.1 The role of the Independent Communications Authority of South Africa (ICASA)

The ICASA is an independent body that regulates the communications, broadcasting and postal services sectors of South Africa. The ICASA was established in 2000 by the *Independent Communications Authority of South Africa Act* (*ICASA Act*)[124] to, *inter alia*, oversee the regulation of the telecommunications and broadcasting sectors of South Africa in the public interest. The ICASA took over from the Independent Broadcasting Authority (IBA) and the South African Telecommunications Regulatory Authority (SATRA). The merging of the former bodies into ICASA was generally informed by the need to adapt to and/or comply with the rapid technological developments that are constantly occurring in South Africa and other countries globally. The ICASA is statutorily empowered under schedule 1 of the *Public Finance Management Act* 1 of 1999, the *ECTA*, the *Postal Services Act* 24 of 1998, the *Broadcasting Act* 4 of 1999 and the *ICASA Act* to grant licences, monitor the licensee's compliance with the terms and conditions of their licences and develop relevant regulations to protect consumers. The ICASA develops regulations for the communications, broadcasting and postal services sectors of South Africa.[125] It manages the radio frequency spectrum and it protects consumers against unfair business practices and poor-quality services. It also ensures that all people in South Africa have access to affordable basic communication services. All licensees are obliged to contribute to the Universal Service and Access Fund.

---

122 Section 14 of the Cybercrimes Bill.

123 Ghosh and Turrini *Cybercrimes* 15-370; Smith, Grabosky and Urbas *Cyber Criminals* 65-200; Button and Cross *Cyber Frauds* 56-200.

124 *Independent Communications Authority of South Africa Act* 13 of 2000, as amended (*ICASA Act*) ss 3 and 4.

125 Achimugu *et al* 2009 *JITI* 40-46.

The ICASA is empowered to receive complaints from the public about poor services provided by telecommunications, broadcasting and postal services licensees in South Africa.[126] It also resolves such complaints or refers them to the Complaint and Compliance Committee for further adjudication. Moreover, the ICASA is a Chapter 9 institution which supports democracy in accordance with the Constitution. It is further obliged to promote international and regional co-operation and the interoperability of networks. It has a duty to promote the interests of consumers with regard to price, quality and the variety of electronic communications services, and to ensure information security and network reliability in South Africa.[127] However, the ICASA does not specifically provide for the use of 5G and AI measures to detect, investigate, prevent and curb cybercrimes in South African banks, companies and other related financial institutions. Furthermore, the ICASA is not expressly provided for under the ECTA and the Cybercrimes Bill.

4.2 The role of the SAPS

Although the role of the SAPS in relation to cybercrimes is not adequately outlined in the Cybercrimes Bill, the ECTA and the POPIA, it is expected that all electronic communications service providers and financial institutions are obliged to report cybercrime activities to the SAPS.[128] For instance, the Cybercrimes Bill obliges all persons, including banks, electronic communications service providers and other financial institutions, to report all incidents of cybercrimes to the SAPS.[129] The Cybercrimes Bill stipulates that the Minister of Police must take relevant measures to build capacity in the SAPS so as to effectively deal with cybercrime activities in South Africa.[130] The SAPS is also obliged to create mechanisms for cooperation and mutual assistance between foreign states in cross-border investigations to prevent and combat cybercrime in South Africa.[131] The SAPS is also empowered to inspect, search and/or seizure any relevant materials from suspected cyber criminals under the ECTA.[132] In this regard, the SAPS works closely with the cyber inspectors. Thus, it is empowered to investigate, access, search and/or seize any article, document or material used in the commission of cybercrime activities in South Africa. The Cybercrime Bill correctly provides that the SAPS should obtain search

126 Sections 3 and 4 of the *ICASA Act*.
127 Section 2 read with ss 3 and 4 of the *ICASA Act*; Achimugu *et al* 2009 *JITI* 40-46.
128 Sections 24-30, 35, 45(3), 52 and 54 of the Cybercrimes Bill.
129 Section 52 read with ss 24-30, 35, 45(3) and 54 of the Cybercrimes Bill.
130 Section 52 read with ss 24-30, 35, 45(3) and 54 of the Cybercrimes Bill.
131 Section 45(3) read with s 46 of the Cybercrimes Bill.
132 Sections 80-89 of the ECTA.

warrants prior to any search for evidence, data or computers from any person, premises or vehicle in relation to the commission of cybercrimes in South Africa.[133] The SAPS also participates in the development of anti-cybercrime policies and strategies in South Africa. It further provides specialised investigative capacity and interaction with other relevant national and international stakeholders such as banks to curb cross-border cybercrimes in South Africa. Cybersecurity is mainly enforced by the State Security Agency (SSA) in South Africa.[134] A specifically designated police official may issue an expedited direction for the preservation of data to an individual or entity that is in possession of or may receive data relevant to the commission of cybercrime offences in South Africa.[135]

The SAPS should play a pivotal role in the combating of cybercrime, since South Africa is among the countries that have the highest rates of cybercrimes in the world.[136] In this regard, it is important to note that the SAPS Directorate for Priority Crime Investigation (SAPS DPCI or Hawks) is directly involved in the curbing of cybercrime, financial crimes and corruption in South Africa. The Hawks should employ better approaches to authenticate hardware, software and data on computer systems and to verify user identities to enhance its monitoring and detecting of cybercrimes in South Africa. The SAPS must adopt a holistic approach in the fight against cybercrime and work harder to understand social media-related risks and illegal corporate espionage.[137]

4.3 The role of the 24/7 Point of Contact and the CRC

The 24/7 Point of Contact is established under the Cybercrimes Bill.[138] The 24/7 Point of Contact is administered by the Minister of Police and must operate on a twenty-four hour, seven-day-a-week basis to provide expedited assistance in all cybercrime investigations and/or related proceedings.[139] The 24/7 Point of Contact is empowered to provide

133 Section 27 read with ss 29, 30 and 31 of the Cybercrimes Bill, which empowers police officers to access, search or seize any data or evidence from any accused persons without a search warrant; see the related discussion by Chawki *et al Cybercrime* 25-120.

134 Dlamini and Mbambo 2019 *Cogent Social Sciences* 1-13; Bossler and Berenblum 2019 *Journal of Crime and Justice* 495-499.

135 Sections 40-42 of the Cybercrimes Bill; Dlamini and Mbambo 2019 *Cogent Social Sciences* 1-13.

136 Sections 40-42 of the Cybercrimes Bill; Dlamini and Mbambo 2019 *Cogent Social Sciences* 1-13.

137 Sections 40-42 of the Cybercrimes Bill; Dlamini and Mbambo 2019 *Cogent Social Sciences* 1-13.

138 Section 50(1) of the Cybercrimes Bill.

139 Section 50(2) and (3) of the Cybercrimes Bill.

assistance with cybercrime in South Africa and other foreign countries.[140] This means that the 24/7 Point of Contact has extra-territorial jurisdiction to provide assistance in all cybercrime investigations and/or related proceedings.[141] The 24/7 Point of Contact is obliged to provide technical advice and facilitate or provide legal assistance, identify and locate an article or a suspect, and cooperate with the appropriate authorities of a foreign country regarding any cybercrime investigations.[142] The Minister of Police may make regulations and impose additional duties on the 24/7 Point of Contact to enhance the curbing of cybercrime in South Africa.[143] The National Director of Public Prosecutions (NDPP) is obliged to provide legal assistance to the 24/7 Point of Contact for it to effectively conduct its duties.[144] The 24/7 Point of Contact is required to report all incidents of cybercrimes to the SAPS for further adjudication. Be that as it may, the 24/7 Point of Contact does not expressly provide for the use of AI and 5G to detect and combat cybercrimes in South Africa.

On the other hand, the CRC is established under the Cybercrimes Bill to deal with cyber security threats in South Africa.[145] The Minister of State Security appoints a chairperson, and whenever the chairperson is absent the Minister of State Security assumes the responsibilities and duties of the chairperson.[146] The work and functions of the CRC must be performed by a secretariat consisting of designated administrative members of the SSA.[147] The CRC is statutorily obliged to implement any government policy on cybersecurity in South Africa.[148] The Minister of State Security must submit a report to the chairperson of the Joint Standing Committee on Intelligence regarding the progress and functions of the CRC.[149] The Cybercrimes Bill does not expressly oblige the CRC to employ AI and 5G measures to detect, investigate and curb cyber-related activities in South Africa.

140 Section 50(3)(a) of the Cybercrimes Bill.
141 Section 50(3)(a)(iii)(bb) of the Cybercrimes Bill.
142 Section 50(3)(b) of the Cybercrimes Bill.
143 Section 50(4) of the Cybercrimes Bill.
144 Section 50(5) of the Cybercrimes Bill.
145 Section 53(1) of the Cybercrimes Bill.
146 Section 53(3) and (6) of the Cybercrimes Bill.
147 Section 53(4) of the Cybercrimes Bill.
148 Section 53(5) of the Cybercrimes Bill.
149 Section 53(7) of the Cybercrimes Bill.

5 The use of 5G, AI and other technological approaches to curb cybercrimes in South African financial institutions

As stated above, cybercrime also affects banks and other financial institutions. For instance, South African banks are constantly being affected by phishing scams and other cybercrimes.[150] Most of these crimes are perpetrated through the Internet and are exacerbated by technological advancements. As a result, the security of the Internet has become very important for the past four generations of wireless systems and will continue to be treated as such under any new generation of technology.[151] Furthermore, the cheaper that computation gets and as more new technology emerges, the more chances there will be that banks and other financial institutions will be susceptible to cybercrimes.[152] Therefore, newer generations of wireless systems must carefully improve their Internet requirements without compromising Internet security.[153] Mobile broadband will be increasingly used for Internet access and cloud services and this will increase the vulnerability to cybercrimes of banks, companies and other financial institutions in South Africa. 5G networks transport large amounts of data which are also used in the South African banking institutions. Thus, connectivity to any Internet-connected household entry must be carefully audited to prevent unlawful entry and cybercrimes in the South African banking institutions.[154] AI and 5G presents unique opportunities for financial institutions to enhance their operations. In this regard, South African banks, companies and other financial institutions should seriously consider adopting 5G, AI and other technological measures to detect and prevent cybercrimes. 5G has fast-virtualising software which provides better network functions that could be useful in the curbing of cybercrimes. Likewise, AI sub-types such as machine learning, deep learning, neural networks and analytic AI could enable banks and other financial institutions to timeously detect and effectively curb cybercrime in South Africa.

6 Concluding remarks

As discussed above, cybercrime is outlawed under both common law and the ECTA in South Africa. Nonetheless, both the common law and the ECTA have so far struggled to effectively regulate and combat cybercrime

150 Cassim 2010 *JICLT* 118-123; Herselman and Warren 2004 *Issues in Informing Science and Information Technology* 253-266.
151 Petrillo, De Felice and Cioffi *Digital Transformation* 40-120.
152 Petrillo, De Felice and Cioffi *Digital Transformation* 40-120.
153 Vacca *Guide to Wireless Network Security* 102-600.
154 Lukonga *Fintech, Inclusive Growth and Cyber Risks* 1-51.

offences in South Africa. This position is worsened by the fact that cybercrime is not expressly outlawed under the RICA and the POPIA. Consequently, cybercrime is still problematic in South African banks, companies and other related financial institutions. Cybercriminals often target electronic banking or payment services of banks and other financial institutions and/or financial customers to fraudulently hack and steal money from their accounts. This has given rise to the introduction of the Cybercrimes Bill. However, the Bill is yet to be passed into law and it does not provide for the use of AI, 5G or other technological measures to curb cybercrime in South Africa. Thus, notwithstanding the commendable efforts adopted so far by South Africa to regulate and combat cybercrime, cyber-related activities are still rife and still affect most persons, banks and other related financial institutions. Moreover, it remains uncertain whether banks and other financial institutions have adopted 5G and AI to detect and combat cybercrimes in South Africa. In this regard, it is submitted that banks, companies and other financial institutions should adopt 5G, AI and/or other robust technological measures to enhance their detection, prevention and curbing of cybercrime offences in South Africa. This approach could further enable banks and other financial institutions to discourage and timeously prevent cybercriminals from committing financial crimes such as money laundering and insider trading in South Africa. It is also submitted that the South African policy makers should carefully revise the Cybercrimes Bill to embrace the use of AI and 5G to detect and combat cybercrimes in South African banks and related financial institutions.[155] The other option is to amend the ECTA to expressly oblige banks, financial institutions, companies and other enforcement authorities to utilise technological measures such as 5G and AI so as to effectively detect, prevent and curb cybercrimes such as theft of bank card payment data, the theft of corporate data, and cyber extortion in South Africa. The ICASA should be empowered to specifically provide for the use of 5G and AI measures to detect, investigate, prevent and curb cybercrimes in South African banks, companies and other related financial institutions.

155 Lukonga *Fintech, Inclusive Growth and Cyber Risks* 1-51; Zeviar-Geese 1997-1998 *GJIL* 119-146.

Bibliography

Literature

Abawajy *et al Internet and Distributed Computing Advancements*
Abawajy JH *et al Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications* (IGI Global Hershey 2012)

Achimugu *et al* 2009 *JITI*
Achimugu P *et al* "Adoption of Information and Communication Technologies in Developing Countries: An Impact Analysis" 2009 *JITI* 37-46

Armstrong *et al Access to Knowledge*
Armstrong C *et al Access to Knowledge in Africa: The Role of Copyright* (UCT Press Claremont 2010)

Axelrod *Violence Goes to the Internet*
Axelrod EM *Violence Goes to the Internet: Avoiding the Snare of the Net* (Charles C Thomas Springfield 2009)

Bhateja *et al Intelligent Computing*
Bhateja V *et al Intelligent Computing and Communication* (Springer Singapore 2020)

Bidgoll *Internet Encyclopedia*
Bidgoll H *The Internet Encyclopedia Volume 1* (Wiley New Jersey 2004)

Bossler and Berenblum 2019 *Journal of Crime and Justice*
Bossler AM and Berenblum T "Introduction: New Directions in Cybercrime Research" 2019 *Journal of Crime and Justice* 495-499

Brenner 2006 *Crime Law Soc Change*
Brenner SW "Cybercrime Jurisdiction" 2006 *Crime Law Soc Change* 189-206

Brenner *Threats from Cyberspace*
Brenner SW *Cybercrime: Criminal Threats from Cyberspace* (Greenwood Santa Barbara 2010)

Brenner "Cybercrime"
Brenner SW "Cybercrime: Re-thinking Crime Control Strategies" in Jewkes Y (ed) *Crime Online* (Routledge New York 2011) 12-29

Brynjolfsson and Mcafee 2017 *HBR*
Brynjolfsson E and Mcafee AN "The Business of Artificial Intelligence" 2017 *HBR* 3-11

Burgmann *Globalization*
Burgmann V *Globalization and Labour in the Twenty-First Century* (Routledge London 2016)

Button and Cross *Cyber Frauds*
Button M and Cross C *Cyber Frauds, Scams and their Victims* (Routledge London 2017)

Buys *Cyberlaw*
Buys R *Cyberlaw: The Law of the Internet in South Africa* (Van Schaik Pretoria 2000)

Carlan, Nored and Downey *Introduction to Criminal Law*
Carlan P, Nored LS and Downey RA *An Introduction to Criminal Law* (Jones and Bartlett Sudbury 2011)

Casey *Digital Evidence*
Casey E *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Elsevier London 2011)

Cassim 2009 *PELJ*
Cassim F "Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study" 2009 *PELJ* 36-79

Cassim 2010 *JICLT*
Cassim F "Addressing the Challenges Posed by Cybercrime: A South African Perspective" 2010 *JICLT* 118-123

Cassim 2011 *CILSA*
Cassim F "Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players" 2011 *CILSA* 123-138

Cassim 2012 *PELJ*
Cassim F "Addressing the Spectre of Cyber Terrorism: A Comparative Perspective" 2012 *PELJ* 381-415

Chawki *et al Cybercrime*
Chawki M *et al Cybercrime, Digital Forensics and Jurisdiction* (Springer New York 2015)

Chitimira 2020 *Acta Universitatis Danubius Juridica*
Chitimira H "The Reliance on Artificial Intelligence Measures to Curb Money Laundering Practices in the South African Banking Institutions and Real Estate Sector" 2020 *Acta Universitatis Danubius Juridica* 28-43

Cruz-Cunha and Portela *Handbook of Research on Digital Crime*
Cruz-Cunha MM and Portela IM *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (IGI Global Hershey 2015)

Dawson and Omar *New Threats and Countermeasures*
Dawson M and Omar M *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (IGI Global Hershey 2015)

Dilek, Çakır and Aydın 2015 *IJAIA*
Dilek S, Çakır H and Aydın M "Applications of Artificial Intelligence Techniques to Combat Cybercrimes: A Review" 2015 *IJAIA* 21-34

Dlamini and Mbambo 2019 *Cogent Social Sciences*
Dlamini S and Mbambo C "Understanding Policing of Cyber-Crime in South Africa: The Phenomena, Challenges and Effective Responses" 2019 *Cogent Social Sciences* 1-13

Ennew and Waite *Financial Services Marketing*
Ennew CT and Waite N *Financial Services Marketing: An International Guide to Principles and Practice* (Elsevier Oxford 2007)

Ericsson, Monserrat and Nokia *5G Mobile*
Ericsson OA, Monserrat JF and Nokia PM *5G Mobile and Wireless Communications Technology* (Cambridge University Press Cambridge 2016)

Ezrachi and Stucke 2017 *U Ill L Rev*
Ezrachi A and Stucke ME "Artificial Intelligence and Collusion: When Computers Inhibit Competition" 2017 *U Ill L Rev* 1775-1809

Franklin *Investigator's Guide*
Franklin CJ *The Investigator's Guide to Computer Crime* (Thomas Springfield 2006)

Ghosh and Turrini *Cybercrimes*
Ghosh S and Turrini E *Cybercrimes: A Multidisciplinary Analysis* (Springer Berlin 2010)

Goldfarb and Prince 2008 *Information Economics and Policy*
Goldfarb A and Prince J "Internet Adoption and Usage Patterns are Different: Implications for the Digital Divide" 2008 *Information Economics and Policy* 2-15

Gordon and Ford 2006 *Journal in Computer Virology*
Gordon S and Ford R "On the Definition and Classification of Cybercrime" 2006 *Journal in Computer Virology* 13-20

Herselman and Warren 2004 *Issues in Informing Science and Information Technology*
Herselman M and Warren M "Cyber Crime Influencing Businesses in South Africa" 2004 *Issues in Informing Science and Information Technology* 253-266

Johnson *Forensic Computer Crime Investigation*
Johnson TA *Forensic Computer Crime Investigation* (Taylor and Francis Boca Raton 2005)

Joshi *Digital Finance*
Joshi VC *Digital Finance, Bits and Bytes: The Road Ahead* (Springer Singapore 2020)

Kelemen, Romportl and Zackova *Beyond Artificial Intelligence*
Kelemen J, Romportl J and Zackova E (eds) *Beyond Artificial Intelligence: Contemplations, Expectations, Applications* (Springer Science and Business Media New York 2012)

Kovacich and Jones *Crime Investigator's Handbook*
Kovacich GL and Jones A *High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program* (Elsevier Burlington 2006)

Liang and Lu 2010 *J Contemp Crim Justice*
Liang B and Lu H "Internet Development, Censorship, and Cyber Crimes in China" 2010 *J Contemp Crim Justice* 103-120

Lukonga *Fintech, Inclusive Growth and Cyber Risks*
Lukonga I *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions* (International Monetary Fund Washington DC 2018)

Madhusanka *et al Comprehensive Guide*
Madhusanka L *et al A Comprehensive Guide to 5G Security* (Wiley Hoboken 2018)

Mbelli and Dwolatzky "Cyber Security"
Mbelli TM and Dwolatzky B "Cyber Security, A Threat to Cyber Banking in South Africa: An Approach to Network and Application Security" in *IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (25-27 June 2016 Beijing) 1-6

Moore *Cybercrime*
Moore R *Cybercrime: Investigating High-Technology Computer Crime* (Routledge Amsterdam 2010)

Orji *Cybersecurity Law and Regulation*
Orji UJ *Cybersecurity Law and Regulation* (Wolf Legal Nijmegen 2012)

Orji 2019 *Tilburg L Rev*
Orji UJ "Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria" 2019 *Tilburg L Rev* 105-124

Osterburg, Ward and Miller *Criminal Investigation*
Osterburg JW, Ward RH and Miller LS *Criminal Investigation: A Method for Reconstructing the Past* (Routledge London 2019)

Paula *et al* "Deep Learning Anomaly Detection"
Paula EL *et al* "Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering" in *15th IEEE International Conference on Machine Learning and Application* (18-20 December 2016 Anaheim) 954-960

Petrillo, De Felice and Cioffi *Digital Transformation*
Petrillo A, De Felice F and Cioffi R *Digital Transformation in Smart Manufacturing* (InTech Rijeka 2018)

Pitts *Cyber Crimes*
Pitts V *Cyber Crimes: History of World's Worst Cyber Attacks* (VIJ Books New Delhi 2017)

Pollicino and Graziella *Internet and Constitutional Law*
Pollicino O and Graziella R *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe* (Routledge London 2016)

Rajput *Cyber Economic Crime*
Rajput B *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation* (Springer Cham 2020)

Reuvid *Easy Steps to Managing Cybersecurity*
Reuvid J *Easy Steps to Managing Cybersecurity* (Legend Press London 2018)

Richardson *Cyber Crime*
Richardson M *Cyber Crime: Law and Practice* (Wildy Simmonds & Hill London 2019)

Robinson and Baker *Artificial Intelligence*
Robinson PH and Baker DJ *Artificial Intelligence and the Law: Cybercrime and Criminal Liability* (Routledge London 2020)

Savona *Crime and Technology*
Savona EU *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research* (Springer Dordrecht 2004)

Sharma *E-Governance*
Sharma P *E-Governance: The New Age Governance* (APH Publishing New Delhi 2004)

Siegel and Mirakovits *Forensic Science*
Siegel JA and Mirakovits K *Forensic Science: The Basics* (Routledge London 2016)

Smith, Grabosky and Urbas *Cyber Criminals*
Smith RG, Grabosky P and Urbas G *Cyber Criminals on Trial* (Cambridge University Press London 2004)

Snail 2009 *JILT*
Snail S "Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities" 2009 *JILT* 1-13

Solove *Digital Person*
Solove DJ *The Digital Person: Technology and Privacy in the Information Age* (New York University Press New York 2004)

Thomas *et al Cybercrime and Digital Forensics*
Thomas JH et al *Cybercrime and Digital Forensics: An Introduction* (Routledge London 2015)

Thornton *et al Telecommunications Law*
Thornton L *et al Telecommunications Law in South Africa* (STE Publishers Johannesburg 2006)

Tillman *Global Pirates*
Tillman R *Global Pirates: Fraud in the Offshore Insurance Industry* (Northeastern University Press Boston 2002)

Vacca *Guide to Wireless Network Security*
Vacca JR *Guide to Wireless Network Security* (Springer New York 2006)

Van der Merwe *et al Information and Communications Technology Law*
Van der Merwe DP *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Van Niekerk and Chandarman 2017 *AJIC*
Van Niekerk B and Chandarman R "Students' Cybersecurity Awareness at a Private Tertiary Educational Institution" 2017 *AJIC* 133-155

Vishnevsky and Kozyrev *Distributed Computer and Communication Networks*
Vishnevsky V and Kozyrev D *Distributed Computer and Communication Networks: 18th International Conference, DCCN 2015, Moscow, Russia, October 19-22, 2015, Revised Selected Papers* (Springer Cham 2016)

Waschke *Personal Cybersecurity*
Waschke M *Personal Cybersecurity: How to Avoid and Recover from Cybercrime* (Apress Washington DC 2017)

Wells *Internet Fraud Casebook*
Wells JT *Internet Fraud Casebook: The World Wide Web of Deceit* (John Wiley Hoboken 2010)

Zeviar-Geese 1997-1998 *GJIL*
Zeviar-Geese G "The State of the Law on Cyber-Jurisdiction and Cybercrime on the Internet" 1997-1998 *GJIL* 119-146

Ziska *Handbook of Research on Information*
Ziska F *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (IGI Global Hershey 2018)

Case law

Narlis v South African Bank of Athens 1976 2 SA 573 (A)

S v Mashiyi 2002 2 SACR 387 (Tk)

Legislation

Broadcasting Act 4 of 1999

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Electronic Communications and Transactions Act 25 of 2002

Independent Communications Authority of South Africa Act 13 of 2000

Postal Services Act 24 of 1998

Protection of Personal Information Act 4 of 2013

Public Finance Management Act 1 of 1999

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Government publications

Cybercrimes Bill B6-2017

International instruments

Council of Europe Convention on Cybercrime ETS No 185 (2001)

Internet sources

Bottomley 2020 https://www.businessinsider.co.za/the-personal-details-of-millions-of-south-africans-have-just-been-hacked-2020-8

Bottomley EJ 2020 *Personal Details of 24 Million South Africans may have been Exposed after Attack on Credit Bureau* https://www.businessinsider.co.za/the-personal-details-of-millions-of-south-africans-have-just-been-hacked-2020-8 accessed 13 March 2021

Council of Europe 2021 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=L3MN1W5t?
Council of Europe 2021 *Chart of Signatures and Ratifications of Treaty 185* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=L3MN1W5t? accessed 24 June 2021

Galal and O'Halloran 2020 http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf
Galal H and O'Halloran D 2020 *The Impact of 5G: Creating New Value Across Industries and Society* http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf accessed 23 June 2021

Smith *et al* 2006 https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf
Smith C *et al* 2006 *The History of Artificial Intelligence - University of Washington Research Paper* https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf accessed 24 June 2021

Tamarkin 2014 https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime
Tamarkin E 2014 *South Africa must Pay More Attention to Cybercrime* https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime accessed 30 January 2021

List of Abbreviations

4IR	Fourth Industrial Revolotion
5G	fifth generation network technology
ABSA	Amalgamated Banks of South Africa
AI	artificial intelligence
AJIC	African Journal of Information and Communication
CILSA	Comparative and International Law Journal of Southern Africa
CRC	Cyber Response Committee
Crime Law Soc Change	Crime, Law and Social Change
ECTA	Electronic Communications and Transactions Act
FNB	First National Bank
GJIL	Gonzaga Journal of International Law
HBR	Harvard Business Review

ICASA	Independent Communications Authority of South Africa
IJAIA	International Journal of Artificial Intelligence and Applications
J Contemp Crim Justice	Journal of Contemporary Criminal Justice
JICLT	Journal of International Commercial Law and Technology
JILT	Journal of Information, Law and Technology
JITI	Journal of Information Technology Impact
PELJ	Potchefstroom Electronic Law Journal
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act
SAPS	South African Police Service
SSA	State Security Agency
Tilburg L Rev	Tilburg Law Review
U Ill L Rev	University of Illinois Law Review