Acta Universitatis Danubius
JURIDICA

Of Anonymity and Attribution and the Challenges of Controlling Cybercrime in South Africa

Abiodun Omotayo Oladejo[1], Nontyatyambo Pearl Dastile[2]

Abstract: The advent of the digital age has considerably changed the way we live because of the pervasiveness of human-technology interface. While the myriads of cyber technologies have enhanced the human world, they have also produced undesirable consequences, the major of which is cybercrime. In South Africa, cybercrime is fast becoming an endemic issue, affecting businesses, individuals, and the public sector. The usual narratives about cybercrime control have centred more on the legislative and institutional frameworks rather than the nature of the crime, which is largely intangible. This paper, relying on critical review technique, foregrounds anonymity and attribution as critical factors impeding the effectiveness of cybercrime prosecution. To circumnavigate these challenges, we advocate for improved investigative and cyberspace knowledge (such as the state-of-the-art digital forensics) for the South African Police Service and collaboration with private cybersecurity and computer technology companies. Although difficult given the rapid pace of technological development, these are necessary steps if there will be a rise in the effectiveness of cybercrime control in South Africa.

Keywords: crime; digital innovations; SAPS; virtual space

[1] Directorate of Research Innovation and Development, Walter Sisulu University, Mthatha, South Africa, Address: Nelson Mandela Drive, 5117 Mthatha, Eastern Cape, South Africa, Corresponding author: aoladejo@wsu.ac.za.

[2] Faculty of Law, Humanities and Social Science, Walter Sisulu University, Mthatha, South Africa, Address: Nelson Mandela Drive, 5117 Mthatha, Eastern Cape, South Africa, E-mail: aoladejo@wsu.ac.za.

Copyright: © 2024 by the authors.
Open access publication under the terms and conditions of the
Creative Commons Attribution-NonCommercial (CC BY NC) license
(https://creativecommons.org/licenses/by-nc/4.0/)

1. Introduction

With the rapid advancement of technology and digitalisation, there has been a significant increase in the use of technology (Hassani et al., 2021; Myoyella, Karacuka & Haucap, 2020). The Google effect, Internet/technology dependency, and social media are manifestations of the cyberreality in today's world. In 2023, the number of Internet users worldwide stood at 5.3 billion, which means that around two thirds of the global population is currently connected to the world wide web (Statista, 2024). However, because crime is endemic in every sector of the human society, cyberspace is also ridden with criminal activities known as cybercrime, which has become a major concern for law enforcement agencies and policymakers in the world (Borwell, Jansen & Stol, 2021; Oreku & Mtenzi, 2017). The use of the Internet, digital technology, and the processing of personal data have increased, which have led to a rise in cybercrimes and cyberattacks, including identity theft, cyberfraud, cyberbullying and data breaches. South Africa ranks 5th in global cybercrime density list (Moyo, 2024). Research by VPN provider and cyber security firm Surfshark, which created the Data Vulnerability Thermometer by fusing research algorithms with open-source FBI data, served as the foundation for this. According to a survey from Surfshark, 801,000 individuals globally became victims of cybercrime in 2022. There have been documented cybercrimes against 56 out of a million Internet users in South Africa, or 2000 victims overall.

A few issues have been identified in literature as co-constitutive of the challenges facing the fight against cybercrimes in South Africa. The South African common law has proven to be ineffective in addressing cybercrime, the criminal sanctions in cybercrime laws are inadequate, and courts adopt a cautious approach to cybercrime cases (Snail ka Mtuze & Musoni, 2022; Cassim, 2010). No specialized court to hear cybercrime cases (Eboibi, 2020). Insufficient and ineffective regulatory and/or legislative measures (Graham, 2023; Mabunda, 2021). It is our argument however that, whereas, overwhelmingly, scholars have explained the rising cases of cybercrime in South Africa in relation to inadequate legal provisions and institutional constraints, not much has been said about the nature of the crime itself in terms of how it consists of attributes that make taming it seemingly intractable. In this paper, we argue that cybercrime inheres with anonymity and attribution, which may affect the ability of the police service's prosecutorial work. The miry realities of cybercrime, coupled with the inherent un-traditionality thus require the upscaling of investigative and prosecutorial competence by the police service. In the sections that follow, we historicise and analyse the legal framework for combating

cybercrimes in South Africa and assess the performance of the legal system in relation to cybercrime. Then we discuss the prosecutorial limitations of cybercrime and conclude with a suite of interventions that may help strengthen anti-cybercrime prosecution in South Africa.

2. The Legal Framework for Combating Cybercrimes in South Africa

The first attempt at cybercrime law globally is often attributed to the Council of Europe's Convention on Cybercrime - commonly known as the Budapest Convention of 2001, which was opened for signature in Budapest, Hungary, on November 23, 2001. This convention, being the only binding international instrument on cybercrime, is considered the first international treaty seeking to address Internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations (Spiezia, 2022; Wicki-Birchler, 2020). Since then, countries, including South Africa, have made laws bordering on cybercrime. In the subsections below, these legislative efforts in South Africa will be discussed.

2.1. Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

The pioneering legislation in South Africa that tangentially touches on cybercrime is the Electronic Communications and Transactions Act 25 of 2002 (ECT Act). The ECT Act was enacted in South Africa to steer legal issues concerning electronic communications, electronic transactions, and information technology (Chuma & Ngoepe, 2022; Coetzee, 2004). The Act's origins can be traced back to the early 2000s, when the fast growth of the Internet and digital technology necessitated the need for a legal framework to oversee online activities and transactions. As some scholars have argued, ECT Act 2002 was an effective piece of legislation which strives to put South African law on the map of the evolving global world (Mabeka, 2021). The Act aims to enhance the development of a national e-strategy, prevent abuse of information systems and encourage the use of e-government services. However, it is important to note that this legislation is largely focused on e-commerce rather than the multidimensional nature of cybercrime.

2.2. Protection of Personal Information Act (POPIA or POPI Act) 2013

Another landmark legislation on cybercrime is the Protection of Personal Information Act (POPIA) assented to by the President in 2013 and had its commencement date as 1 July 2020. The Protection of Personal Information Act (POPIA) in South Africa is a comprehensive piece of law aimed at promoting the protection of personal information processed by both public and commercial entities. POPIA was introduced to combat predatory data practices (Jones, 2021). The Act corresponds with worldwide data protection standards, such as the EU's General Data Protection Regulation (GDPR) and aims to ensure that South African residents' personal information is handled safely and ethically.

Section 2 of the Act lays out the purpose of the Act which includes: (a) giving effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at — balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic and across international borders; (b) regulating the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information; (c) providing persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and (d) establishing voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

POPIA has been greeted with varied reactions. It has been argued that POPIA has helped to enhance data protection awareness among organisations and the public with respect to the essence of data protection because, as a legal framework, it compels businesses and government bodies to treat personal information with much prudence (Burman, 2021). POPIA's alignment with international standards on data has also been commended. POPIA, according to Kwet (2020), is aligned with international data protection and this alignment with international data security standards like the GDPR has enhanced South Africa's standing globally and helped to maintain business relationships with international partners because businesses around the world now hold a view that South Africa as a jurisdiction with strong data protection laws. In the same vein, the introduction of POPIA, as argued by Naidoo and Naidoo (2021), has led to improved corporate compliance and data governance. According to them, the Act has engendered the adoption of stronger data governance

practices and implementation of measures to ensure compliance, such as appointing information officers and conducting data impact assessments. The Act's creation of the information regulator – an independent body to enforce the Act – has been hailed as a significant step (Moloi, 2022). This regulating authority is saddled with the responsibility of ensuring compliance and providing a legal apparatus for recourse when cases of data breaches or misuse have been established.

Conversely, the delayed implementation of the Act has been criticised. The Act was enacted in 2013 but did not come into effect until 2021. Du Toit (2020) argues that the delay created a long period of irresolution and inadequate preparedness among organizations and significantly affected the effectiveness of the Act at its inception. In complete contrast to other Acts, such as the Employment Equity Act, 177 which governs vicarious liability of employers, there are no such clauses in POPIA that may protect employers in the event that an employee of the responsible party intentionally or carelessly violates POPIA (Millard & Bascerano, 2016). The cost implications of compliance with POPIA for small and medium-scale enterprises are believed to be significant (Phakati, 2022). Some of the costs identified as compounding the running costs for these enterprises include the costs associated with data protection measures, legal advice, and training. Another issue that has been identified as constituting a challenge to the effectiveness of the Act is limited public awareness and understanding of the Act, which may limit individuals' ability to exercise their rights under the Act (Dlamini & Mkhize, 2021). Enforcement challenges including paucity of funds, bureaucratic delays, and the complexity of determining the commission of data breaches or misuse have been identified as leading to insufficient sanctions for noncompliance (Van der Merwe, 2023; Jogwe, 2021; Theys, 2020).

2.3. Cybercrime Act 2021

The Act aims to reduce and prevent cybercrime in South Africa, enforce law and protect the people of South Africa from cybercriminals (Cybercrime Act, 2021). The coming on board of Cybercrime Act 2021 was a watershed moment in South Africa. This is because, prior to this Act, common law principles used to be extended as widely as possible to cater for the arrest and prosecution of cybercriminals (Snail ka Mtuze & Musoni, 2023). Currently, Cybercrime Act 2021 is the major legal instrument for combating cybercrime in South Africa. Chapter two of the Act introduces the crimes of hacking, unlawful interception of data, ransomware, cyber forgery and uttering, cyber extortion, and malicious communications. The scope of

the Act covers trans-border cooperation because cybercrimes often transcend national borders and on a geographically borderless platform (Sekati, 2022). This essentially requires collaboration with other countries and address challenges around harmonising laws with international standards and other legal jurisdictions. The Act also accentuates the importance of collaboration between the law enforcement and private sector. Section 54 of the Act provides that an electronic communications service provider (ECSP) or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must— 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 preserve any information which may be of assistance to the South African Police Service in investigating the offence.

As the major legal instrument for controlling cybercrime in South Africa, one may ask, to what extent has it lived up to the expectations of stemming the tide of cybercrime? In the section that follows, an appraisal of this Act and its effectiveness to cybercrime prosecution will be analysed. Specifically, also, the roles of the South African Police Service in implementing this Act will be looked at.

3. Appraisal of Cybercrime Control in South Africa Under the Cybercrime Act 2021

A major precondition for the enactment of the Cybercrime Act 2021 was the inadequacy of the common law principles to address criminality as novel as cybercrime. It is thus analytically useful to determine whether the Act has provided utility to the criminal justice apparati saddled with the responsibility of curtailing cybercrime in South Africa. The Act has been dubbed a very comprehensive legislation and believed to cover a spectrum of cyber activities that are unlawful under global standards for cybercrime laws (Mabunda, 2021). The Act has transcended the limited finance approach to include such offences such as child exploitation, terrorism and harassment. This is particularly fitting considering that the cyberspace is an alternate reality for most people today. Hence, individuals who have criminal tendencies may find ways to leverage cyber platforms for nefarious activities. The Act is also believed to provide prescient coverage for cybercrime and accommodate emerging technologies. This may be explained using the reality of

cybercriminals constantly evolving new methods. The Act, as argued by Ramluckan and Mkhonza (2021), adopts a victim-centred approach. The Act is attuned to broader collective goals of protecting the vulnerable individuals and has at its core the protection of victims from such offences as revenge porn, cyber harassment and the use of the cyberspace to commit gender-based violence (Mueller & Padayachee, 2021; Botha & Pieterse, 2020).

Oppositely, some scholars have raised concerns about the applicability and functionality of the Act. Mulaudzi raises a concern about the resources and institutional capacity to implement the Act effectively. This position rests on the criticality of technical expertise of law enforcement agencies and their ability to gather digital evidence, conduct cyber forensics, and prosecute offenders if the implementation will be successful. The propensity of the law enforcement officers to overextend in the course of implementing the Act has been adduced. The allowance given to them to intercept communications and access private data could lead to abuse in terms of infringing on privacy and civil liberty, if not diligently regulated (Mueller & Padayachee, 2021). They advance a careful balance between national security interests and individual's inalienable rights in the discharge of their duties. The uncertainty of trans-jurisdictional cooperation, which is a critical requirement for the successful implementation of the cybercrime legal framework, from jurisdictions with weak or non-existent cybercrime laws is another issue that may contend with the implementation the Cybercrime Act. Cybercrime trends have revealed that online criminal behaviours are increasingly originating from regions where sanctions are often non-existent or operate as 'on-costs,' and enforcement is less robust (Broadhurst, 2010). This therefore means that whereas the Act empowers South Africa's criminal justice system to prosecute cyber criminality, it still relies heavily on the cooperation of foreign entities and countries to tackle cybercrime effectively. The challenge of mass awareness and capacity building has been surmised as a major challenge that may contend against the fruitful implementation of the Act. Widespread public education efforts are crucial, according to Nel and Bezuidenhout (2020), in order to make sure that people and organizations know how to stay safe online and adhere to new legal requirements.

Whereas there appears to be a dearth of official statistics on cybercrime prosecution by the South African Police Service, the overwhelming consensus in literature suggests a below-average performance. According to Naidoo (2024), there is a growing concern about the effectiveness of the measures put in place to detect and prosecute cybercrime threats against companies, which relates to SAPS officials'

lack of skills in policing cybercrime (Pillay, Ntuli & Ehiane, 2023). There is still a wide gap between the between the capabilities and ingenuities of cybercriminals and the skills of law enforcement officials (Moyo & Motloutsi, 2021). Paucity of resources, including both financial and technological, has been adduced as a cog in the wheel of justice and prosecution of cybercriminals. The broad spectrum of cyberthreats (ranging from ransomware and hacking to more complex financial fraud) has led to criticism of SAPS for underfunding its cyber sections. The hiring of expert staff as well as the purchase of forensic equipment and software required for investigations are impacted by the tight budget (Govender & MacKenzie, 2020).

In a study aimed at analysing the use of digital evidence for computer fraud in the Springs policing area, Gauteng Province, Ngcobo (2024) found that investigators in the Springs SAPS are unable to successfully deal with computer fraud due to a lack of knowledge, skills, and resources to conduct computer forensics during the investigation of computer fraud. According to Ngcobo, between the fiscal years 2019/2020 and 2020/2021, 88 computer fraud cases were registered at Springs SAPS, and a preliminary case docket analysis to determine whether computer fraud crime scenes were observed during the forensic investigation process to identify digital evidence was conducted. The success rate of these cases in terms of establishing a link through forensic investigation and obtaining a conviction in court was very low. Only 12 cases resulted in convictions and 9 cases resulted in a not guilty sentence, while 25 cases were filed as undetected, and 42 cases were withdrawn in court. While the Cybercrime Act 2021 appears to have provided SAPS with leeway to make progress in terms of investigation and prosecution of cybercrime, significant challenges remain. In the section that follows, discussion will be done on the challenges anonymity and attribution pose to cybercrime and they may be circumnavigated.

4. Anonymity and Attribution Issues in Cybercrime

The threat landscape has changed, and cybercrime is becoming more sophisticated, widespread, and financially impactful. Additionally, there are more criminals and threat actors, which makes jurisdiction a challenge. Prosecuting cybercrime is quite tasking. Attribution is complex in cyber contexts because – cybercriminals hide their identities and just finding the computer or a device with which a cybercrime has been committed is not sufficiently indicative of the actual culprits. When a cybercrime has been detected, having precise prosecutable evidence that pinpoints the actual

perpetrator often requires complex, resource-intensive methods. However, police officers have often the technique described by Boebert (2010) as technical attribution, that is, the identification of the host - any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means - responsible for initiating the attack or cybercrime. Reliance on this technique alone however may not be sufficient except where there is adequate digital evidence, which undeniably links the host to the cybercriminal. Misattributions remain a major impediment to cybercrime prosecution in South Africa (Swate, Sithungu & Lebea 2024).

Often, cybercriminals conceal their IP addresses utilising proxy servers or virtual private networks (VPNs), thus compounding the work that investigators need to do to trace their true location. They also deploy the dark web and use such tools as TOR (The Onion Router) to obscure their identifying information and make intelligence gathering extremely herculean. The multi-layered encryption masks both the criminal's identity and the destination of their communications, and the anonymous nature of cybercrime creates a barrier for law enforcement officials. Cryptocurrencies like Bitcoin are frequently used for financial activities like ransomware payments and money laundering because they provide a level of secrecy that regular banking systems do not. (Bele, 2021). The organised criminal underworld, increasingly, has found a haven in cryptocurrencies. The deliberate planting of false evidence or the execution of attacks from compromised systems by cybercriminals can mislead investigators and give the impression that another party is behind the attacks. This is especially problematic in cases of politically motivated cybercrimes or state-sponsored attacks, as misattribution can have dire diplomatic repercussions. Another angle to anonymity and attribution constraints is that since certain cybercrimes are carried out by mercenary organizations or loose alliances of hackers employed by a third party, it can be very difficult to identify specific members of these groups without intimate knowledge (see Rid, 2020; Goldsmith & Wu, 2006). As a result, it is infamously challenging to demonstrate attribution to the degree needed for legal prosecution. Although courts typically demand a high standard of proof, a large portion of the evidence in cybercrime prosecutions may be technical or circumstantial. Convincing a judge or jury can be challenging since they might not be completely aware of the intricate technology involved.

The foregoing may account for the ineffectiveness of the fight against cybercrime in South Africa. Apart from the documented inadequacies of the South African Police Service (see Burger, 2015; Redpath & Nagla-Luddy, 2015), these issues, clearly, are

difficult to circumnavigate without extensive digital forensics and partnership between the government and the private sector such as cybersecurity firms, technology firms etc, which may enhance police investigative efforts. These companies, usually, possess more resources or specialized knowledge about cyber threats and may be able to assist law enforcement with technical capability.

5. Conclusion

This article has looked at the existential burden that cybercrime places on the South African society and her criminal justice system, especially the South African Police Service. It has shown the country's responsiveness in relation to lawmaking and prosecutorial oversight. Regardless of these efforts, as the paper shows, the cybercrime seems not to reduce in intensity. We have thus argued for an increased focus on the anonymity and attribution problems associated with cybercrime. The problems reflect the growing complexity of the digital landscape with technological advancements empowering criminals to hide and obfuscate their actions. Fortuitously, the digital system also has inherent tools that may help law enforcement agencies to counter these threats. This however requires continuous education of law enforcement officers on technological innovations and adaptation to the evolving nature of cybercrime. Law enforcement officers need to keep abreast of the innovations in digital forensics such as network traffic analysis, blockchain forensics (in the case of cryptocurrencies), and malware reverse engineering, which may provide the necessary digital evidence to unmask cybercriminals. Gathering digital evidence requires high-order skills which traditional policing knowledge and skills may not be sufficient for. Hence, the South African Police Service (SAPS) with other relevant agencies within the South Africa's criminal justice architecture needs to rise to the occasion to combat these non-traditional and intangible crimes by scaling up its investigative and prosecutorial competence.

References

Bele, J. L. (2021). Cryptocurrencies as facilitators of cybercrime. In *SHS Web of Conferences* (Vol. 111, p. 1005). EDP Sciences.

Boebert, W. E. (2010). A survey of challenges in attribution. In *Proceedings of a workshop on Deterring CyberAttacks* (pp. 41-54).

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, *3*(3), 85-110.

Botha, J., & Pieterse, J. (2020). Legal Protections for Vulnerable Internet Users: A Comparative Study of South Africa's Cybercrimes Bill*, Journal of African Law, 64*(3), 415-433.

Broadhurst, R. (2010). A new global convention on cybercrime. *Pakistan Journal of Criminology*, *2*(4), 1-10.

Burger, J. (2015). Assessing review mechanisms of SAPS performance. *SA Crime Quarterly*, *2015*(53), 49-58.

Burman, P. (2021). The Impact of POPIA on South African Businesses. *South African Journal of Information Technology*, 12(2), 45-58.

Chuma, K. G., & Ngoepe, M. (2022). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, *31*(2), 179-195.

Coetzee, J. (2004). The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce. *Stellenbosch Law Review*, *15*(3), 501-521.

Dlamini, N., & Mkhize, M. (2021). Public Awareness of Data Protection Rights in South Africa. *Journal of Public Administration*, 56(2), 213-227.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404.

Du Toit, D. (2020). The Challenges of Implementing POPIA in South Africa. *African Journal of Information Systems*, 10(3), 120-135.

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, *46*(1), 78-109.

Goldsmith, Jack L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York: Oxford University Press.

Govender, D., & MacKenzie, J. (2020). Financial and Technological Limitations in Combating Cybercrime in South Africa. Policing: *An International Journal of Police Strategies & Management, 43*(4), 625-642.

Graham, A. (2023). *Cybercrime: Traditional Problems and Modern Solutions*. Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155-1175.

Hassani, H., Xu, H, & Silva, M. The human digitalisation journey: Technology first at the expense of humans? *Information*, 12(7), 267.

Jogwe, S. (2021). *The compliance of Internet of Things devices with the POPI Act*. Master's thesis, University of Johannesburg, South Africa.

Jones, B. (2021). Is Popia Bad Business for South Africa? Comparing the GDPR to Popia and Analyzing Popia's Impact on Businesses in South Africa. *Penn State Journal of Law and International Affairs*, *10*, 217.

Kwet, M. (2020). Global Data Privacy Trends: South Africa's POPIA in Context. *Journal of Comparative Law & Security Studies*, *5*(1), 34-49.

Mabeka, N. Q. (2021). An analysis of the implementation of the caselines system in South African courts in the light of the provisions of section 27 of the electronic communications and transactions act 25 of 2002: a beautiful dream to come true in civil procedure. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *24*(1).

Mabunda, S. M. (2021). *The South African legislative response to cybercrime*.

Millard, D., & Bascerano, E. G. (2016). Employers' statutory vicarious liability in terms of the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *19*(1).

Mmabatho Aphane, J. M. (2021). South african police service capacity to respond to cybercrime: challenges and potentials. *Journal of Southwest Jiaotong University*, *56*(4).

Moloi, T. (2022). The Role of the Information Regulator in Enforcing POPIA. *South African Law Review*, *67*(4), 102-115.

Moyo, A. (2024). *Cyber criminals hack SA's Legal Practitioners Fidelity Fund*. https://www.itweb.co.za/article/cyber-criminals-hack-sas-legal-practitioners-fidelity-fund/dgp45MaBomLqX9l8.

Moyo, N. & Motloutsi, P. (2021). Challenges in the Investigation and Prosecution of Cybercrime in South Africa. *Journal of Information Warfare, 20*(2), 45-61.

Mueller, J., & Padayachee, K. (2021). Surveillance, Privacy, and the Cybercrimes Act: A Critical Review. *African Journal of Information Security, 5*(3), 112-127.

Mulaudzi, T. (2021). The Cybercrimes Act: Enforcement Challenges in South Africa. *Journal of Cybersecurity Law*, *12*(2), 89-102.

Myovella, G., Karacuka, M., & Haucap, J. (2020). Digitalization and economic growth: A comparative analysis of Sub-Saharan Africa and OECD economies. *Telecommunications Policy*, *44*(2), 101856.

Naidoo, R., & Naidoo, R. (2021). Corporate Governance and Data Privacy: Lessons from POPIA. *Journal of Corporate Law Studies*, *28*(3), 55-70.

Naidoo, S. (2024). *The effectiveness of detection and prosecution of cybercrime threats against companies in South Africa*. https://wiredspace.wits.ac.za/items/e4f2c8c0-6ae8-4360-92a1-24847c04d16b.

Nel, S., & Bezuidenhout, C. (2020). Cybercrime in South Africa: A Public Awareness Perspective, *South African Law Review*, *37*(1), 45-60.

Ngcobo, M. A. T. (2024). *Analyzing the use of digital evidence for computer fraud in the Springs policing area, Gauteng Province*.

https://www.academia.edu/119030682/Analysing_the_use_of_Digital_Evidence_for_Computer_Fraud_in_the_Springs_Policing_Area.

Oreku, G. S., & Mtenzi, F. J. (2017). Cybercrime: Concerns, challenges and opportunities. *Information Fusion for Cyber-Security Analytics*, 129-153.

Phakathi, S. (2022). Economic Impacts of POPIA Compliance on SMEs in South Africa. *Journal of Economic Studies*, 47(6), 132-148.

Ramluckan, T., & Mkhonza, S. (2021). Cybercrimes Act: A Lifeline for Victims of Online Harassment and Revenge Porn in South Africa. *South African Journal of Information and Communication Technology, 28*(2), 34-46.

Redpath, J., & Nagla-Luddy, F. (2015). 'Unconscionable and irrational' SAPS human resource allocation. *South African Crime Quarterly*, *53*, 15-26.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Sekati, P. N. M. (2022). *Assessing the effectiveness of extradition and the enforcement of extra-territorial jurisdiction in addressing trans-national cybercrimes*.

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299-323.

Spiezia, F. (2022, May). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. In *ERA Forum* (Vol. 23, No. 1, pp. 101-108). Berlin/Heidelberg: Springer Berlin Heidelberg.

Statista (2024). *Internet usage worldwide - Statistics & Facts*. https://www.statista.com/topics/1145/internet-usage-worldwide/#topicOverview.

Theys, M. W. (2020). *Exploring compliance with the protection of Personal Information Act: implementation considerations in small software development companies in South Africa*. Doctoral dissertation, Cape Peninsula University of Technology.

Van der Merwe, A. (2023). Enforcement Challenges under South Africa's POPIA. *Journal of African Law*, *67*(1), 89-102.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?. *International Cybersecurity Law Review*, *1*(1), 63-72.