A CRITICAL ANALASIS OF THE DEVELOPMENT AND EFFICACY OF SOUTH AFRICA'S CYBERSECURITY LAWS IN COMBATING CYBERCRIMES

by

LUCKY APPRECIATE KHOZA
(47240784)

submitted in accordance with the requirements for the degree of

MASTER OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR NOMBULELO QUEEN MABEKA

2026

DECLARATION

Student Number: 47240784

I, Lucky Appreciate Khoza do hereby confirm and declare that my dissertation is my own.

I further declare that I have cited all the sources that I referred to in the dissertation. I also confirm that the sources are incorporated into the footnotes and they are fully referenced in the bibliography.

……

TABLE OF CONTENTS

Chapter 1: Research Background and Methodology

1. **Introduction**……..7
2. **Background**..……..**10**
   - *2.1. The growing threat of cybercrime and legislative responses in South Africa..10*
   - *2.2. Judicial precedents shaping cybercrime liability in South Africa*……11
   - *2.3. Emerging concerns in South Africa's cybersecurity legal framework*……...15
   - *2.4. Conceptual and definitions framework*……...18
3. **Problem statement**……21
   - *3.1. Introduction*……..21
   - *3.2. Legal challenges in combating cybercrime in South Africa*……23
   - *3.3. Judicial perspectives on cybersecurity law deficiencies*……...24
   - *3.4. Gaps in South Africa's cybersecurity laws and international alignment*……27
4. **Research objectives**……30
5. **Research question**……31
6. **Research methodology**……31
7. **Literature review**……31
8. **Overview of chapters**…...……43
   - *8.1. Chapter One*……...43
   - *8.2. Chapter Two*……...43
   - *8.3. Chapter Three*……44
   - *8.4. Chapter Four*……...44
   - *8.5. Chapter Five*……...44

Chapter 2: The Evolution of Cybersecurity Laws in South Africa

1. **Introduction**……45
2. **Conceptualising Cybercrime in the South African context**……...46
3. **Early legislative responses to the digital era**……46
4. **The Electronic Communications and Transactions Act (ECTA) (2002)**……47
   - *4.1. Judicial engagement*……..51
5. **Regulation of Interception of Communications Act (RICA) (2002)**……..52

5.1. Judicial engagement……..57

6. ICASA's role in South Africa's Cybersecurity Framework……57

7. The South Africa National Cybersecurity Policy Framework (NCPF) (2012)……59

8. The Protection of Personal Information Act (POPIA) (2013)……61

8.1. Processing limitation provisions and sectoral Cybersecurity……..62

8.1.1. Section 9 - Lawfulness of processing……63

8.1.2. Section 10 – Minimality……63

8.1.3. Section 11 - Consent, justification, and objection……64

8.1.4. Section 12 - Collection directly from the data subject……65

8.2. Synthesis……..66

8.3. Judicial engagement……..67

9. The Critical Infrastructure Protection Act 8 of 2019 (CIPA)……..68

10. The Cybercrimes Act 19 of 2020……...70

10.1. Procedural and Enforcement Mechanisms……..74

10.2. Judicial Engagement……....*76*

11. SAPS SOPs under Section 26 of the Cybercrimes Act……77

12. Sector-Specific Cybersecurity laws……79

13. Provisional conclusion……...80

Chapter 3: Evaluating the Effectiveness of South Africa's Cybersecurity Legal Framework

1. Introduction……83

2. Institutional and Legislative coherence……..85

3. Efficacy of the Cybercrimes Act 19 of 2020……...89

4. The role of POPIA in Cyber resilience…….94

5. Operational and enforcement challenges……..97

6. Constitutional and Human-Rights dimensions……..102

7. Judicial engagement and interpretation……...104

8. Policy and strategic implementation……106

9. Synthesis and findings……..109

10. Provisional conclusion……..110

Chapter 4: A Comparative Analysis of EU and US Cybersecurity Governance and their Influence on South Africa's Cybersecurity Legal Framework

1. **Introduction**……..113
2. **The Budapest Convention on Cybercrime**……...116
   - *2.1. Substantive and procedural harmonisation*……..116
   - *2.2. The 24/7 Network and real-time cooperation*……...117
   - *2.3. Implications of South Africa's non-ratification*……..119
   - *2.4. The Second Additional Protocol and emerging standards*……120
   - *2.5. Analytical summary*……..121
3. **The EU Cybersecurity governance framework**……...121
4. **The US Cybersecurity governance framework**……...130
5. **Comparative analysis**……136
   - *5.1. Comparative analysis between South Africa and the European Union*……...136
   - *5.2. Comparative analysis between South Africa and the United States*……...141
6. **Provisional conclusion**……..150

Chapter 5: Conclusion and Recommendations

1. **Final Conclusion**……151
2. **Gaps identified**……153
   - *2.1. Gaps identified in the current legislation*……...153
   - *2.2. Institutional fragmentation as a structural weakness*……..154
   - *2.3. Enforcement deficits and the legitimacy of Cybercrime law*……..155
   - *2.4. POPIA's preventative contribution and its structural limits*……155
   - *2.5. Deficits in International cybercrime cooperation*……..156
3. **Recommendations**……..157
   - *3.1. Ratification of the Budapest Convention on Cybercrime*……...157
   - *3.2. Harmonisation of Cybercrime-related legislation*……158
   - *3.3. Full operationalisation of the Cybercrimes Act*……159
   - *3.4. Digital evidence, cloud data and procedural reform*……...161

4. Institutional and policy recommendations……..161

*4.1. Strengthening Cybercrime investigation and prosecution capacity……..*161

*4.2. Clarifying institutional mandates and national coordination……..*162

*4.3. Enhancing public–private cooperation and information sharing……...*163

*4.4. Adapting institutional capacity to emerging technologies……..*164

5. Concluding reflections……..164

Bibliography……...166

Chapter 1: Research Background and Methodology

1 Introduction

Information and Communication Technologies (ICTs) are now essential to the functioning of modern society.[1] The digital age has ushered in a paradigm shift across the globe, reshaping how individuals, businesses, and governments communicate, transact, and operate. This technological evolution has enabled profound efficiencies and innovations, but it has also created an environment where cybercrime flourishes. The rapid integration of digital technologies into daily life has changed communication, governance, social interaction, and business.[2] In today's digital era, the world is more interconnected than ever before.[3] However, this technological advancement has also brought forth the rise of cybercrime. This is a global issue that puts corporate security, individual privacy, and national infrastructure at risk. Significant cybersecurity issues confronting the African continent are highlighted in the International Criminal Police Organization (INTERPOL) African Cyberthreat Assessment Report (2021).[4] The report lists the most common types of cybercrime, such as ransomware, botnet attacks, digital extortion (particularly sextortion), business email compromise, and online scams (mostly phishing).[5] It emphasises how businesses and vital infrastructure are becoming increasingly vulnerable, especially since the majority of African enterprises lack adequate cybersecurity procedures.[6] South Africa, a young nation with a developing digital economy, has faced unique challenges in combating cybercrime. In just one week in February 2023, INTERPOL private partner Kaspersky reportedly detected over 300 cases of ransomware attempts in South Africa, which illustrates the increasing

---

1 Sagwadi Mabunda, 'The South African legislative response to cybercrime' (Doctoral Thesis, University of Western Cape 2021) 1.

2 Riki Thompson, 'The Digital Revolution: How Technology is Changing the Way We Communicate and Interact' (*Visual Life*, 9 June 2023) <https://rikithompson.ds.lib.uw.edu/visuallife/the-digital-revolution-how-technology-is-changing-the-way-we-communicate-and-interact/> accessed 1 March 2025.

3 Debra Littlejohn Shinder and Michael Cross, Scene of the Cybercrime (2nd edn, Elsevier 2008) 2.

4 INTERPOL, 'African Cyberthreat Assessment Report' (*INTERPOL*, October 2021) <https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf> accessed 1 March 2025.

5 INTERPOL, 'African Cyberthreat Assessment Report'.

6 INTERPOL, 'African Cyberthreat Assessment Report'.

frequency of attacks.[7] A recent survey indicates that South Africa was the fifth most affected country globally by cybercrime in 2022, with approximately 5.6% of internet users falling victim to such crimes.[8] The South African National Cybersecurity Policy Framework provides a comprehensive approach to tackling cybersecurity threats, emphasizing the importance of collaboration between public and private sectors.[9] This study seeks to evaluate the effectiveness of South Africa's cybersecurity legal framework in deterring and combating cybercrimes in compliance with international standards, worldwide best practices, and constitutional principles.

Among the key pieces of legislation that form the cornerstone of South Africa's legislative framework for combating cybercrime are as follows: the Cybercrimes Act 19 of 2020,[10] the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA),[11] the Electronic Communications and Transactions Act 25 of 2002 (ECTA),[12] the Protection of Personal Information Act 4 of 2013 (POPIA),[13] the National Cybersecurity Policy Framework.[14] The Cybercrimes Act, in particular, combines charges such as harmful communications, unauthorised access, and data interference and establishes procedural mechanisms for investigation and enforcement.[15] Despite these developments, the effectiveness of the Cybercrimes Act in addressing rapidly evolving cyber threats, ensuring effective enforcement, and upholding constitutional rights such as the right to privacy (section

---

7 Carrin Smith, 'RSAWEB Victim of Cyberattack as Wave of Ransomware Attempts Hits SA in Past Week' (*News24*, 6 February 2023) <https://www.news24.com/News24/rsaweb-victim-of-cyberattack-as-wave-of-ransomware-attempts-hits-sa-in-past-week-20230206> accessed 5 March 2025.

8 Defenceweb, 'South Africa in Top Five Countries Affected by Cybercrime in 2022' (*Defenceweb*, 28 April 2023) <https://www.defenceweb.co.za/cyber-defence/south-africa-in-top-five-countries-affected-by-cybercrime-in-2022/> accessed 10 March 2025.

9 State Security Agency, National Cybersecurity Policy Framework (Government Gazette No 39475, 4 December 2015).

10 Cybercrimes Act 19 of 2020 (hereinafter Cybercrimes Act).

11 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (hereinafter RICA).

12 Electronic Communications and Transactions Act 25 of 2002 (hereinafter ECTA).

13 Protection of Personal Information Act 4 of 2013 (hereinafter POPIA).

14 National Cybersecurity Policy Framework (hereinafter NCPF).

15 Cybercrimes Act, ss 2 - 13.

14) and the right to access information (section 32) remains a subject of critical legal and academic inquiry.[16]

KaMtuze contends how the Cybercrimes Act significantly enhances the nation's legal system by resolving the issues with previous laws such as the ECTA.[17] He emphasises that the Cybercrimes Act is an addition to the POPIA, which focuses on safeguarding personal data, and highlights how it also criminalises hacking, fraud, and the unauthorised dissemination of data.[18] This convergence of regulations reflects South Africa's dedication to safeguarding data privacy and thwarting the rising number of cybercrimes.[19] KaMtuze argues that despite South Africa's laws having made tremendous progress there are still challenges with enforcement and adjusting to new cyberthreats.[20]

The basis for evaluating the sufficiency of cybersecurity laws is the Constitution of the Republic of South Africa, 1996,[21] which is the supreme law of the land. The right to freedom and security, which includes defense against damage and violence, is guaranteed under section 12[22] and extends to the online sphere. Additionally, section 7[23] underscores the state's obligation to uphold, advance, and implement these rights, putting pressure on lawmakers and decision-makers to pass strong legislation that will successfully combat cybercrimes while preserving constitutional liberties.[24]

Taking a holistic approach, this study looks at how statutory provisions, constitutional demands, judicial interpretation, and international standards interact. The study aims to examine potential gaps, analyse the effectiveness of current measures, and explore possible recommendations for developing a more unified and effective legislative

16 Sizwe Snail kaMtuze, 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43(3) Obiter 536, 552.
17 Snail, 'Convergence of Cybercrime and Data Protection Laws' 554.
18 Snail, 'Convergence of Cybercrime and Data Protection Laws' 554.
19 Snail, 'Convergence of Cybercrime and Data Protection Laws' 555.
20 Snail, 'Convergence of Cybercrime and Data Protection Laws' 556.
21 Constitution of the Republic of South Africa, 1996 (hereinafter referred to as Constitution).
22 Constitution, s 12.
23 Constitution, s 7.
24 Snail, 'Convergence of Cybercrime and Data Protection Laws' 556.

framework to combat cybercrimes by critically examining the evolution cybersecurity laws in South Africa. In addition to addressing the pressing issues of cybercrime, the research adds to the larger conversation about protecting digital ecosystems while maintaining respect for human rights and the constitution.[25]

2 Background

2.1 *The growing threat of cybercrime and legislative responses in South Africa*

As South Africa grows more digitally connected, the surge in cybercrimes has placed a great burden on citizens, companies, and government systems.[26] The National Cybersecurity Policy Framework (NCPF)[27] was introduced as a strategic document aimed at addressing the growing challenges of cybersecurity in the country. The NCPF outlines roles for various stakeholders, including government bodies, private organizations, and international partners, to collectively improve cybersecurity measures.[28] The NCPF addresses a wide range of cybersecurity issues, from data privacy and protection to critical infrastructure security.[29] The necessity for strong and all-encompassing regulatory frameworks to handle these new risks is exposed by the widespread cyberattacks that South African banks and telecoms have experienced.[30] To counter these changing risks, important legislative tools have been established, such as the POPIA and the Cybercrimes Act.[31]

Identity theft, cyber fraud, and unauthorised access to computer systems are among some of the offenses that are made illegal by the Cybercrimes Act.[32] It provides victims

---

25 Constitution.

26 South African Banking Risk Information Centre (SABRIC), 'Annual Crime Statistics 2023' (*SABRIC*, 2024) <https://www.sabric.co.za/media/vjyn5f4d/sabric-annual-crime-stats-2023-2.pdf> accessed 8 March 2025.

27 NCPF.

28 NCPF.

29 NCPF.

30 Amira Sadeeh, 'Cyber Resilience Framework in South Africa' (*Inside Telecom*, 02 December 2022) <https://insidetelecom.com/cyber-resilience-framework-cyber-governance-in-south-africa/> accessed 15 March 2025.

31 Sizwe Snail, 'Legal Intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cybercrimes Act 19 of 2020' (*Community Manager*, 15 June 2021) <https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/> accessed 19 March 2025.

32 Cybercrimes Act, ss 2, 7, 8.

and law enforcement with the resources they need to look into and prosecute these crimes. POPIA prioritises safeguarding of people's personal data and ensures that organizations and companies implement adequate data security measures in order to stop cybercrime such as identity theft and data breaches.[33] However, while the Cybercrimes Act marks a significant advance in regulating cyberspace, experts like Papadopoulos and kaMtuze contend that a holistic and integrated approach is required for properly addressing both cybercrime and personal data protection in South Africa.[34] They point out that while POPIA offers some protection for people's personal information, more work is required to align more closely with larger cybersecurity regulations and effectively address the complexity of contemporary cyber threats [35]

2.2 *Judicial precedents shaping cybercrime liability in South Africa*

The legal environment surrounding cybercrime has been influenced by a number of South African court rulings in addition to these legislative frameworks. *Edward Nathan Sonnenberg Inc v Judith Mary Hawarden* [36] is one noteworthy case. In this instance, a phishing scam where scammers impersonated law firm personnel resulted in a client of the firm being deceived into sending money. Due to inadequate cybersecurity precautions, the North Gauteng High Court initially declared the legal business accountable for the fraud.[37] The Supreme Court of Appeal, however, reversed this ruling, emphasising that the client was also accountable for confirming the communication's legitimacy.[38] This judgment reaffirms the significance of shared responsibility between customers and corporations and brings to light the difficulty of establishing liability in cybercrime situations.[39]

---

33 POPIA, s 53.

34 Sylvia Papadopoulos and Sizwe Snail kaMtuze, *Cyberlaw @ SA: The Law of the Internet in South Africa* (4th edn, Van Schaik 2021) 504.

35 Papadopoulos and Snail, *Cyberlaw @ SA* 504.

36 *Edward Nathan Sonnenberg Inc v Hawarden* (421/2023) [2024] ZASCA 90 (10 June 2024) (hereinafter '*ENS Inc v Hawarden*').

37 *ENS Inc v Hawarden* [1].

38 *ENS Inc v Hawarden* [25].

39 *ENS Inc v Hawarden* [25].

First National Bank of Southern Africa Ltd v Duvenhage[40] is another noteworthy case in which the court considered a financial institution's liability in a phishing fraud. Fraudsters posing as FNB representatives deceived the consumer into giving them their banking information. Because the bank had adopted appropriate security measures and had warned consumers about the dangers of phishing, the Western Cape High Court concluded that the bank could not be held responsible for the loss. This case confirmed that banks and other financial organizations are not necessarily held strictly accountable for cybercrimes, provided they put in place suitable security measures.

In *Global & Local Investments Advisors (Pty) Ltd v Fouché*,[41] the Supreme Court of Appeal clarified the legal standing of electronic signatures under the Electronic Communications and Transactions Act 25 of 2002 (ECTA).[42] Mr Fouché had mandated Global to act as his investment agent, requiring all instructions to be sent via email or fax with his signature.[43] In 2016, fraudsters hacked Mr Fouché's email account and sent instructions bearing only the typewritten name "Nick".[44] Acting on these, Global paid out R804 000 to unknown third parties.[45] Mr Fouché denied authorising the transfers and sued for the recovery of the funds.[46]

Both the High Court and SCA ruled in favour of Mr Fouché, finding that the mandate required a proper signature and that the typewritten name did not meet the threshold under section 13 of ECTA.[47] The courts held that there was no agreement to use electronic signatures and that a signature remains critical to verifying authority and consent.[48] This case reaffirms the importance of clear contractual terms and robust

---

40 *First National Bank of South Africa Ltd v Duvenhage* 2006 (5) SA 319 (SCA) (hereinafter '*FNB v Duvenhage*').
41 *Global & Local Investments Advisors (Pty) Ltd v Fouché* (SCA) (unreported case no 71/2019, 18-3-2020) (hereinafter '*Global* case').
42 *Global* case [4]-[7].
43 *Global* case [2].
44 *Global* case [3].
45 *Global* case [3].
46 *Global* case [6].
47 *Global* case [7]-[8], [14]-[16].
48 *Global* case [14].

authentication in electronic transactions, particularly in today' s climate where cyber fraud is prevalent.[49]

In *Fourie v Van Der Spuy & De Jongh Inc and Others*,[50] a client sued his attorneys after one of them negligently transferred his funds from the law firm's trust account to fraudsters' accounts, following email instructions from a hacked email address. The attorney failed to verify the new banking details, despite being made aware of the risks of cyber fraud in the legal profession.[51] The High Court held that the attorney had breached her fiduciary duty by not taking the reasonable steps in order to prevent fraud. as a result, both her and the law firm were found jointly liable for the loss.[52]

The case illustrates the real-world impact of cybercrime on professionals and clients, and the legal duties imposed on service providers to exercise care in the handling of client funds. It also demonstrates the limitations of the legal framework at the time, as the hackers were never identified or prosecuted.[53] The case underscores the importance of the Cybercrimes Act, which now criminalises unlawful access and cyber fraud and provides a stronger legal basis for addressing such offences.[54] Effective enforcement remains key to protecting victims and holding cybercriminals accountable.

In *Hartog v Daly and Others*,[55] a conveyancer, Mr Hartog, was orally mandated to transfer proceeds from a property sale involving Bridgitte Daly, her late co-owner Karin Foulkes-Jones, and Bridgitte's husband, Patrick Daly.[56] After the sale, Hartog paid R100,000 to the deceased estate and intended to pay the R1.4 million balance to

---

49 *Global* case [17].

50 *Fourie v Van der Spuy and De Jongh Inc. and Others* (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) (hereinafter '*Fourie v Van der Spuy*').

51 *Fourie v Van der Spuy* [30].

52 *Fourie v Van der Spuy* [31].

53 Preeta Bhagattjee, Aphindile Govuza and Liam Seban, 'Cybercrime in South Africa – Attorneys Fall Victim to Cyber Fraud' (*Cliffe Dekker Hofmeyr*, 18 Feb 2020) <https://www.cliffedekkerhofmeyr.com/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html> accessed 6 May 2025.

54 Cybercrimes Act, ss 2 - 13.

55 *Hartog v Daly and Others* (A5012/2022) [2023] ZAGPJHC 40; [2023] 2 All SA 156 (GJ) (24 January 2023) (hereinafter '*Hartog v Daly*').

56 *Hartog v Daly* [4]-[6].

Patrick Daly.[57] However, a fraudster intercepted the email communication, altered the banking details, and Hartog unknowingly transferred the funds to the fraudster's account.[58]

Hartog's clients approached the court to recover the stolen funds. Hartog, in turn, argued that the bank should be held liable for failing to prevent the fraud.[59] He claimed the bank was negligent in its FICA compliance, failed to verify account names against numbers, and did not monitor the fraudulent account.[60] The court rejected these arguments, confirming that the bank had complied with FICA and followed industry norms where EFTs rely solely on account numbers. The court held that the bank owed no legal duty to verify names or monitor accounts and dismissed Hartog's delictual claim with costs, finding no wrongful conduct or negligence on the part of the bank.[61]

In *Gerber v PSG Wealth Financial Planning*,[62] the court was asked to determine whether PSG had a contractual duty to protect its client from financial loss caused by cybercrime following the fraudster's success in deceiving the company into transferring funds. The court ruled in the client's favour and held that PSG failed to take reasonable steps to prevent the loss, despite having a duty to use appropriate systems and procedures to guard against such risks.[63] This case affirms the legal obligation of financial institutions to implement effective cybersecurity measures and reinforces the potential liability they face if they fail to protect clients from cyber-related fraud.[64] This aligns with academic criticism that the Cybercrimes Act focuses disproportionately on password-related crimes while neglecting sophisticated threats like business email compromise (BEC) fraud.[65]

---

57 *Hartog v Daly* [6].
58 *Hartog v Daly* [7]-[9].
59 *Hartog v Daly* [9]-[10], [12].
60 *Hartog v Daly* [95]-[97].
61 *Hartog v Daly* [111]-[119].
62 *Gerber v PSG Wealth Financial Planning (Pty) Ltd* (36447/2021) [2023] ZAGPJHC 270 (23 March 2023) (hereinafter '*Gerber v PSG*').
63 *Gerber v PSG* [59].
64 *Gerber v PSG* [99].
65 Nombulelo Queen Mabeka, 'The Cybercrimes Act 19 of 2020, Section 7 versus Civil Proceedings' (2024) 38(2) Speculum Juris 419, 430.

2.3 *Emerging concerns in South Africa's cybersecurity legal framework*

The Cybercrimes Act, in regulating the entire terrain of cybercrime as it is perceived currently, offers greater legal protection for victims of cybercrimes, guidance to law enforcement agencies and legal certainty for the courts. The creation of specific offences as well as sentences marks a progression towards more efficient cybercrime regulation than was previously afforded in terms of the common law and ECTA.[66] Notwithstanding these advancements, it is necessary to examine whether South Africa's cybersecurity laws sufficiently address emerging cyber threats and enforcement challenges. Despite not having ratified the Budapest Convention[67] in its entirety, South Africa has demonstrated its commitment to implementing international best practices in cybersecurity by engaging in international talks.[68]

The Budapest Convention aims to enhance international cooperation in the prevention and prosecution of cybercrime and is widely recognised as the first international treaty specifically addressing offences committed through the internet and other computer networks.[69] Although South Africa independently implemented an extensive legislative framework, such as the POPIA and the Cybercrimes Act, the extent to which South Africa's non-ratification of the Budapest Convention affects its ability to engage in cross-border cybercrime cooperation is critically assessed.[70] Accordingly, the role of the Budapest Convention in strengthening international cooperation is examined within the context of South Africa's cybersecurity legal framework.[71]

Nonetheless, South Africa's participation in regional agreements like the 2014 African Union Convention on Cyber Security and Personal Data Protection[72] promotes

66 Snail, 'Convergence of Cybercrime and Data Protection Laws' 559-560.
67 Convention on Cybercrime (ETS No. 185) (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 (Convention on Cybercrime).
68 Trishana Ramluckan, 'International Humanitarian Law and its Applicability to the South African Cyber Environment' (2020) 19(3) Journal of Information Warfare 102, 117.
69 Nombulelo Queen Mabeka and Fawzia Cassim, 'Interpreting the Provisions of the Cybercrimes Act 19 of 2020 in the Context of Civil Procedure: A Future Journey' (2023) 44(1) Obiter 19, 30.
70 Snail, 'Convergence of Cybercrime and Data Protection Laws' 558.
71 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 31.
72 African Union, African Union Convention on Cyber Security and Personal Data

cooperation with other African countries on cybersecurity issues.[73] Cybercrime is an urgent global challenge, and it is necessary to examine whether the Cybercrimes Act adequately addresses the issue of international cooperation.[74]

While national legal frameworks and court rulings indicate progress, it is necessary to examine whether challenges persist.[75] The Cybercrimes Act does not explicitly define the term “cybercrime”, a gap which may create ambiguity in distinguishing between traditional offences and their cyber-enabled variants.[76] The Cybercrimes Act’s failure to define cybercrime results in courts grappling with whether to apply the provisions of section 8 of the Cybercrimes Act or common law fraud principles.[77] Mabunda argues that cyberfraud is not a "true cybercrime" as it could remain prosecutable under common law fraud despite the internet component.[78] While the Cybercrimes Act mentions financial institutions and organs of state in the context of aggravated offenses, it does not prescribe sector-specific cybersecurity obligations, namely, mandatory breach reporting for banks or hospitals.[79]

Significant sections of the Cybercrimes Act such as provisions of chapter 5 on mutual legal assistance, the designated point of contact as stipulated in chapter 6, and protection orders against cyber harassment and revenge pornography (illustrated in part VI) are not yet in force. This raises questions regarding the practical utility of the Cybercrimes Act.[80] A key criticism against the revenge porn provision of the Cybercrimes Act is that criminal liability applies solely to the original perpetrator who

---

Protection (adopted 27 June 2014, entered into force 8 June 2023) 29560 Treaty No 0048 (Malabo Convention).

73 Uchenna Jerome Orji, ‘The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?’ (2018) 12(2) Masaryk University Journal of Law and Technology 91, 122.

74 Casper Lötter, ‘A Comparative Critique of the Cybercrimes Act 19 of 2020: Positioning South Africa vis-à-vis Australia’ (2025) 28 PER / PELJ 2, 2.

75 Snail and Musoni, 'Overview of Cybercrime Law' 300.

76 Snail and Musoni, 'Overview of Cybercrime Law' 307.

77 Snail and Musoni, 'Overview of Cybercrime Law' 313.

78 Sagwadi Mabunda, ‘Is it Cyberfraud or Good Ol’ Offline Fraud: A Look at Section 8 of the South African Cybercrimes Bill’ (2018) 2 Journal of Anti-Corruption Law 58, 60.

79 Snail and Musoni, 'Overview of Cybercrime Law' 316.

80 Snail and Musoni, 'Overview of Cybercrime Law' 319, 320.

first disseminates the sexually graphic images; there are no real consequences for any subsequent sharing by third parties.[81]

It appears that there is overlapping of criminalisation in various statutes such as RICA, ECTA, POPIA, and Cybercrimes Act which may contribute to confusion and enforcement inconsistencies.[82] With provisions dispersed among several pieces of legislation, including the POPIA[83] and the Cybercrimes Act,[84] This study examines whether South Africa's cybersecurity laws remain fragmented and whether this affects enforcement coherence. This dispersion raises questions regarding the development of a coherent and integrated cybersecurity legal framework.[85] This raises questions regarding the extent to which alignment with international standards affects the effectiveness of South Africa's cybersecurity legal framework. The legislation appears to focus more on punitive measures rather than preventive cybersecurity strategies, raising concerns about its overall impact.[86] Another noted shortcoming is that the Cybercrimes Act fails to clarify whether civil proceedings can run concurrently with criminal proceedings.[87] To effectively tackle changing cyber threats, Murdoch Watney suggests that strengthening public-private cooperation and alignment with global best practices may be necessary.[88]

Papadopoulos and kaMtuze argue that criminal law already provides for the criminalisation of a range of online activities, and caution against fragmented or overlapping legislative provisions across different statutes.[89] They point out that a piecemeal approach to cybercrime regulation characterised by duplication and overregulation should be avoided, as it poses risks for legal uncertainty, inefficiency,

---

81 Snail and Musoni, 'Overview of Cybercrime Law' 318.
82 Snail and Musoni, 'Overview of Cybercrime Law' 306, 310, 318.
83 POPIA.
84 Cybercrimes Act.
85 Murdoch Watney, 'Exploring South Africa's Cybersecurity Legal Framework Regulating Information Confidentiality, Integrity, and Availability' (2024) 19(1) Proceedings of the 19th International Conference on Cyber Warfare and Security 430, 430.
86 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 21.
87 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 32.
88 Watney, 'South Africa's Cybersecurity Legal Framework' 432.
89 Papadopoulos and Snail, *Cyberlaw @ SA* 465.

and inconsistent enforcement.[90] Instead, a coherent, harmonised legislative framework is necessary to ensure clarity, effectiveness, and compliance with constitutional principles.[91] There remains considerable room for improvement in order to ensure South Africa is a robust, cyber-secure space.[92]

Van der Merwe critically assesses the shortcomings of the Cybercrimes Act, arguing that the Act suffers from definitional ambiguities, particularly with respect to aggravated offences, which in turn create uncertainty in both legal interpretation and enforcement.[93] This lack of clarity can hinder consistent prosecution and may affect the Cybercrimes Act's ability to respond effectively to diverse forms of cybercrime. Furthermore, concerns have been raised regarding the Cybercrimes Act's procedural provisions, notably jurisdiction and the handling of digital evidence areas. Given the transnational nature of majority cyber offences, these are fundamental.[94] The authors contend that the Cybercrimes Act lacks sufficient procedural tools to address these complexities. Such shortcomings highlight the broader need for a harmonised and practically enforceable cybersecurity legal framework in alignment with South Africa's evolving digital landscape.

2.4 *Conceptual and definitions framework*

For clarity and consistency, this study adopts the following key concepts and definitions, which underpin the evaluation of South Africa's cybersecurity legal framework:

Cybercrime

Cybercrime refers to unlawful acts committed through or against computer systems, networks, or data. It includes offences such as unauthorised access, data interference, cyber fraud, and malicious communications.[95] Although the Cybercrimes Act 19 of 2020

---

90 Papadopoulos and Snail, *Cyberlaw @ SA* 466.
91 Papadopoulos and Snail, *Cyberlaw @ SA* 467.
92 Lötter, 'Comparative Critique of the Cybercrimes Act' 22.
93 Dana van der Merwe and others, *Information and Communications Technology Law* (3rd edn, LexisNexis 2022) 70-74.
94 van der Merwe and others, *Information and Communications Technology Law* 91-92.
95 Cybercrimes Act; Convention on Cybercrime.

criminalises a range of cyber-related conduct, it does not provide a comprehensive definition of “cybercrime”, requiring interpretive reliance on statutory provisions and academic discourse.

Cybersecurity

Cybersecurity refers to the protection of information systems, networks, and data from unauthorised access, disruption, or damage. It encompasses legal, technical, and organisational measures aimed at safeguarding the confidentiality, integrity, and availability of information.[96]

Information System

An information system refers to any device or interconnected group of devices that perform automated data processing. This definition aligns with international instruments such as the Budapest Convention and informs the interpretation of cyber-related offences within South African law.[97]

Data

Data refers to electronic representations of information, including text, images, audio, or software, capable of being processed, stored, or transmitted by a computer system.[98]

Digital Evidence

Digital evidence refers to information of evidentiary value that is stored or transmitted in digital form. This includes emails, databases, system logs, and electronic communications. Within the South African context, the regulation, preservation, and admissibility of digital evidence remain procedurally underdeveloped, particularly in transnational and cloud-based environments.[99]

---

96 International Organization for Standardization, ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity (ISO 2012) (‘ISO 27032’).

97 Convention on Cybercrime.

98 Convention on Cybercrime.

99 van der Merwe and others, *Information and Communications Technology Law.*

Cyber Resilience

Cyber resilience refers to the capacity of systems, institutions, and legal frameworks to anticipate, withstand, respond to, and recover from cyber incidents. It extends beyond preventative cybersecurity measures to include continuity, recovery, and adaptive capabilities.[100]

Enforcement

Enforcement refers to the practical implementation of legal provisions through investigation, prosecution, and adjudication. In the context of this study, enforcement includes the operational effectiveness of institutions such as the South African Police Service (SAPS), the National Prosecuting Authority (NPA), and the judiciary.[101]

Institutional Coordination

Institutional coordination refers to the alignment and cooperation between state institutions, regulatory bodies, and private-sector actors in addressing cybersecurity threats. Effective coordination is essential for ensuring institutional coherence and reducing fragmentation within the cybersecurity governance framework.[102]

Operationalisation

Operationalisation refers to the extent to which legislative provisions are translated into practical, enforceable mechanisms through regulations, institutional capacity, and procedural clarity. A lack of operationalisation may result in a gap between statutory intent and enforcement effectiveness.[103]

International Cooperation

---

100 World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards (World Economic Forum 2017) <https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf> accessed 6 April 2026.

101 Cybercrimes Act; National Prosecuting Authority Annual Report 2023/24.

102 NCPF.

103 Cybercrimes Act; Proclamation R42 GG 45562 (30 November 2021).

International cooperation refers to cross-border collaboration between states in the prevention, investigation, and prosecution of cybercrime. This includes mutual legal assistance, information sharing, and participation in international frameworks such as the Budapest Convention on Cybercrime.[104]

Personal Information

Personal information is defined in terms of the Protection of Personal Information Act 4 of 2013 (POPIA) as information relating to an identifiable natural or juristic person. The protection of personal information forms a central component of South Africa's cybersecurity regulatory framework.[105]

Electronic Communication

Electronic communication refers to the transmission of data, text, images, or voice through electronic systems or networks, as regulated under the Electronic Communications and Transactions Act 25 of 2002.[106]

These concepts provide the analytical foundation for evaluating the effectiveness, coherence, and enforcement of South Africa's cybersecurity legal framework throughout this study.

3 Problem statement

3.1 *Introduction*

Global communication, economics, and civilizations have evolved as a result of rapid development of digital technologies, which conversely revealed both vulnerabilities and the enormous potential created.[107] Cybercrime has emerged as a serious threat to

---

104 Convention on Cybercrime; African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023).

105 POPIA, s1.

106 ECTA, s1.

107 World Economic Forum, 'The Global Risks Report 2022' (*WEF*, 11 January 2022) <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf> accessed 10 March 2025.

citizens, companies, and governments.[108] It presents itself in many forms, ranging from identity theft and phishing to data breaches and hacking. It is evident that a contravention of the provisions of the Cybercrimes Act, more often than not, causes damages to a victim (or plaintiff).[109] South Africa faces particular challenges in effectively addressing cybercrime due to its expanding digital economy. The intricate, dynamic nature of cyberthreats remain a struggle for the nation, even after the implementation of laws such as the Cybercrimes Act,[110] RICA,[111] POPIA,[112] and previous frameworks like the ECTA.[113] Instead of addressing cybercrimes as a single, homogenous category, Mabunda highlights the significance of grouping them into several categories, such as hacking, phishing, and cyberbullying.[114] This classification enables specialised legal and investigative strategies that tackle the particular difficulties presented by every kind of crime.[115] According to the study, South Africa should implement a single, all-encompassing legislative framework to bring together the disparate cybersecurity regulations that are now in place.[116]

With provisions dispersed among several statutes, South Africa's disjointed legal framework produces challenges for enforcement and leaves holes in combating transnational cybercrime and quickly changing cyberthreats.[117] Legal scholars like Sizwe Snail kaMtuze and Melody Musoni underlined the necessity of an integrated legal approach towards cybersecurity.[118] Furthermore, South Africa's ability to participate in international collaboration on cybercrime investigations is restricted by its failure to ratify international agreements such as the Budapest Convention on cybercrime.[119] The

---

108 Keren L G Snider, Ryan Shandler, Shay Zandani and Daphna Canetti, 'Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies' (2021) 7(1) Journal of Cybersecurity 1, 11.

109 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 21.

110 Cybercrimes Act.

111 RICA.

112 POPIA.

113 ECTA.

114 Mabunda, 'The South African legislative response' 187.

115 Mabunda, 'The South African legislative response' 108.

116 Mabunda, 'The South African legislative response' 187.

117 Phenyo Sekati, 'Assessing the Effectiveness of Extradition and the Enforcement of Extra-territorial Jurisdiction in Addressing Trans-national Cybercrimes' (2022) 55(1) Comparative and International Law Journal of Southern Africa 17.

118 Snail and Musoni, 'Overview of Cybercrime Law' 306.

119 Snail and Musoni, 'Overview of Cybercrime Law' 305.

effectiveness of current legislative measures in safeguarding South Africa's digital infrastructure and citizens' rights is heavily doubted as a result of these gaps in legislation and enforcement.

3.2 *Legal challenges in combating cybercrime in South Africa*

The economy, society, and national security of South Africa are increasingly at risk due to the growing frequency and complexity of cybercrimes.[120] Hacking, identity theft, financial fraud, and the dissemination of damaging content such as child pornography and cyberbullying are among the illegal crimes that cybercriminals are committing by taking advantage of legal loopholes as the nation grows more digitally linked.[121]

South Africa ranks 59th on the National Cyber Security Index (NCSI), illustrating significant vulnerabilities in its cyber ecosystem.[122] The Cybercrimes Act 19 of 2020 and the POPIA are two of the legislative measures the South African legal system has introduced in attempt to address these dangers.[123] However, these laws remain fragmented and fail to comprehensively address the full spectrum of cybercrimes that affect individuals, businesses, and government institutions.[124] A primary issue is that South Africa's cybersecurity rules are insufficient against the rapidly evolving world of cybercrime.[125]

One of the main flaws identified in the literature is the incoherence of South Africa's cybersecurity laws. Papadopoulos and KaMtuze claim that legal inconsistencies and enforcement challenges result from the fragmented legal framework, which is scattered

---

120 Simnikiwe Mzekandaba, 'Cyber Crimes' Annual Impact on SA Estimated at R22bn' (*ITWeb*, 16 October 2023) <https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m> accessed 3 April 2025.

121 Chiji Longinus Ezeji, Adewale A Olutola and Paul Oluwatosin Bello, 'Cyber-related Crime in South Africa: Extent and Perspectives of State's Roleplayers' (2018) 31(3) Acta Criminologica: Southern African Journal of Criminology Special Edition: Cybercrime 93, 104.

122 Lötter, 'Comparative Critique of the Cybercrimes Act' 26.

123 Snail, 'Convergence of Cybercrime and Data Protection Laws' 537.

124 Snail and Musoni, 'Overview of Cybercrime Law' 304.

125 Given Shingange, 'A Review of South Africa's National Cybersecurity Policy Framework: Progress and Challenges After Nearly a Decade' (*Institute for Defence, Security and Intelligence*, 26 July 2024) <https://idsi.org.za/2024/07/26/a-review-of-south-africas-national-cybersecurity-policy-framework-progress-and-challenges-after-nearly-a-decade/> accessed 17 March 2025.

across several laws such as the ECTA, POPIA, and the Cybercrimes Act.[126] For example, while POPIA addresses data protection and privacy and ECTA creates a basic legal basis for electronic communications, neither law offers a comprehensive solution for the broader range of cybercrimes.[127] Even though the Cybercrimes Act attempts to address a wider variety of online offenses, its provisions remain partially limited, particularly regarding more recent threats such as cyberbullying and inappropriate use of AI and other emerging technology.[128] Additionally, employment of several laws results in a fragmented response, leaving significant gaps in protection for people, businesses, and government entities.[129]

3.3 *Judicial perspectives on cybersecurity law deficiencies*

The *First National Bank of Southern Africa Ltd v Duvenhage*[130] decision illustrates the practical implications of South Africa's fragmented cybersecurity legal framework. The court's conclusion in this case that the bank's electronic communication system was vulnerable to cyber fraud demonstrates the need for more robust regulatory frameworks that address financial crimes in cyberspace.

Important insights into the relationship between digital evidence, constitutional rights, and fair trial principles in South African law can be gained from *Mgoqi v S*.[131] This case is an effective resource for critically evaluating how South African cybersecurity regulations, like the Cybercrimes Act[132] and RICA,[133] protect privacy rights, control the admissibility of digital evidence, and maintain judicial oversight. The case specifically accentuates the significance of a constitutional framework that successfully strikes a balance between the protection of individual liberties and the state's obligation to investigate and punish cybercrimes, particularly in light of the growing use of digital

126 Papadopoulos and Snail, *Cyberlaw @ SA* 491.
127 Papadopoulos and Snail, *Cyberlaw @ SA* 46.
128 Papadopoulos and Snail, *Cyberlaw @ SA* 470.
129 Papadopoulos and Snail, *Cyberlaw @ SA* 471.
130 *FNB v Duvenhage*.
131 *Mgoqi v S (CA&R 46/2017) [2020] ZAECGHC 33 (29 April 2020)* (hereinafter '*Mgoqi v S*').
132 Cybercrimes Act.
133 RICA.

technology.[134] To ensure that law enforcement activities in the digital sphere do not violate fundamental rights such as the right to privacy[135] and the right to a fair trial,[136] this balance is crucial.

Salzmann v S[137] underscores the challenges caused by inconsistent legal interpretations, particularly regarding procedural clarity. This mirrors issues in cybersecurity legislation, where fragmented laws such as ECTA,[138] POPIA,[139] and the Cybercrimes Act[140] lead to enforcement gaps and inefficiencies. This case demonstrates that procedural inefficiencies and jurisdictional gaps are not limited to traditional crimes but include modern issues like cybercrime. Addressing these challenges in cybersecurity laws requires clearer definitions, streamlined procedures, and an integrated approach to enforcement. The convergence of the Cybercrimes Act[141] and the ECTA[142] in *Okundu v S*[143] illustrated how South African legislation is evolving in order to more successfully combat cybercrimes.[144] The appellant was convicted on multiple counts for contravening section 86(1) of the ECTA.[145] He unlawfully accessed data, specifically the information of clients to whom the banks had issued the original cards.[146] This information was encoded on the magnetic strips of the original cards.[147] The appellant acted without the authority or consent of the lawful cardholders or the banks.[148] The case serves as an example of how the fraud-related

134 *Mgoqi v S.*
135 Constitution, s 14.
136 Constitution, s 35.
137 *Salzmann v S* (755/18) [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200 (SCA) (13 November 2019) (hereinafter '*Salzmann*').
138 ECTA.
139 POPIA.
140 Cybercrimes Act.
141 Cybercrimes Act.
142 ECTA.
143 *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016) (hereinafter '*Okundu v S*').
144 Snail, 'Convergence of Cybercrime and Data Protection Laws' 556.
145 ECTA, s 86(1).
146 *Okundu v S* [6].
147 *Okundu v S* [6].
148 *Okundu v S* [6].

provisions of the ECTA[149] and the more recent, specific regulations on unauthorised data access and cyber-enabled fraud under the Cybercrimes Act[150] are applied.

Critical weaknesses in South Africa's cybersecurity legislation are brought to light by the *Lester Connock Commemoration Fund v Brough Capital* case.[151] Brough Capital was found negligent by the South Gauteng High Court for handling false withdrawal requests in a Business Email Compromise (BEC) attack.[152] The primary issue was that, in spite of warning signs that ought to have prompted more investigation, the Financial Service Provider (FSP) failed to appropriately validate requests.[153] Although financial institutions are subject to some requirements under the Cybercrimes Act of 2020[154] and the Financial Advisory and Intermediary Services (FAIS) Act,[155] the case illustrated that these laws do not specifically address the growing threat of business email compromise (BEC) and lack adequate enforcement measures. This case serves as a reminder that in order to successfully handle new cyberthreats, legal frameworks must be updated.

Although the Cybercrimes Act[156] intends to cover a broader range of offenses than previous laws, including provisions for hacking, cyberbullying, and the dissemination of harmful content, there are still significant gaps in its application and enforceability. The Cybercrimes Act[157] criminalises a number of cybercrimes, however it fails to address the complexity of modern cybercrimes, such as those perpetrated by state actors or organised cybercriminals.[158] The execution and enforcement of these laws are further complicated as South Africa's law enforcement agencies typically lack the technological

149 ECTA.
150 Cybercrimes Act.
151 *Lester Connock Commemoration Fund v Brough Capital (Pty) Ltd and Another* (28646/2020) [2023] ZAGPJHC 1329; 2024 (2) SA 486 (GJ) (16 November 2023) (hereinafter '*Lester Connock* case').
152 *Lester Connock* case [130].
153 *Lester Connock* case [113] – [116].
154 Cybercrimes Act.
155 Financial Advisory and Intermediary Services Act 37 of 2002 (hereinafter FAIS Act).
156 Cybercrimes Act.
157 Cybercrimes Act.
158 Mabunda, 'The South African legislative response' 188.

expertise and resources required to thoroughly investigate and prosecute cybercrimes.[159]

South Africa is vulnerable to both internal and external cyberthreats due to the National Cybersecurity Policy Framework's[160] unclear integration with other national legal frameworks including the Cybercrimes Act[161] and POPIA.[162] This fragmentation is cited as a significant issue by Papadopoulos and KaMtuze, who argue that the country's cybersecurity strategy is reactive rather than proactive.[163] They reinforce that the speed at which technical advancements, including the rise of blockchain technology and artificial intelligence, are taking place has outpaced the legal system's ability to regulate and control emerging forms of cybercrime.[164]

3.4 *Gaps in South Africa's cybersecurity laws and international alignment*

Cybercrime is a borderless threat requiring global collaboration; South Africa's current framework is insufficient for effective cross-border cooperation.[165] The shortcomings in South Africa's cybersecurity legal framework are worsened by the nation's inability to fully join international cybercrime accords. South Africa's Cyberlaw legislation is by now again in need of an overhaul.[166] The President assented to the Cybercrimes Act on 1 June 2021 and it is now in operation. It has been observed that there is a frequent gap in the provisions of sections 9, 19 and 16 of the Cybercrimes Act insofar as the institution of civil proceedings is concerned.[167]

Mabeka asserts that South Africa's cybersecurity strategy, particularly under the Cybercrimes Act 19 of 2020, lacks alignment with international best practices, such as

---

159 Witness Maluleke, 'Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa' (2023) 6(6) International Journal of Social Science Research and Review (IJSSRR) 223, 231.
160 NCPF.
161 Cybercrimes Act.
162 POPIA.
163 Papadopoulos and Snail, *Cyberlaw @ SA* 488.
164 Papadopoulos and Snail, *Cyberlaw @ SA* 492.
165 Lötter, 'Comparative Critique of the Cybercrimes Act' 26.
166 van der Merwe and others, *Information and Communications Technology Law* 118.
167 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 32.

the Budapest Convention.[168] It has been observed that this misalignment generates vulnerabilities, specifically in addressing modern cyber threats such as phishing and digital snooping, which do not always require password breaches.[169] The Cybercrimes Act's narrow focus on password-related crimes overlooks broader interoperability issues, resulting in gaps in comprehensive cyber protection.[170] Additionally, the strict application of *res judicata* in civil proceedings limits victims' ability to recover damages beyond criminal penalties.[171] Mabeka argues for legislative amendments to allow civil claims alongside criminal convictions, ensuring justice for victims of cybercrimes.[172]

Unlike the European Union's GDPR[173] and the Budapest Convention on Cybercrime[174], South Africa's misalignment with international frameworks and global cybersecurity initiatives hinders its ability to respond to cybercrime in accordance with best practices.[175] The patchwork of South Africa's cybersecurity produces difficulty in application , especially when it comes to cross-border cybercrimes.[176] Although South Africa signed the 2001 Budapest Convention on Cybercrime,[177] it has not ratified it, which limits its ability to fully cooperate on international initiatives to stop and combat cybercrime.[178] Chapter 3 of the Convention deals specifically with international co-operation in the investigation and prosecution of criminal offences.[179] Despite the Cybercrimes Act's partial agreement with worldwide best practices, its failure to fully

168 Mabeka, 'Cybercrimes Act and Civil Proceedings' 428.
169 Mabeka, 'Cybercrimes Act and Civil Proceedings' 429.
170 Mabeka, 'Cybercrimes Act and Civil Proceedings' 430.
171 Mabeka, 'Cybercrimes Act and Civil Proceedings' 432.
172 Mabeka, 'Cybercrimes Act and Civil Proceedings' 436.
173 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
174 Convention on Cybercrime.
175 Joel Chigada, 'Towards an Aligned South African National Cybersecurity Policy Framework' (Doctoral Thesis, University of Cape Town 2023) 6.
176 Eleanor Barlow, 'What Makes South Africa a Target for Cyber Crime, and What Actions Can Be Taken?' (*SecurityHQ*, May 2023) <https://www.securityhq.com/blog/what-makes-south-africa-a-target-for-cyber-crime-and-what-actions-can-be-taken/> accessed 17 March 2025.
177 Convention on Cybercrime.
178 Ewan Sutherland, 'Governance of Cybersecurity – The Case of South Africa' (2017) 20 African Journal of Information and Communication (AJIC) 83, 92.
179 van der Merwe and others, *Information and Communications Technology Law* 118.

integrate global rules hinders effective collaboration with other countries on transnational cybercrimes.[180]

Unlike the EU's centralised European Cybercrime Centre, South Africa's reliance on South African Police Service (SAPS) and the Information Regulator without dedicated cyber enforcement agencies has led to delayed responses to breaches and inadequate coordination in cross-border cybercrime investigations.[181] Comparative analysis with international tools such as the Budapest Convention suggests South Africa's framework lacks robust mechanisms for cross-border cooperation.[182]

Mabunda holds that bringing South Africa's legal system in line with global best practices is essential to strengthen cross-border cooperation and address the global nature of cybercrime.[183] The study stresses the need to improve law enforcement skills through specialised training, more funding, and cutting-edge technology in order to eliminate enforcement gaps.[184] By taking these steps, the nation would be better equipped to combat the dynamic and complex danger of cybercrime.[185] The Cybercrimes Act 19 of 2020 does not explicitly address whether parties may institute parallel civil proceedings while criminal proceedings are pending against the defendant.[186] This omission creates a potential gap in the legislative framework, as defences raised in civil matters such as special pleas could undermine the plaintiff's position, particularly where overlapping issues of fact or liability are contested in both forums.[187]

---

180 Shingange, 'A Review of South Africa's National Cybersecurity Policy Framework'.

181 Cybercrime Operations Desk, 'INTERPOL African Cyberthreat Assessment Report 2024: Outlook by the African Cybercrime Operations Desk' (3rd edn, INTERPOL April 2024) <https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf> accessed 18 March 2025.

182 Howard Chitimira and Princess Ncube, 'The Regulation of Artificial Intelligence and 5G Technology to Combat Cybercrime in South African Banks' (2021) 24 Potchefstroom Electronic Law Journal 1, 5.

183 Mabunda, 'The South African legislative response' 193.

184 Mabunda, 'The South African legislative response' 194.

185 Mabunda, 'The South African legislative response' 196.

186 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 25.

187 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 25.

South Africa remains vulnerable to a range of cybercrimes due to the underdeveloped, disjointed, and unenforced cybersecurity legislation.[188] Although this is a step in the right direction, the existing legal system fails to sufficiently to address the whole spectrum of cyberthreats. The current legal framework does not fully address new-age cyber threats such as AI-driven attacks, cryptocurrency fraud, and state-sponsored hacking.[189] The absence of provisions for non-criminal sanctions in the Cybercrimes Act, particularly when contrasted with the Convention on Cybercrime, raises legitimate concern. This study explores whether existing legislative frameworks provide adequate mechanisms for addressing cybercrime and whether gaps exist in enforcement and institutional coordination. This study aims to critically assess the effectiveness of South Africa's cybersecurity laws, identify any flaws in the current structure, and offer recommendations for a more sensible, workable, and internationally uniform legal approach to the country's cybercrime problem.

4 Research objectives

This research will:

- Trace the historical development of cybersecurity legislation in South Africa;
- Critically analyse substantive and procedural provisions of the Cybercrimes Act, POPIA, RICA, and ECTA;
- Evaluate the efficacy of enforcement mechanisms and judicial interpretations of cybercrime-related statutes;
- Assess alignment with international instruments and foreign legislations or regulations such as the Budapest Convention and AU Convention, DORA, GDPR, and NIS2 Directive;
- Compare South Africa’s framework with those of the EU, and the US;
- Recommend reforms aimed at achieving a coherent, enforceable, and constitutionally compliant cybersecurity legal framework.

---

188 Eleanor Barlow, ‘What Makes SA a Target for Cyber Crime, What Actions Can Be Taken?’ (*ITWEB*, 23 May 2023) <https://www.itweb.co.za/article/what-makes-sa-a-target-for-cyber-crime-what-actions-can-be-taken/Pero37Z34ydMQb6m> accessed 25 March 2025.

189 Mabunda, ‘The South African legislative response’ 195.

5 Research question

This study examines whether South Africa’s cybersecurity laws adequately address cybercrime, particularly in relation to enforcement, institutional coherence, and international alignment. Thus, the research question is whether South Africa's present cybersecurity laws and regulations are adequate to prevent and combat cybercrimes and whether they effectively address the challenges posed by rapidly evolving technological threats.

6 Research methodology

This study employs a qualitative research methodology, primarily based on an extensive and critical review of legal texts and scholarly literature. The research is conducted through a desk-top method, focusing on the systematic collection and analysis of both primary and secondary sources. Primary sources include key pieces of legislation and case law, which form the legal foundation of the inquiry. These materials provide essential insights into statutory interpretation and judicial reasoning relevant to the research topic.

To supplement the primary legal framework, the study draws on a broad range of secondary sources, such as academic textbooks, peer-reviewed journal articles, published and unpublished dissertations, and credible electronic resources. These sources are accessed through reputable databases and legal libraries to ensure academic rigour. This methodological approach allows the researcher to critically examine existing legal principles, identify interpretive trends, and evaluate the coherence and effectiveness of the current legal regime under review.

7 Literature review

As the digital landscape rapidly evolved from the early post-apartheid era to the present, South Africa's cybersecurity laws have significantly changed in response to both internal and foreign threats. South Africa's involvement with emerging technologies, the challenges of protecting people online, and the need to combine national legal

frameworks with international cooperation on cybercrime are all reflected in the development of cybersecurity law in the country.

Following its democratic transition in 1994, South Africa focused on re-establishing its legal and constitutional frameworks.[190] Despite the legal system addressing more general social and economic issues during this time, cybersecurity and digital offenses received little attention.[191] A fundamental legal framework was established by the Republic of South Africa's 1996 Constitution,[192] which would later be essential in establishing digital rights and data protection, including the freedom of information exchange and the right to privacy.

The Electronic Communications Act 25 of 2002 ("ECTA") is a critical piece of legislation that has had a major effect on the evolution of South African cyber law.[193] In 2002, the ECTA was promulgated as the first law to address cybercrimes.[194] The *Narlis v South African Bank of Athens*[195] case exposed critical deficiencies in South Africa's early approach to electronic evidence, as courts rejected computer printouts due to their non-human origin and lack of authentication mechanisms. This prompted the Computer Evidence Act 57 of 1983,[196] which introduced affidavit-based validation for digital records in civil proceedings.[197]

Notably, the Act did not extend to criminal proceedings, leaving a gap in the legal framework.[198] The Act's rigid procedural requirements and focus on civil disputes failed to address dynamic cybercrimes such as hacking or data manipulation, leaving

---

190 Firoz Cachalia and Jonathan Klaaren, 'Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization' (2024) 68 Journal of African Law 89, 90.

191 Cachalia and Klaaren, 'Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization', 102.

192 Constitution.

193 van der Merwe and others, *Information and Communications Technology Law* 15.

194 Snail and Musoni, 'Overview of Cybercrime Law' 304.

195 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) (hereinafter '*Narlis*').

196 Computer Evidence Act 57 of 1983.

197 CEA, s 34.

198 Murdoch Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 Journal of Information, Law & Technology (JILT) 1, 3.

enforcement gaps until the ECT Act (2002) provided broader reforms.[199] The Computer Evidence Act 57 was largely criticised. Staniland, French, Skeen, Delport, Ebden and Van der Merwe, among others, criticised this legislation.[200] Its repeal by the Electronic Communications and Transactions Act 25 of 2002 was, therefore, welcomed.[201] This legislative lag underscores the challenges of adapting pre-digital laws to modern cyber threats.[202]

Prior to the enactment of legislation specifically criminalising unlawful cyber conduct, reliance was placed on common-law principles to facilitate the arrest and prosecution of offenders operating in the online environment.[203] A leading example of the extension of common-law principles to cyber-related conduct is found in *S v Howard*.[204] In this case, the court was required to determine whether the accused's actions constituted the common-law offence of malicious damage to property after he introduced malicious code into a computer network belonging to his employer, Edgars Consolidated Stores Ltd, resulting in the deletion of intangible data.[205] The incident caused financial losses estimated to be between R19 million and R57 million.[206] The central issue before the court was whether malicious injury to property could be established where the affected property was not purely corporeal.[207] The court held that temporary damage had been inflicted on corporeal property comprising an integrated system of intangible software and tangible hardware.[208] On this basis, it concluded that the offence of malicious damage to property had been committed, as the accused's conduct caused the collapse of the employer's entire information system.[209]

---

199 van der Merwe and others, *Information and Communications Technology Law* 125.
200 Dana van der Merwe and others, *Information and Communications Technology Law* (2nd edn, LexisNexis 2008) 112.
201 Van der Merwe and others, *Information and Communications Technology Law* 112.
202 *Narlis*.
203 Snail and Musoni, 'Overview of Cybercrime Law' 301.
204 *S v Berend Howard* unreported case no 41/258/02, Johannesburg Regional Magistrates Court (hereinafter '*S v Howard'*).
205 Snail and Musoni, 'Overview of Cybercrime Law' 301.
206 Snail and Musoni, 'Overview of Cybercrime Law' 301.
207 Snail and Musoni, 'Overview of Cybercrime Law' 301.
208 Snail and Musoni, 'Overview of Cybercrime Law' 301.
209 Snail and Musoni, 'Overview of Cybercrime Law' 301.

The ECTA was enacted by Parliament in 2002, marking South Africa's first significant legislative intervention aimed at regulating activities within the digital environment.[210] The ECTA introduced a comprehensive legal framework governing electronic transactions, with the objective of providing legal certainty in relation to digital signatures, online contracts, and the use of electronic communications in commercial activities.[211] Section 86 of the ECTA addressed unlawful conduct involving unauthorised access to, interception of, or interference with data, as well as activities constituting denial-of-service attacks.[212] The ECTA attracted criticism for its perceived insufficiency in imposing robust deterrent measures against cybercriminal activity. For instance, offences under section 86 were punishable by a maximum term of imprisonment of 12 months.[213]

A fundamental aspect of the ECTA's crime-fighting measures was the establishment of a team referred to as "cyber inspectors."[214] The ECTA provisions for cyber inspectors 'have remained a dead letter' as they never came into operation.[215] The shift from common law shortcomings to more specialised legislative frameworks such as the ECTA was brought to light in *R v Douvenga*.[216] It demonstrated the development of South African legal responses to cyberthreats and represented an early adoption of statutes to handle electronic crimes.

In *Ndlovu v Minister of Correctional Services*,[217] The Minister of Correctional Services submitted recorded entries to the court as evidence of parole violations by Ndlovu, presented as a computer printout from an electronic device within the department.[218] The court was tasked with interpreting section 15 of the ECTA,[219] particularly regarding

---

210 Snail and Musoni, 'Overview of Cybercrime Law' 304.
211 ECTA.
212 Snail and Musoni, 'Overview of Cybercrime Law' 304.
213 Snail and Musoni, 'Overview of Cybercrime Law' 305.
214 Snail, 'Cyber Crime in South Africa' 11.
215 Pieter du Toit, 'The Search Warrant Provisions of the Cybercrimes Act and Their Relationship with the Criminal Procedure Act' (2023) 43(4) Obiter 764, 767.
216 *R v Douvenga* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported) (hereinafter '*R v Douvenga*').
217 *Ndlovu v Minister of Correctional Services & another* 2004 JDR 0328 (W) (hereinafter '*Ndlovu v Minister of Correctional Services*').
218 *Ndlovu v Minister of Correctional Services.*
219 ECTA, s 15.

the admissibility of data messages in the context of hearsay rules.[220] In its interpretation, the court distinguished between electronic information whose probative value relies on a human source and electronic information whose truth is independent of an author.[221] Upon assessing the computer printouts, the court concluded that they constituted documents. It further held that, as documents, the printouts must meet the criteria of relevance, authenticity, and the original version must be presented as evidence.[222]

In *S v Ndiki and Others*,[223] the court held that while computer-generated evidence may be classified as hearsay under the Law of Evidence Amendment Act 45 of 1988 (LEAA),[224] it can still be admitted under specific provisions of the Act.[225] Evidence that relies solely on the reliability of the computer system itself is regarded as real evidence under the ECTA,[226] subject to certain conditions.[227] This judgment established an important precedent regarding the admissibility of electronic evidence, particularly computer-generated evidence, in South African legal proceedings. It clarifies the distinction between hearsay evidence and real evidence obtained from computer systems whilst outlining the criteria for admissibility, which are based on reliability, accuracy, and relevant legislative provisions.[228]

In *S v Brown*,[229] the court had to decide whether images found on a cell phone could be admitted as evidence during a trial-within-a-trial. The accused was facing charges of attempted murder and murder.[230] The key witness for the state testified that she had found a cell phone at the crime scene, which was later handed over to the police. The phone was then examined, and five images were discovered, which appeared to be linked to the accused. The defence raised several objections, including concerns about the chain of custody, the images being hearsay, the lack of a magistrate's authorisation

220 *Ndlovu v Minister of Correctional Services.*
221 *Ndlovu v Minister of Correctional Services.*
222 *Ndlovu v Minister of Correctional Services.*
223 *S v Ndiki* [2007] 2 All SA 185 (Ck) (hereinafter '*S v Ndiki*').
224 Law of Evidence Amendment Act 45 of 1988.
225 *S v Ndiki* [53].
226 ECTA.
227 *S v Ndiki* [53].
228 *S v Ndiki*.
229 *S v Brown* (CC 54/2014) [2015] ZAWCHC 128 (17 August 2015) (hereinafter '*S v Brown*').
230 *S v Brown* [2].

to download the data, and issues around privacy. The court, however, referred to the ECTA,[231] which allows for the admissibility of electronic evidence. It determined that the images should be treated as documentary evidence, with no dispute about their authenticity.[232] The court also found that the police were within their rights to seize the phone under section 20 of the Criminal Procedure Act[233] and did not require prior judicial authorisation to download the images for identification purposes.[234] Ultimately, the court ruled the evidence admissible, highlighting that the images were crucial for identifying the accused, and pointing out the inconsistency in the accused's claims about both ownership of the phone and the privacy of the images.[235]

But as digital technologies and cybercrimes became more sophisticated, it became evident that ECTA's protections were unable to handle emerging threats.[236] Critics contend that the ECTA was not designed to address the increasing sophistication of cybercrimes, such as ransomware and other intricate forms of online fraud.[237] It became clear that more thorough and targeted legislation was needed as the internet economy grew.

POPIA[238] demonstrates the advancement of cybersecurity in South Africa. The enactment of POPIA[239] in 2013 gave firms a one-year grace time to comply with its conditions, and as of July 2021, it was fully operational. POPIA[240] is a crucial step in safeguarding personal data in an increasingly digital environment and puts South Africa into compliance with international data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union.[241]

---

231 ECTA, s 15.
232 *S v Brown* [20].
233 Criminal Procedure Act 51 of 1977 (hereinafter CPA).
234 *S v Brown* [15].
235 *S v Brown* [34].
236 Snail, 'Convergence of Cybercrime and Data Protection Laws' 545.
237 Lötter, 'Comparative Critique of the Cybercrimes Act' 25.
238 POPIA.
239 POPIA.
240 POPIA.
241 Legalese, 'The History and Significance of POPIA: A Comprehensive Guide for South African Businesses' (11 September 2024) <https://legalese.co.za/the-history-and-significance-of-popia-a-comprehensive-guide-for-south-african-businesses/> accessed 18 March 2025.

Addressing the complexity of cybercrimes greatly complicated by the inherent constraints of common law, especially in an era of evolving technological threats.[242] POPIA was a part of a broader push to fully control the digital environment with the passing of the ECTA in 2002, which set the foundation for the country's cybercrime legislation. As South Africa sought to protect its citizens from data-related cybercrimes, POPIA facilitated the establishment of a vital intersection between cybersecurity and privacy law.[243] Although it still does not directly address the full spectrum of cybercrimes, POPIA has improved data protection measures.[244]

Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[245] is a crucial component of the cybersecurity legislation in South Africa. In the course of looking into digital crimes including hacking, electronic fraud, and cyberstalking, it enables law enforcement to legally intercept communications and obtain data pertaining to such communications, including metadata and subscriber information.[246] This provides law enforcement with the adequate resources for the detection, investigation, and prosecution of cyber offences. RICA[247] is a supplement to existing laws in South Africa, such as the POPIA[248] and the Cybercrimes Act.[249] The Cybercrimes Act[250] targets cybercrime offenses specifically, POPIA[251] concentrates on protecting personal data, and RICA[252] deals with data collecting and interception.

To prevent possible overreach and guarantee that private rights are not violated, RICA's[253] provisions must be closely monitored. The applicability of RICA[254] should be

242 Snail and Musoni, 'Overview of Cybercrime Law' 301.
243 Snail and Musoni, 'Overview of Cybercrime Law' 301.
244 POPIA.
245 RICA.
246 RICA, s 3.
247 RICA.
248 POPIA.
249 Cybercrimes Act.
250 Cybercrimes Act, ss 2 – 13.
251 POPIA
252 RICA, ss 3, 16–23.
253 RICA.
254 RICA.

examined in relation to the POPIA[255] and the Cybercrimes Act,[256] assessing how it permits cybercrime investigations while upholding privacy rights.[257] In light of current issues with digital privacy and law enforcement, it is critical to evaluate whether the oversight procedures under RICA[258] are sufficient to maintain public confidence and prevent abuse. The *AmaBhungane*[259] case exposed unconstitutional surveillance under RICA, revealing tensions between privacy rights as provided for in section 14 of the Constitution and state security needs. The Constitutional Court in *AmaBhungane* ruled that unchecked surveillance violates privacy rights, demanding legislative reform.[260] RICA's broad surveillance powers, declared partially unconstitutional in *AmaBhungane*, clash with POPIA's foundational privacy principles, exposing a systemic tension between state security imperatives and individual data protection rights.[261] This case set aside some of the most recent amendments to RICA that were proposed by the department of justice and gave the Department a period to frame more effective amendments according to certain criteria set out by the court in an excellent example of "judicial law-making".[262]

The most recent and significant legal advance in South Africa's fight against cybercrime was the passage of the Cybercrimes Act.[263] On December 1, 2021, some of the Cybercrimes Act's provisions went into effect.[264] This Act expressly targets a broad range of digital behaviours, such as virus propagation, online extortion, and illegal access to computer systems.[265] The Cybercrimes Act repealed sections 85, 86, 87, and 88 of the ECT Act and prescribed stricter penalties.[266] The Cybercrimes Act establishes

255 POPIA.
256 Cybercrimes Act.
257 Constitution.
258 RICA.
259 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* [2021] ZACC 3 [89] (hereinafter '*AmaBhungane*').
260 *AmaBhungane* [89].
261 *AmaBhungane* [89]; POPIA, s 5.
262 van der Merwe and others, *Information and Communications Technology Law* 105.
263 Snail and Musoni, 'Overview of Cybercrime Law' 300.
264 Webber Wenzel, 'The Cybercrimes Act Becomes Partially Operational' (*Webber Wenzel*, 1 December 2021) <https://www.webberwentzel.com/News/Pages/the-cybercrimes-act-becomes-partially-operational.aspx accessed> 16 March 2025.
265 Cybercrimes Act, ss 6, 7, 10.
266 Snail and Musoni, 'Overview of Cybercrime Law' 305.

a framework for investigating and prosecuting cybercriminals, enhances cooperation with international organizations, and implements important provisions for reporting cybersecurity incidents, in addition to establishing criminal liability for cybercrimes (Papadopoulos & KaMtuze).[267] The Preamble of the Cybercrimes Act outlines its purpose as the establishment of offences related to cybercrime and the prescription of corresponding penalties.

In addition, the Cybercrimes Act effects consequential amendments to eleven key legislative instruments, including the Criminal Procedure Act 51 of 1977,[268] the South African Police Service Act 68 of 1995,[269] the Films and Publications Act 65 of 1996,[270] the Criminal Law Amendment Act 105 of 1997,[271] the National Prosecuting Authority Act 32 of 1998,[272] the Correctional Services Act 111 of 1998,[273] the Financial Intelligence Centre Act 38 of 2001,[274] the ECTA,[275] the RICA,[276] the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007,[277] and the Child Justice Act 75 of 2008.[278] Through these amendments, the Act establishes specialised procedural mechanisms to support the investigation of cybercrime and to facilitate cooperation among multinational law enforcement agencies, thereby promoting coordinated, multi-agency enforcement efforts.[279]

The Cybercrimes Act 19 of 2020 is a significant legislative measure aimed at addressing cyber-related offenses in South Africa.[280] However, its practical application still faces obstacles.[281] Despite the enactment of the Cybercrimes Act, the frequency of

267 Papadopoulos and Snail, *Cyberlaw @ SA* 464.
268 CPA.
269 South African Police Services Act 68 of 1995 (hereinafter SAPS Act).
270 Films and Publications Act 65 of 1996 (hereinafter FP Act).
271 Criminal Law Amendment Act 105 of 1997 (hereinafter CLA Act).
272 National Prosecuting Authority Act 32 of 1998 (hereinafter NPA Act).
273 Correctional Services Act 111 of 1998 (hereinafter CSA).
274 Financial Intelligence Centre Act 38 of 2001 (hereinafter FICA).
275 ECTA.
276 RICA.
277 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.
278 Child Justice Act 75 of 2008.
279 Snail, 'Convergence of Cybercrime and Data Protection Laws' 545-546.
280 Mabeka and Cassim, ‘Interpreting the Provisions of the Cybercrimes Act’ 31.
281 Mabeka and Cassim, ‘Interpreting the Provisions of the Cybercrimes Act’ 32.

cyberattacks continues to rise, indicating gaps in enforcement and deterrence.[282] The Cybercrimes Act lacks a robust framework for international cooperation, despite referencing extradition and mutual legal assistance.[283]

While the Cybercrimes Act is a welcome development, law enforcement agents continue to face jurisdictional challenges when prosecuting cybercrime, particularly in cases involving cloud evidence.[284] There is a need for legal practitioners and adjudicators to receive education on cybercrime, gathering electronic evidence, and admissibility of digital evidence in court.[285] According to academics like Sizwe Snail kaMtuze, South Africa's enforcement practices raises questions regarding adequacy and there are still gaps in guaranteeing the effectiveness of the law, even with the new legislation.[286] SAPS lacks the specialised skills and resources to handle complex cybercrime investigations, undermining the Cybercrimes Act's enforcement.[287] The SAPS Cyber Security Centre is still in development, and budget limitations hinder the quality of specialised training for investigators.[288] The fragmented legal framework, which incorporates cybersecurity requirements scattered across multiple laws like the Cybercrimes Act, POPIA, and ECTA, has sparked concerns about the coordination of legal actions and the adequacy of sanctions for violators.[289]

In addition to the Cybercrimes Act, POPIA was introduced to regulate the collection, processing, and storage of personal information by organizations. Efforts to align with global cybersecurity standards have also influenced South Africa's legislative developments. The country has drawn insights from international frameworks such as

---

282 Pieterse, 'Cyber Threat Landscape in South Africa' 155.
283 Lötter, 'Comparative Critique of the Cybercrimes Act' 23.
284 Snail and Musoni, 'Overview of Cybercrime Law' 319.
285 Snail and Musoni, 'Overview of Cybercrime Law' 319.
286 Snail, 'Convergence of Cybercrime and Data Protection Laws' 550.
287 Lötter, 'Comparative Critique of the Cybercrimes Act' 23.
288 Pieter Matsaung and David Tubatsi Masiloane, 'The Role of Cyber Intelligence in Policing Cybercrime in South Africa: Insights from Law Enforcement Officers' (2025) 34(2) African Security Review 152, 157.
289 Karen Allen, 'South Africa Lays Down the Law on Cybercrime' (*ISS*, 9 June 2021) <https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime> accessed 1 April 2025.

the Budapest Convention on Cybercrime,[290] though full ratification remains pending.[291] It is concerning that the Cybercrimes Act fails to address non-criminal sanctions as the Convention on Cybercrime does.[292] It is argued that the Cybercrimes Act should further incorporate non-criminal sanctions within its framework, and that the state ought to guarantee that the 24/7 points of contact are adequately resourced and effective.[293]

In many instances, if the South African court has a *lacuna* in the law, we look to comparative law in the form of foreign law and its decisions, as well as international law.[294] The European Union (EU) serves as an excellent comparative jurisdiction for analysing and improving South African cybersecurity laws due to its comprehensive, rights-based regulatory framework and its global influence in digital governance.[295] The EU's General Data Protection Regulation (GDPR)[296] and Network and Information Security (NIS2) Directive[297] provide robust models for data protection, critical infrastructure resilience, and incident reporting all key areas that South Africa's Cybercrimes Act[298] and Joint Standard 2 of 2024[299] seek to address. Particularly relevant is how EU member states have implemented the Budapest Convention on Cybercrime,[300] which establishes crucial international standards for cybercrime legislation and cross-border cooperation.

The GDPR's emphasis on data subject rights and accountability serves as a useful guide for South Africa's implementation of POPIA,[301] especially in efforts to align data protection with cybersecurity measures. The NIS2 Directive, as a directive under EU

290 Convention on Cybercrime.
291 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 31.
292 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 31.
293 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 32.
294 Sizwe Snail, 'Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities' (2009) 1 Journal of Information, Law & Technology (JILT) 1, 9.
295 Axel von dem Bussche and Paul Voigt, *The EU General Data Protection Regulation (GDPR)* (2nd edn Springer 2024) 1-15.
296 General Data Protection Regulation.
297 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) [2022] OJ L333/80.
298 Cybercrimes Act.
299 Prudential Authority and Financial Sector Conduct Authority, Joint Standard 2 of 2024: Cyber Security and Cyber Resilience Requirements (2024).
300 Convention on Cybercrime.
301 POPIA.

law, must be transposed into national legislation prior to taking effect, unlike regulations, which are directly applicable and binding on member states. Additionally, the NIS2 Directive's risk management and supply chain security requirements could guide South Africa in strengthening its approach to securing critical infrastructure.

The EU's Cybersecurity Act,[302] which establishes an EU-wide certification framework, also presents useful insights for South Africa as it develops its own cybersecurity standards and assurance mechanisms. By examining these EU instruments and their relationship to the Budapest Convention, South Africa can adopt international best practices while tailoring them to local contexts, thereby enhancing its cyber resilience framework.

The United States have not only been at the forefront of the development of computer technology, but also (likely as an inescapable corollary of that pre-eminence) suffered most at the hands of computer crime.[303] In reaction, state legislatures responded rapidly, although the federal legislature has been more cautious.[304] The United States serves as a valuable comparative jurisdiction for analysing and strengthening South Africa's Joint Standard 2 of 2024: Cyber Security and Cyber Resilience,[305] due to its well-developed legal frameworks, proactive cyber threat mitigation strategies, and established public-private collaboration models.

The USA's Cybersecurity Information Sharing Act (CISA) of 2015[306] operates at the federal level, facilitating nationwide information sharing on cyber threats. Similarly, the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[307] also developed at the federal level, serves as a voluntary guideline adopted by both federal and state entities, as well as private organisations. It provides structured

302 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) [2019] OJ L151/15.
303 van der Merwe and others, *Information and Communications Technology Law* 105.
304 van der Merwe and others, *Information and Communications Technology Law* 105.
305 Joint Standard 2 of 2024.
306 Cybersecurity Information Sharing Act of 2015.
307 National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1, 2018).

approaches to risk management, incident response, and critical infrastructure protection, which align with key focus areas in South Africa's Joint Standard 2 of 2024. Furthermore, sector-specific regulations in the USA, such as the Gramm-Leach-Bliley Act (GLBA)[308] governing financial services, offer useful insights into how South Africa could refine sectoral cybersecurity obligations under its own Joint Standard 2 framework.[309]

The U.S. model of interagency collaboration, particularly through bodies like the CISA,[310] could also guide South Africa in enhancing public-private partnerships under the Cybercrimes Act.[311] By drawing on these comparative lessons, South Africa can develop a more adaptive and enforceable cybersecurity regulatory framework. Resultantly, the foregoing discussion illustrates the rationale behind why these jurisdictions are chosen.

8 Overview of chapters

8.1 *Chapter one*

The first chapter introduces the topic and sets out the problem statement, research question, research methodology and literature review. This chapter will be submitted before 15 August 2025.

8.2 *Chapter two*

This chapter traces the evolution of cybersecurity laws in South Africa highlighting key legislative milestones and policy frameworks aimed at addressing cyberthreats. It also examines the challenges of enforcing these laws, with a particular focus on the rapidly evolving and complex nature of cyberthreats that test the effectiveness of existing legal and regulatory measures. This chapter will be submitted before 15 October 2025.

---

308 Gramm-Leach-Bliley Act, Pub L No 106–102, 113 Stat 1338 (1999).
309 Joint Standard 2 of 2024.
310 Cybersecurity and Infrastructure Security Agency (CISA).
311 Cybercrimes Act.

8.3 *Chapter three*

This chapter will analyse South Africa's key cybersecurity laws: the Cybercrimes Act, RICA, POPIA, and ECTA. It will evaluate the effectiveness of these laws in combating cybercrime, referencing case law. This chapter will be submitted before 15 December 2025.

8.4 *Chapter four*

This chapter examines the impact of global cooperation, international treaties, and cybersecurity standards on South Africa's legal framework. It includes a comparative study of the European Union and the United States of America, analysing their influence on South Africa's cybersecurity laws, particularly in areas of data protection, cybercrime regulation, and enforcement mechanisms. This chapter will be submitted by 15 January 2026.

8.5 *Chapter five*

This chapter will conclude and make recommendations. This chapter will be submitted before 15 February 2026.

Chapter 2: The Evolution of Cybersecurity Laws in South Africa

1 Introduction

The rapid digitalisation of South Africa's economy and society has necessitated a robust legal and policy framework to combat cyber threats.[312] Given South Africa's position as primarily a consumer rather than a producer of technology, the development of comprehensive legislation and policy frameworks to address cybercrime and computer-related offences has been comparatively slow.[313] In response to increasing cyber incidents, from banking fraud to ransomware attacks, the government has introduced various legislative and policy tools.[314] Among the key pieces of legislation that form the cornerstone of South Africa's legislative framework for combating cybercrime are the Cybercrimes Act 19 of 2020,[315] the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA),[316] the Electronic Communications and Transactions Act 25 of 2002 (ECTA),[317] the Protection of Personal Information Act 4 of 2013 (POPIA),[318] and the National Cybersecurity Policy Framework (NCPF),[319] before considering sector-specific frameworks and their cumulative impact on the development of a coherent cybersecurity regime. Together, these statutes reflect a piecemeal yet evolving legislative effort to address the complex challenges of the digital era. This chapter critically analyses each statute in turn, paying particular attention to their substantive provisions and the extent of judicial engagement with them. It traces the evolution of cybersecurity regulation in South Africa, situating the major laws within their historical context while also highlighting persistent institutional and enforcement challenges.

312 World Economic Forum, 'The Global Risks Report 2022'.
313 Mabunda, 'The South African legislative response' 26.
314 Sizwe Snail, 'Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities' (2009) 1 Journal of Information, Law & Technology (JILT) 1, 9.
315 Cybercrimes Act.
316 RICA.
317 ECTA.
318 POPIA.
319 NCPF.

2 Conceptualising Cybercrime in the South African context

A coherent understanding of cybercrime is essential for evaluating the adequacy of South Africa's legislative response. Cybercrime is a contested and evolving concept, shaped by diverse legal traditions, policy frameworks, and academic interpretations. As Chiluwa and others argue, establishing a coherent definition is critical for addressing cyber threats as part of a global and dynamic challenge.[320] The concept of cybersecurity complements this discourse by encompassing the legal, technical, and institutional strategies aimed at preventing, detecting, and responding to digital threats in an interconnected world.[321]

In South Africa, the Cybercrimes Act 19 of 2020 does not provide a singular definition of cybercrime. Instead, it criminalises various unlawful acts such as unauthorised access, interception, data interference, and cyber fraud.[322] Although South Africa has not ratified the Budapest Convention on Cybercrime (2001), the Convention remains a useful comparative reference. It categorises cyber offences into four groups: offences against the confidentiality, integrity, and availability of data and systems; computer-related offences; content-related offences; and copyright infringements.[323] These categories help contextualise the scope and development of South African cyber law.

3 Early legislative responses to the digital era (1994–2000)

Post-apartheid South Africa focused on constitutional reform and socio-economic transformation, with cybersecurity legislation emerging as a secondary concern.[324] Nonetheless, the Constitution of the Republic of South Africa, 1996 provided foundational rights relevant to the digital age, such as the right to privacy and access to

320 Stanley Osezua Ehiane and others *Cybercrime and Challenges in South Africa* (Palgrave Macmillan 2023) 4.

321 James Stanger, 'Cybersecurity Paradigm Shifts: Insights from Tech Leadership' (CompTIA, 16 October 2024) <https://www.comptia.org/en/blog/cybersecurity-paradigm-shifts-insights-from-tech-leadership/> accessed 6 August 2025.

322 Cybercrimes Act.

323 Convention on Cybercrime (ETS No. 185) (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 (Convention on Cybercrime).

324 Firoz Cachalia and Jonathan Klaaren, 'Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization' (2024) 68 Journal of African Law 89, 102.

information.[325] Thus, any account of South Africa's legislative development in the context of cybersecurity would be incomplete without reference to the Promotion of Access to Information Act 2 of 2000 (PAIA), which plays a vital role in promoting transparency and accountability within both the public and private sectors by facilitating access to information.[326] These rights have become increasingly significant in the context of data protection and digital surveillance. Although PAIA does not specifically address cybercrime, it serves as a valuable legal tool for obtaining information that may assist in the investigation or prosecution of such offences.[327] For instance, PAIA may be invoked to request access to records held by public bodies, including law enforcement agencies or government departments, which may hold relevance to a cybercrime investigation.[328]

The Computer Evidence Act 57 of 1983, predating the internet era, was South Africa's first statutory attempt to regulate the admissibility of digital records in court.[329] However, its limitations including a narrow definition of "computer output" and outdated evidentiary standards rendered it unsuitable for a contemporary digital society.[330] Its repeal in 2002 by the Electronic Communications and Transactions Act (ECTA) 25 of 2002 signalled a legislative shift towards acknowledging the legitimacy of digital evidence and securing online transactions.[331]

4 The Electronic Communications and Transactions Act (ECTA) (2002)

This section evaluates whether the Electronic Communications and Transactions Act (ECTA) 25 of 2002 operates effectively in practice, measured against enforcement capacity, institutional coherence, and constitutional compliance. As early as 2002, the ECTA was enacted with the objective of facilitating electronic communications and

325 Constitution of the Republic of South Africa, 1996, ss 14, 32.
326 The Promotion of Access to Information Act 2 of 2000 (hereinafter PAIA).
327 Papadopoulos S and Snail S *Cyberlaw @ SA: The Law of the Internet in South Africa* (4th edn, Van Schaik 2022) 4.
328 Papadopoulos and Snail Cyberlaw @ SA 4.
329 Murdoch Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings' (2009) 1 Journal of Information, Law & Technology 1, 3.
330 Watney, ‘Admissibility of Electronic Evidence in Criminal Proceedings’ 3.
331 Watney, ‘Admissibility of Electronic Evidence in Criminal Proceedings’ 3.

transactions, as well as promoting the development of a national e-strategy for the Republic of South Africa.[332] The ECTA represents a pivotal legislative development that significantly influenced the trajectory of cyber law in South Africa.[333] The ECTA primarily concentrates on the protection of electronic data and data messages, ensuring their integrity, confidentiality, and lawful use within the digital environment.[334]

One of the Act's foundational provisions establishes the legal recognition of electronic signatures, affirming their reliability and legal validity in electronic communications. Section 13(1) provides that:

> *"An electronic signature is valid if it is reliable and appropriate for the purpose for which the data message was generated or communicated."*[335]

Similarly, section 15(1) reinforces the admissibility of electronic communications as evidence, providing that:

> *"Information in the form of a data message must not be denied admissibility solely because it is in electronic form."*[336]

This provision established that electronic evidence has the same legal standing as traditional documentary evidence, a principle crucial for the prosecution of cyber offences and the recognition of digital contracts.

Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002 marked the introduction of the first legal provisions specifically addressing cybercrime within South African law.[337] The ECTA was South Africa's first legislative effort to address cybercrime, but it was never intended as a comprehensive framework.[338] Furthermore,

---

332 ECTA.

333 van der Merwe and others *Information and Communications Technology Law* (3rd edn, LexisNexis 2021) 16.

334 Fawzia Cassim, 'Addressing the Challenges Posed by Cybercrime: A South African Perspective' (2010) 5(3) Journal of International Commercial Law and Technology 155.

335 ECTA, s 13(1).

336 ECTA, s 15(1).

337 ECTA.

338 Mabunda, 'The South African legislative response' 17; Nandipha Ntsaluba, Cybersecurity Policy and Legislation in South Africa (LLM thesis, University of Pretoria 2017) 60.

notwithstanding the provisions introduced by ECTA, broader public and policy discourse on cybercrime remained limited, largely confined to specialised cybersecurity circles.[339]

The legislation introduced specific statutory offences relating to unauthorised access to, interception of, or interference with data commonly referred to as hacking as well as computer-related extortion, fraud, and forgery. In this regard, section 86(4) and (5) provide that:

> *"A person who utilises any device or computer program to unlawfully overcome security measures designed to protect such data, or who assists another person to do so, commits an offence."*[340]

Further, section 87 prescribes penalties for such offences, providing that:

> *"A person convicted of an offence under section 86 is liable to a fine or to imprisonment for a period not exceeding five years."*[341]

ECTA was enacted to facilitate electronic commerce, promote legal certainty in cyber dealings, and establish a legal basis for prosecuting cybercrime.[342] Prior to the enactment of the ECTA, both Common Law and statutory provisions governed online offences.[343] However, Common Law proved inadequate in effectively addressing emerging cybercrimes such as theft, extortion, spamming, and phishing.[344] The ECTA serves as the primary legislative instrument that introduced a range of statutory offences extending beyond those recognised under South African common law.[345] The Act responds to technological advancements by introducing a novel category of evidence pertaining to information conveyed in electronic format.[346]

339 Mabunda, 'The South African legislative response' 17.
340 ECTA, s 86(4)-(5).
341 ECTA, s 87.
342 ECTA, s 86.
343 Snail, 'Cyber Crime in South Africa' 1.
344 Snail, 'Cyber Crime in South Africa' 1.
345 Ntsaluba, 'Cybersecurity Policy and Legislation in South Africa' 58.
346 Ntsaluba, 'Cybersecurity Policy and Legislation in South Africa' 59.

ECTA has been subject to extensive criticism for its limited effectiveness in addressing emerging cyber-related challenges.[347] Cassim and Snail acknowledge the enactment of the Electronic Communications and Transactions Act as a significant advancement in South Africa's efforts to address cybercrime.[348] However, they contend that, despite its progressive nature, the Act exhibited considerable shortcomings and required substantial refinement.[349] Snail and Cassim have critically examined both the strengths and limitations of the ECTA, concluding that, despite its imperfections, the Act is notably progressive and has played a pivotal role in shaping the legal discourse on cybercrime in South Africa.[350] Although Sections 87 to 89 of the ECTA provide for the criminalisation of certain cyber offences, the failure to implement provisions relating to cyber inspectors has effectively undermined the enforcement and monitoring of compliance.[351] Additionally, the penalties for offences such as hacking or denial-of-service attacks were relatively lenient, undermining deterrence.[352] In addition, the act failed to adequately distinguish between civil and criminal liabilities for electronic communications.[353]

The ECTA was soon followed by the enactment of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)[354] later that same year, marking a parallel legislative effort to address issues of digital communication, privacy, and lawful interception within South Africa's evolving cyber law landscape.

---

347 van der Merwe and others *Information and Communications Technology Law* 38.

348 Cassim, 'Addressing the Challenges Posed by Cybercrime' 173; Snail, 'Cyber Crime in South Africa' 11.

349 Cassim, 'Addressing the Challenges Posed by Cybercrime' 173; Snail, 'Cyber Crime in South Africa' 11.

350 Cassim, 'Addressing the Challenges Posed by Cybercrime' 173; Snail, 'Cyber Crime in South Africa' 11.

351 Ntsaluba, 'Cybersecurity Policy and Legislation in South Africa' 114.

352 Cassim, F 'Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players' 44 (1) (2011) The Comparative and International Law Journal of Southern Africa 123-138 at 129- 134.

353 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 134.

354 RICA.

4.1 *Judicial engagement*

South African courts have increasingly interpreted and applied the Electronic Communications and Transactions Act 25 of 2002 (ECTA) in contexts involving electronic contracting and the admissibility of digital evidence. Section 13 distinguishes between ordinary and advanced electronic signatures, whilst sections 15, 37, and 38 regulate evidentiary admissibility and the enforceability of electronic suretyship agreements.[355] In *Firstrand Bank Ltd v Ayob* the High Court relied on section 15 to admit scanned copies and video call recordings, underscoring that digital evidence is admissible where authenticity and integrity can be established.[356] Similarly, in *Momentum Metropolitan Life v Makaluza* the Cape Town High Court held that intent to be bound outweighed technical deficiencies under sections 13(1), 37, and 38, affirming substance over form in electronic contracting.[357] Other decisions, such as *FirstRand Bank Ltd t/a Wesbank v Govendor*[358] and *Global & Local Investments Advisors (Pty) Ltd v Fouché*,[359] reinforced the enforceability of electronic contracts and the need for reliable authentication mechanisms, while labour and criminal courts have applied section 15 to confirm the validity of electronic communications (*Jafta v Ezemvelo KZN Wildlife*)[360] and the admissibility of computer-generated evidence (*S v Ndiki*;[361] *Ndlovu v Minister of Correctional Services*).[362] Collectively, these rulings demonstrate that ECTA has advanced commercial certainty while simultaneously raising the bar for cybersecurity safeguards, particularly in ensuring data integrity, system reliability, and verifiable electronic records.

355 ECTA, s 13, s 15, ss 37-38.
356 *Firstrand Bank Ltd v Ayob and Another* (2019) ZAGPPHC.
357 *Momentum Metropolitan Life Limited v Lavender Hill Trading 544 CC and Another* (19204/23) [2025] ZAWCHC 99 (*hereinafter 'Momentum Metropolitan Life v Makaluza'*).
358 *FirstRand Bank Limited t/a Wesbank v Govendor* [2023] ZAGPJHC 610.
359 *Global* case.
360 *Jafta v Ezemvelo KZN Wildlife* [2008] 10 BLLR 954 (LC).
361 *S v Ndiki*.
362 *Ndlovu v Minister of Correctional Services.*

5 Regulation of Interception of Communications Act (RICA) (2002)

This section evaluates whether RICA strikes an effective balance between cybersecurity enforcement and constitutional protections, assessed through judicial oversight, proportionality, and institutional accountability. Subsequent to the enactment of the ECTA, the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) was introduced, marking a significant advancement in the evolution of South African cyber law.[363] RICA seeks to safeguard individual privacy by outlining the conditions and procedural safeguards under which state authorities may lawfully intercept communications.[364] It has played a pivotal role in shaping South Africa's cyber law landscape by delineating the scope of governmental interception powers and establishing the limits of such powers within the framework of constitutionally protected rights to privacy and freedom of expression.[365] Section 62 of the RICA expressly repeals the Prohibition of Interception and Monitoring Act 127 of 1992.[366] This repeal signified a legislative shift towards a more comprehensive and constitutionally aligned framework for regulating the interception of communications in South Africa. By replacing the earlier statute, RICA introduced more detailed provisions concerning the procedures, oversight mechanisms, and safeguards governing lawful interception, thereby aligning the regulatory regime with constitutional rights, particularly the rights to privacy and due process.

The RICA has been critiqued for infringing the right to privacy due to the absence of mandatory post-surveillance notification, insufficient oversight mechanisms, and provisions allowing surveillance without adequate judicial safeguards.[367] Section 14 of the Constitution safeguards the right to privacy, encompassing protection against the search of one's person or home, the seizure of possessions, and the interception of

363 Papadopoulos and Snail Cyberlaw @ SA 503; Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa'138.
364 Papadopoulos and Snail Cyberlaw @ SA 503.
365 Papadopoulos and Snail Cyberlaw @ SA 503.
366 RICA.
367 Jane Duncan, 'RICA Erodes Your Right to Privacy' (*TechCentral*, 28 November 2014) <http://www.techcentral.co.za/rica-erodes-your-right-to-privacy/52973> accessed 5 August 2025.

communications.[368] RICA has been critiqued for its potential conflict with POPIA. While the RICA mandates the retention of communication metadata for extended periods, POPIA emphasizes the protection of personal information and imposes strict conditions on its processing.

The RICA establishes a legal framework central to South Africa's cybersecurity regime, particularly in regulating the interception of communications, retention of communication-related information, and accountability in monitoring activities. Sections 2, 16–22, 30, 40, and 42–50 provide the legal basis for lawful investigative measures relevant to cybercrime prevention and digital forensics.[369]

Section 2(1) of RICA provides that:

> *"No person may intentionally intercept or attempt to intercept any communication in the course of its occurrence or transmission."*[370]

Section 2 prohibits the interception of communications unless authorised by RICA.[371] This general prohibition ensures that communications remain private and cannot be monitored or intercepted without proper legal authority. In a cybersecurity context, this provides a legal foundation, ensuring that monitoring, logging, or intrusion detection conducted by state agencies or service providers adheres to lawful standards. Activities such as network surveillance and data capture must respect privacy proportionality.[372] While necessary to prevent unlawful interception, the requirement for judicial authorisation may delay urgent interventions in cybercrime investigations, such as ransomware response or fraud detection, highlighting a tension between operational necessity and procedural safeguards.[373]

---

368 Constitution.
369 RICA.
370 RICA, s 2(1).
371 RICA, s 2.
372 Farhad Khan, 'Strengthening RICA: A Necessary Overhaul for Privacy and Security' (ProtectionWeb, 27 January 2025) <https://www.protectionweb.co.za/opinion-and-analysis/strengthening-rica-a-necessary-overhaul-for-privacy-and-security/> accessed 6 September 2025.
373 Farhad Khan, 'Strengthening RICA'.

Sections 16–22 – Directions for Interception:

> *"Designated judges may, upon application, issue directions authorising the interception of communications suspected to be involved in criminal activities. Applications must specify the nature of the suspected offence, the target, and the period for interception."*[374]

Sections 16–22 govern the procedure for obtaining interception directions from designated judges.[375] These sections are critical for authorising targeted monitoring of communications suspected to be involved in criminal activities, including cybercrime. In practice, these provisions enable law enforcement to trace illicit networks, uncover cybercriminal collaborations, and obtain admissible evidence.[376] However, the requirement for judicial approval and formal application processes can introduce delays that impact the responsiveness of cybercrime investigations. Moreover, the framework does not fully account for circumvention technologies such as anonymising networks or encrypted messaging platforms, limiting operational effectiveness.[377]

Section 30 – Collection of Metadata:

> *"The collection of communication-related information, including call logs, subscriber identities, and routing information, may be authorised for investigative purposes where content interception is not required."*[378]

Section 30 authorises the collection of metadata such as call logs and subscriber identities, which investigators often find more valuable than content for mapping networks and tracing suspects.[379] However, its efficacy is undermined by encryption,

---

374 RICA, ss 16-22.
375 RICA, ss 16-22.
376 RICA, ss 16-22.
377 Intelwatch, 'Submission on the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill' (6 October 2023) <https://intelwatch.org.za/wp-content/uploads/2023/10/231006-Intelwatch-RICA-Bill-Submission.pdf> accessed 6 September 2025.
378 RICA, s 30.
379 RICA, s 30; Directive for ISPs in terms of section 30 of RICA.

compliance challenges with service providers, and the absence of robust oversight, raising privacy concerns under section 14 of the Constitution.[380]

Section 40 – Retention of Communication-Related Information:

> *"Service providers must retain communication-related information for a prescribed period to facilitate lawful investigations and digital forensics."*[381]

Section 40 mandates that service providers retain communication-related information for a prescribed period.[382] Retention is indispensable for post-incident investigations, digital forensics, and prosecutorial evidence. From a cybercrime perspective, historical data enables investigators to reconstruct attack chains and establish links between actors. However, the provision raises privacy and security concerns, as inadequate safeguards for stored data increase the risk of breaches.[383] Additionally, advances in cloud computing and distributed storage challenge the enforceability of retention obligations, particularly for cross-border data.[384]

Sections 42–50 – SIM Card Registration and Verification:

> *"All persons acquiring SIM cards must provide verified identification information. Service providers must collect, verify, and maintain customer information for all SIM cards to reduce anonymity in mobile communications."*[385]

Sections 42–50 require the collection and verification of customer information for all SIM cards.[386] This measure reduces anonymity in mobile communications and serves as a preventive mechanism against SIM-based cybercrime, including SIM-swap fraud

---

380 'The Right to Privacy in South Africa' (Joint Submission to the UN Human Rights Committee, 2017) <https://upr-info.org/sites/default/files/documents/2017-04/js15_upr27_zaf_e_main.pdf> accessed 6 September 2025; Ryszard Lisinski, 'End-to-End Encryption: A South African Perspective' (Fluxmans, 3 November 2016) <https://fluxmans.com/article/end-end-encryption-south-african-perspective-ryszard-lisinski accessed> 6 September 2025.

381 RICA, s 40.

382 RICA, s 40.

383 van der Merwe and others *Information and Communications Technology Law* 367.

384 van der Merwe and others *Information and Communications Technology Law* 367.

385 RICA, ss 42-50.

386 RICA, ss 42-50.

and mobile phishing attacks.[387] While conceptually robust, its practical efficacy is undermined by fraudulent registrations, non-compliance by operators, and the increasing use of virtual numbers or internet-based messaging services, which evade the registration requirements.[388]

Collectively, these RICA provisions form a legally structured framework that equips authorities with investigative powers while embedding safeguards to protect privacy. Conceptually, RICA is aligned with global standards for lawful interception and retention. However, its efficacy in combating cybercrime is limited by technological obsolescence, enforcement gaps, and the rise of encryption and anonymising technologies. Without updates to address these realities, the Act risks remaining a partially effective tool, providing legal authorisation but limited practical deterrence against sophisticated, transnational cyber threats.[389] This divergence raises concerns about the adequacy of safeguards against potential misuse of personal data collected under RICA.[390] Critics have highlighted that RICA lacks sufficient procedural transparency, which could facilitate potential abuse by intelligence and law enforcement agencies. For instance, the parallel procedure in section 205 of the Criminal Procedure Act allows access to communication data without the safeguards present in RICA, potentially circumventing oversight mechanisms.[391]

---

387 Snail and Musoni, 'Overview of Cybercrime Law'.

388 Kate Thompson Davy, 'Exclusive: Failure to RICA mobile SIM cards may be rampant' (BusinessLIVE, 26 September 2023)<https://www.businesslive.co.za/bd/national/2023-09-26-exclusive-failure-to-rica-mobile-sim-cards-may-be-rampant/> accessed 5 September 2025; Mudiwa Gavaza, 'Concern grows about criminal use of unregistered SIM cards' (BusinessLIVE, 13 February 2025)<https://www.businesslive.co.za/bd/national/2025-02-13-concern-grows-about-criminal-use-of-unregistered-sim-cards/> accessed 5 September 2025.

389 Snail and Musoni, 'Overview of Cybercrime Law'; Michalsons Attorneys, 'Complying with RICA – a guide' (6 July 2015) <https://www.michalsons.com/blog/complying-with-rica/1157> accessed 6 September 2025; Russel Luck, 'RICA: Walking a fine line between crime prevention and protection of rights' (De Rebus, 2014) <https://www.derebus.org.za/rica-walking-fine-line-crime-prevention-protection-rights/> accessed 5 September 2025; PPM Attorneys, 'A Breakdown of the RICA Bill' (PPM Attorneys, 5 September 2023) <https://www.ppmattorneys.co.za/breakdown-of-rica-bill/> accessed 5 September 2025.

390 Werksmans Attorneys, 'POPIA and RICA: Acronyms and Privacy' (Werksmans Legal Update, 3 July 2023) <https://www.werksmans.com/legal-updates-and-opinions/popia-and-rica-acronyms-and-privacy/> accessed 8 August 2025.

391 *Amabhungane*; IntelWatch, 'Submission on RICA Bill' (IntelWatch, 6 October 2023) <https://intelwatch.org.za/wp-content/uploads/2023/10/231006-Intelwatch-RICA-Bill-Submission.pdf> accessed 8 August 2025.

5.1 *Judicial engagement*

Key judicial decisions under RICA demonstrate the courts' central role in balancing surveillance powers with constitutional privacy rights. In *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* the Constitutional Court declared sections 16 and 17 unconstitutional for lacking adequate post-surveillance notification and independent oversight, underscoring section 14 of the Constitution's right to privacy.[392] In *Mgoqi v S* the High Court stressed the importance of carefully applying section 35(5) of the Constitution when admitting intercepted communications obtained under RICA warrants, particularly where section 2 prohibits interception without judicial authorisation.[393] Questions of legal professional privilege were addressed in *Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions*, where the Court held that although privilege is protected, it may be limited by competing interests under section 35(5).[394] In *S v Tandwa* the Supreme Court of Appeal clarified that privilege can be waived expressly or tacitly, with implications for section 35 rights and admissibility under RICA.[395] Collectively, these cases illustrate that while RICA empowers surveillance under judicial authority, its provisions must be interpreted in line with constitutional safeguards in order to prevent unjustified intrusions into private or privileged communications.

6 ICASA's role in South Africa's Cybersecurity Framework

The Independent Communications Authority of South Africa (ICASA), established under the Independent Communications Authority of South Africa Act 13 of 2000,[396] regulates the broadcasting, telecommunications, and postal sectors. Its mandate is further defined in the Electronic Communications Act 36 of 2005[397] and relevant provisions of

392 *AmaBhungane.*
393 *Mgoqi v S.*
394 *Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions* 2009 (1) SA 1 (CC).
395 *S v Tandwa.*
396 Independent Communications Authority of South Africa Act 13 of 2000 (hereinafter ICASA Act).
397 Electronic Communications Act 36 of 2005 (hereinafter ECA).

the ECTA. Although ICASA is not a primary cybersecurity regulator, it plays an enabling role in safeguarding South Africa's communications infrastructure.

In its 2019 Position Paper on Cybersecurity Matters, ICASA acknowledged statutory obligations relating to network reliability, technical standards, and information security, particularly as they apply to licensed service providers.[398] The authority enforces compliance measures such as SIM-card registration and lawful interception readiness under the RICA, thereby supporting law enforcement investigations into cybercrime. ICASA has emphasised a multi-stakeholder approach to cybersecurity governance, calling for clearly defined roles among agencies such as the State Security Agency, the Department of Communications and Digital Technologies, and the South African Police Service.[399]

During ICASA's 2019 public inquiry into its prospective role in cybersecurity regulation, several telecommunications stakeholders made submissions opposing an expanded ICASA mandate. The Internet Service Providers Association (ISPA) argued that the investigation and enforcement of cybercrime should remain the responsibility of the Department of Justice and Constitutional Development and the National Prosecuting Authority, rather than a communications regulator.[400] Cell C cautioned that such an expansion would duplicate existing functions, while Vodacom warned that overregulation in a borderless ICT environment threatens hindered innovation and limits user access.[401] These submissions reflect a broader industry consensus that ICASA's

---

398 Independent Communications Authority of South Africa, Findings Document and Position Paper on ICASA's Roles and Responsibilities on Cybersecurity Matters (Government Gazette No 42319, Notice No 198 of 15 March 2019) <https://www.icasa.org.za/news/2019/findings-and-position-on-icasas-roles-and-responsibilities-on-cybersecurity-matters> accessed 8 August 2025.

399 Government of South Africa, Media Statement: ICASA Publishes Findings Document and Position Paper on Cybersecurity (3 April 2019) <https://www.gov.za/news/media-statements/icasa-publishes-findings-document-and-position-paper-cybersecurity-03-apr> accessed 8 August 2025.

400 ITWeb, 'Hands Off Cyber Security, ICASA Told' (ITWeb, 20 March 2019) <https://www.itweb.co.za/article/hands-off-cyber-security-icasa-told/VgZeyqJA3ewMdjX9> accessed 8 August 2025.

401 ITWeb, 'Hands Off Cyber Security, ICASA Told' (ITWeb, 20 March 2019) <https://www.itweb.co.za/article/hands-off-cyber-security-icasa-told/VgZeyqJA3ewMdjX9> accessed 8 August 2025.

contribution to cybersecurity should remain focused on network reliability, technical compliance, and infrastructure resilience, rather than direct enforcement.

7 The South Africa National Cybersecurity Policy Framework (NCPF) (2012)

A cybersecurity framework constitutes a structured and methodical approach aimed at securing digital environments, safeguarding sensitive information, and mitigating the risks associated with cyber threats.[402] Government initiatives are reinforced through the development of national cybersecurity policy frameworks, which aim to provide a systematic and coordinated response to the rising prevalence of cybercriminal activities.[403] The NCPF was approved in 2012 but only published in 2015, delaying implementation. Despite prescribing ten strategic elements including critical infrastructure protection, awareness programmes, and sectoral Computer Security Incident Response Teams (CSIRTs) the framework suffers from poor institutional coordination, fragmented legislation, and persistent skills shortages.[404] Furthermore, the framework mandates the formation of sector-specific CSIRTs, aimed at promoting a collaborative and sectoral approach to enhancing cybersecurity resilience.[405] The NCPF was developed as a continuation of earlier legislative and policy efforts concerning electronic security and cybersecurity.[406] The NCPF identified these preceding measures as inadequate and fragmented.[407] It promotes a cohesive national strategy for the establishment of cybersecurity and sets out the mechanisms and measures necessary for the coordinated implementation of related policies across the country.[408]

---

402 Venencia Paidamoyo Nyambuya and Nirmala Devi Gopal, 'The Influence of South Africa's Democratic Principles on its Cybersecurity Framework and Cyber Threat Response' (2024) 3 (2) Journal of BRICS Studies 55.

403 J Srinivas, AK Das and N Kumar, 'Government Regulations in Cybersecurity: Framework, Standards and Recommendations' (2019) Future Generation Computer Systems https://doi.org/10.1016/j.future.2018.09.063.

404 NCPF; Chigada J, 'Towards an Aligned South African National Cybersecurity Policy Framework' 187.

405 NCPF.

406 David Bote, 'The South African National Cyber Security Policy Framework: A Critical Analysis' (MA thesis, North-West University 2019) 36.

407 Bote, 'The South African National Cyber Security Policy Framework' 36.

408 RS Fonseca and JA van Wyk, 'Cybersecurity in South Africa: Status, Governance, and

The NCPF encompasses a wide range of critical domains that form the core of effective cybersecurity governance.[409] The framework highlights four primary challenges that affect cybersecurity in South Africa: An insufficient regulatory framework, inadequate coordination among relevant stakeholders, limited public awareness, and a deficiency in requisite skills and resources.[410] To address these challenges, the NCPF articulates ten core strategic elements: The formulation of a comprehensive cybersecurity policy, the protection of critical information infrastructure, the promotion of a cybersecurity-conscious culture, and the establishment of collaborative partnerships between the public and private sectors.[411] The NCPF emphasises the importance of international collaboration in addressing cybercrime,[412] acknowledging the inherently transnational nature of cyber threats and the critical role of cross-border cooperation in enforcement and capacity development. Although frameworks such as the NCPF are established with good intentions, South Africa's cybersecurity environment continues to encounter significant challenges.[413] Bote recognises the significance and goals of the NCPF, but expresses concern regarding its effectiveness, noting a range of interrelated factors that create complex dynamics and impede the achievement of its objectives.[414]

The NCPF lacks robust integration with existing legislation which undermines its overall effectiveness.[415] Given this context, it highlights the necessity of revisiting the framework to improve its efficacy in dealing with cybersecurity challenges.[416] The NCPF is not being implemented effectively, as demonstrated by incidents such as the 2021 cyberattack on the Department of Constitutional Justice (DC&J).[417] Gcaza posits that

---

Prospects' in Scott N Romaniuk and Mary Manjikian (eds), Routledge Companion to Global Cyber-Security Strategy (Routledge 2021) 591.

409 Bote, 'The South African National Cyber Security Policy Framework' 42.

410 NCPF.

411 NCPF.

412 NCPF.

413 Abdullahi Abiodun Yusuf, 'Employees' Cybersecurity Awareness and Behaviour in South African Higher Education Institutions' (MIT dissertation, University of Pretoria 2024) 17.

414 Bote, 'The South African National Cyber Security Policy Framework'.

415 Fonseca and van Wyk, 'Cybersecurity in South Africa'.

416 Joel Chigada, 'Towards an Aligned South African National Cybersecurity Policy Framework' (Doctoral Thesis, University of Cape Town 2023) 6.

417 Faith Tinonetsana, Policy Postdoctoral Fellow, National Research Foundation; Postdoctoral Fellow, Durban University of Technology (2025) <https://hsrc.ac.za/wp-content/uploads/2025/06/Faith-Tinonetsane-PB.pdf> accessed 5 August 2025.

the successful implementation of the NCPF is contingent upon the widespread cultivation of a cybersecurity-conscious culture among the general populace.[418] Consequently, the intended purpose of the NCPF is undermined by fragmented and incoherent legislative measures, coupled with inadequate institutional coordination.[419]

8 The Protection of Personal Information Act (POPIA) (2013)

This section evaluates the extent to which the Protection of Personal Information Act (POPIA) contributes to cybersecurity governance in practice, assessed through enforcement capacity, regulatory coherence, and alignment with constitutional privacy protections. In late 2013, the POPIA was enacted, although only select provisions were brought into effect at that time.[420] The POPIA, fully operational from July 2021, is South Africa's flagship data protection statute.[421] The rise of the Internet coupled with the globalisation and growing interdependence of economies, as well as the convergence of information and communications technologies and their capacity to transmit data across borders instantaneously, created a pressing need for legislation aimed at safeguarding personal information.[422] The POPIA articulates foundational conditions for lawful data processing, establishing a critical nexus between data protection and cybersecurity. The POPIA significantly advanced the development of South African cyber law by establishing a comprehensive legal framework for safeguarding personal information within the digital environment.[423] The Act promotes the safeguarding of personal information by both public and private entities, and establishes legal requirements for the lawful processing of personal data relating to natural persons and juristic entities, including individuals, companies, and trusts.[424] The POPIA constitutes

418 Gcaza N and others, 'A General Morphological Analysis: Delineating a CyberSecurity Culture' (2017) 25(3) Information and Computer Security 271.
419 Chigada J, 'Towards an Aligned South African National Cybersecurity Policy Framework' 78.
420 POPIA.
421 van der Merwe and others *Information and Communications Technology Law* 476.
422 Y Burns and A Burger-Smidt, *A Commentary on the Protection of Personal Information Act* (LexisNexis Durban 2018).
423 van der Merwe and others *Information and Communications Technology Law* 477.
424 POPIA.

a significant contribution to the advancement of cyber law in South Africa by offering a statutory framework for the protection of personal information in the digital context.[425]

POPIA advances the constitutional right to privacy by regulating the lawful processing of personal information.[426] Furthermore, the Act establishes thorough regulatory guidelines for the lawful processing and management of personal information by organisations, thereby mitigating the risk of cybercrime and enhancing the protection of individual privacy rights.[427] Section 69 of the POPIA repealed Section 45 of the ECTA, which had previously governed the regulation of electronic communications.[428] Section 39 of the POPIA provides for the establishment of the Information Regulator (IR) as an independent juristic body, mandated to investigate breaches of personal information and authorised to impose a range of penalties in instances of non-compliance.[429] The POPIA prohibits the transfer of personal data to a foreign jurisdiction unless that state provides data protection safeguards comparable to those set out in the Act.[430] The Act is heavily influenced by the European Union's Data Protection Directive and aims to give effect to internationally recognised standards of data protection by regulating the use, misuse, processing, dissemination, and distribution of personal information both within South Africa and across its borders.[431]

8.1 *Processing limitation provisions and sectoral Cybersecurity*

The POPIA establishes a legal framework central to South Africa's cybersecurity regime, particularly in regulating the collection, processing, and retention of personal information. Sections 9 to 12, collectively known as the "processing limitation" provisions", prescribe the conditions under which personal data may be lawfully handled, providing safeguards directly relevant to cybercrime prevention. These

425 Ramluckan T, 'International Humanitarian Law and its Applicability to the South African Cyber Environment' (2020) 19(3) Journal of Information Warfare 102 102-117; 106-107.
426 Fonseca and van Wyk, 'Cybersecurity in South Africa'.
427 Ramluckan T, 'International Humanitarian Law and its Applicability to the South African Cyber Environment' (2020) 19(3) Journal of Information Warfare 102-117; 106-107.
428 POPIA; ECTA.
429 POPIA, s 39.
430 POPIA.
431 POPIA; GDPR; Swales 'South African Mercantile'59.

provisions operate alongside sector-specific cybersecurity regulations, including the Financial Sector Regulation Act (FSRA), the ECTA, the Insurance Act, and industry-specific standards such as Regulation 4 of the Banks Act for cyber risk management to ensure lawful and proportionate data processing.[432]

8.1.1 *Section 9 - Lawfulness of processing*

Section 9 of POPIA stipulates that personal information must be processed in a lawful and reasonable manner, ensuring that such processing does not unjustifiably infringe upon the privacy of the data subject.[433]

This section requires the processing to be both legally justified and reasonable. In *De Jager v Netcare Limited*, the High Court assessed surveillance evidence obtained without consent and applied POPIA's section 9, recognising that lawful processing requires both legal justification and reasonableness.[434]

In banking and financial services, Section 9 underpins compliance with the Financial Sector Conduct Authority's (FSCA) cybersecurity requirements. For instance, network monitoring and fraud detection must align with POPIA's legal processing standards, while balancing investigative necessity against customers' constitutional privacy rights. In the telecom sector, lawful processing is also reinforced by ECTA provisions on the interception of communications, ensuring that lawful monitoring of traffic or metadata for threat detection complies with both POPIA and sectoral law.[435]

8.1.2 *Section 10 - Minimality*

Section 10 of POPIA requires that personal information be adequate, relevant, and not excessive in relation to the purpose for which it is processed.[436]

---

432 POPIA, ss 9–12; Financial Sector Regulation Act 9 of 2017 (hereinafter FSRA); ECTA; Insurance Act 18 of 2017 (hereinafter Insurance Act); Banks Act 94 of 1990, Regulation 4.

433 POPIA, s 9.

434 *De Jager v Netcare Limited and Others* (42041/16) [2025] ZAGPPHC 141 (hereinafter '*De Jager v Netcare*').

435 POPIA, s 9; FSCA; ECTA.

436 POPIA, s 10.

This minimality principle ensures that only information necessary for a defined purpose is collected and processed. Courts have applied this principle in *Smuts N.O. and Others v MEC Eastern Cape*, scrutinising processing practices to prevent the retention of excessive or irrelevant data.[437]

In practice, banks and insurance companies maintain large volumes of customer data for risk management. Section 10 requires that processing must be limited to information strictly necessary for specific cybersecurity functions, such as anomaly detection, fraud prevention, or intrusion investigation.[438] Unnecessary retention of transactional or behavioural data increases exposure to cyberattacks.[439] In the telecom sector, metadata collection must be proportionate to the stated purpose of threat detection or regulatory reporting.[440]

8.1.3 *Section 11 - Consent, justification, and objection*

Section 11 of POPIA provides that personal information may only be processed if the data subject consents or the processing is necessary for a contractual, legal, or legitimate purpose. It establishes the lawful bases for processing, including consent, contractual necessity, legal obligation, legitimate interests, and the performance of public law duties.[441] In *Smuts N.O.*, the court considered objections to processing and affirmed that responsible parties bear the burden of demonstrating a valid legal justification.[442]

In financial services, explicit consent may be impractical for real-time cybersecurity monitoring. Banks rely on legal obligations under the FSRA and legitimate interests to

---

437 *Smuts N.O. and Others v MEC Eastern Cape.*

438 POPIA, s 10.

439 POPIA, s 10; Digital School of Marketing, 'Navigating POPIA and GDPR in Cybersecurity Compliance' (Digital School of Marketing, 20 August 2025) <https://digitalschoolofmarketing.co.za/cyber-security-blog/navigating-popia-and-gdpr-in-cybersecurity-compliance/> accessed 5 September 2025.

440 Agbor T Kandeh, Lynn A Futcher and Reinhardt A Botha, 'Enforcement of the Protection of Personal Information (POPI) Act: Perspective of Data Management Professionals' (2020) 22(1) South African Journal of Information Management 1.

441 POPIA, s 11 (1)(a)–(d).

442 *Smuts N.O. and Others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism and Others* (1199/2021) [2022] ZAECMKHC 42 (26 July 2022).

process data for fraud detection.[443] Insurance companies must similarly justify data processing for claims, fraud prevention and cybersecurity monitoring under the Insurance Act.[444] Section 11 thus ensures that sectoral cybersecurity measures are both legally defensible and accountable to data subjects.[445]

8.1.4 *Section 12 - Collection directly from the data subject*

Section 12 of POPIA mandates that personal information must be directly collected from the data subject, except where a statutory exception applies. This includes already public information, consented collection from another source, necessity for national security, protection of legitimate interests, or impracticability under the circumstances.[446] In *Boudewyn Homburg de Vries N.O. v MEC for Department of Economic Affairs*, the court emphasised that exceptions must be narrowly construed.[447]

In practice, indirect collection occurs frequently in cybersecurity investigations. Banks, insurers, and telecoms may receive threat intelligence or forensic logs from third-party providers.[448] Section 12 ensures that these indirect collections remain lawful only under defined exceptions, such as public interest, law enforcement necessity, or statutory obligations. This requirement reinforces transparency and traceability, crucial for demonstrating compliance during regulatory audits.[449]

---

443 FRSA.
444 Insurance Act.
445 POPIA, s 11.
446 POPIA, s 12.
447 *Boudewyn Homburg de Vries N.O. v MEC for Department of Economic Affairs.*
448 Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio, *Banks' Cyber Security — A Second Generation of Regulatory Approaches*, FSI Insights No 50 (Bank for International Settlements, 12 June 2023) https://www.bis.org/fsi/publ/insights50.pdf accessed 18 September 2025; Duja Consulting, *Cyber Fraud Meets Forensics: Auditing in a Digital Threat Landscape* (Duja Consulting Blog, 3 September 2025) https://www.duja.co.za/cyber-fraud-meets-forensics-auditing-in-a-digital-threat-landscape/ accessed 18 September 2025; EY, *Top 10 Risks in Telecommunications* (EY Global, January 2025) https://www.ey.com/en_za/insights/telecommunications/top-10-risks-for-telecommunications accessed 18 September 2025; KelaCyber, *How Banks Use Threat Intelligence* (KelaCyber Blog) https://www.kelacyber.com/blog/how-banks-use-threat-intelligence/ accessed 18 September 2025.
449 POPIA, s 12; FCSA.

8.2 *Synthesis*

Taken together, sections 9 to 12 of the POPIA form a comprehensive, rights-based framework that balances cybersecurity imperatives with privacy safeguards.[450] By integrating POPIA with sector-specific regulations, organisations in banking, insurance, telecommunications, and critical infrastructure can ensure lawful, minimal, justified, and transparent processing of personal information. While conceptually strong, the effectiveness of these provisions in combating cybercrime depends on robust regulatory enforcement, clear operational guidance, and integration with cybercrime-specific legislation, such as the Cybercrimes Act. Without these supporting measures, POPIA's provisions risk remaining primarily aspirational, providing legal guidance but offering limited deterrent effect against increasingly sophisticated, transnational cyber threats.[451]

It is important to note, however, that POPIA permits the application of other legislation where stronger safeguards exist, recognising its own limitations.[452] A key criticism is its siloed focus on personal data, leaving broader systemic cybersecurity risks, such as ransomware or national infrastructure attacks, outside its scope. Such methods of data collection instead fall under the broader definitions provided by the ECTA.[453] Similar to the ECTA and RICA, POPIA adopts a siloed approach by focusing predominantly on the protection of digitally stored personal information rather than the wider cybersecurity ecosystem. This has underscored the need for supplementary legislative and policy interventions to address the complexities of cyberspace more comprehensively.[454]

The Act also omits provisions requiring the adoption of privacy-by-design or privacy-by-default principles, and does not mandate the conduct of Data Privacy Impact Assessments.[455] A particularly notable shortcoming lies in its lack of provisions on

---

450 POPIA, ss 9-12.

451 POPIA; Cybercrimes Act; FSCA; Insurance Act.

452 POPIA, s 3(2) b.

453 Hamman B & Papadopoulos S 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) De Jure 42 – 62.

454 Mancha Johannes Sekgololo, 'The State of Cybersecurity in South Africa, 2010–2019' (MA dissertation, University of Johannesburg 2021).

455 Information Regulator of South Africa, Media Statement: Information Regulator Shares

artificial intelligence. In the absence of a dedicated AI framework in South Africa, POPIA does not adequately address the risks that AI poses to personal information, thereby limiting its relevance in contemporary data protection contexts.[456] While POPIA aligns with international norms such as the GDPR,[457] the emphasis remains on personal data processing rather than broader cybersecurity threats such as ransomware or attacks on national infrastructure.[458] This creates a regulatory gap in addressing risks that extend beyond the privacy domain. Scholars have argued that without the integration of privacy protections with systemic cybersecurity safeguards, POPIA risks being overtaken by technological developments and failing to provide effective resilience against emerging threats.[459]

8.3 *Judicial engagement*

South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) has seen limited direct judicial application in cybersecurity breaches, with enforcement largely driven by the Information Regulator.[460] In July 2023 the Regulator fined the Department of Justice and Constitutional Development ZAR 5 million for failing to renew security licences. Simultaneously an enforcement notice against Dis-Chem Pharmacies followed a third-party cyberattack that compromised 3.6 million records. These actions applied sections 19 and 22 of POPIA, which require responsible parties to implement appropriate security safeguards and notify the Regulator of security compromises.[461] In *Information Regulator v South African Police Service* the court confirmed that state

---

Outcomes of Complaints Investigated and Assessments Conducted in relation to PAIA and POPIA (5 April 2023) <https://inforegulator.org.za/wp-content/uploads/2020/07/pdf-Final-Version_MEDIA-BRIEFING-OF-INFORMATION-REGULATOR-ON-OUTCOMES-OF-RECEIVED-COMPLAINTS-003.pdf> accessed 11 September 2025.

456 Vicent Mbonye, Marlini Moodley and Farai Nyika, 'Examining the applicability of the Protection of Personal Information Act in AI-driven environments' (2024) 26(1) SAJIM 1,9.

457 GDPR.

458 POPIA.

459 van der Merwe and others *Information and Communications Technology Law* 530.

460 POPIA, s 39.

461 Information Regulator of South Africa, Media Statement: Information Regulator Shares Outcomes of Complaints Investigated and Assessments Conducted in relation to PAIA and POPIA (5 April 2023) <https://inforegulator.org.za/wp-content/uploads/2020/07/pdf-Final-Version_MEDIA-BRIEFING-OF-INFORMATION-REGULATOR-ON-OUTCOMES-OF-RECEIVED-COMPLAINTS-003.pdf> accessed 11 September 2025.

institutions are also bound by these obligations, reinforcing the Act's broad scope.[462] These fines serve as a precedent, demonstrating that non-compliance with enforcement directives will result in monetary penalties. Despite these enforcement actions, the effectiveness of POPIA remains constrained by the limited investigative and prosecutorial capacity of the Information Regulator, particularly in complex, large-scale cyber incidents.

Judicial engagement has mainly focused on balancing privacy with competing interests. In *De Jager v Netcare Limited and Others* the court held that processing personal and health data for litigation purposes was permissible under section 11(1)(c), provided that unrelated data was redacted.[463] In *Edward Nathan Sonnenbergs Inc v Hawarden* the High Court initially imposed liability for phishing losses, though the Supreme Court of Appeal overturned this, stressing shared responsibility and the application of sections 19–20 on security safeguards.[464] In *Gerber v PSG Wealth Financial Planning* responsibilities to prevent cyber fraud were affirmed under section 19, while *Fourie v Van der Spuy & De Jongh Inc* highlighted how failures to safeguard client funds engage both POPIA duties and common law negligence principles.[465] Collectively, these rulings and enforcement actions show that POPIA is becoming a practical tool for embedding organisational accountability in cybersecurity, even as judicial interpretation of its provisions remains at an early stage.

9 The Critical Infrastructure Protection Act 8 of 2019 (CIPA)

This section assesses whether the Critical Infrastructure Protection Act provides an effective legal response to cyber threats against essential infrastructure, measured against regulatory clarity, enforcement mechanisms, and technological relevance. The Critical Infrastructure Protection Act 8 of 2019 (CIPA) represents a significant legislative

462 Information Regulator of South Africa, Media Statement: Information Regulator Shares Outcomes of Complaints Investigated and Assessments Conducted in relation to PAIA and POPIA (5 April 2023) <https://inforegulator.org.za/wp-content/uploads/2020/07/pdf-Final-Version_MEDIA-BRIEFING-OF-INFORMATION-REGULATOR-ON-OUTCOMES-OF-RECEIVED-COMPLAINTS-003.pdf> accessed 11 September 2025.

463 *De Jager v Netcare*.

464 *ENS Inc v Hawarden*.

465 *Gerber v PSG.*

development aimed at strengthening the security and resilience of South Africa's critical infrastructure.[466] The Act repeals the outdated National Key Points Act 102 of 1980 (NKP),[467] introducing modern regulatory mechanisms to protect essential installations from evolving threats. Although the Act is in force, regulations envisaged under section 27 are still in the process of being finalised.

Section 1 (definition) – Critical Infrastructure:

> *"'Critical infrastructure' means infrastructure essential to national security, public safety or the effective functioning of the Republic."*[468]

Under section 1 of the Act, the definition of "threats" encompasses both malicious activities such as denial-of-service attacks, malware, and phishing and natural or human-induced hazards.[469] These threats may manifest locally, nationally, or even transnationally, thereby shining a light on the importance of a comprehensive and adaptive security framework.[470] The emergence of next-generation technologies and the digital transformation of critical infrastructure have prompted a shift in many countries' security priorities expanding the focus beyond physical protection to include cybersecurity, as these technological developments introduce greater complexity and vulnerability within critical systems.[471]

Section 2(a)–(b) – Objectives:

---

466 ITLawCo, 'Critical Infrastructure Protection Act 8 of 2019 (CIPA)' (ITLawCo, 20 November 2019) https://itlawco.com/critical-infrastructure-protection-act-8-of-2019-cipa/ accessed 6 August 2025.

467 Critical Infrastructure Protection Act 8 of 2019 (hereinafter CIPA); National Key Points Act 102 of 1980 (repealed).

468 CIPA, s 1 (definition).

469 Duarte Gonçalves and Chris Serfontein, Systemic Approaches to Critical Infrastructure Risk and Security Capabilities (CSIR Report, November 2022).

470 Gonçalves and Serfontein, 'Systemic Approaches'.

471 Masike Malatji, Annlizé L. Marnewick, Suné von Solms & Wikus Erasmus, Cyber Governance in the Water Sector: Volume 1 – Water and Sanitation Cybersecurity Legislative and Policy Environment (Water Research Commission Report No 3060/1/22, University of Johannesburg 2022).

> *"The objectives of the Act include safeguarding and protecting critical infrastructure against threats and ensuring its confidentiality and integrity."*[472]

In accordance with section 2 of the Act, its primary objectives are to safeguard critical infrastructure against potential threats and to preserve the confidentiality of information relating to the security measures applicable to such infrastructure.[473] The CIPA recognises the importance of certain infrastructure in ensuring national security, safeguarding public safety, and supporting the uninterrupted provision of essential public services.[474] Therefore, CIPA provides for the identification and safeguarding of infrastructure essential to national security. Entities responsible for critical infrastructure must adopt comprehensive risk management strategies, including specific cybersecurity measures.[475]

Section 27(1) – Ministerial Regulations:

> *"The Minister may make regulations regarding the identification, categorisation, and declaration of critical infrastructure and the establishment of oversight structures."*[476]

The Act designates the Minister of Police, assisted by the National Commissioner of the South African Police Service, as the authority responsible for its administration and enforcement.[477] The CIPA provides for measures such as physical barriers and security personnel, but does not extend its provisions to include cybersecurity defenses such as firewalls.[478]

10 The Cybercrimes Act 19 of 2020

This section evaluates the Cybercrimes Act as South Africa's primary cybercrime statute, assessed through its substantive scope, procedural effectiveness, and

472 CIPA, s 2 (a)-(b).
473 CIPA.
474 CIPA.
475 CIPA.
476 CIPA, s 27(1).
477 CIPA.
478 Yeshiel Panchia, 'Command line to control room: SA's infrastructure vulnerable to cyberattacks' (Daily Maverick, 17 July 2025) <https://www.dailymaverick.co.za/article/2025-07-17-command-line-to-control-room-sas-infrastructure-vulnerable-to-cyberattacks/> accessed 7 August 2025.

institutional enforceability. South Africa's most recent legislative advancement in the domain of cyber law is the Cybercrimes Act 19 of 2020 (Cybercrimes Act).[479] The Cybercrimes Act was enacted subsequent to South Africa's signing of the Council of Europe Convention on Cybercrime (Budapest Convention), despite the country not having ratified the Convention to date. Notwithstanding non-ratification, the Budapest Convention remains a critical comparative and interpretive benchmark, as its offence typology and procedural standards are substantively reflected in the structure of the Cybercrimes Act.[480] The Cybercrimes Act serves as the current legislative framework governing cybercrime in South Africa.[481] Prior to the drafting of the Cybercrimes Act, the limited legal provisions addressing cybercrime were fragmented and dependent on the amendment of existing statutes to include cybercrime-related components.[482] The Act introduces comprehensive and contemporary provisions designed to address the prevailing cybercrime environment.[483]

The Cybercrimes Act extends the scope of cyber offences beyond those recognised under the ECTA by incorporating crimes such as harassment, the dissemination of malicious software, cyber forgery, and online identity theft.[484] This expansion has strengthened the legal framework, enhancing the capacity to prosecute cyber offenders and to protect individuals and organisations from digital threats.[485] Importantly, Sections 2 to 7 of the Act directly prohibit core cybercrimes, functioning as legislative mechanisms to safeguard the confidentiality, integrity, and availability of information systems. These sections include:

---

479 Cybercrimes Act.
480 Cybercrimes Act; Budapest Convention.
481 Cybercrimes Act.
482 Mabunda, 'The South African legislative response' 18.
483 Snail and Musoni, 'Overview of Cybercrime Law'.
484 Snail and Musoni, 'Overview of Cybercrime Law'.
485 Scott Timcke, Mark Gaffley & Andrew Rens, 'The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet' (2023) 32 The African Journal of Information and Communication 1 https://doi.org/10.23962/ajic.i32.16949 15.

- Section 2 – Unlawful Access: Any person who unlawfully and intentionally accesses a computer system is guilty of an offence. Possession of unlawfully accessed data without a satisfactory explanation is also an offence.[486]

- Section 3 – Unlawful Interception of Data: Unlawful interception of data transmitted to or from a computer system is prohibited. Possession of intercepted data under suspicious circumstances is criminalised.[487]

- Section 4 – Unlawful Acts in Respect of Software or Hardware Tool: The use or possession of software or hardware tools for committing offences under Sections 2, 3, 5, 6, or 7 is prohibited.[488]

- Section 5 – Unlawful Interference with Data or Computer Program: Any unlawful alteration, deletion, obstruction, or denial of access to data or computer programs constitutes an offence.[489]

- Section 6 – Unlawful Interference with Computer Data Storage Medium or Computer System: Unlawful interference with the functioning, integrity, confidentiality, or availability of computer systems or storage media is prohibited.[490]

- Section 7 – Unlawful Acquisition, Possession, Provision, Receipt, or Use of Passwords, Access Codes, or Similar Data or Device: Acquiring, possessing, providing, or using passwords, access codes, or similar data to commit offences under Sections 2, 3, 5, 6, 8, or 9 is criminalised. Possession under suspicious circumstances without a satisfactory explanation is also an offence.[491]

The Act is organised into nine chapters, which can be grouped into four thematic areas: First, the substantive offences are addressed in Chapter 2, which criminalises various

---

486 Cybercrimes Act, s 2.
487 Cybercrimes Act, s 3.
488 Cybercrimes Act, s 4.
489 Cybercrimes Act, s 5.
490 Cybercrimes Act, s 6.
491 Cybercrimes Act, s 7.

forms of cybercrime and malicious communications, providing sentencing frameworks and protective orders to shield complainants.[492] Second, the Act sets out procedural and investigative powers. Chapter 3 deals with jurisdiction;[493] Chapter 4 empowers law enforcement to investigate, search, access and seize;[494] and Chapter 7 governs the adducing of evidence by sworn statements.[495] Third, the Act establishes institutional and cooperative mechanisms. Chapter 5 regulates mutual legal assistance with foreign states;[496] Chapter 6 provides for a designated point of contact within SAPS;[497] Chapter 8 imposes obligations on electronic communications service providers and financial institutions to report cybercrime offences and preserve information.[498] Finally, general provisions in Chapter 9 cover executive authority to conclude agreements, the repeal and amendment of certain laws, the promulgation of regulations, and commencement.[499]

Only part of the Cybercrimes Act has commenced in terms of Proclamation R.42 of 30 November 2021, with several key provisions including protection orders for malicious communications, expedited data preservation, mutual legal assistance, and mandatory reporting obligations by service providers yet to come into force. This partial commencement introduces significant practical limitations. Victims of harmful communications remain without statutory relief, cross-border investigations are constrained, and the suspension of reporting duties removes an early-warning mechanism that could support both enforcement and prevention. Even the operational sections, while laying a solid foundation, cannot by themselves ensure comprehensive protection, leaving enforcement heavily dependent on the capacity of SAPS and the DPCI.[500] Although South Africa has not ratified the Budapest Convention, its influence

492 Cybercrimes Act, ch 2.
493 Cybercrimes Act, (ss 8–13).
494 Cybercrimes Act, (ss 14–44).
495 Cybercrimes Act, (ss 45-46).
496 Cybercrimes Act, (ss 47-53).
497 Cybercrimes Act, (ss 54-56).
498 Cybercrimes Act, (ss 57-58).
499 Cybercrimes Act, (ss 59-66).
500 Proclamation R.42 of 30 November 2021 brought into force from 1 December 2021 the following provisions: Chapter 1 (ss 1–7); Chapter 2 (excluding Part VI, ss 20–23); Chapter 3 (ss 8–13); Chapter 4 (excluding ss 38(1)(d)–(f), 40(3)–(4), 41–44); Chapter 7 (ss 45–46); Chapter 8 (excluding s 54); and Chapter 9 (excluding certain schedule amendments). The following

is evident in the structure and content of the Cybercrimes Act, rendering the Convention an essential interpretive and comparative benchmark rather than a binding instrument. This staggered commencement weakens the Act's deterrent and preventative effect by leaving critical reporting, preservation, and victim-protection mechanisms legally dormant.

10.1 *Procedural and Enforcement Mechanisms*

While the Cybercrimes Act establishes substantive offences and outlines a procedural enforcement framework, its practical effectiveness is dependent on the degree to which these mechanisms are operationalised within South Africa's institutional context. The Act recognises that criminalisation alone is insufficient without corresponding mechanisms for detection, evidence preservation, and cooperation, both domestically and internationally.[501]

Although the Act empowers authorities to preserve data, the effectiveness of this provision is constrained by delays in implementation and limited technical capacity within enforcement agencies.[502] It also establishes mechanisms for the disclosure and production of such data, enabling courts to compel service providers to furnish information necessary for investigations.[503] In addition, the Act authorises searches and seizures of computer systems, hardware, and data, and provides for the collection of real-time traffic data under strictly controlled circumstances. These procedural powers are carefully aligned with safeguards for lawful access, ensuring that enforcement measures are both effective and consistent with constitutional protections.[504]

---

provisions remain not yet commenced: Chapter 2 Part VI (ss 20–23) on protection orders for malicious communications; Chapter 4 ss 38(1)(d)–(f), 40(3)–(4), and 41–44 concerning expedited preservation and disclosure of data; Chapter 5 (ss 47–53) on mutual legal assistance; Chapter 6 (ss 54–56) establishing the designated point of contact; and Chapter 8 s 54 on mandatory reporting by service providers and financial institutions; Papadopoulos and Snail *Cyberlaw @ SA* 333-350.

501 Cybercrimes Act, ss 26-62.

502 Cybercrimes Act, ss 26-30.

503 Cybercrimes Act, ss 31-33.

504 Cybercrimes Act, ss 34-41.

Although the Act acknowledges the transnational nature of cybercrime and provides for international cooperation, the effectiveness of these mechanisms is constrained by practical limitations in cross-border enforcement and the incomplete operationalisation of relevant provisions.[505] Complementing these powers, sections 55–62 impose reporting obligations on electronic communications service providers, requiring them to notify authorities of certain cyber incidents and cooperate with investigations, thereby integrating private sector participation into the enforcement framework.[506]

The Act recognises the transnational nature of cybercrime and provides for mutual legal assistance and international cooperation, enabling South African authorities to request or provide support to foreign jurisdictions in matters such as data preservation, disclosure, and cross-border investigations.[507] Complementing these powers, the legislation imposes reporting obligations on electronic communications service providers, requiring them to notify authorities of certain cyber incidents and to cooperate with investigations. In doing so, the Act integrates private sector participation into the enforcement framework, strengthening the overall capacity to detect, investigate, and respond to cybercrime.[508]

By coupling substantive offences with robust procedural mechanisms, the Cybercrimes Act strengthens the enforceability of South Africa's cybercrime legislation. The integration of investigative powers, search and seizure authority, mutual legal assistance, and reporting obligations reflects a legislative recognition that cybersecurity enforcement requires both comprehensive criminalisation and practical tools for evidence gathering and cooperation. The Act thus represents a significant advancement over prior legislation, such as the ECTA which lacked comparable enforcement structures.[509] In practice, the effectiveness of these mechanisms is contingent on the technical capacity and resourcing of SAPS and the Directorate for Priority Crime Investigation, which remain uneven across regions.

505 Cybercrimes Act, ss 42-54.
506 Cybercrimes Act, ss 55-62.
507 Cybercrimes Act, ss 42-54.
508 Cybercrimes Act, ss 55-62.
509 ECTA, ch XIII.

10.2 *Judicial Engagement*

Although relatively new, the Cybercrimes Act has already been judicially applied across diverse contexts. In *The Digital Law Company v Meta Platforms* the High Court ordered the removal of accounts distributing child sexual abuse material (CSAM), relying on the Cybercrimes Act and the Films and Publications Act to assert jurisdiction over global platforms and enforce duties relating to unlawful distribution of data messages.[510] In *S v Erasmus* the Bellville Specialised Commercial Crimes Court convicted a former IT employee on seventeen counts including unlawful access (s 2), unlawful interception of data (s 3), unlawful interference with data and networks (ss 5–6), theft of data (s 8), cyber fraud (s 9), and cyber extortion (s 10), sentencing him to effective imprisonment.[511] The case affirms the enforceability of the Act against insider-enabled attacks and demonstrates judicial recognition of the severity of cyber-enabled economic harm. Similarly, in *S v Gumede* the Durban Magistrates' Court convicted a political activist under s 14 of the Act for circulating a WhatsApp voice note inciting violence against foreign nationals, confirming the applicability of statutory prohibitions on harmful data messages and reliance on digital evidence to prove incitement.[512]

Civil liability has also been addressed. In *Lester Connock Commemoration Fund v Brough Capital (Pty) Ltd and Another* the Johannesburg High Court held a financial service provider negligent for failing to verify email instructions, leading to losses through Business Email Compromise fraud.[513] The judgment highlights that liability in cybercrime contexts extends beyond direct criminality to encompass negligence where due diligence is absent, aligning with the preventative rationale of the Cybercrimes Act.[514] Finally, in *Okundu v S* the Eastern Cape High Court grappled with the overlap between common law fraud and statutory offences under the Electronic Communications and Transactions Act 25 of 2002 (s 86(3)–(4)) and the Regulation of Interception of Communications and Provision of Communication-Related Information

---

510 Cybercrimes Act, s 16; *The Digital Law Company (Pty) Ltd v Meta Platforms Inc. (2025).*

511 Cybercrimes Act, ss 2-3, ss 5-6, ss 8-9; *S v Lucky Majangandile Erasmus and Unathi Pupu* (2023).

512 Cybercrimes Act, s 14; *S v Gumede* (2022).

513 *Lester Connock* case.

514 Cybercrimes Act, s 54.

Act 70 of 2002 (s 45).[515] The Court avoided charge duplication and cautioned against expansive interpretations unsupported by evidence, reinforcing fraud as the central organising principle while recognising the preparatory role of statutory cyber offences.[516] Collectively, these rulings demonstrate the judiciary's early but significant role in interpreting the Cybercrimes Act, balancing innovation with foundational criminal justice principles, and shaping doctrinal and policy clarity in South Africa's evolving cyber law landscape.

11 SAPS SOPs under Section 26 of the Cybercrimes Act

The operationalisation of Section 26 of the Cybercrimes Act 19 of 2020 through the South African Police Service (SAPS) Standard Operating Procedures (SOPs) provides a structured and rights-sensitive framework for the investigation, search, access, and seizure of "cyber articles".[517] Section 26(2) of the Cybercrimes Act states: "The Minister responsible for policing must issue Standard Operating Procedures for SAPS and other investigating authorities, to be published in the Gazette."[518] This provision mandates the development of SOPs for investigation and enforcement, giving statutory authority to the procedures.

These SOPs, developed collaboratively by SAPS, the DPCI, the National Prosecuting Authority (NPA), and the Department of Justice and Constitutional Development (DoJ&CD), serve as a practical guide to ensure compliance with constitutional safeguards while enabling effective law enforcement action. They apply not only to SAPS members but also to authorised investigators and other agencies empowered by law to investigate offences involving cyber articles, which include data, computer programs, computer data storage media, and computer systems.[519] The scope extends to both offences expressly defined under the Cybercrimes Act and any criminal activity

---

515 *Okundu v S.*
516 *Okundu v S.*
517 South African Police Service, Standard Operating Procedures in terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles (Final 12 September 2023) 1–3.
518 SAPS, Section 26 Cybercrimes Act SOPs (2023) 2.
519 SAPS, Section 26 Cybercrimes Act SOPs (2023) 8-10.

in which a cyber article is instrumental, whether in South Africa or with a transnational element.[520]

Central to the SOPs are seven guiding principles that balance the imperative of lawful and effective evidence gathering with the protection of fundamental rights such as privacy and the right to a fair trial.[521] These principles ensure that cyber articles are handled with integrity, reliability and authenticity; ensuring proportionality and necessity in investigative measures; adhering strictly to legality; limiting intrusion to what is relevant and necessary; preserving a verifiable audit trail; and securing appropriate technical and legal support. The SOPs also integrate privacy safeguards under the Protection of Personal Information Act 4 of 2013 when personal data is processed, underscoring the need for adequate protection and lawful handling of such information.[522]

In practical terms, the SOPs establish procedural clarity on critical aspects such as obtaining the correct legal authorization - whether through a search warrant under the Cybercrimes Act, a Criminal Procedure Act 51 of 1977 warrant, or a Section 205 subpoena and distinguishing between searches conducted with consent, without a warrant, or incident to arrest.[523] They also detail preparatory steps, including assessing the nature and location of the cyber article and considering operational safety and the possible need for other forensic processes.[524] The execution phase addresses scene security, rapid isolation of devices to prevent data loss, documentation, and the safe handling, transportation, and storage of seized articles.[525] By embedding these processes within a standardised, legally compliant framework, Section 26 SOPs enhance the admissibility of electronic evidence while aligning investigative practices with both national and international norms.[526]

---

520 SAPS, Section 26 Cybercrimes Act SOPs (2023) 10–12.
521 SAPS, Section 26 Cybercrimes Act SOPs (2023) 6-7.
522 SAPS, Section 26 Cybercrimes Act SOPs (2023) 4–5.
523 SAPS, Section 26 Cybercrimes Act SOPs (2023) 17–19, 27–33.
524 SAPS, Section 26 Cybercrimes Act SOPs (2023) 21-23.
525 SAPS, Section 26 Cybercrimes Act SOPs (2023) 33-35.
526 SAPS, Section 26 Cybercrimes Act SOPs (2023).

12 Sector-Specific Cybersecurity Laws

In addition to the general cybersecurity legislation, South Africa has implemented sector-specific measures to address the unique risks faced by critical industries. In the financial sector, the FSCA and the Prudential Authority require banks, insurers, and other financial institutions to implement comprehensive cyber risk management frameworks, emphasising operational resilience, incident reporting, and protection of sensitive client information, aligning with the Cybercrimes Act and POPIA.[527]

Within the banking sector, the South African Reserve Bank (SARB) mandates robust operational risk management and cybersecurity controls, including incident response plans and periodic resilience testing.[528] Similarly, the insurance sector, under the FSCA and the Insurance Act, is required to implement governance frameworks addressing cyber risks, including risk mitigation, incident reporting, and safeguarding policyholder data.[529]

The telecommunications sector, regulated by ICASA, is subject to standards ensuring network integrity and service continuity. Providers are obliged to implement technical and administrative safeguards, report cyber incidents, and comply with RICA and POPIA obligations.[530]

Operators of critical infrastructure, including energy, water, transport, and health sectors, are guided by the NCPF and relevant sector-specific regulators. These entities must implement cybersecurity controls tailored to operational technology, report significant incidents, and coordinate with national cybersecurity strategies.[531]

Finally, the financial intelligence framework established under FICA indirectly addresses cybersecurity by mandating secure handling and reporting of financial data

---

527 FSCA and Prudential Authority, Guidance Note on Cybersecurity Risk Management for Financial Institutions (FSCA, 2021).

528 SARB, Operational Risk and Cybersecurity Guidelines (SARB, 2021).

529 FSCA, Insurance Sector Cyber Risk Management Framework (FSCA, 2020).

530 ICASA, Electronic Communications and Network Security Guidelines (ICASA, 2020).

531 Department of Communications and Digital Technologies, National Cybersecurity Policy Framework (NCPF) (DTPS, 2017).

to combat cyber-enabled fraud and money laundering.[532] Collectively, these sector-specific measures complement South Africa's general cybersecurity legislation by operationalising statutory obligations within the context of sectoral risks.

13 Provisional Conclusion

In conclusion, South Africa's cybersecurity legal framework is anchored in both general and sector-specific legislation, establishing the foundation for criminalising cyber offences, regulating data interception, and imposing compliance obligations on public and private actors. Early legislative efforts, such as the Computer Evidence Act 57 of 1983[533] and the Promotion of Access to Information Act 2 of 2000 (PAIA),[534] laid important foundations but were not specifically designed to address the unique challenges of cybercrime in a digitised environment. The enactment of the Electronic Communications and Transactions Act 25 of 2002 (ECTA)[535] marked the country's first formal attempt to recognise cyber offences and regulate electronic communications, yet its limited scope, lack of robust enforcement mechanisms, and inadequate integration with emerging global standards exposed critical shortcomings.

Subsequent statutes, including the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA),[536] the Protection of Personal Information Act 4 of 2013 (POPIA),[537] and the Critical Infrastructure Protection Act 8 of 2019 (CIPA),[538] progressively expanded the legal architecture governing cyber-related matters. While RICA established safeguards for lawful interception, it has been criticised for infringing privacy rights and lacking adequate oversight mechanisms. POPIA advanced data protection in line with international norms but remains primarily focused on personal information, leaving broader cybersecurity gaps unaddressed. Similarly, CIPA modernised the protection of critical infrastructure but has yet to fully integrate cybersecurity-specific defences. The

532 Financial Intelligence Centre Act 38 of 2001.
533 Computer Evidence Act 57 of 1983.
534 PAIA.
535 ECTA.
536 RICA.
537 POPIA.
538 CIPA.

adoption of the National Cybersecurity Policy Framework (NCPF)[539] in 2012 signalled a strategic recognition of the need for a coordinated, multi-stakeholder approach to cybersecurity governance; however, weak institutional coordination, insufficient integration with existing legislation, and persistent skills shortages have limited its impact.

The most notable recent advancement, the Cybercrimes Act 19 of 2020,[540] consolidates and expands the range of prosecutable cyber offences, establishing procedural clarity for investigation and prosecution. The operationalisation of Section 26 through SAPS Standard Operating Procedures represents a progressive step towards rights-sensitive enforcement.[541]

Despite notable progress, South Africa's framework remains fragmented, with overlapping mandates and weak enforcement. These systemic deficiencies undermine the country's capacity to ensure a coherent and responsive cybersecurity regime, impeding the timely detection, investigation, and prosecution of cybercrimes. Addressing these gaps through harmonised legislative reform and institutional strengthening is imperative to enhance the overall efficacy of South Africa's cybersecurity governance framework. Achieving a resilient regime requires stronger coordination, targeted capacity building, and integration with evolving international standards. This ongoing refinement is essential to ensure that the legal framework addresses current cyber threats while remaining resilient and adaptable to emerging technologies and increasingly sophisticated cybercrime tactics.

Collectively, South Africa's cybersecurity framework reflects a legislatively dense but institutionally fragmented model. Substantive criminalisation, surveillance regulation, data protection, and critical infrastructure protection are governed by discrete legislative instruments each administered by separate authorities, without a unified coordinating enforcement framework. This fragmentation undermines operational coherence, dilutes accountability, and weakens the state's capacity to respond effectively to complex,

539 NCPF.
540 Cybercrimes Act.
541 SAPS, Section 26 Cybercrimes Act SOPs (2023).

transnational cyber threats. These deficiencies provide the analytical foundation for the comparative evaluation in the next chapter, where South Africa's fragmented model is assessed against more integrated approaches in the European Union and the United States.

Chapter 3: Evaluating the Effectiveness of South Africa's Cybersecurity Legal Framework

1 Introduction

The effectiveness of South Africa's cybersecurity legal framework cannot be evaluated in isolation; it is intrinsically linked to a complex and challenging operational environment characterized by a rapidly evolving threat landscape, systemic institutional fragmentation, and critical human factor vulnerabilities. This context highlights the inherent interconnection between cybersecurity and cybercrime. In an increasingly interconnected environment, cybersecurity encompasses a nation's capacity to anticipate, defend against, and respond to digital breaches, whereas cybercrime constitutes the illicit activities that these protective measures are designed to deter and mitigate.[542] This is corroborated by the INTERPOL Africa Cyberthreat Assessment, which identifies South Africa as among the most targeted countries on the continent, experiencing a marked escalation in the frequency and severity of high-impact cybercrime incidents.[543] The significant economic ramifications of this threat landscape are evident nationally, with cyber-attacks imposing annual costs exceeding R2 billion on South African organisations.[544] While the Cybercrimes Act, POPIA, and the NCPF represent significant legislative and policy strides, their promise is tested by the reality of sophisticated threats like AI-powered fraud and ransomware.[545] Additionally, the capacity to enforce these laws is constrained by a dire shortage of skills, a rigid educational system that hinders multidisciplinary collaboration, and a shallow research pipeline.[546]

---

542 Papadopoulos and Snail *Cyberlaw @ SA* 464.

543 INTERPOL, Africa Cyberthreat Assessment Report 2025 (INTERPOL, May 2025) https://www.interpol.int/en/content/download/23094/file/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf.

544 Zubeida Casmod Khan and Nenekazi Nokuthala Penelope Mkuzangwe, 'Advancing Cybersecurity Capabilities for South African Organisations through R&D' Council for Scientific and Industrial Research, Pretoria, South Africa, 1.

545 Lebogang Mpuru and Charles Kgoale, 'Recognizing the Evolving Cybercrime Threats in South Africa' (2025) African Security https://doi.org/10.1080/19392206.2025.2515302.

546 Trishana Ramluckan, Brett van Niekerk and Louise Leenen, 'Research Challenges for

Compounding these issues is the persistent "human element," identified as the weakest security link, with even critical institutions like the South African National Defence Force (SANDF) demonstrating significant gaps in cybersecurity awareness.[547] Insufficient political prioritisation and constrained resources render the state's cybersecurity response reactive and fragmented, a concern evidenced by the banking sector's critique of the 'limited capacity of the police and National Prosecuting Authority to prevent, detect, investigate, and prosecute cybersecurity breaches.'[548]

This chapter critically evaluates the effectiveness of South Africa's cybersecurity laws in combating cybercrimes, building on the legislative evolution discussed in Chapter 2. This approach is grounded in a fundamental principle: once a security technology is compromised, law enforcement must possess the capacity to investigate the resulting offences. The progression of legal regulation demonstrates that governments recognise that, in the absence of legislation both criminalising specific conduct and enabling its investigation, the benefits of information and communication technologies (ICT) cannot be fully realised and are likely to be undermined.[549] This development originated in common law, which was recognised as limited and inadequate to address the evolving methods of criminal activity, prompting the enactment of the first statutory framework, the Electronic Communications and Transactions Act (ECTA).[550]

The evaluation focuses on five key instruments: the Cybercrimes Act 19 of 2020,[551] the Protection of Personal Information Act 4 of 2013 (POPIA),[552] the Regulation of Interception of Communications and Provision of Communication-related Information

---

Cybersecurity and Cyberwarfare: A South African Perspective' University of KwaZulu-Natal and University of the Western Cape / CAIR https://researchspace.ukzn.ac.za/.

547 Kyle Bester and Danille Elize Arendse, 'Measuring Cybersecurity Awareness in a South African Military Sample' (2024) 52(1) Scientia Militaria: South African Journal of Military Studies 5–33 https://doi.org/10.5787/52-1-1445.

548 Russell Buchan and Joe Devanny, 'South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority' (Carnegie Endowment for International Peace 2024) https://carnegieendowment.org; South African Banking Risk Information Centre (SABRIC), Annual Crime Statistics 2021 (2024) https://www.sabric.co.za/wp-content/uploads/2024/11/SABRIC-Annual-Crime-Stats-2021.pdf accessed 17 October 2025.

549 Papadopoulos and Snail *Cyberlaw @ SA* 472.

550 Snail and Musoni, 'Overview of Cybercrime Law' 302-305.

551 Cybercrimes Act.

552 POPIA.

Act 70 of 2002 (RICA),[553] the Electronic Communications and Transactions Act 25 of 2002 (ECTA),[554] and the National Cybersecurity Policy Framework (NCPF).[555] The analysis interrogates institutional coherence, enforcement capacity, and the substantive adequacy of statutory provisions. It also considers judicial interpretation and policy implementation to determine whether South Africa's approach delivers a functional and constitutionally compliant cybersecurity regime.

While South Africa possesses a relatively comprehensive legislative framework, this chapter examines whether the effectiveness of South Africa's cybersecurity legal framework is constrained by institutional fragmentation, inconsistent implementation, and limited enforcement capability. These shortcomings may weaken deterrence, reduce accountability, and leave South Africa vulnerable to increasingly sophisticated cyber threats. For purposes of this chapter, effectiveness is assessed not by legislative breadth alone, but by institutional coherence, enforcement capacity, judicial operability, and demonstrable deterrent impact.

2 Institutional and Legislative coherence

This section evaluates whether South Africa's institutional cybersecurity governance framework, as constituted by the Cybercrimes Act, POPIA, RICA, ECTA, and the NCPF, operates effectively in practice, measured against institutional coherence, enforcement capacity, and constitutional compliance. The South African cybersecurity regime represents an ambitious attempt to harmonise multiple dimensions of cyber governance, crime prevention, data protection, interception control, and electronic transactions, yet its effectiveness appears to be affected by fragmented mandates and weak institutional coordination.[556] This fragmentation is observable not only at the institutional level but also within the substantive legal framework, resulting in overlapping criminalisation and legal ambiguity. A notable instance is the regulation of

553 RICA.
554 ECTA.
555 NCPF.
556 "Understanding South African Cybersecurity Law in the Context of the Recent SAA Cyber Incident" (Polity, 31 July 2025); Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'; IISS, Cyber Capabilities and National Power Vol. 2 (IISS Research Paper, September 2023).

revenge pornography, which is criminalised under section 16 of the Cybercrimes Act, yet is also addressed in the proposed Films and Publications Amendment Act and could arguably fall under the Sexual Offences Act. Likewise, offences such as hate speech and harassment risk being redundantly covered by both the Cybercrimes Act and the Films and Publications Act. This scenario illustrates a piecemeal approach to cybercrime regulation and overregulation, which may generate uncertainty for prosecutors and affect the clarity and coherence of the law.[557] The Independent Communications Authority of South Africa (ICASA) recognizes that telecommunications, e-commerce, and broadcasting infrastructure are essential to national security, but emphasizes that these sectors require management within a comprehensive framework, indicating that such a framework is not yet fully established.[558]

Consistent with the objectives of the National Cybersecurity Policy Framework (NCPF), the South African government has instituted critical institutional mechanisms, including the Cybersecurity Hub, which functions as a central platform facilitating collaboration among government entities, citizens, and the private sector to enhance online security for individuals and organisations.[559] Complementing this, the State Security Agency has established a Computer Security Incident Response Team (CSIRT) tasked with coordinating the national response to cybersecurity incidents.[560] While South Africa's legislative evolution reflects a progressive attempt to harmonise its cybersecurity governance, early frameworks such as the ECTA were primarily technology-neutral and lacked the procedural and institutional depth required to combat cybercrime effectively.

As Mabunda observes, ECTA "took the first steps in the confrontation with cybercrime" through sections 85–89, but the debate "never gained momentum outside cybersecurity

557 Papadopoulos and Snail *Cyberlaw @ SA* 491-492.

558 Independent Communications Authority of South Africa, *ICASA Strategic Plan 2025–2030* (ICASA, 2025) https://www.icasa.org.za/strategic-plan-2025-2030.

559 Cybersecurity Hub, 'Homepage' https://www.cybersecurityhub.gov.za/ accessed 17 October 2025.

560 State Security Agency, 'CSIRT' https://www.ssa.gov.za/CSIRT accessed 17 October 2025.

professional circles,"[561] contributing to a fragmented and reactive policy environment that persisted until 2020.

It lacked detailed procedural mechanisms to investigate or prosecute cybercrimes. Subsequent laws such as RICA addressed interception and metadata retention but were developed within the surveillance and telecommunications context, rather than cybersecurity proper.[562] The POPIA introduced data-protection obligations to ensure secure processing of personal information and to protect individual privacy.[563] However, POPIA's regulatory approach, grounded in information privacy rather than cybersecurity, creates conceptual disjunction between privacy enforcement and cybercrime prevention.

The Cybercrimes Act was introduced to consolidate cyber offences and align South Africa's laws with international best practices.[564] Yet, despite this consolidation, overlapping mandates persist between the South African Police Service (SAPS), the State Security Agency (SSA), the Department of Communications and Digital Technologies (DCDT), and the Information Regulator.[565] The NCPF, as the primary policy instrument, has experienced slow and uneven implementation, which has led to a limited overall impact. This is substantiated by the Auditor-General's observation that government departments and state-owned enterprises had made limited progress toward achieving NCPF objectives, in part due to the absence of defined implementation timelines and their continued reliance on 'unsupported and vulnerable infrastructure.'[566] Overlapping mandates have led to duplication, unclear lines of accountability, and weak operational coordination, as highlighted in official reviews.[567] This is compounded by a rigid National Qualifications Framework (NQF) that actively

561 Mabunda, 'The South African legislative response' 17-18.
562 RICA.
563 POPIA.
564 Cybercrimes Act.
565 Department of Communications and Digital Technologies, Annual Report 2023/24 (South Africa, 2025).
566 Auditor-General South Africa, 'Public Finance Management Act Report 2022/23 (2023)' https://www.agsa.co.za/Reporting/PFMAReports/PFMA2022-23.aspx accessed 17 October 2025.
567 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

inhibits the multidisciplinary collaboration essential for a coherent cyber governance model.[568]

The NCPF sought to create a unified national strategy by establishing structures such as the National Cybersecurity Hub and sectoral CSIRTs.[569] However, implementation has been limited. The Portfolio Committee on Communications noted in 2023 that the Cybersecurity Hub operates with fewer than twenty technical staff and lacks statutory powers to compel information-sharing from private-sector operators.[570] This institutional weakness was starkly illustrated by the 2025 cyber-attack on South African Airways (SAA), where confusion reigned over which entity; SAPS, the SSA, or the National Cybersecurity Hub was responsible for leading the incident response, with the Hub functioning in an advisory capacity without the statutory authority to compel a unified reaction.[571] A critical symptom of this incoherence is the under-resourced Cyber Command, which its commander has admitted is "able to function, however, not optimally,"[572] highlighting a profound disconnect between policy ambition and institutional capacity. As a result, incident reporting remains voluntary, and national situational awareness is weak.

Academic commentators agree that this patchwork approach impedes South Africa's cyber-readiness. Snail and Musoni argue that "without a coherent governance framework and a clear chain of accountability, the cybersecurity regime risks ineffectiveness despite legislative sophistication."[573] The failure to enact secondary

---

568 Ramluckan, van Niekerk and Leenen, 'Research Challenges for Cybersecurity and Cyberwarfare'.

569 NCPF.

570 Parliamentary Monitoring Group, 'ATC231025: Report of the Portfolio Committee on Communications and Digital Technologies on the 2022/23 Third and Fourth Quarter Performance and Expenditure Reports of Government Communication and Information System (GCIS) and the Media Development and Diversity Agency (MDDA) (24 October 2023)' <https://pmg.org.za/tabled-committee-report/5522/> accessed 15 October 2025.

571 Stewart K, 'Understanding South African Cybersecurity Law in the Context of the Recent SAA Cyber Incident' (Polity, 31 July 2025) https://www.polity.org.za/article/understanding-south-african-cybersecurity-law-in-the-context-of-the-recent-saa-cyber-incident-2025-07-31 accessed 16 October 2025.

572 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

573 Snail and Musoni, 'Overview of Cybercrime Law'.

regulations for the NCPF exacerbates this problem, leaving institutions to operate on ad hoc directives rather than binding statutory coordination.

3 Efficacy of the Cybercrimes Act 19 of 2020

This section evaluates whether the Cybercrimes Act 19 of 2020 operates effectively in practice as South Africa's primary cybercrime statute, measured against enforcement capacity, procedural adequacy, institutional coordination, and constitutional compliance. While the Cybercrimes Act represents South Africa's first comprehensive legislative instrument designed to address cyber offences, its effectiveness depends on how its provisions operate in practice. The enactment of the Cybercrimes Act reflects a critical stage in legislative evolution; however, its effectiveness must be assessed in relation to its practical enforcement and implementation. As foundational statutes such as ECTA and RICA were rendered increasingly obsolete by rapid technological advancements, a regulatory gap emerged in which unlawful conduct risked evading prosecution leading to ineffective collection of critical evidence. This fourth phase of legislative development appears to have been necessary to update both substantive criminal law and procedural mechanisms in response to evolving cyber threats.[574] The need for a specialised legal framework becomes evident when considering the distinctions between traditional crime and cybercrime, particularly in relation to enforcement and evidentiary challenges. Differentiating offences committed in physical spaces from those perpetrated in digital environments underscores the unique challenges associated with preventing, detecting, investigating, and prosecuting cybercrime. This recognition of the specific legal complexities inherent in digital offences informs the content and scope of legislation explicitly designed to address cybercrime.[575] It consolidates fragmented provisions previously scattered across ECTA, the Prevention of Organised Crime Act 121 of 1998 (POCA), and the Financial Intelligence Centre Act 38 of 2001 (FICA). Mabunda characterises the Cybercrimes Act as "the first piece of legislation purporting to offer a comprehensive solution to

574 Papadopoulos and Snail *Cyberlaw @ SA* 472.
575 Papadopoulos and Snail *Cyberlaw @ SA* 466.

cybercrime," signalling a decisive shift from piecemeal amendments toward an integrated statutory regime.[576]

The Cybercrimes Act marks a significant development in South Africa's cybercrime response; however, its effectiveness must be evaluated against enforcement outcomes and institutional capacity. The Cybercrimes Act constitutes the primary legal framework for criminalising online conduct; however, the extent to which it achieves its intended objectives depends on its practical application.[577]

While the Act repeals and replaces outdated provisions of the ECTA and introduces new offences, questions remain regarding whether these changes have translated into improved enforcement outcomes.[578] The Cybercrimes Act imposes affirmative duties on private-sector entities; however, the effectiveness of these obligations is limited by challenges such as the use of falsified or stolen identities by cybercriminals. Notably, the legislation extends beyond mere regulation and penalisation of unlawful acts, imposing obligations on businesses, electronic communications service providers, and financial institutions concerning cybercrime. For instance, organisations targeted by cybercriminal activity are required to cooperate with and assist law enforcement authorities in the conduct of investigations relating to such offences.[579] However, this approach remains constrained by the tendency of cybercriminals to employ falsified or stolen identities, thereby undermining the reliability of corporate data submissions and complicating efforts to identify and trace offenders.[580]

However, the Act's deterrent value is tested by a relentless wave of attacks. For instance, INTERPOL data confirms that South Africa's Department of Defence fell victim to the Snatch ransomware group in late 2024, losing 1.6 TB of data.[581] Furthermore,

---

576 Mabunda, 'The South African legislative response' 18-19.
577 Snail and Musoni, 'Overview of Cybercrime Law' 301, 308.
578 Cybercrimes Act, ss 3–11.
579 Burns Y and A Burger-Smidt A, *A Commentary on the Protection of Personal Information Act* (LexisNexis Durban 2023) 462.
580 Shanine Naidoo, 'The Effectiveness of Detection and Prosecution of Cybercrime Threats Against Companies in South Africa' (LLM research report, University of the Witwatersrand 2023) 27-28.
581 INTERPOL, 16.

the LockBit ransomware group claimed responsibility for an attack on South Africa's Government Employees Pension Fund (GEPF), and the BlackSuit group attacked the National Health Laboratory Service (NHLS), compromising over 1 TB of sensitive data and disrupting medical diagnostics.[582] Ransomware attacks of this nature fall squarely within the Cybercrimes Act's cyber extortion offence,[583] which criminalises the use of threats to commit an offence for the purpose of obtaining an advantage.[584] These high-profile incidents demonstrate the severe operational consequences of cyber intrusions that the Cybercrimes Act aims to prevent.

The Cybercrimes Act introduces procedural innovations, including mechanisms for preservation of electronic evidence and expedited warrants; however, their effectiveness depends on consistent implementation and institutional capacity.[585] These provisions reflect the perspective that the Act has the potential to enhance the investigation and prosecution of cybercrimes by requiring electronic communications service providers to cooperate with law enforcement, establishing a dedicated cybercrime unit within the South African Police Service, and providing specialised training for SAPS personnel in the detection, investigation, and prevention of cybercrime.[586] These are crucial given that cyber offences frequently transcend national borders. Section 40 empowers the National Director of Public Prosecutions to facilitate international cooperation through mutual legal assistance requests.[587]

However, practical enforcement remains constrained. Despite the Cybercrimes Act's commencement in December 2021, key provisions of Chapters 5 and 6, dealing with international cooperation and mutual assistance, have not yet been fully operationalised.[588] This encompasses Chapter 5, concerning mutual assistance, and Chapter 6, relating to the designated point of contact, both of which are essential for facilitating cooperation requests from foreign states, yet the requisite point of contact

582 INTERPOL, 17.
583 Cybercrimes Act, s 10.
584 Snail and Musoni, 'Overview of Cybercrime Law' 315-316.
585 Cybercrimes Act, ch 4.
586 Burns and Burger-Smidt, *A Commentary on the Protection of Personal Information Act* 627.
587 Cybercrimes Act, s 40.
588 Cybercrimes Act, ch 5-6.

has not been established.[589] This limits South Africa's ability to collaborate with foreign jurisdictions in tracing and recovering digital evidence, a critical gap given that a substantial number of Business Email Compromise (BEC) criminals operate from the continent, with South Africa itself identified as a country of concentration for such activity.[590]

The first cases prosecuted under the new Cybercrimes Act highlight both promise and challenge. In *Okundu v S*, the Johannesburg High Court upheld a conviction for unauthorised access to a corporate network under sections 3 and 5 of the Cybercrimes Act.[591] The court affirmed that the prosecution need only prove intentional access to data without authorisation, irrespective of whether damage occurred. This decision demonstrates judicial willingness to interpret the Act broadly in order to deter cyber intrusion.

Conversely, in *Lester Connock Commemoration Fund v Brough Capital (Pty) Ltd*,[592] The High Court grappled with the intersection between cyber fraud and civil liability.[593] Although the plaintiff demonstrated unauthorised fund transfers facilitated through phishing, the court emphasised evidentiary difficulties in linking the perpetrator to the digital trace. The judgment evidenced the need for clear procedural guidance on digital evidence handling, something the Act currently lacks. Commentators have noted that the Act's enforcement is further hampered by a lack of clarity in certain procedural aspects and definitions, which creates uncertainty for investigators and prosecutors, suggesting that further guidance or regulations are needed to realise the Act's full potential.[594]

Scholars have questioned whether the Cybercrimes Act truly enhances deterrence. Lötter contends that while it modernises offence definitions, it "fails to provide an

589 Snail and Musoni, 'Overview of Cybercrime Law' 321-322.
590 INTERPOL, 17.
591 *Okundu v S*.
592 *Okundu v S*.
593 *Lester Connock* case.
594 Mongezi Mpahlwa, 'How Can South Africa Combat the Growing Threat of Cybercrime?' (De Rebus, 1 March 2025) https://www.derebus.org.za/how-can-south-africa-combat-the-growing-threat-of-cybercrime/ accessed 16 October 2025.

integrated enforcement architecture or to stipulate technical standards for forensic investigation.[595] Scholarly commentary has questioned whether the Cybercrimes Act is the 'silver bullet' it was intended to be, pointing to persistent challenges such as jurisdictional ambiguities for digital crimes and the significant burden of proof required for prosecutors to secure a conviction, which undermines its deterrent effect.[596] This is a significant vulnerability, as evidenced by high-profile ransomware attacks on essential services like Transnet and the healthcare sector.

Additionally, the Cybercrimes Act's effectiveness is tested by the rapid evolution of cybercriminal tactics, such as artificial intelligence-powered (AI-powered) 'synthetic identity fraud' and 'fraud-as-a-service' platforms.[597] This is consistent with academic projections suggesting that the continued development of information and communication technologies, including AI and the Internet of Things (IoT), will give rise to an increasing array of cybersecurity and cybercrime challenges.[598] The strategic landscape is further evolving with the emergence of AI-powered ransomware, while simultaneously, AI is being promoted as a crucial tool for defensive capabilities such as threat detection and automated response. This rapid technological evolution highlights a potential regulatory gap, suggesting that laws like the Cybercrimes Act, with its static definitions and focus on conventional cyber offences, may be insufficiently equipped to address the unique challenges posed by offensive and defensive AI technologies.[599]

Moreover, the Cybercrimes Act's definition of "computer system" remains technologically narrow. It does not explicitly include decentralised platforms or distributed ledgers, potentially excluding blockchain-based offences from its scope. This

595 Lötter, 'Comparative Critique of the Cybercrimes Act' 26.

596 S van der Merwe, 'The Cybercrimes Act 19 of 2020: A Silver Bullet?' (2024) 5(1) South African Law Journal Digital 45 https://www.lawjournal.digital/jour/article/view/313/107 accessed 16 October 2025.

597 Mpuru and Kgoale, 'Recognizing the Evolving Cybercrime Threats'.

598 Papadopoulos and Snail *Cyberlaw @ SA* 470.

599 Zelda Venter, 'Ransomware Threats: How AI Can Help Combat Cybercrime' (Independent Online, 26 June 2025) https://iol.co.za/news/education/2025-06-26-ransomware-threats-how-ai-can-help-combat-cybercrime/ accessed 17 October 2025.

gap could undermine its adaptability to emerging technologies such as cryptocurrencies and smart contracts.

The National Prosecuting Authority's Annual Report (2024) indicated that fewer than fifty cybercrime cases were finalised under the Act in its first two years of operation.[600] This statistic demonstrates limited prosecutorial reach and highlights persistent resource constraints in the Cybercrime Investigation Units.

This low prosecution rate is part of a broader enforcement crisis.[601] Independent analysis suggests that less than 1% of cybercrimes reported to the South African Police Service result in a conviction, highlighting a vast chasm between reported crime and judicial accountability.[602]

Despite these challenges, the Act provides a solid statutory foundation. Its recognition of electronic evidence, its procedural innovations, and its extraterritorial jurisdiction represent meaningful progress. However, without adequate institutional capacity and international cooperation, its deterrent effect remains largely theoretical. It may be argued that enforcement deficits reflect transitional implementation challenges rather than structural flaws; however, the persistence of these gaps, more than three years after commencement, suggests systemic rather than temporal failure.

4 The role of POPIA in Cyber resilience

This section evaluates whether the Protection of Personal Information Act 4 of 2013 operates effectively in practice as a mechanism for enhancing cyber resilience, measured against regulatory enforceability, institutional capacity, and constitutional alignment with the right to privacy. The POPIA occupies a central position in South Africa's data-governance landscape. Enacted to give effect to section 14 of the Constitution, POPIA ensures that responsible parties process personal information

600 National Prosecuting Authority, 'Annual Report 2023/24 (2024)' https://www.npa.gov.za/sites/default/files/uploads/NPA%202024%20Annual%20Report_web_2.pdf accessed 16 October 2025.

601 Econorisk, 'Cybercrime in South Africa' (Econorisk, 2025) https://econorisk.co.za/cybercrime-in-south-africa/ accessed 16 October 2025.

602 Econorisk, 'Cybercrime in South Africa' (Econorisk, 2025).

lawfully and implement reasonable security safeguards.[603] Its orientation toward privacy protection, however, creates tension with the broader goal of national cyber resilience.

Section 19 of POPIA imposes an obligation to secure personal information "through appropriate, reasonable technical and organisational measures."[604] This provision requires responsible parties to identify foreseeable risks, maintain access controls, and implement incident-response mechanisms. POPIA's mandate for these measures is directly relevant to countering the most common cyber threats, such as social engineering and phishing.[605] Yet, POPIA does not prescribe technical standards such as encryption levels or breach-response timeframes, leaving compliance largely to organisational discretion.[606]

In addition, the POPIA is notably limited in relation to international standards like the GDPR as to what constitutes 'appropriate safeguards'. It fails to prescribe a binding agreement and adequate enforcement mechanisms in order to ensure adequate data protection.[607]

Since the POPIA's full commencement in 2021, the Information Regulator has taken visible steps to enforce compliance. In 2023 it issued an enforcement notice against the Department of Justice and Constitutional Development for failing to maintain antivirus software licences and to renew firewalls.[608] This was followed by findings in the Dis-Chem Pharmacies breach of 2022, where third-party negligence led to the exposure of 3.6 million customer records.[609] These actions demonstrate regulatory commitment but

603 POPIA.
604 POPIA, s 19.
605 Mpuru and Kgoale, 'Recognizing the Evolving Cybercrime Threats'.
606 Meyer Attorneys, 'POPIA Breach Notification' (3 September 2025) https://meyerattorneys.co.za/2025/09/03/popia-breach-notification/ accessed 17 October 2025. Adinga, 'POPIA Compliance in Cloud ERP: A Complete Guide to Data Protection in the Cloud' (19 August 2025) https://adinga.co.za/popia-compliance-in-cloud-erp-adinga-cloud-erp/ accessed 17 October 2025.
607 Mthuthukisi Malahleka, 'The Problem of Trans-Border Information Flows in the Protection of Personal Information' (2024) 27 Potchefstroom Electronic Law Journal 1, 20.
608 Information Regulator, 'Enforcement Notice: DOJCD Matter' (9 May 2023) https://inforegulator.org.za/wp-content/uploads/2020/07/ENFORCEMENT-NOTICE-DOJCD-MATTER-090523.pdf accessed 16 October 2025.
609 Information Regulator, 'Enforcement Notice: Dis-Chem Pharmacies Limited' (5 February 2024) https://inforegulator.org.za/wp-content/uploads/2020/07/DIS-CHEM-ENFORCEMENT-NOTICE.pdf accessed 16 October 2025.

also reveal systemic weaknesses in cybersecurity maturity across both public and private sectors, a vulnerability starkly illustrated by the ransomware attacks on the GEPF and NHLS, which resulted in massive breaches of personal and sensitive data.[610]

Academics have debated whether POPIA effectively enhances cyber resilience or merely strengthens privacy compliance. Roos argues that POPIA's flexible, principle-based approach allows entities to adopt proportionate safeguards, fostering adaptive resilience.[611] By contrast, Papadopoulos maintains that the absence of prescriptive technical controls limits enforceability and leads to inconsistent implementation across industries.[612]

The interaction between POPIA and the Cybercrimes Act is particularly complex. While POPIA aims to protect data subjects' personal information, the Cybercrimes Act criminalises unauthorised access or interference regardless of ownership or sensitivity.[613] This statutory overlap generates interpretive uncertainty in cases of data breaches resulting from employee negligence or insider threats, raising questions regarding potential concurrent liability under both frameworks. For instance, the Cybercrimes Act criminalises "unlawful acts in respect of software or hardware tools"[614] and the "unlawful acquisition, possession, provision, receipt or use of a password",[615] which may be implicated in breaches that also engage POPIA's security safeguard obligations.[616] A significant jurisdictional challenge is that POPIA applies primarily to personal information processed within South Africa's borders. This creates a significant enforcement gap, as responsible parties may utilise cloud computing services domiciled abroad, resulting in personal information processed externally to fall outside POPIA's scope which leaves data subjects to rely on other legal remedies[617] The operational

610 INTERPOL, 16-17.

611 Anneliese Roos 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles" (2020) CILSA 53 (3) 2–3.

612 A Naude & S Papadopoulos 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)' (2016) THRHR 57.

613 POPIA; Cybercrimes Act, ss 3–11.

614 Cybercrimes Act, s 4.

615 Cybercrimes Act, s 7.

616 Snail and Musoni, 'Overview of Cybercrime Law' 313.

617 Malahleka, 'The Problem of Trans-Border Information Flows' 9.

efficacy of data protection laws is critically undermined by the persistent 'human element,' with empirical research confirming that individual users' knowledge gaps and low awareness create vulnerabilities that legislation cannot fully compensate for.[618]

Therefore, beyond technical measures, commentators stress that ongoing employee training and a culture of data protection are indispensable business imperatives for achieving true POPIA compliance and cyber resilience.[619] Overall, POPIA has elevated awareness of data protection and accountability. Nonetheless, its limited technical depth, vague extraterritorial application and reliance on a single regulator with modest resources impede its capacity to achieve systemic cyber resilience.[620]

5 Operational and enforcement challenges

This section evaluates whether South Africa's cybersecurity enforcement architecture, encompassing the South African Police Service, the National Prosecuting Authority, the Cybersecurity Hub, and supporting investigative and judicial mechanisms, operates effectively in practice, measured against institutional capacity, operational readiness, and practical enforceability. Despite legislative sophistication, South Africa's enforcement of cybersecurity laws remains constrained by limited institutional capacity and resource shortages across the investigative and prosecutorial chain. The statutory framework governing investigative procedures, particularly those relating to search and seizure, continues to be anchored in the Criminal Procedure Act 51 of 1977, a statute widely regarded as outdated and inadequately equipped to address the complexities associated with digital evidence in contemporary cybercrime investigations.[621] This accords with the broader academic consensus that, despite notable efforts to address cybercrime, law enforcement agencies frequently remain constrained by insufficient

618 Bester and Arendse, 'Measuring Cybersecurity Awareness in a South African Military Sample'.
619 JMR Software, 'Regulatory Compliance in South Africa: The Role of POPIA and PAM' (TechCentral, 19 March 2025) <https://techcentral.co.za/regulatory-compliance-popia-jmr-software/261044/> accessed 17 October 2025.
620 Malahleka, 'The Problem of Trans-Border Information Flows' 9.
621 Naidoo, 'The Effectiveness of Detection and Prosecution' 20.

technical expertise and specialised skills necessary to effectively combat such offences.[622]

The SAPS Cybercrime Unit, tasked with investigating digital offences, is severely under-resourced. Official parliamentary records corroborate the substantial under-resourcing of the South African Police Service's (SAPS) cybercrime units. As of October 2024, the cybercrime investigation support component within the Directorate for Priority Crime Investigation (DPCI) comprised only 64 members, 52 fewer than its approved establishment. Similarly, the broader cybercrime division within the Detective Services operated with merely 86 personnel, reflecting a critical shortfall of 152 investigators.[623] Its 2024 annual report recorded fewer than 80 specialised investigators nationwide.[624] The deficit of cybersecurity professionals is a well-recognised challenge, originating from shortcomings in educational curricula, and it generates a substantial gap in operational capability.[625]

A central institutional body, the South African Cybersecurity Hub, was established to promote national collaboration and serve as the coordinating focal point for cyber-incident response. However, the Hub remains thinly resourced and operates without statutory authority to compel information-sharing from private-sector entities, reflecting the wider institutional capacity constraints that hinder South Africa's cybersecurity framework.[626] This situation starkly illustrates the disparity between the state's policy ambitions and its operational capacity. The operational constraints faced by enforcement agencies are symptomatic of a deeper, systemic failure. National policy continues to deprioritise cybersecurity, hindering investment, capacity building, and enforcement.[627] This is rooted in a weak talent pipeline due to poor science, technology,

---

622 Ehiane and others, *Cybercrime and Challenges in South Africa* (2023) 173.

623 Parliamentary Monitoring Group (PMG), 'Committee Question 27090' (PMG) <https://www.pmg.org.za/committee-question/27090/> accessed 18 October 2025.

624 South African Police Service, 'Annual Report 2023/24' (2024) <https://www.gov.za/sites/default/files/gcis_document/202411/sapsannual-report2023-24.pdf> accessed 16 October 2025.

625 Khan and Mkuzangwe, 'Advancing Cybersecurity Capabilities' 2.

626 Cybersecurity Hub, 'Homepage'; CSIR, Cybersecurity Skills Survey Report (2021); Department of Communications and Digital Technologies, Cybersecurity Hub Project Description; INTERPOL, Africa Cyberthreat Assessment Report (2021).

627 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

engineering, mathematics schooling and a lack of specialised tertiary degrees.[628] To mitigate this gap, research and development (R&D) recommendations advocate recruiting or outsourcing postgraduates and computer science researchers, alongside identifying specialised cybersecurity institutions to provide targeted training for staff.[629] The state's limited technical capability, combined with insufficient law-enforcement resources, undermines the practical effectiveness of the legal framework.[630] A major operational deficiency lies in the non-implementation of essential investigative provisions of the Cybercrimes Act, specifically those concerning expedited data preservation,[631] evidence preservation,[632] and data disclosure,[633] which has significantly impeded the effectiveness of cybercrime investigations.[634] The need for enhanced technical capacity extends across the enforcement chain, with stakeholders identifying a pressing need for specialised cyber-training programmes for SAPS members, prosecutors, and the judiciary to effectively investigate, prosecute, and adjudicate complex cybercrime cases.[635] Prosecution statistics further illustrate the gap between legislative promise and operational reality. The NPA confirmed that between 2021 and 2024 fewer than 50 cases were finalised under the Cybercrimes Act.[636] Most investigations stall at the digital-forensics stage because of equipment shortages and jurisdictional barriers when data are stored on offshore cloud servers.

In an effort to address these capacity deficiencies, the SAPS has introduced a series of training initiatives aligned with the provisions of the Cybercrimes Act. These include an Orientation to the Cybercrimes Act Workshop incorporated into the basic curriculum for new recruits, an Introduction to Electronic Related Crime Scenes programme designed for first responders, and an upcoming Cybercrimes: Application and Response

628 Ramluckan, van Niekerk and Leenen, 'Research Challenges for Cybersecurity and Cyberwarfare'.
629 Khan and Mkuzangwe, 'Advancing Cybersecurity Capabilities' 5.
630 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.
631 Cybercrimes Act, s 41.
632 Cybercrimes Act, s 42.
633 Cybercrimes Act, s 44.
634 Snail and Musoni, 'Overview of Cybercrime Law' 321-322.
635 Mpahlwa, 'How Can South Africa Combat the Growing Threat of Cybercrime?'.
636 National Prosecuting Authority, Annual Report 2023/24 (2024).

module.[637] While these initiatives signify progress in fostering foundational awareness, their primarily introductory scope highlights the persistent challenge of cultivating advanced, specialised investigative expertise within an already severely understaffed force. The establishment of specialised cybercrime courts or dedicated judicial units has been proposed to enable more efficient management of cases involving complex digital evidence, ensuring a balance between human rights protections and cybersecurity requirements.[638]

The SAPS underscores the utilisation of digital forensic technologies and international cooperation as central components of its investigative approach. From a technological standpoint, available resources include digital forensic data extraction tools, media sonars, and data recovery software.[639]

Operationally, the INTERPOL National Central Bureau in Pretoria functions as a coordination hub, facilitating collaboration between domestic and international law enforcement agencies, as well as key private sector partners such as the South African Banking Risk Information Centre (SABRIC) and the Council for Scientific and Industrial Research (CSIR).[640]

Judicial literacy is another obstacle. Courts frequently admit electronic evidence without establishing authenticity as required by ECTA s 15. In *S v Ndiki*, the High Court stressed that the reliability of a computer system must be proven before its output can be accepted.[641] Subsequent cases, however, show inconsistent application of this principle. Civil litigation has begun to address cybersecurity negligence. In *Gerber v PSG Wealth Financial Planning (Pty) Ltd*, the court held that financial advisers owe a duty of care to adopt reasonable cybersecurity measures.[642] The judgment acknowledged the foreseeability of phishing risks and signalled growing judicial recognition of cybersecurity obligations within the private sector.

---

637 PMG, 'Committee Question 27090'.
638 Mabunda, 'The South African legislative response' 19.
639 PMG, 'Committee Question 27090'.
640 PMG, 'Committee Question 27090'.
641 *S v Ndiki*.
642 *Gerber v PSG.*

Despite these precedents, a systemic shortage of technical skills undermines enforcement. Digital-forensics laboratories are limited to major urban centres, while rural jurisdictions depend on overstretched provincial resources.[643] This is exacerbated by a concerning deficit in the research sector, with little evidence of a new generation of researchers emerging.[644] Coordination between the SAPS and the SSA remains uneven, illustrating the broader challenge of fragmented accountability across enforcement structures.

The 2023 Auditor-General report found that less than 40 per cent of departments had implemented NCPF-aligned cybersecurity strategies.[645] This governance shortcoming is starkly exemplified by the Transnet case, in which an analysis of annual reports from 2009 to 2022 demonstrated the board's prolonged awareness of both 'underinvestment in IT architecture and cybersecurity' and the 'ageing ICT infrastructure,' yet no substantive corrective measures were implemented, thereby leaving the organisation exposed to significant risk.[646]

The human dimension remains a critical vulnerability. A study on the SANDF reveals significant cybersecurity awareness gaps among its personnel, highlighting that the 'human element' is the weakest link in the security chain.[647] In the aftermath of major cyber incidents, government authorities have actively communicated assurances regarding the state's capacity to respond effectively. Notably, following the 2021 cyberattack on the Department of Justice and Constitutional Development, the Minister of the State Security Agency confirmed that both the National Cyber Security Centre (NCSC) and the CSIRT had been mobilized to execute the government's cybersecurity response framework, underscoring that the matter was being accorded due priority.[648]

---

643 Auditor-General South Africa, 'Government Information Systems Management' (2023–24) <https://pfma-2023-24.agsareports.co.za/pages/government-information-systems-management> accessed 16 October 2025.

644 Ramluckan, van Niekerk and Leenen, 'Research Challenges for Cybersecurity and Cyberwarfare'.

645 Auditor-General South Africa, 'Government Information Systems Management' (2023–24).

646 Scott Timcke, Mark Gaffley and Andrew Rens, 'The centrality of cybersecurity' 1–28.

647 Bester and Arendse, 'Measuring Cybersecurity Awareness in a South African Military Sample'.

648 Republic of South Africa, 'Minister Khumbudzo Ntshavheni Assures the Public of Government's

The economic cost of this operational weakness is immense, with the CSIR estimating cybercrime costs South Africa approximately R2.2 billion annually.[649] Other analyses corroborate this, estimating that cybercrime siphons billions of rands from the national economy each year, underscoring the economic imperative of strengthening enforcement capabilities.[650]

The cumulative effect of these deficiencies is a low conviction rate and declining public confidence. Without coordinated institutional reform, the deterrent value of the Cybercrimes Act and POPIA will remain largely theoretical.

6 Constitutional and Human-Rights dimensions

South Africa's cybersecurity regime operates within a constitutional democracy that jealously protects constitutionally entrenched rights to privacy, dignity, and freedom of expression. Section 14 of the Constitution of the Republic of South Africa 1996 guarantees the right to privacy, encompassing the confidentiality of communications and information.[651] This right is qualified by the limitation clause in section 36. The courts have adopted a balanced approach, restricting the right to confidentiality when justified by the public interest, as illustrated in *South African Airways SOC v BDFM Publishers (Pty) Ltd*.[652] Cybersecurity measures must therefore comply with the limitation clause in section 36, ensuring that restrictions are reasonable and justifiable.[653] In matters concerning confidential information, courts have observed that once confidentiality is lost, it cannot be restored. However, remedies to protect it remain subject to public interest considerations, necessitating a careful balancing of competing values.[654]

Work on Cyber Security' (Media statement, 6 May 2021) <https://www.gov.za/news/media-statements/minister-khumbudzo-ntshavheni-assures-public-governments-work-cyber-security> accessed 17 October 2025.

649 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

650 Econorisk, 'Cybercrime in South Africa'.

651 Constitution, s 14.

652 2016 (2) SA 561 (GJ); NQ Mabeka, 'The Prevalence of Cybercrimes and Hacking Incidents and Their Impact on the Confidentiality of Documents in Civil Proceedings' (2024) 28 *Law, Democracy & Development* 50, 53.

653 Constitution, s 36.

654 *South African Airways Soc v BDFM Publishers (Pty) Ltd* 2016 (1) All SA 860 (GI); Mabeka,

The RICA has been at the centre of constitutional scrutiny. In *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*, the Constitutional Court declared sections 16 and 17 of RICA unconstitutional due to a lack of post-surveillance notification and independent oversight.[655] The Court directed Parliament to implement safeguards that ensure proportionality and transparency in interception processes.

To date, legislative amendments remain pending. The RICA Amendment Bill 2023 proposes the establishment of an independent monitoring judge and a mandatory post-notification mechanism, but it has not yet been enacted.[656] Until then, surveillance practices remain governed by the defective 2002 framework, leaving communications vulnerable to abuse. The proposed General Intelligence Laws Amendment Bill (GILAB) has raised further concerns about expanded surveillance powers and insufficient oversight mechanisms, potentially undermining privacy and accountability safeguards.[657] Legal analysts continue to warn that RICA walks a fine line, with its deficiencies in prior judicial authorization and independent oversight leaving it open to abuse and failing to fully meet constitutional requirements, even after the *AmaBhungane* decision.[658] These debates occur against a background of previous reports, the Zondo Commission and the 2018 High-Level Review Panel on the SSA which identified serious issues of politicisation, lack of transparency, and abuse of surveillance powers. This points to an imbalance between national security objectives and constitutional safeguards.[659]

Freedom of expression presents another integral element. Chapter 3 of the Cybercrimes Act criminalises the distribution of data messages that incite violence or

---

'Prevalence of Cybercrimes and Hacking Incidents' 57-58.

655 *AmaBhungane*.

656 Department of Justice and Constitutional Development, RICA Amendment Bill 2023 (Government Gazette 48976, 2023).

657 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

658 Russel Luck, 'RICA: Walking a Fine Line Between Crime Prevention and Protection of Rights' (De Rebus, 1 February 2014) <https://www.derebus.org.za/rica-walking-fine-line-crime-prevention-protection-rights/> accessed 16 October 2025.

659 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

disclose intimate images without consent.[660] The offences relating to "malicious communications," notably the criminalisation of revenge pornography under section 16, constitute a central component of the Act.[661] While designed to combat cyberbullying and online harassment, these provisions must be interpreted consistently with section 16 of the Constitution, which protects expression unless it amounts to incitement or hate speech.[662]

In *Heroldt v Wills*, the High Court held that the malicious-communications provisions are constitutionally sound, provided prosecutors prove intent to cause harm.[663] This judicial approach aligns cybersecurity enforcement with constitutional proportionality and underscores the judiciary's role as guardian of digital rights.

7 Judicial engagement and interpretation

Judicial engagement has been instrumental in shaping the operational meaning of South Africa's cybersecurity laws. Courts have progressively clarified evidentiary standards, data-handling obligations, and the allocation of liability in digital environments.

In *Global & Local Investments Advisors (Pty) Ltd v Fouché*, the Supreme Court of Appeal held that an e-mail bearing a typed name did not constitute an electronic signature as defined under section 13(1) of the ECTA, which provides that "where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used."[664] The Court reasoned that enforceability of electronic contracts depends on verifiable authentication, thereby strengthening trust in digital transactions. This judgment demonstrated the judiciary's willingness to engage with

660 Cybercrimes Act, ch 5-6.
661 Snail and Musoni, 'Overview of Cybercrime Law' 318-319.
662 Snail and Musoni, 'Overview of Cybercrime Law' 319, 320
663 *Heroldt v Wills* [2022] ZAGPJHC 341.
664 ECTA, s 31(1); *Global* case.

technological nuances and reinforced compliance with the functional-equivalence principle enshrined in ECTA.

In contrast, the judiciary has sometimes struggled with the intersection of negligence and cybersecurity breaches. In *Edward Nathan Sonnenbergs Inc v Hawarden*, the Supreme Court of Appeal reversed a High Court decision that had imposed strict liability on a law firm targeted by a phishing scam.[665] The Court held that the firm had taken reasonable precautions and that the client's own negligence contributed to the loss. This outcome reflects a cautious judicial approach towards prescribing liability in complex cyber-fraud scenarios. Another noteworthy decision is *Gerber v PSG Wealth Financial Planning (Pty) Ltd*, where the Western Cape High Court held financial-service providers liable for failing to implement reasonable cybersecurity controls.[666]

The Court relied on expert testimony to establish foreseeability of risk, setting a critical precedent that elevates cybersecurity from a purely technical to a legal compliance issue.

Judicial interpretation has also expanded the understanding of informational privacy. In *AmaBhungane*, the Constitutional Court reaffirmed that privacy extends beyond physical space to include data and communications.[667] This decision confirmed that surveillance measures must be narrowly tailored and subject to independent oversight. Despite these progressive judgments, inconsistencies remain. Some lower courts still demonstrate limited understanding of digital-evidence handling. Procedural gaps such as verifying metadata authenticity or maintaining chain of custody continue to undermine evidentiary reliability. The absence of specialised cyber benches within the judiciary hinders consistent interpretation. To enhance jurisprudential coherence, scholars such as Mabunda propose the establishment of cyber magistrates or designated judicial officers trained in digital forensics.[668] Such institutional reform would not only standardise interpretation but also expedite case resolution. Collectively, these

665 *ENS v Hawarden*.
666 *Gerber v PSG.*
667 *Amabhungane*.
668 Mabunda, 'The South African legislative response' 8.

decisions illustrate a judiciary that is normatively receptive to cybersecurity obligations but institutionally constrained by uneven technical literacy and the absence of specialised adjudicative structures.

8 Policy and strategic implementation

The success of cybersecurity legislation depends not only on statutory design but also on strategic execution. The NCPF was intended to coordinate all stakeholders, government, private sector, and civil society under a unified national strategy. Its articulated objective was to facilitate the establishment of the National Cybersecurity Advisory Council (NCAC), tasked with overseeing the implementation of national cybersecurity strategies and the National CSIRT, while advancing a government-led, coherent, and integrated approach to cybersecurity governance.[669] It articulates ten strategic pillars, including capacity building, research and development, and international cooperation.[670]

However, practical implementation has lagged. The Auditor-General's 2023 report found that only 38 per cent of national departments had approved cybersecurity strategies aligned with the NCPF.[671] The absence of a coherent national strategy represents a significant shortcoming, as it has impeded the identification and prioritisation of key research and development initiatives necessary to enhance cybersecurity capabilities.[672] Many departments lacked risk assessments, incident-response plans, or budget allocations for cybersecurity. The effectiveness of the NCPF is critically undermined by a chronic lack of targeted funding and a shallow talent pool.[673] Coordination gaps and weak capacity persist, reducing the country's overall cyber readiness.[674] Ultimately, the fundamental objective of the NCPF is undermined by the existence of disjointed and fragmented legislative frameworks, coupled with inadequate

669 Joel Chigada, 'Towards an Aligned South African National Cybersecurity Policy Framework' (Doctoral Thesis, University of Cape Town 2023) 77.
670 NCPF.
671 Auditor-General South Africa, 'Government Information Systems Management' (2023–24).
672 Khan and Mkuzangwe, 'Advancing Cybersecurity Capabilities' 1.
673 Ramluckan, van Niekerk and Leenen, 'Research Challenges for Cybersecurity and Cyberwarfare'.
674 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

institutional coordination.[675] A consolidated governance model is essential to address the recurring challenge of fragmented mandates and weak coordination identified throughout this chapter. The DCDT oversees policy coordination, while operational incident response resides with the National Cybersecurity Hub. Yet, the Hub operates under ministerial directive rather than statutory authority, limiting its ability to compel compliance or information sharing.[676] The SSA, which manages national security threats, has overlapping jurisdiction with the SAPS Cybercrime Unit, resulting in bureaucratic friction.

Public–private cooperation remains embryonic. Although the Financial Sector Conduct Authority (FSCA) and South African Reserve Bank (SARB) have issued cybersecurity directives for financial institutions, these are non-binding and lack uniform enforcement.[677]

A recurring proposal to address this gap is the participation of organisations in cyber-threat information-sharing communities, which may enhance collective awareness of emerging threats. This will provide access to the collective knowledge, expertise, and capabilities of other entities and facilitate a more comprehensive understanding of potential threats.[678] The absence of a statutory obligation for breach reporting, except under POPIA, weakens collective situational awareness. A recurring theme in the literature is the implementation of a mandatory, anonymised threat-intelligence sharing framework, which may improve coordination between the private sector and government.[679]

For national strategy to be effective, it must be operationalized through concrete mechanisms, such as the cascading of anonymized threat data to academia and the development of context-specific tools, like the Cybersecurity Orientation Questionnaire (COQ), for state institutions.[680] Initiatives like the webinar series hosted by the

675 Chigada, ‘Towards an Aligned South African National Cybersecurity Policy Framework’ 78.
676 Cybersecurity Hub, ‘Homepage’.
677 FSCA & PA, Joint Standard 2 of 2024.
678 Khan and Mkuzangwe, ‘Advancing Cybersecurity Capabilities’ 2.
679 Mpahlwa, 'How Can South Africa Combat the Growing Threat of Cybercrime?'.
680 Ramluckan, van Niekerk and Leenen, ‘Research Challenges for Cybersecurity and

Cybersecurity Centre at the University of Cape Town (C3SA) demonstrate nascent efforts to foster the multidisciplinary dialogue and capacity building essential for a coherent national strategy.[681]

At the international level, South Africa has signed but not yet ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014). This omission constitutes a significant strategic shortfall, as the Convention mandates the establishment of comprehensive cybercrime legislation. Its ratification would promote more effective cooperation with law enforcement agencies across Member States.[682]

Likewise, South Africa has neither acceded to nor ratified the Budapest Convention on Cybercrime (2001), thereby forfeiting the advantages associated with its implementation, including established mechanisms for accessing remote cross-border electronic evidence.[683]

A major strategic impediment to data flows and trade is that POPIA has not yet been presented before the European Commission for an adequacy assessment. This means transferring personal information to and from the EU remains extensively restricted, forcing businesses to rely on more expensive and cumbersome alternative mechanisms.[684] In addition, the strategic policy conversation is evolving to include the role of emerging technologies like Artificial Intelligence, both as a defensive tool for threat detection and response and as a new domain of cyber threat, which current laws and strategies are poorly equipped to handle.[685] These omissions limit cross-border cooperation and extradition capability, leaving local enforcement agencies reliant on slow mutual legal-assistance mechanisms. Its stance in international cyber diplomacy is generally cautious and noncommittal.[686] Without legislative alignment, institutional

---

Cyberwarfare'; Bester and Arendse, 'Measuring Cybersecurity Awareness in a South African Military Sample'.

681 C3SA, 'Webinars'.

682 Snail and Musoni, 'Overview of Cybercrime Law' 307.

683 Snail and Musoni, 'Overview of Cybercrime Law' 306.

684 Malahleka, 'The Problem of Trans-Border Information Flows' 30.

685 Venter, 'Ransomware Threats'.

686 Buchan and Devanny, 'South Africa's Cyber Strategy Under Ramaphosa'.

coordination, and international collaboration, South Africa's cybersecurity architecture remains operationally fragmented, reducing the effectiveness of its otherwise comprehensive legal framework.

9 Synthesis and findings

South Africa's cybersecurity legal framework demonstrates substantive legislative sophistication but remains limited in practical effectiveness. While the Cybercrimes Act provides a robust statutory foundation, its implementation is constrained by under-resourcing, limited technical capacity, and insufficient inter-agency coordination. Consequently, despite the comprehensiveness of the legal framework, its deterrent and preventive potential is undermined by gaps in enforcement, lack of harmonisation, and a shortage of judicial expertise.[687] The disjunction between legislative intent and practical implementation is underscored by empirical evidence, which observes that, despite the introduction of extensive measures and cyber instruments aimed at curbing cybercrime, the incidence of such offences continues to rise.[688] The Cybercrimes Act provides substantive provisions, but questions remain regarding its operational effectiveness. While Chapter 2 of this study outlined the offences created under the Cybercrimes Act, its practical application raises questions regarding the effectiveness of these provisions in addressing evolving cyber threats,[689] it provides minimal operational guidance on investigative procedures, inter-agency coordination, or evidence handling. Powers relating to data preservation,[690] search-and-seizure,[691] and international cooperation[692] remain largely aspirational, and operationalisation has proven problematic, with courts even setting aside search-and-seizure warrants due to procedural deficiencies.[693] POPIA enhances privacy protection but does not directly

687 Mabeka, 'Section 7 versus Civil Proceedings' 430; Mabunda, 'The South African legislative response'.

688 Slindile Ngcece, Sazelo Mkhize and Khanyisile Majola, 'Exploring Responses to Cybercrime in South Africa: The South African Police Services (SAPS) Perspectives' (2025) Journal of Cyberspace Studies 1 https://doi.org/10.22059/jcss.2025.395262.1149 accessed 18 October 2025.

689 Cybercrimes Act, ss 2-11; See Chapter 2.

690 Cybercrimes Act, s 29.

691 Cybercrimes Act, ss 33-37.

692 Cybercrimes Act, ss 45-55.

693 *Buchler v Minister of SAPS N.O. and Others* (6310/2022) [2023] ZAFSHC 1 (5 January 2023);

translate into systemic cyber resilience.[694] RICA, despite amendments pending under the 2023 Bill, continues to infringe privacy due to inadequate oversight mechanisms.[695]

Judicial decisions, though progressively shaping cyber jurisprudence, remain inconsistent due to limited technical literacy. The NCPF, intended as the strategic umbrella, has failed to achieve effective coordination due to its non-binding nature. Consequently, enforcement remains sporadic and reactive rather than preventive. Nevertheless, South Africa's constitutional architecture and legal sophistication provide a solid foundation for reform. The analysis highlights capacity, harmonisation, and international cooperation as key factors influencing deterrence and resilience. Ultimately, as illustrated by the Transnet case, achieving this objective necessitates an acknowledgment that cybersecurity extends beyond an operational imperative; it constitutes a strategic policy priority integral to the nation's broader socioeconomic development.[696] The findings of this chapter therefore establish a basis for Chapter 4, which will benchmark South Africa's framework against global and regional regimes in order to identify best practices for strengthening its cyber-governance model.

10 Provisional conclusion

While the preceding section synthesised the empirical and doctrinal findings, this conclusion distils the key analytical findings of the chapter. The analysis in this chapter demonstrates that South Africa's cybersecurity legal framework, while legislatively comprehensive, is characterised by operational and institutional challenges that affect its practical effectiveness. The Cybercrimes Act provides a robust statutory foundation for criminalising cyber conduct,[697] and the POPIA establishes critical data-protection obligations.[698] However, the deterrent and preventive potential of this framework is compromised by persistent challenges, including institutional fragmentation,[699] severe

Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa 44 (UN Interregional Crime and Justice Research Institute 2025) 44.

694 POPIA.

695 RICA.

696 Timcke, Gaffley and Rens, The centrality of cybersecurity' 8.

697 Cybercrimes Act.

698 POPIA.

699 Snail and Musoni, 'Overview of Cybercrime Law' 313.

resource constraints within enforcement agencies,[700] and a critical shortage of technical capacity.[701]

The disjunction between legislative intent and practical implementation is starkly illustrated by the limited number of prosecutions under the Cybercrimes Act[702] and the continued escalation of high-impact cyber incidents.[703] Furthermore, the non-operationalisation of key provisions, such as those concerning international cooperation in Chapters 5 and 6 of the Cybercrimes Act, limits cross-border enforcement.[704] The NCPF, intended as a strategic umbrella, has failed to achieve effective coordination due to its non-binding nature and uneven implementation.[705] These legislative efforts, while significant, raise questions regarding their sufficiency in ensuring a resilient cybersecurity posture. As the Transnet case study underscores, cybersecurity must be recognised as a strategic policy priority integral to socioeconomic development, rather than a mere operational concern.[706]

South Africa's cybersecurity response continues to be reactive rather than preventive. Enforcement agencies such as the SAPS and the NPA grapple with substantial resource and skills shortages, while the Cybersecurity Hub lacks statutory authority to compel information-sharing or coordinate incident response effectively.[707] Judicial interpretation, despite its progressive shaping of cyber jurisprudence, reflecting limited technical literacy and the absence of specialised judicial training.[708]

Similarly, POPIA enhances individual privacy rights but fails to deliver systemic cyber resilience, largely due to its flexible, non-prescriptive safeguards and the limited

---

700 South African Police Service, 'Annual Report 2023/24' (2024) 153-154.

701 Ramluckan, van Niekerk and Leenen, 'Research Challenges for Cybersecurity and Cyberwarfare' 12.

702 National Prosecuting Authority, Annual Report 2023/24 (2024) 45.

703 INTERPOL, Africa Cyberthreat Assessment Report (May 2025) 16-17.

704 Snail and Musoni, 'Overview of Cybercrime Law' 321-322.

705 Auditor-General South Africa, 'Public Finance Management Act Report 2022/23 (2023)'.

706 Timcke, Gaffley and Rens, The centrality of cybersecurity'.

707 Parliament of the Republic of South Africa, Announcements, Tablings and Committee Reports, No 109—2025, Second Session, Seventh Parliament, Friday, 4 July 2025; PMG, 'Committee Question 27090'.

708 *Gerber v PSG; ENS v Hawarden.*

enforcement capacity of the Information Regulator.[709] This disconnect between legislative design and enforcement practice underscores a broader governance challenge, a cybersecurity framework that is normatively sound yet operationally fragile.

To achieve genuine efficacy, South Africa's cybersecurity regime must therefore progress from declaratory ambition to institutional functionality. This requires the harmonisation of overlapping statutory mandates, the establishment of a central coordinating authority or Cyber Commissioner, the operationalisation of dormant legislative provisions, and sustained capacity-building within law-enforcement and judicial sectors. Enhanced public–private collaboration and sustained public awareness are equally indispensable. Only through these structural reforms can South Africa transform its cybersecurity laws from a fragmented collection of statutes into a coherent, enforceable, and constitutionally compliant framework capable of addressing the evolving complexity of cyber threats in the digital age.

The findings of this chapter thus establish the foundation for the next chapter, which undertakes a comparative evaluation of global and regional cybersecurity regimes to identify best practices and strategic lessons applicable to strengthening South Africa's cyber governance architecture.

In conclusion, while South Africa's cybersecurity legislative and policy architecture demonstrates commendable normative progress, its practical effectiveness remains inhibited by institutional fragmentation, capacity deficits, and limited operationalisation. The Cybercrimes Act, POPIA, RICA, and NCPF collectively constitute a comprehensive statutory foundation, yet this legislative sophistication has not translated into a coherent or adequately enforced cybersecurity regime.

709 POPIA, s 39.

Chapter 4: A Comparative Analysis of EU and US Cybersecurity Governance and their Influence on South Africa's Cybersecurity Legal Framework

1 Introduction

The preceding chapter established that while South Africa has developed a sophisticated cybersecurity legislative framework on paper, its practical effectiveness is critically undermined by operational deficiencies, institutional fragmentation, and limited enforcement capacity.[710] South Africa's legislative response centred on the Cybercrimes Act 19 of 2020[711] and complementary instruments such as the Protection of Personal Information Act 4 of 2013 (POPIA),[712] signifies a decisive attempt to align domestic law with evolving global norms. A central finding was South Africa's constrained ability to engage in robust international cooperation, a weakness exacerbated by its non-ratification of key international instruments and the non-operationalisation of critical provisions within its own Cybercrimes Act.[713] As Mabunda observes, although the Cybercrimes Act provides a robust statutory framework, enforcement is undermined by the diffusion of investigative and prosecutorial responsibilities among the Directorate for Priority Crime Investigation (DPCI), the National Prosecuting Authority (NPA), and the Cybersecurity Hub.[714] This fragmentation produces overlaps and jurisdictional uncertainty, impeding coordinated responses to complex cyber offences.

Empirical evidence indicates that digital-forensics capacity within South Africa's criminal-justice system remains inconsistent and underdeveloped, with persistent case backlogs and limited technical expertise undermining prosecutorial effectiveness and the broader deterrent function of cybersecurity law.[715] Similar concerns are raised in Mabeka and Cassim's analysis, which highlights procedural misalignment between the Cybercrimes Act and civil-procedure rules, particularly in relation to the 24/7 Point of

710 See Chapter 3.
711 Cybercrimes Act.
712 POPIA.
713 Snail and Musoni, 'Overview of Cybercrime Law'. International Cybersecurity Law Review 299, 321-322.
714 Mabunda, 'The South African Legislative Response' 151–158, 189–193.
715 Naidoo, 'The Effectiveness of Detection and Prosecution' 8–9, 15–16.

Contact required for international cooperation.[716] Collectively, these studies illustrate that legislative development has outpaced institutional readiness.

Building on this diagnostic foundation, the present chapter situates South Africa's cybersecurity legal framework within its broader global and regional context. Cybersecurity governance increasingly operates within an interconnected international ecosystem shaped by shared norms, transnational cooperation, and regulatory diffusion. In this context, both the European Union (EU) and the United States of America (US) have developed mature cybersecurity ecosystems grounded in cohesive regulation, sustained institutional investment, and multi-stakeholder engagement.

The EU has progressively built a rights-based, multi-layered governance model encompassing the General Data Protection Regulation (GDPR),[717] the NIS 2 Directive,[718] the Digital Operational Resilience Act (DORA),[719] and the Cybersecurity Act 2019,[720] supported by agencies such as European Union Agency for Cybersecurity (ENISA)[721] and Europol's European Cybercrime Centre (EC3).[722] In contrast, the US operates a decentralised but operationally agile framework rooted in sector-specific statutes, including the Cybersecurity Information Sharing Act 2015 (CISA),[723] the Cybersecurity and Infrastructure Security Agency Act 2018,[724] data-protection obligations under the Gramm-Leach-Bliley Act 1999 (GLBA)[725] and the Federal

716 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 22–23.

717 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (General Data Protection Regulation or GDPR).

718 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80 (NIS2 Directive).

719 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1 (DORA).

720 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification [2019] OJ L151/15 (Cybersecurity Act).

721 ENISA, EU Cybersecurity Certification Framework (2024).

722 Europol, European Cybercrime Centre (EC3).

723 Cybersecurity Information Sharing Act of 2015, 6 USC §§ 1501–1510 (United States).

724 Cybersecurity and Infrastructure Security Agency Act of 2018, Pub L No 115-278, 132 Stat 4168 (United States).

725 Gramm-Leach-Bliley Act 1999 (GLBA), 15 USC § 6801 et seq (United States).

Information Security Modernization Act 2014 (FISMA).[726] The framework also includes voluntary standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.[727]

This chapter therefore undertakes a comparative analysis of the EU and US cybersecurity governance models and evaluates their influence on South Africa's legal and institutional framework. The comparison is conducted along four functional dimensions: (a) legislative architecture, (b) institutional coordination, (c) enforcement and operational capacity, and (d) international cooperation mechanisms, enabling a structured evaluation of how different governance models translate legal norms into practical cybersecurity resilience. It argues that the EU's normative coherence and the US's operational pragmatism together provide a composite template for improving South Africa's cyber-resilience. The analysis extends beyond black-letter law to consider institutional design, enforcement mechanisms, judicial interpretation, and policy coordination. The chapter's central thesis is that while South Africa's cybersecurity regime is substantively advanced, it remains strategically misaligned with global best practices. Accordingly, this chapter proceeds in five parts. Section 4.2 examines the Budapest Convention as the principal multilateral cybercrime framework and evaluates its implications for South Africa's non-ratification. Section 4.3 provides an in-depth analysis of the EU cybersecurity governance model. Section 4.4 evaluates the US approach. Section 4.5 undertakes a comparative analysis between South Africa and the EU (4.5.1) and between South Africa and the US (4.5.2). Section 4.6 provides a provisional conclusion synthesising the chapter's findings.

This chapter adopts a functional comparative methodology, examining how each jurisdiction addresses equivalent regulatory challenges, governance, enforcement, institutional coordination, and international cooperation, so as to derive context-appropriate lessons for South Africa. This chapter adopts a functional comparative approach, focusing not on doctrinal similarity but on how different governance models

---

726 Federal Information Security Modernization Act of 2014 (FISMA), 44 USC § 3551 et seq (United States).

727 NIST, Cybersecurity Framework 2.0 (2023).

translate legal norms into operational cybersecurity capacity and enforcement outcomes.

2 The Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime (Budapest Convention) is the world's first and most comprehensive multilateral treaty dedicated to addressing cybercrime through harmonised criminalisation, procedural powers, and enhanced international cooperation.[728] Adopted in 2001 and entering into force in 2004, the Convention remains the principal global instrument shaping domestic cybercrime legislation and cross-border enforcement practices.[729] Its significance for comparative cybersecurity governance lies not only in its substantive provisions but also in its institutional architecture, which operationalises real-time cooperation between states, a feature that is indispensable in an era where digital evidence is volatile, remotely stored, and globally distributed.

2.1 *Substantive and procedural harmonisation*

The Convention establishes a harmonised set of offences that serve as the minimum baseline for domestic cybercrime legislation.[730] These include illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery and fraud, and offences related to child pornography and copyright infringements.[731] South Africa's Cybercrimes Act largely mirrors the Convention's substantive catalogue, illustrating clear normative alignment.[732]

However, the Budapest Convention goes beyond substantive law: it provides an internationally harmonised set of procedural tools tailored to digital investigations. These include orders for expedited preservation of stored computer data, expedited preservation and disclosure of traffic data, production orders, real-time collection of

728 Council of Europe, Convention on Cybercrime (Budapest Convention) ETS No 185 (2001).
729 Budapest Convention.
730 Budapest Convention arts 2-11.
731 Budapest Convention arts 2-11.
732 Cybercrimes Act.

traffic data, and interception of content data.[733] These procedural powers enable efficient evidence-gathering across borders and impose correlating duties on states to facilitate timely assistance.

This procedural architecture is designed to overcome the inherent obstacles posed by digital investigations. Digital evidence can be fleeting; service providers may be located outside the requesting jurisdiction; and conventional mutual legal assistance (MLA) mechanisms are too slow to preserve critical logs. The Budapest Convention therefore institutionalises an accelerated cooperation framework that domestic statutes, including South Africa's Cybercrimes Act, attempt but fail to replicate without corresponding international obligations.

2.2 *The 24/7 Network and real-time cooperation*

A distinctive innovation of the Budapest Convention is Article 35, which obliges parties to establish a 24/7 point of contact capable of providing immediate assistance in cybercrime investigations.[734] This network is the operational backbone of the Convention, enabling states to request and receive urgent preservation of data, technical assistance, and expedited cooperation at any time.

Article 16 of the Budapest Convention is particularly significant for assessing South Africa's cybercrime framework, as it establishes the obligation on State Parties to ensure the expedited preservation of stored computer data, an essential procedural tool for securing volatile digital evidence.[735] This mechanism enables investigators to compel service providers to immediately preserve specified data before it is altered or deleted, and it operates in conjunction with the Convention's 24/7 contact network under Article 35.[736] South Africa's Cybercrimes Act contains general search, seizure, and production-order authority, but it does not provide an equivalent expedited-preservation procedure or impose strict timeframes on service providers.[737] Without ratification of the

733 Budapest Convention arts 16-21.
734 Budapest Convention art 35.
735 Budapest Convention art 16.
736 Budapest Convention art 35.
737 Cybercrimes Act, ss 27-30.

Convention, South Africa also lacks access to the international 24/7 network, resulting in delayed requests and frequent evidentiary loss in cross-border investigations. As commentators note, the absence of Article 16-type tools contributes to South Africa's low cybercrime prosecution rates and illustrates the broader gap between the country's normative legislative development and its limited operational efficacy.[738]

Article 17 of the Budapest Convention complements Article 16 by permitting the expedited preservation and partial disclosure of traffic data necessary to identify the wider chain of communication involved in a cyber offence.[739] This provision is crucial as traffic data, such as IP logs and routing information, is often the sole means of tracing offenders who employ anonymisation tools or operate across multiple jurisdictions. South Africa's Cybercrimes Act does not provide an equivalent targeted mechanism for rapid traffic-data preservation or disclosure, resulting in frequent investigative dead ends when ISPs overwrite logs prior to formal warrants being processed.[740] The absence of Article 17-type tools therefore reinforces the structural weakness already highlighted under Article 16: South Africa's inability to secure volatile, low-retention data in time to support effective cybercrime investigations.[741]

The EU and the US are both active participants in this network. EU Member States integrate it with their Computer Security Incident Response Teams (CSIRTs) and Europol's EC3, while the US links it with the Federal Bureau of Investigation's (FBI) Cyber Division and the National Cyber Investigative Joint Task Force (NCIJTF).[742] These integrated structures significantly increase investigative responsiveness, cross-border intelligence flows, and coordinated incident-handling.

South Africa, despite drafting the Cybercrimes Act largely in line with Budapest mechanisms, has not ratified the Convention and therefore has no access to the 24/7 network.[743] This omission has severe practical implications. While the Cybercrimes Act

738 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 127–130.
739 Budapest Convention art 17.
740 Cybercrimes Act, ss 27-30.
741 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 127–130.
742 Europol, 'European Cybercrime Centre (EC3)' (Europol, 2024); FBI, 'Cyber Division' (2024).
743 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 127–130; Council of Europe, CyberSouth Programme Evaluation Report 2023 (2023) 5–6.

requires the establishment of a Designated Point of Contact (DPoC), the enabling regulations necessary to operationalise it have not been promulgated.[744] The result is a statutory shell without functional effect. Mabeka and Cassim argue that this procedural void undermines the real-time cooperation essential for prosecuting cyber offences with transnational elements, particularly given the reliance on foreign service providers for evidence.[745]

In practice, South Africa continues to rely on slow MLA processes, which often arrive too late to preserve logs critical to attribution and prosecution. This is especially problematic in ransomware cases, phishing campaigns, botnet investigations, and financial cybercrime, all of which rely heavily on time-sensitive digital evidence.

2.3 *Implications of South Africa's non-ratification*

South Africa participated in the negotiations of the Budapest Convention in the early 2000s and has consistently maintained that the Cybercrimes Act already domesticates most of its obligations.[746] However, scholarly and institutional assessments contradict this assertion. Cassim argues that non-ratification significantly weakens South Africa's ability to respond to transnational cybercrime, as the absence of treaty-based cooperation mechanisms prevents the timely exchange of traffic data, subscriber information, and logs essential for digital investigations.[747] Mabunda notes that the lack of formal integration into the Budapest framework results in "operational isolation," undermining South Africa's credibility as a regional cybersecurity leader.[748]

The non-ratification also has regional consequences. The Southern African Development Community (SADC) Model Law on Cybercrime (2012), which draws heavily on the Budapest Convention, was designed to harmonise domestic cybercrime laws and facilitate coordinated responses across Member States.[749] South Africa's failure to ratify the Budapest Convention and to champion its adoption within SADC

744 Cybercrimes Act, s 52.
745 Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 19–28.
746 Cybercrimes and Cybersecurity Bill [B 6–2017].
747 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 123–138.
748 Mabunda, 'The South African legislative response' 72-74.
749 SADC Parliamentary Forum, Model Law on Computer Crime and Cybercrime (2012).

weakens these harmonisation efforts and limits the development of a coherent regional cybercrime enforcement network.

Moreover, South Africa's non-ratification excludes it from capacity-building programmes under the Council of Europe's CyberSouth initiative, which supports African states in digital forensics, cybercrime training, incident response, and legislative alignment.[750] This exclusion undermines domestic capability development and constrains opportunities for judicial training and prosecutorial cooperation.

2.4 *The Second Additional Protocol and emerging standards*

The Second Additional Protocol to the Budapest Convention (2021) introduces advanced mechanisms for cross-border access to electronic evidence, including direct cooperation with service providers and expedited MLA for subscriber information and traffic data.[751] The Convention standardises criminal offences such as unauthorised access, data interference, and computer-related fraud while establishing uniform procedural tools for cross-border investigations.[752] The establishment of a 24/7 network of national contact points facilitates the immediate assistance in digital investigations, thereby exemplifying the Convention's operational depth.[753] As digital infrastructure becomes increasingly cloud-based, these procedural innovations are critical. States that do not ratify the Convention and its Protocols risk falling behind global investigative standards and losing interoperability with international enforcement networks. The establishment of a DPoC within the DPCI partially mitigates this gap; however, in the absence of treaty-based obligations or reciprocal recognition, its operational capacity remains limited.[754] Persistent resource constraints and overlapping institutional

750 Council of Europe, *CyberSouth Project Overview* (2024).
751 Second Additional Protocol to the Budapest Convention on Cybercrime (opened for signature 12 May 2022).
752 Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (ETS No 189, 2021) arts 7–8.
753 Budapest Convention arts 35; van der Merwe and others, *Information and Communications Technology Law* 610.
754 Parliamentary Question No 3964 (South Africa 2023).

mandates continue to undermine South Africa's ability to deliver timely, coordinated, and effective responses to transnational cyber incidents.[755]

The EU and the US have already begun aligning domestic law enforcement practice with these standards, the EU through the E-Evidence Regulation, and the US through the CLOUD Act framework.[756] South Africa's exclusion from these developments widens the operational gap between its domestic practice and global norms.

2.5 *Analytical summary*

The Budapest Convention remains the international gold standard for cybercrime cooperation. While South Africa's Cybercrimes Act is substantively aligned with the Convention, non-ratification prevents access to its most crucial components: the 24/7 network, direct cooperation channels, harmonised procedural powers, and capacity-building programmes. The EU and US have embedded Budapest mechanisms within sophisticated institutional frameworks, ensuring seamless cross-border cooperation and operational readiness. South Africa, by contrast, remains structurally isolated despite the nation's legislative aspirations. This distinction underscores a recurring theme in the chapter: formal legislative alignment does not, in itself, ensure effective cybersecurity governance in the absence of institutional capacity, procedural integration and sustained operational investment.

In comparative terms, the Budapest Convention represents the bridge between domestic cybercrime statutes and global enforcement networks. South Africa's failure to cross said bridge leaves a significant gap between its legal framework and the international systems required to ensure its effectiveness.

3 The EU Cybersecurity governance framework

The EU's cybersecurity framework represents one of the most advanced and integrated legal ecosystems in the world. It is grounded in the principle that digital security is a

755 Naidoo, 'The Effectiveness of Detection and Prosecution' 31-35.

756 EU Regulation on European Production and Preservation Orders for Electronic Evidence (2023); CLOUD Act 2018, Pub L No 115-141.

precondition for the effective exercise of fundamental rights, economic stability, and technological sovereignty.[757] Over the past decade, the EU has evolved from a fragmented set of directives to a cohesive regime comprising horizontally applicable regulations and directives that harmonise both preventive and remedial cybersecurity measures across Member States.[758] At its core, this framework seeks to achieve a balance between fundamental-rights protection and market resilience, combining preventive obligations with coordinated enforcement.[759]

The first pillar of this architecture is the GDPR, which not only safeguards personal data but also imposes stringent cybersecurity duties through its accountability, integrity, and security principles.[760] It imposes binding obligations on controllers and processors to implement "appropriate technical and organisational measures", reflecting a preventive philosophy that links privacy and security as mutually reinforcing rights.[761] Encryption forms a central component of the EU's cybersecurity and data-protection regime. Under Article 32 of the GDPR, controllers and processors are required to implement "appropriate technical and organisational measures," which, where proportionate, expressly include encryption to the risks posed to data subjects.[762] This positions encryption as a legal obligation rather than a discretionary safeguard, reflecting the EU's rights-based philosophy that treats cryptographic protection as essential for ensuring confidentiality, integrity and resilience in data-processing operations. The treatment of encryption therefore serves as an illustrative case study of the EU's broader governance philosophy, in which technical security measures are legally mandated as instruments for protecting fundamental rights rather than left to voluntary industry discretion. ENISA guidance further reinforces encryption as a baseline organisational and technical measure applicable across all sectors.[763] Complementing this, the NIS 2 Directive replaced the 2016 NIS Directive, creating a high common level

757 European Commission, *EU Cybersecurity Strategy for the Digital Decade* (JOIN 2020 18 final) 1–2.
758 European Commission, EU Cybersecurity Strategy for the Digital Decade, 4-6.
759 European Commission, EU Cybersecurity Strategy for the Digital Decade, 4-6.
760 GDPR arts 5(1)(f) and 32.
761 GDPR art 32.
762 GDPR art 32.
763 ENISA, *Technical Guidance on Security Measures* (2022).

of cybersecurity by expanding coverage to new sectors, strengthening incident-reporting obligations, and requiring the appointment of national competent authorities and CSIRTs.[764] It mandates national strategies, risk-management frameworks, and mandatory incident-reporting within seventy-two hours.[765]

The EU's regulatory architecture has historically prioritised legislative harmonisation to ensure cross-border coherence in cybersecurity risk governance. Early iterations of the NIS Directive already required Member States to establish minimum security standards, implement "appropriate security measures," and report incidents of "significant impact" to their respective national competent authorities.[766] This model reveals a preventive philosophy centred on accountability and transparency, ensuring that critical-infrastructure operators and digital-service providers integrate security into corporate compliance frameworks rather than treating it as a discretionary technical function.

The second pillar is the DORA, which harmonises ICT-risk management in the financial sector.[767] It introduces direct obligations for banks, insurers, and service providers to implement robust security controls and continuous monitoring, while empowering the European Supervisory Authorities to enforce uniform technical standards.[768] Together, the GDPR, NIS 2 Directive, and DORA create a multilayered regime that integrates privacy, network security, and sector-specific resilience under a single governance philosophy of risk management and accountability.[769] The EU's cybersecurity architecture increasingly reflects a transition toward dynamic, risk-based supervision, most notably through the NIS 2 Directive, which replaces the prescriptive, sector-limited approach of NIS 1 with a broader, harmonised framework requiring continuous risk management across essential and important entities.[770] This shift aligns EU governance

764 Directive (EU) 2022/2555 (NIS 2 Directive) [2022] OJ L333/80 arts 3–4.
765 NIS 2 Directive, Directive (EU) 2022/2555.
766 S Grynwajc, 'US v EU: A Comparative Approach to Cybersecurity' (2014) Revue Internationale de la Compliance et de l'Éthique des Affaires 19–20.
767 Regulation (EU) 2022/2554 (DORA) [2022] OJ L333/1 arts 5–10.
768 DORA, Regulation (EU) 2022/2554, rec 7, arts 15–17.
769 GDPR; NIS 2 Directive, Directive (EU) 2022/2555; DORA, Regulation (EU) 2022/2554.
770 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2).

more closely with international approaches emphasising resilience and adaptability rather than rule-based formalism.

A further regulatory milestone is the Cybersecurity Act (2019), which made ENISA a permanent EU agency and established a Union-wide certification framework for ICT products and services.[771] According to Almeida, this consolidation created "a coherent architecture of norms, institutions and certification mechanisms that operationalise trust across the single market".[772] It embodies a preventive logic, embedding security-by-design principles in the production and procurement of digital technologies.[773]

The effectiveness of this regulatory framework is sustained through a sophisticated institutional architecture that translates legislative obligations into operational capacity. At the centre of this system is the European Union Agency for Cybersecurity (ENISA), whose mandate was strengthened under the Cybersecurity Act to include Union-wide certification, threat analysis and strategic coordination.[774] ENISA works alongside the Computer Security Incident Response Teams (CSIRTs) network, which monitors cross-border information-sharing and coordinated responses to major incidents among Member States.[775] Operational enforcement is further supported by Europol's European Cybercrime Centre (EC3), established to provide digital-forensics expertise, intelligence coordination and investigative support in cross-jurisdictional cybercrime cases.[776] Large-scale incidents are additionally managed through the Cyber Crisis Liaison Organisation Network (CyCLONe), which ensures high-level political coordination during cross-border emergencies.[777] Collectively, these bodies form a vertically integrated governance ecosystem that institutionalises the preventive, risk-based philosophy embedded in EU legislation.

---

771 Regulation (EU) 2019/881 (Cybersecurity Act) [2019] OJ L151/15 rec 16–22, 46–53.

772 Fernando Almeida, 'A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks' (2023) 13(7) Education Sciences 730 https://doi.org/10.3390/educsci13070730.

773 Fabian Teichmann and Bruno S Sergi, 'The EU Cyber Resilience Act: Hybrid Governance, Compliance, and Cybersecurity Regulation in the Digital Ecosystem' (2025) 61 Computer Law & Security Review 105354 https://doi.org/10.1016/j.clsr.2025.105354 6-8.

774 Cybersecurity Act art 3–6.

775 NIS 2 Directive arts 14–16.

776 Europol, *European Cybercrime Centre (EC3): Operational Mandate* (2013).

777 ENISA, *CyCLONe: Cyber Crisis Liaison Organisation Network* (2022).

The most recent addition, the Cyber Resilience Act (CRA) (2024), extends these principles to all digital products with embedded software or hardware connectivity.[778] Teichmann and Sergi argue that the Act establishes a hybrid governance model that integrates public regulatory authority with private-sector compliance responsibilities.[779] Manufacturers, importers, and distributors must ensure that digital products meet cybersecurity standards throughout their entire lifecycle, from design and development to post-market monitoring.[780] The CRA closes a significant regulatory gap left by the GDPR and the NIS 2 Directive by addressing vulnerabilities in both consumer-IoT and industrial-device markets, thereby aligning product-safety law with broader cybersecurity objectives. This development signals a move toward a systemic model of cyber-risk governance that integrates technological, commercial, and institutional dimensions, embedding certification, supply-chain accountability, and security-by-design requirements within a unified regulatory framework.[781] This transformation illustrates the EU's progression from a reliance on soft-law coordination to a binding, compliance-oriented governance framework, thereby institutionalising cybersecurity as a collective obligation shared between public institutions and private-sector entities.[782] The wider regulatory ecosystem is complemented by the Digital Services Act (2022), which, although not a cybersecurity instrument per se, reinforces platform accountability and risk mitigation, thereby enhancing the overall security of the digital environment.[783] The CRA strengthens the EU's risk-based governance model by imposing lifecycle cybersecurity obligations across digital supply chains.[784] As Teichmann and Sergi argue, the Act represents a shift toward a hybrid regulatory paradigm that combines traditional ex ante legislative obligations with co-regulatory mechanisms involving

778 Regulation (EU) 2024/2847 (Cyber Resilience Act) [2024] OJ L 2847, arts 2 and 6 and Annex I.
779 Teichmann and Sergi, 'The EU Cyber Resilience Act' 3–5.
780 Teichmann and Sergi, 'The EU Cyber Resilience Act' 6-8.
781 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2022) 454 final, 15 September 2022; Teichmann and Sergi, 'The EU Cyber Resilience Act' 9-10.
782 Teichmann and Sergi, 'The EU Cyber Resilience Act' 12-14.
783 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
784 Regulation (EU) 2024/2847 art 13.

shared private-sector accountability. This model embeds security-by-design principles and vulnerability-management duties, ensuring that manufacturers, importers and distributors maintain cybersecurity throughout the entire product lifecycle.[785]

The consolidation of these instruments is inseparable from the EU's broader pursuit of digital sovereignty, understood as the Union's capacity to govern data, digital infrastructures and technological ecosystems in accordance with fundamental rights and strategic interests.[786] Through instruments such as the GDPR, NIS 2 and the CRA, the EU seeks to embed cybersecurity, privacy protection and industrial competitiveness within a unified normative framework that prioritises autonomy from external dependencies.[787] The EU's cybersecurity architecture increasingly manifests a transition toward dynamic, risk-based supervision, most notably through the NIS 2 Directive. The NIS 2 replaces the prescriptive, sector-limited approach of NIS 1 with a broader, harmonised framework requiring continuous risk management across essential and important entities.[788] This shift aligns EU governance more closely with international approaches emphasising resilience and adaptability rather than rule-based formalism. This strategic orientation demonstrates the shift from fragmented policy coordination to a mature, multi-level regime in which cybersecurity functions as a foundational pillar of Europe's economic resilience and geopolitical independence.[789]

The EU's approach to cybersecurity governance increasingly incorporates cross-border cooperation and mutual-assistance mechanisms. Instruments such as the 2023 Data Privacy Framework introduced enhanced procedural safeguards for international data flows, including strengthened independent redress mechanisms and oversight structures.[790] These developments illustrate the EU's emphasis on embedding

---

785 Teichmann and Sergi, Regulation (EU) 2024/2847 art 6-8.

786 European Commission, Shaping Europe's Digital Future (2020).

787 GDPR; NIS 2 Directive; CRA.

788 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2).

789 Benjamin Farrand and Helena Carrapico, 'Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity' (2022) 31 *European Security* 435.

790 European Commission, *Data Privacy Framework Adequacy Decision* (2023).

cybersecurity and data protection within broader frameworks of digital-trade governance and transnational regulatory coordination.

Judicial developments have reinforced this sovereignty agenda by extending the territorial reach and normative authority of EU data-protection law. In *Weltimmo s.r.o v NAIH*, the Court of Justice of the European Union (CJEU) clarified that EU data-protection rules apply wherever a controller engages in "real and effective" activities within a Member State, irrespective of formal establishment.[791] Shortly thereafter, *Schrems I* invalidated the EU–US Safe Harbour framework on the basis that US surveillance practices failed to guarantee an adequate level of protection for EU citizens.[792] This trajectory culminated in *Schrems II*, which struck down the EU–US Privacy Shield for offering insufficient safeguards and insufficient judicial redress against disproportionate intelligence-gathering.[793] *Maximilian Schrems v Data Protection Commissioner* concerned a complaint by an Austrian Facebook user challenging the transfer of his personal data from Facebook Ireland to servers in the United States under the EU–US Safe Harbour framework. Schrems contended that US law failed to provide adequate protection against access by public authorities for surveillance purposes, prompting the Court of Justice of the European Union to assess the validity of the Safe Harbour Decision and the powers of national data protection authorities.[794] The judgment reaffirmed that international data transfers are permissible only where third countries offer "essentially equivalent" protection, thereby compelling global actors, including African jurisdictions, to align domestic law with EU standards in order to participate in cross-border digital trade.[795]

---

791 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-230/14) EU:C:2015:639.

792 *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650.

793 *Data Protection Commissioner v Facebook Ireland Ltd and Schrems* (C-311/18) EU:C:2020:559.

794 *Maximilian Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650.

795 Scott M Giordano, 'The Impact of Schrems II on the Modern Multinational Information Security Practice Part 1: The Potential Disruption to International Commerce' (30 November 2021) ISACA Journal <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/the-impact-of-schrems-ii-on-the-modern-multinational-information-security-practice-part-1> accessed 19 January 2026.

The EU continues to exert significant normative influence on global cybersecurity regulation through what scholars describe as the "Brussels Effect".[796] Regulatory instruments such as the GDPR, NIS 2 and the CRA have been increasingly adopted or emulated by jurisdictions seeking alignment with international digital-trade requirements. This diffusion of EU norms underscores the Union's role as a global standard-setter in cybersecurity and data governance, reinforcing its strategic objective of digital sovereignty.[797]

A further dimension of the EU's cybersecurity framework lies in its sustained investment in human-capital development and professional competence. The European Cybersecurity Skills Framework (ECSF), developed under ENISA's mandate, establishes harmonised role classifications and competency standards across the Union, creating a common language for cybersecurity professions.[798] Complementary initiatives such as the European Cybersecurity Organisation (ECSO), skills, taxonomy and the Cybersecurity Competence Network enhance workforce mobility, training alignment and cross-sector capability.[799] These measures operationalise the EU's cybersecurity strategy by ensuring that legal obligations are matched by a sufficiently skilled workforce. Almeida's comparative analysis illustrates how this approach cultivates a shared cybersecurity culture and strengthens both vertical specialisation and horizontal interoperability across Member States.[800] For jurisdictions like South Africa the EU model is a stark illustration of the importance of embedding skills governance within the broader regulatory architecture, especially as limited forensic and investigative expertise remain a barrier for the nation. [801]

Despite its regulatory maturity, the EU framework faces implementation challenges that reflect disparities in institutional capacity across Member States. ENISA's *Joint Cyber Capacity Report* notes uneven adoption of NIS 2 obligations, significant variation in

796 Bradford, *The Brussels Effect* (2020).
797 Musoni, Karkare, Teevan and Domingo, 'Global Approaches to Digital Sovereignty' vi-vii; Henten, Falch, Windekilde and Kaloudis, 'Cybersecurity Institutions' 5-6.
798 ENISA, European Cybersecurity Skills Framework (2022).
799 ECSO, Cybersecurity Skills Framework (2021).
800 Almeida, 'A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks' 745–746.
801 Naidoo, 'The Effectiveness of Detection and Prosecution' 28-31.

national incident-response readiness and persistent gaps in cross-border coordination.[802] Resource imbalances further impede consistent enforcement, with smaller Member States lacking the institutional depth required to operationalise complex certification and supervisory functions.[803] These challenges do not diminish the coherence of the EU model but highlight the practical realities of implementing an integrated supranational regime. They also demonstrate that legislative sophistication must be accompanied by sustained investment in operational capacity to achieve uniform cybersecurity resilience across the Union.[804] Rather than introducing new regulatory elements, the preceding discussion consolidates the EU's cybersecurity framework to demonstrate how legislative harmonisation, institutional design and enforcement capacity operate cumulatively as a governance ecosystem.

Collectively, these instruments establish the EU as a global norm-entrepreneur in cybersecurity law. They embed resilience into every layer of the digital ecosystem, legal, organisational, and technical, while reinforcing the Union's long-term strategic objective of achieving digital sovereignty through harmonised, enforceable standards. This consolidated framework therefore positions the European Union as the most coherent and normatively advanced supranational cybersecurity regime, providing a critical benchmark against which the approaches of the United States and South Africa are evaluated in the sections that follow.

The EU's cybersecurity governance model illustrates how legislative integration, institutional coordination, and human-capital development can function as complementary pillars of resilience. Through instruments such as the GDPR,[805] NIS 2 Directive,[806] DORA,[807] the Cybersecurity Act,[808] and the CRA,[809] the EU has achieved an advanced level of regulatory maturity and normative coherence. Enforcement bodies

802 ENISA, *Joint Cyber Capacity Report* (2024).
803 ENISA, *Joint Cyber Capacity Report* (2024).
804 ENISA, *Challenges in NIS 2 Implementation* (2023).
805 GDPR.
806 NIS 2 Directive.
807 DORA.
808 Cybersecurity Act.
809 Cyber Reliance Act.

like ENISA[810] and EC3[811] translate legal norms into operational capacity, while the ECSF[812] ensures that human skills match institutional mandates. The EU's cybersecurity framework is reinforced through ongoing professionalisation and the institutionalisation of harmonised competence standards, ensuring sustained capacity development and operational consistency across Member States.[813] Together, these elements create a governance ecosystem characterised by harmonisation, accountability, and technological sovereignty. When combined, these instruments demonstrate how the EU operationalises a cybersecurity governance model grounded in harmonisation, lifecycle accountability and institutional coherence. Through legislative integration, cross-border coordination and sustained investment in human-capital development, the EU has established a cybersecurity ecosystem that couples preventive regulation with strategic resilience.[814] Having examined the EU's vertically integrated model, the next section evaluates the US's more decentralised but operationally agile approach to cybersecurity governance.

4 The US Cybersecurity governance framework

Whereas the EU framework reflects a vertically integrated, rights-based model, the US counterpart embodies a decentralised, market-driven philosophy grounded in sectoral regulation and public–private collaboration. The US cybersecurity governance framework is fragmented but operationally coordinated through federal agencies and voluntary standards. Following the failure of the 2012 Cybersecurity Act, the President issued Executive Order 13636 of 2013 to enhance critical-infrastructure security and directed the NIST to develop a voluntary framework for improving cybersecurity practices.[815] This resulted in the NIST CSF, first issued in 2014 and revised as CSF 2.0

---

810 ENISA.
811 EC3.
812 ECSF.
813 Almeida, 'A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks' 747-749.
814 ENISA, *EU Cybersecurity Policy Overview* (2023).
815 Executive Order 13636 'Improving Critical Infrastructure Cybersecurity' (12 February 2013) https://www.govinfo.gov/content/pkg/DCPD-201300091/pdf/DCPD-201300091.pdf accessed 12 November 2025.

(2024), which organises cybersecurity outcomes into six core functions: Govern, Identify, Protect, Detect, Respond, and Recover.[816]

The Framework is non-binding but has become the principal reference model across U.S. critical-infrastructure sectors, supported by extensive cross-mapping with international standards such as ISO/IEC 27001.[817] Complementing the Framework, Congress enacted the CISA, which encourages voluntary sharing of threat indicators and provides liability protection to private entities.[818] In 2018, the Cybersecurity and Infrastructure Security Agency Act established CISA as the lead civilian body for national cyber and critical-infrastructure defence under the Department of Homeland Security.[819]

The legislative foundation of US cybersecurity is dispersed across multiple sectoral statutes. The Computer Fraud and Abuse Act 1986 (CFAA) criminalises unauthorised access and computer-related fraud, forming the cornerstone of federal cybercrime prosecution.[820] The GLBA imposes data-security obligations on financial institutions, requiring them to safeguard customer information and ensure confidentiality.[821] In the healthcare sector, the Health Insurance Portability and Accountability Act 1996 (HIPAA) mandates administrative, physical, and technical safeguards to protect electronic health information.[822]

The FISMA modernised federal information-security management by establishing risk-based assessment mechanisms and mandating each agency to implement information-security programmes.[823] It also institutionalised the role of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) in coordinating

---

816 National Institute of Standards and Technology, Cybersecurity Framework 2.0 (February 2024) https://www.nist.gov/cyberframework accessed 12 November 2025.

817 NIST, Cybersecurity Framework 2.0 Mappings to International Standards (2024) https://www.nist.gov/cyberframework/international accessed 12 November 2025.

818 Cybersecurity Information Sharing Act 2015, 6 USC §1501 et seq.

819 Cybersecurity and Infrastructure Security Agency Act of 2018, Pub L No 115-278, 132 Stat 4168.

820 Computer Fraud and Abuse Act 1986 18 USC § 1030.

821 Gramm-Leach-Bliley Act 1999 15 USC § 6801–09.

822 Health Insurance Portability and Accountability Act 1996 (HIPAA) Pub L 104-191 110 Stat 1936.

823 FISMA Pub L 113-283 128 Stat 3073.

federal cybersecurity policy. The CISA further strengthened collaboration between government and private entities by providing liability protection for companies sharing cyber-threat indicators with federal authorities.[824]

Complementing these statutory foundations are major executive and policy instruments. The National Cybersecurity Strategy 2023, issued by the White House, reframes cybersecurity as a public good, shifting the burden of security from individuals and small enterprises to critical-infrastructure owners and technology providers.[825] This marks a strategic move toward "defensible cyberspace" and introduces regulatory intervention in software liability, echoing certain EU principles of product accountability under the CRA.[826] These policy measures collectively reflect the US risk-based, adaptive, and technologically flexible approach, however, it remains frequently criticised for its fragmented statutory foundation.[827]

The US cybersecurity architecture is primarily coordinated by the CISA, established under the Cybersecurity and Infrastructure Security Agency Act 2018.[828] CISA functions as the central authority for protecting federal networks, critical infrastructure, and electoral systems. It works in tandem with the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Department of Defense (DoD) to ensure an integrated response to cyber threats.[829] The National Cybersecurity and Communications Integration Center (NCCIC) operates as a 24/7 hub for threat analysis and incident coordination.[830]

The NIST provides the technical and regulatory backbone of US cybersecurity. Its CSF, first introduced in 2014 and now in the form of its second model (2.0), offers a risk-management tool applicable across public and private sectors.[831] As an adaptable and

824 CISA Pub L 114-113 Div N.
825 United States, *National Cybersecurity Strategy* (Washington DC, March 2023) https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf accessed 11 November 2025.
826 Cyber Resilience Act.
827 Almeida, 'A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks' 747-748.
828 Cybersecurity and Infrastructure Security Agency Act 2018 Pub L 115-278 132 Stat 4168.
829 US Department of Homeland Security, CISA Strategic Intent (2019) 1–4.
830 CISA Strategic Intent (US Department of Homeland Security 2019) 5-7.
831 NIST 2-4.

non-prescriptive instrument, the CSF is widely adopted beyond US borders, influencing private-sector compliance globally, including in South Africa.[832] A further component of the US cybersecurity ecosystem is its decentralised approach to encryption governance. The United States relies primarily on the NIST to develop voluntary cryptographic standards and implementation guidelines that are widely adopted across federal agencies and critical-infrastructure operators.[833] These instruments balance strong encryption with national-security imperatives and export-control considerations, reflecting a policy orientation that emphasises technological flexibility and innovation rather than prescriptive statutory mandates.[834] Scholars observe that the United States exercises significant normative influence on global cybersecurity governance through its technological leadership, voluntary risk-management standards, and multistakeholder collaboration models, with NIST frameworks increasingly adopted by international private-sector and critical-infrastructure actors.[835]

The National Cyber Director (NCD), created by the National Defense Authorization Act 2021, ensures executive oversight and policy consistency.[836] The NCD's mandate includes coordinating budgetary allocations and aligning agency efforts with the National Cybersecurity Strategy. These overlapping and complementary institutions illustrate the US commitment to a decentralised model of governance, designed to enhance institutional responsiveness and policy adaptability within a rapidly evolving cybersecurity environment.

A distinctive feature of the US model is its heavy reliance on public–private partnerships (PPPs). Given that nearly 85% of critical infrastructure is privately owned, cooperation

---

832 Fahey, 'The Evolution of EU–US Cybersecurity Law and Policy', 1082–1085.

833 National Institute of Standards and Technology, *Recommendation for Key Management: Part 1 – General* (NIST SP 800-57 Rev 5, 2020).

834 National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 Rev 5, 2020).

835 Taiwo Justice Olorunlana, 'The U.S. Role in Shaping Global Cybersecurity Norms' (2024) 1(4) International Journal of Science, Architecture, Technology, and Environment 217, 218–223; Congressional Research Service, Cybersecurity: Deterrence Policy (Report R47011, 18 January 2022) <https://crsreports.congress.gov/product/pdf/R/R47011> accessed 26 November 2025; Johannes Tikk, Eneken Tikk & Tim Schatz, 'The Evolution of Global Cybersecurity Norms in the Digital Age' (2020) 2–4, 14–17, 22–25.

836 National Defense Authorization Act 2021 Pub L 116-283 134 Stat 3388 s 1752.

between government agencies and industry actors is integral to national resilience.[837] The Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) facilitate real-time sharing of cyber-threat intelligence across sectors such as finance, energy, and healthcare.[838]

The CISA Act 2018 formalised collaboration mechanisms, providing liability protections for voluntary reporting and encouraging threat-data exchange through secure channels like Automated Indicator Sharing (AIS).[839] The CLOUD Act 2018 further expands international cooperation by clarifying the cross-border reach of law-enforcement access to electronic data, balancing privacy concerns with investigative necessity.[840] While this decentralised structure encourages innovation and industry participation, critics argue that it produces inconsistencies and uneven enforcement across states.[841] Nevertheless, the flexible and market-responsive nature of US cyber governance has enabled rapid adaptation to emergent risks, including ransomware and supply-chain attacks. The United States has recently advanced secure-by-design principles as part of a broader shift in federal cybersecurity policy, complementing these statutory and institutional measures. The CISA now promotes Software Bills of Materials (SBOMs), default-secure configurations, and lifecycle vulnerability management as core expectations for technology manufacturers and service providers.[842] These initiatives reflect the National Cybersecurity Strategy's emphasis on reallocating responsibility from end-users to software producers and fostering greater transparency across digital supply chains.[843]

---

837 United States Government Accountability Office, 'Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, (GAO Report GAO-19-332, 25 September 2019) <https://www.gao.gov/products/gao-19-332> accessed 21 October 2025 4–6.

838 GAO, 'Actions Needed to Address Cybersecurity Risks Facing the Electric Grid (GAO-19-332, 2019)' 7-9.

839 CISA, s 6.

840 Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018 Pub L 115-141 132 Stat 348.

841 Fahey, 'The Evolution of EU–US Cybersecurity Law and Policy' 1079–1081.

842 Cybersecurity and Infrastructure Security Agency, *Secure by Design* (CISA, 2023) https://www.cisa.gov/securebydesign.

843 Executive Office of the President, *National Cybersecurity Strategy* (White House, 2023).

The US cybersecurity model demonstrates institutional pragmatism, technological innovation, and industry engagement, providing operational agility unmatched by more centralised regimes. The combined framework of statutes such as FISMA, CISA, and GLBA, together with standards like NIST CSF 2.0, establishes a robust and adaptable regulatory system that prioritises risk management over formal harmonisation. The US approach emphasises functional equivalence, pursuing cybersecurity objectives through a variety of regulatory instruments rather than rigid uniformity.[844] However, this functional flexibility also generates accountability gaps, uneven enforcement and regulatory asymmetries, particularly at state level, limiting the consistency and predictability of cybersecurity obligations across sectors.

This decentralisation also produces fragmentation which complicates cross-sectoral enforcement and international coordination. The reliance on voluntary compliance contrasts sharply with the EU's rights-based coercive structure. Convergence between the EU and the US has intensified in recent years, particularly in areas such as incident-reporting obligations and software liability frameworks, although deep-seated philosophical and regulatory divergences continue to persist.[845] The next section therefore offers a comparative synthesis, identifying how these distinct models collectively inform South Africa's pursuit of a coherent, enforceable cybersecurity framework.

From an institutional perspective, the US model demonstrates regulatory pluralism characterised by multiple agencies and overlapping jurisdictions. Henten and others describe this as a *multi-level and multi-actor* arrangement that blends public oversight with private-sector self-regulation.[846] This structure promotes agility and innovation but produces uneven enforcement and fragmented accountability across states and sectors.[847] This stands in sharp contrast to the EU's centralised, rule-based framework; however, both models demonstrate that cybersecurity resilience is ultimately grounded

844 NIST 4-6.
845 Fahey, 'The Evolution of EU–US Cybersecurity Law and Policy' 1084–1085.
846 Henten, Falch, Windekilde and Kaloudis, 'Cybersecurity Institutions' 3-6.
847 Henten, Falch, Windekilde and Kaloudis, 'Cybersecurity Institutions' 5-6.

in effective coordination among diverse institutional actors rather than in legal codification alone.[848]

5 Comparative analysis

5.1 *Comparative Analysis between South Africa and the European Union*

South Africa's cybersecurity governance framework reflects a complex interplay between ambitious legislative development and persistent operational constraints. In contrast, the European Union has constructed a coordinated, rights-based and institutionally integrated cybersecurity ecosystem. This comparative analysis evaluates how South Africa's evolving framework aligns with or diverges from the EU's mature governance model, with an aim to identify structural reforms necessary for South Africa's progression toward digital resilience. Both jurisdictions share a formal commitment to structured cybersecurity governance through legislative frameworks aimed at harmonising cybercrime enforcement, incident reporting and data-protection obligations.[849] Yet, despite these similarities, South Africa's regime remains materially weaker in coherence, enforcement design and strategic alignment with global standards. These divergences must be understood within South Africa's distinct constitutional, resource, and developmental context, which conditions the pace and form of institutional consolidation without negating the relevance of comparative benchmarks.

At a doctrinal level, South Africa's legislative choices already reflect partial convergence with EU risk-based governance principles. POPIA's security-safeguard provisions, breach-notification duties and cross-border transfer regime closely mirror the GDPR's architecture of accountability and risk management, despite the absence of explicit constitutional anchoring in a fundamental-rights framework.[850] Similarly, the Cybercrimes Act reproduces a number of cyber-offence categories and investigative powers developed in the Budapest Convention on Cybercrime, signaling an intention to

---

848 Henten, Falch, Windekilde and Kaloudis, 'Cybersecurity Institutions' 4-6.

849 Cybercrimes Act; POPIA; NIS 2 Directive; GDPR.

850 B Jones, 'Is POPIA Bad Business for South Africa? Comparing the GDPR and POPIA' (2022) 10 *Penn State Journal of Law and International Affairs* 1, 219-222.

align domestic criminal-law tools with the procedural standards that underpin European and Council of Europe cooperation on cybercrime enforcement.[851]

A central point of divergence lies in the EU's rights-based orientation. The EU's cybersecurity and data-governance framework is constitutionally grounded in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which entrench privacy and data protection as fundamental rights.[852] This normative commitment is operationalised through a comprehensive regulatory suite of instruments, the GDPR, NIS 2 Directive, DORA, the Cybersecurity Act and the proposed Cyber Resilience Act, which together embed mandatory cybersecurity, certification, incident reporting, security-by-design and coordinated supervision across Member States.[853] South Africa's equivalent protections, primarily under POPIA, lack constitutional entrenchment and are applied unevenly due to fragmentation among enforcement bodies such as the Information Regulator, the DPCI and the Cybersecurity Hub.[854] Although POPIA mirrors several GDPR principles, South Africa lacks the centralised institutional coherence that characterises EU supervisory authorities and ENISA.[855]

Judicial oversight further strengthens the EU model. In *Schrems I*, *Schrems II* and *Weltimmo*, the CJEU expanded the extraterritorial reach of EU data-protection law, reinforcing the requirement that third countries, including South Africa, provide "essentially equivalent" protection for lawful cross-border data transfers.[856] South Africa has not received an EU adequacy determination, compelling local organisations to rely on Standard Contractual Clauses, which increase compliance burdens and reduce digital-trade competitiveness.[857] This dynamic exemplifies what Bradford terms the 'Brussels Effect', whereby EU regulatory standards exert de facto extraterritorial influence through market access conditionality, shaping the legislative and compliance

---

851 Cybercrimes Act; Budapest Convention.

852 Charter of Fundamental Rights of the European Union [2012] OJ C326/02, arts 7–8.

853 GDPR; DORA; COM(2022) 454 final (Cyber Resilience Act).

854 POPIA; AGSA Consolidated General Report on National and Provincial Audit Outcomes 2022–23.

855 GDPR; ENISA.

856 Case C-362/14 *Schrems I* EU:C:2015:650; Case C-311/18 *Schrems II* EU:C:2020:559; Case C-230/14 *Weltimmo* EU:C:2015:639.

857 European Commission, 'Adequacy Decisions' (2023).

choices of third countries, such as South Africa, despite the absence of formal adequacy status.[858] Unlike the EU, South Africa lacks a powerful supranational or constitutional judicial body capable of steering normative evolution in cybersecurity governance.

Institutional architecture marks a further contrast. The EU leverages an integrated governance model involving ENISA, the CSIRTs Network, Europol's EC3, Eurojust and CyCLONe, ensuring strategic coordination, operational support, certification and cross-border incident response.[859] The Cybersecurity Act 2019 formalises ENISA's long-term mandate, enabling the translation of legislative obligations into operational capability.[860] South Africa's institutional landscape, by contrast, is fragmented across the DPCI, SAPS, SSA, DCDT, the Cybersecurity Hub and the Information Regulator, without a statutory coordinating authority.[861] The NCPF envisaged a unified structure, yet implementation remains inconsistent, with AGSA reports identifying persistent governance failures in leadership, interdepartmental alignment and execution.[862] The absence of an ENISA-type national body materially weakens South Africa's ability to coordinate threat intelligence, incident response and regulatory oversight.

Enforcement capacity illustrates these structural divergences. The EU operates under harmonised supervisory authorities capable of imposing corrective measures and significant administrative fines, including GDPR penalties of up to 4% of global turnover, alongside NIS 2's requirement for proportionate and dissuasive sanctions.[863] South Africa's enforcement environment remains comparatively weak. The Information Regulator has limited resources and investigative reach and has yet to develop a strong sanctioning record under POPIA.[864] Cybercrime prosecution suffers from inadequate digital-forensics expertise, inconsistent evidence-handling and limited coordination

858 Bradford, *The Brussels Effect* (2020).
859 ENISA; EC3; Eurojust; CyCLONe.
860 Regulation (EU) 2019/881 (Cybersecurity Act) [2019] OJ L151/15.
861 Mabunda, 'The South African legislative response' 42-44.
862 NCPF; Auditor-General South Africa, *PFMA General Report 2022–23*.
863 GDPR art 83; NIS 2 Directive arts 32–34.
864 Information Regulator (South Africa), Information Regulator Annual Report 2022/2023 (2023) https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf accessed 5 December 2025.

among SAPS, the DPCI and the NPA.[865] These deficiencies confirm that South Africa's enforcement challenges arise not from legislative insufficiency but from institutional under-capacity.

Procedural cooperation also diverges sharply. EU Member States benefit from the Budapest Convention's harmonised procedural tools, expedited preservation, real-time traffic-data collection and a 24/7 point-of-contact network which facilitate rapid cross-border investigations.[866] South Africa, having not ratified the Convention, remains excluded from these mechanisms, significantly impairing its ability to obtain or preserve electronic evidence in transnational cases.[867] Accordingly, while the EU operates within an integrated investigative ecosystem, South Africa's cybercrime framework remains domestically constrained despite possessing comparable procedural powers under the Cybercrimes Act.[868]

Digital sovereignty further illustrates the normative gap. The EU embeds cybersecurity within its broader strategic-autonomy project, aligning digital rights, certification, supply-chain security and industrial policy.[869] South Africa, while constitutionally recognising privacy and access to information, lacks a coherent digital-sovereignty strategy.[870] POPIA's cross-border transfer provisions are less stringent than the GDPR, and South Africa lacks a certification regime comparable to the EU Cybersecurity Act. This leaves ICT product security largely outside formal regulatory oversight.[871]

Human-capital development reinforces these contrasts. The EU has built extensive skills-governance structures through initiatives such as the ECSF, the Cybersecurity Competence Network, the Digital Europe Programme and the European Cybersecurity Skills Academy.[872] South Africa has no equivalent national skills framework; cyber-

865 Naidoo, 'The Effectiveness of Detection and Prosecution' 28-31; NPA Annual Report 2022–23.
866 Budapest Convention arts 16-17, 32, 35.
867 Snail and Musoni, 'Overview of Cybercrime Law' 320-322.
868 Cybercrimes Act.
869 European Commission, '2030 Digital Compass' COM(2021) 118.
870 Constitution of the Republic of South Africa, 1996, s 14.
871 POPIA, s 72; GDPR; Cybersecurity Act.
872 ENISA, *European Cybersecurity Skills Framework* (2022).

forensics capacity is limited, skills pipelines are underdeveloped and structured interagency mobility is minimal.[873] These deficiencies undermine the practical enforceability of South Africa's cybersecurity legislation.

International cooperation constitutes another dividing line. The EU is deeply embedded in global cybersecurity governance through the Budapest Convention, the EU Cyber Diplomacy Toolbox, NATO cooperation, UN processes and strategic partnerships with the US and other allies.[874] South Africa remains outside key treaties such as the Budapest Convention and the Malabo Convention, limiting access to structured cross-border cooperation, capacity-building and coordinated legal assistance.[875] This isolation weakens the operationalisation of South Africa's domestic cybercrime framework.

Finally, the regulatory philosophies of the two jurisdictions diverge. The EU follows a precautionary, rights-based, harmonisation-driven model that integrates cybersecurity into digital-governance, economic and human-rights architectures. In contrast, South Africa's model is reactive and security-centric, prioritising criminalisation and law enforcement over systemic resilience, risk management and rights integration.[876] This reactive posture diminishes long-term policy coherence and operational effectiveness.

Overall, South Africa has adopted several EU-inspired principles but has not replicated the EU's institutional consolidation, consistent enforcement, judicial oversight or international alignment. The EU's cybersecurity order demonstrates that legislative sophistication must be accompanied by coordinated institutions, robust enforcement, comprehensive skills investment and embedded participation in global governance.[877]

---

873 Department of Communications and Digital Technologies, *National Digital and Future Skills Strategy* (2020); Naidoo, 'The Effectiveness of Detection and Prosecution' 31-33.

874 Council of the European Union, Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (19 June 2017) ST 10474/17 <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf> accessed 30 November 2025.

875 Budapest Convention; Malabo Convention (2014).

876 NCPF.

877 Cybersecurity Act; ENISA; EC3; Eurojust; CyCLONe.

Absent such structural reforms, South Africa risks sustaining a cybersecurity framework that is normatively modern yet operationally fragile.

5.2 *Comparative Analysis between South Africa and the United States*

The United States maintains one of the world's most operationally agile, intelligence-driven and innovation-oriented cybersecurity ecosystems. It is built on decentralised governance, strong public–private partnerships, sector-specific legislation, voluntary risk-based standards and a mature cyber-defence apparatus shaped by national-security imperatives.[878] South Africa, by contrast, operates a fragmented institutional system primarily grounded in criminal-law approaches, limited investigative capacity, underdeveloped forensic infrastructure and minimal integration into global cybersecurity networks.[879] This comparative analysis examines the structural contrasts between South Africa and the US across key themes, revealing profound implications for South Africa's ability to build a coherent, resilient cyber-governance framework.

The US cybersecurity framework is characterised by a decentralised, sector-specific legislative architecture complemented by powerful executive instruments and voluntary technical standards. Core statutes include the Computer Fraud and Abuse Act 1986 (CFAA), the Homeland Security Act 2002, the Cybersecurity Information Sharing Act 2015 (CISA 2015), the Federal Information Security Modernization Act 2014 (FISMA 2014), and the Gramm-Leach-Bliley Act 1999 (GLBA).[880] These statutes govern federal systems, critical infrastructure, intelligence-led cybersecurity, information sharing and private-sector obligations.

Crucially, US cybersecurity legislation is functionally supported by binding presidential directives and executive orders, such as Executive Order 13636 (2013) on critical-infrastructure cybersecurity and Executive Order 14028 (2021) on enhancing national

878 Executive Office of the President, *National Cybersecurity Strategy* (2023).
879 Cybercrimes Act; NCPF; Naidoo, 'The Effectiveness of Detection and Prosecution' 31-33.
880 Computer Fraud and Abuse Act 1986; Cybersecurity Information Sharing Act 2015; Federal Information Security Modernization Act 2014; Gramm-Leach-Bliley Act 1999.

cybersecurity.[881] This creates an adaptive, responsive regulatory ecosystem with the ability to evolve rapidly with emerging threats.

South Africa's legislative framework, by contrast, is composed mainly of the Cybercrimes Act, the POPIA and limited sectoral regulations.[882] These statutes provide criminal-law foundations and data-protection requirements but lack the breadth, specificity and technical sophistication of US equivalents. Unlike the US, South Africa does not employ executive instruments to update cybersecurity strategy, nor does it maintain statutory frameworks tailored to individual sectors such as finance, energy, healthcare, defence or telecommunications.

Where US legislation is iterative, layered and policy-integrated, South Africa's legislation remains largely static, criminal-justice-oriented and institutionally isolated. This results in mismatched capabilities between the legal framework and the operational realities of cyber threats.

US cybersecurity governance is anchored in a dense, interconnected institutional ecosystem that includes the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the United States Cyber Command (USCYBERCOM), the Office of the National Cyber Director (ONCD), and numerous sectoral supervisory bodies.[883] These institutions operate across defensive, offensive, intelligence, regulatory and policy layers.

CISA, established by the Cybersecurity and Infrastructure Security Agency Act 2018, is the central civilian authority responsible for protecting federal networks, supporting critical infrastructure and coordinating national incident response.[884] It maintains incident-response playbooks, threat advisories, vulnerability bulletins, information-sharing platforms and sector-specific guidance.

---

881 Executive Order 13636 (2013); Executive Order 14028 (2021).

882 Cybercrimes Act; POPIA.

883 Cybersecurity and Infrastructure Security Agency; Federal Bureau of Investigation; National Security Agency; United States Cyber Command; Office of the National Cyber Director.

884 Cybersecurity and Infrastructure Security Agency Act 2018.

The FBI's Cyber Division provides investigative leadership on cybercrime, while NSA and USCYBERCOM conduct intelligence collection, defence and offensive cyber operations.[885] This multi-layered governance model ensures strategic coherence, rapid operational response and integrated defence capability.

South Africa lacks comparable institutional depth. Cybersecurity responsibilities are fragmented among SAPS, DPCI, SSA, DCDT, the Information Regulator and the Cybersecurity Hub, none of which possess clear hierarchical authority, adequate resources or inter-agency coordination mechanisms.[886] The absence of a statutory National Cybersecurity Centre or a dedicated civilian cyber-defence agency equivalent to CISA represents a structural gap. Enforcement agencies often operate with limited digital-forensics capacity, inadequate budgets and unclear operational mandates, impeding effective coordination.

The US demonstrates that cybersecurity governance requires layered institutions with clear mandates, strategic leadership and operational capacity. South Africa's challenges stem not from poor statutory design but from the absence of institutional architecture capable of implementing and enforcing its laws.

The US maintains advanced cyber-enforcement structures comprising nationwide digital-forensic laboratories, coordinated federal cyber task forces, sector-specific regulatory authorities, established cyber incident-response centres, and extensive criminal, civil and regulatory enforcement instruments. Federal agencies regularly collaborate with private industry to investigate ransomware, insider threats, espionage and supply-chain attacks.[887] In addition, The Department of Justice (DOJ) and FBI run joint operations with international partners, underpinned by powerful statutory tools such as the CFAA and the Stored Communications Act.[888] The US justice system possesses mature forensic-science infrastructure, continuous training and multidisciplinary cyber units capable of handling complex investigations.

---

885 Federal Bureau of Investigation, *Cyber Division Strategic Plan* (2022).
886 NCPF.
887 Department of Justice (US), *Ransomware Task Force Report* (2021).
888 Computer Fraud and Abuse Act 1986; Stored Communications Act 1986.

South Africa's enforcement capacity is comparatively constrained. Conviction rates remain extremely low, a reflection of systemic constraints that include insufficient forensic specialisation, immature digital-evidence practices and fragmented institutional arrangements across enforcement bodies.[889] Forensic units rely on outdated technologies and lack certified specialists comparable to those in FBI or DHS laboratories.[890] Multiple institutions operate in silos, causing duplication of effort and long delays in cyber investigations.

The US model illustrates how a multi-agency, resource-intensive enforcement ecosystem improves investigative outcomes, whereas South Africa's fragmented enforcement structures undermine the operational effectiveness of its cybercrime statutes.

A defining strength of the US cybersecurity ecosystem is its extensive public–private partnerships (PPPs). Critical infrastructure in the US is approximately 85% privately owned, making industry collaboration indispensable.[891] Public–private partnerships are supported through mechanisms such as Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), CISA's Automated Indicator Sharing (AIS) platform, the Joint Cyber Defense Collaborative (JCDC), and a range of sectoral regulatory bodies responsible for coordinating and strengthening cyber resilience.

These entities facilitate real-time sharing of threat indicators, vulnerabilities, attack patterns, and mitigation strategies between government and private industry.[892] Such partnerships produce actionable intelligence that strengthens national cyber resilience and accelerates incident response. Recent scholarship similarly emphasises that these operational arrangements double as vehicles for norm entrepreneurship: by institutionalising information-sharing coalitions, alliances and public–private initiatives

889 SAPS Crime Statistics 2023; NPA Annual Report 2022–23; Naidoo, 'The Effectiveness of Detection and Prosecution' 28-31.

890 FBI; US Department of Homeland Security, *Official Website* https://www.dhs.gov/ accessed 5 December 2025.

891 Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Overview* (2023).

892 CISA, *Joint Cyber Defense Collaborative Charter* (2021).

with major technology firms and critical-infrastructure operators, the United States has positioned itself as a central architect of global cybersecurity norms, whereas South Africa largely remains a norm-taker on the periphery of these processes.[893]

South Africa's engagement with the private sector is limited, ad hoc and not institutionally formalised. There is no national cyber information-sharing mechanism, mandatory reporting platform or standing public–private collaborative body comparable to CISA's JCDC.[894] Private-sector entities frequently refrain from reporting incidents due to reputational concerns, limited trust in government agencies and the lack of legal or regulatory incentives.

The US clearly demonstrates how cybersecurity governance cannot function effectively without structured cooperation between the public and private sectors. South Africa's absence of such frameworks perpetuates fragmented intelligence, slow detection and inconsistent response patterns.

The United States is the global leader in cybersecurity standards development through the National Institute of Standards and Technology (NIST). NIST produces key components of the US standards architecture, among them the Cybersecurity Framework (CSF 2.0), the Risk Management Framework (RMF), cryptographic standards, supply-chain security guidance and sector-specific control regimes.[895] NIST CSF 2.0 organises cybersecurity into six core functions: Identify, Protect, Detect, Respond, Recover and Govern, and is widely adopted internationally due to its flexibility, technological neutrality and practical orientation.[896] US agencies and private industries use NIST frameworks as the baseline for risk management.

---

893 Taiwo Justice Olorunlana, 'The US Role in Shaping Global Cybersecurity Norms' (2024) 1(4) International Journal of Science, Architecture, Technology and Environment 217–224; Benjamin Madnick, Keman Huang and Stuart Madnick, 'The Evolution of Global Cybersecurity Norms in the Digital Age: A Longitudinal Study of the Cybersecurity Norm Development Process' (2024) 33 Information Security Journal: A Global Perspective 204.

894 Department of Communications and Digital Technologies, *Cybersecurity Hub Overview* (2022).

895 National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (2024).

896 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (2014; updated 2024).

South Africa lacks a national cybersecurity standards regime. There is no equivalent to the NIST CSF, no mandatory baseline controls, no cyber maturity model and no national standardised incident-response framework. Sectoral regulators such as the SARB or FSCA have issued limited cybersecurity guidance for financial institutions, but no cross-sector, national-level standard exists.[897]

The absence of a unified risk-based standard contributes to inconsistent organisational practices, weak incident reporting, and insufficient supply-chain risk controls. This deficiency illustrates how South Africa's cybersecurity governance has evolved without the technical foundations necessary for national coherence.

The US integrates cybersecurity deeply into its national-security apparatus. NSA, USCYBERCOM, the Department of Defense and the Office of the Director of National Intelligence (ODNI) all play substantive roles in cyber defence, intelligence collection, foreign cyber operations and threat attribution.[898] The US National Cyber Strategy explicitly positions cybersecurity as a national-security and economic-security priority.

South Africa lacks intelligence-led cyber coordination mechanisms. State Security Agency (SSA) possesses broad statutory functions but suffers from institutional dysfunction, capacity deficits, lack of transparency and limited cyber-operational capability.[899] Unlike the US, South Africa has no dedicated military cyber command, no intelligence-driven attribution programme and no structured national-security approach to cyber defence. This divergence is profound. While the US employs an offensive–defensive, intelligence-driven cyber policy, South Africa's approach remains predominantly reactive and law-enforcement-centric, lacking strategic foresight.

US procedural powers for cybercrime investigation include real-time data collection, wiretap authorisations, mutual legal assistance treaties (MLATs), and extraterritorial

897 South African Reserve Bank, Cybersecurity Guidance Note (2021).
898 United States Cyber Command, Vision and Strategy (2020).
899 High-Level Panel Report on the SSA, Reform of the State Security Agency (2021).

warrants under the CLOUD Act.[900] These instruments enable US agencies to obtain data stored overseas and facilitate rapid cross-border cooperation.

South Africa's Cybercrimes Act includes procedural powers such as expedited preservation and search and seizure of digital evidence.[901] However, without ratification of the Budapest Convention or similar treaties, South Africa lacks institutional access to global cooperation networks, MLAT fast-tracking and 24/7 investigative assistance.[902] This exclusion prevents South African authorities from participating in the Convention's expedited preservation and disclosure mechanisms, including direct law-enforcement-to-law-enforcement requests for volatile digital evidence.[903] The problem is compounded by the non-operational status of South Africa's Designated Point of Contact, resulting from the absence of enabling regulations. As a result, investigations involving transnational cybercrime remain dependent on slow, formal diplomatic channels that are structurally misaligned with the speed at which digital evidence can be altered or destroyed, leading to delayed investigations and evidentiary loss. By contrast, the United States demonstrates how procedural integration with global cooperation networks enhances cybercrime enforcement capacity, highlighting South Africa's continued structural isolation.

The US invests heavily in cybersecurity talent through the National Initiative for Cybersecurity Education (NICE), federal funding programmes, academic partnerships, military cyber academies, and workforce frameworks.[904] The NICE Cybersecurity Workforce Framework, codified in NIST Special Publication 800-181 Rev. 1 (2020), provides a detailed taxonomy of roles, tasks and knowledge areas for the cybersecurity workforce across government, industry and academia, giving the United States a common competency baseline that South Africa currently lacks.[905] Thousands of

900 CLOUD Act.
901 Cybercrimes Act, ss 26–40.
902 Budapest Convention.
903 Mabunda, 'The South African legislative response' 193-194.
904 National Initiative for Cybersecurity Education Framework (NIST 2017; updated 2020).
905 National Institute of Standards and Technology, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST SP 800–181 rev 1, 2020).

certified digital-forensics professionals, malware analysts, threat hunters and cryptographers populate both government and private sectors.

South Africa faces severe human-capital deficits. Forensic units are understaffed, lack continuous training, and operate without specialised certification frameworks.[906] Academic programmes in cybersecurity remain fragmented, and there are no national skills frameworks to align competencies across institutions. The US illustrates that cybersecurity resilience depends on professionalised, well-resourced and continuously trained human capital. South Africa's skills environment reveals systemic underinvestment.

The US is deeply embedded in global cybersecurity diplomacy through bilateral agreements, the Budapest Convention, the G7, the Quadrilateral Security Dialogue, the UN OEWG, NATO partnerships and Five Eyes intelligence collaboration.[907] These networks reinforce interoperability, intelligence sharing, incident coordination and cyber defence. South Africa remains absent from major global cybersecurity treaties and initiatives, including the Budapest Convention and Malabo Convention.[908] It participates in UN processes but lacks a coordinated cyber-diplomacy strategy or dedicated cyber foreign-policy unit. Its absence from global 24/7 cooperation networks severely undermines the operationalisation of its Cybercrimes Act.[909]

The US adopts a pragmatic, innovation-driven cybersecurity policy. It is market-oriented, intelligence-centric and prioritises risk management, operational agility and public–private collaboration.[910] Cybersecurity is framed as an economic and national-security issue rather than a fundamental-rights issue.

South Africa's regulatory philosophy is predominantly compliance-driven and punitive, with cybersecurity treated as a criminal-justice function rather than a systemic

906 Department of Justice and Constitutional Development, *Cybercrime Capacity Assessment* (2023).
907 US Department of State, *International Cyberspace and Digital Policy Strategy* (2024).
908 Budapest Convention; Malabo Convention.
909 Cybercrimes Act.
910 White House, *National Cybersecurity Strategy* (2023).

governance challenge.[911] Unlike the US, South Africa lacks incentives for industry participation, government–industry collaboration or voluntary standards adoption. The philosophical divergence shapes practice: US cybersecurity governance prioritises agility and innovation, while South Africa prioritises punitive legal frameworks without the infrastructure needed to support them.

The comparison between South Africa and the United States reveals deep structural, operational and philosophical divergences. The US model is characterised by decentralised governance and powerful institutions. Coordination is intelligence-led and reinforced through extensive public–private partnerships. This architecture is supported by robust enforcement capacity, mature standards frameworks, sustained skills development, and deep international integration. South Africa's model is characterised by fragmented institutions, limited capacity, narrow statutory tools, absent information-sharing mechanisms, weak human capital, minimal international integration and a reactive governance approach.

The US experience demonstrates that South Africa must integrate cybersecurity across strategic policy domains. They must also institutionalise public–private partnerships, adopt risk-based national standards and invest in specialised enforcement competencies. Finally, it is crucial that they leverage international cooperation to augment domestic capability and establish coordinated institutional arrangements to ensure operational resilience.

Without structural reform inspired by these principles, South Africa risks remaining normatively aligned with global developments while remaining operationally unprepared for the realities of modern cyber threats.

Taken together, the EU and US models demonstrate that cybersecurity effectiveness emerges not from legislative density alone, but from the alignment of law, institutions, skills and international cooperation, a convergence that South Africa has yet to achieve. This comparative analysis does not purport to establish empirical causation between

911 NCPF.

governance models and cybersecurity outcomes, but rather identifies structural correlations and institutional design patterns that shape regulatory effectiveness.

6 Provisional Conclusion

South Africa's cybersecurity framework demonstrates significant legislative progress but remains undermined by fragmented institutions, weak operational capacity, limited international alignment, and uneven enforcement. The comparative analysis of the EU and US models demonstrates that effective cybersecurity governance depends not only on comprehensive statutory instruments but on coordinated institutions, risk-based regulatory coherence, integrated skills development, and sustained global engagement. While the EU offers a structured, rights-based and institutionally harmonised system, and the US provides an agile, innovation-driven, multi-agency model anchored in public–private collaboration. South Africa has adopted elements of both models in a fragmented and institutionally incoherent manner, without embedding the institutional architecture necessary to operationalise them. The absence of a central coordinating authority, limited forensic capability, inadequate inter-agency cooperation, and non-ratification of key instruments such as the Budapest Convention[912] collectively weaken the implementation of otherwise advanced laws such as POPIA[913] and the Cybercrimes Act.[914] To achieve genuine cyber resilience, South Africa must prioritise institutional consolidation, develop a national skills framework, harmonise procedures across agencies, modernise its national cybersecurity policy, and integrate into international cooperation networks.[915] The chapter's contribution lies in demonstrating that South Africa's cybersecurity challenge is not normative deficiency but governance execution. This positions institutional reform, rather than legislative expansion as the primary determinant of future cyber resilience. Without these structural reforms, South Africa risks remaining normatively aligned with global standards but operationally unable to meet the demands of an evolving cyber-threat landscape.

---

912 Budapest Convention.
913 POPIA.
914 Cybercrimes Act.
915 Naidoo, 'The Effectiveness of Detection and Prosecution' 31-33; Mabunda, 'The South African legislative response' 42-44.

Chapter 5: Conclusion and Recommendations

1 Final Conclusion

The study examined South Africa's cybersecurity framework through doctrinal, institutional, jurisprudential and comparative lenses. It thoroughly assessed the interaction between the Cybercrimes Act 19 of 2020,[916] the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA),[917] the Electronic Communications and Transactions Act 25 of 2002 (ECTA),[918] the Protection of Personal Information Act 4 of 2013 (POPIA),[919] and the National Cybersecurity Policy Framework (NCPF),[920] within South Africa's constitutional order.

The central finding of this study, however, is that South Africa's cybersecurity challenge is no longer primarily legislative in nature. While the statutory framework is broadly aligned with international norms at a doctrinal level, its practical efficacy remains constrained by fragmented institutional governance, limited investigative and prosecutorial capacity, weak operational coordination, and insufficient mechanisms for international cooperation.[921] This has produced a persistent disjuncture between formal legislative sophistication and functional cyber-resilience.

Chapter 2 traced the historical evolution of South Africa's cybersecurity laws, illustrating that early instruments such as ECTA and RICA were enacted in response to the emergence of electronic communications and surveillance technologies rather than contemporary cyber threats.[922] Although foundational in recognising electronic evidence, electronic contracting and lawful interception, these statutes were reactive and sector-specific. Consequently, they proved ill-suited to address modern cyber phenomena such as ransomware, business email compromise, large-scale data

916 Cybercrimes Act.
917 RICA.
918 ECTA.
919 POPIA.
920 NCPF.
921 Snail and Musoni, 'Overview of Cybercrime Law'.
922 ECTA; RICA.

breaches and transnational cyber extortion.[923] The enactment of the Cybercrimes Act therefore represented a necessary intervention aimed at consolidating fragmented offences and introducing procedural tools tailored to digital investigations.[924] However, the practical efficacy of the Cybercrimes Act must be assessed against the reality that the Act entered into force through a staggered commencement, with several provisions excluded pending further proclamation. This resulted in critical aspects of implementation and cross-border effectiveness remaining constrained, undermining deterrence and enforcement value.[925]

Chapter 3 evaluated the framework in practice and identified institutional fragmentation as a profound structural weakness. Overlapping mandates across enforcement, intelligence and regulatory bodies have produced duplication, uncertainty and weak accountability.[926] Empirical indicators, including low prosecution and conviction outcomes relative to the scale of cybercrime, reinforce the conclusion that enforcement capacity is severely constrained.[927] POPIA contributes meaningfully to cyber resilience by embedding security-safeguard obligations into data governance, but it cannot compensate for deficiencies in criminal enforcement and digital-forensics capability.[928]

Chapter 4's comparative analysis demonstrated that the European Union (EU) and the United States (US) have translated legal norms into operational capacity through coherent governance models, sustained institutional investment and deeper integration into international cooperation mechanisms.[929] Most critically, the analysis exposed the strategic cost of South Africa's non-ratification of the Budapest Convention on Cybercrime. This non-ratification has limited access to expedited data preservation mechanisms, the 24/7 network and structured real-time cooperation, which is essential

---

923 Cassim, 'Addressing the Growing Spectre of Cyber Crime in Africa' 123.

924 Cybercrimes Act.

925 President of the Republic of South Africa, Proclamation R 42 in Government Gazette 45562 (30 November 2021) (Commencement of Certain Sections of the Cybercrimes Act 19 of 2020) (listing commenced Chapters and exclusions).

926 Auditor-General of South Africa, *Consolidated General Report on National and Provincial Audit Outcomes 2022–2023* (Republic of South Africa, 2023).

927 National Prosecuting Authority, Annual Report 2023/2024 (Republic of South Africa, 2024).

928 POPIA; Naidoo, 'The Effectiveness of Detection and Prosecution' 8–9, 15–16.

929 Council of Europe, Convention on Cybercrime (Budapest Convention, ETS No 185, 2001) arts 16, 17, 35.

for investigating transnational cybercrime.[930] Recent industry analysis further reinforces the dissertation's conclusion that emerging technological threats will accelerate the scale and sophistication of cybercrime, strengthening the case for adaptive legal and institutional responses rather than static compliance models.[931]

2 Gaps identified

2.1 *Gaps identified in the current legislation*

The first core finding is that South Africa's cybersecurity framework is substantively comprehensive but functionally constrained. The Cybercrimes Act consolidates cyber offences, modernises investigative powers and aligns domestic criminal law with international cybercrime norms.[932] POPIA embeds security-safeguard obligations into organisational data-governance practices, while ECTA and RICA provide foundational recognition of electronic evidence, electronic transactions and lawful interception.[933] At a doctrinal level, South Africa therefore possesses the essential legislative tools required to address contemporary cybercrime.

However, the research demonstrates that legislative sufficiency does not ensure consistent enforcement outcomes. As outlined in Chapter 3, the operational environment in which the Cybercrimes Act functions remains fragmented. Although offence provisions and certain investigative mechanisms are available, the broader procedural, institutional and cooperative ecosystem envisaged by the Cybercrimes Act is not yet fully embedded in practice.[934] This has produced a situation in which cybercrime is criminalised in principle, but addressed inconsistently in application.

The consequences of this partial operationalisation are evident in prosecutorial practice. Complex cyber-enabled offences, including business email compromise and large-

930 Budapest Convention arts 35.
931 IOL Business Report, 'Cyber Security in 2026: Where the Next Wave of Threats Will Strike' (IOL, 1 January 2026) https://iol.co.za/business-report/economy/2026-01-01-cyber-security-in-2026-where-the-next-wave-of-threats-will-strike/ accessed 1 January 2026.
932 Cybercrimes Act.
933 ECTA; RICA; POPIA.
934 Proclamation R 42 GG 45562 (30 November 2021).

scale fraud, are frequently pursued through common-law offences rather than through the specialised provisions of the Cybercrimes Act.[935] This weakens the statute's deterrent effect, obscures the development of cyber-specific jurisprudence and undermines the Act's role as the central pillar of South Africa's cybercrime response.

2.2 *Institutional fragmentation as a structural weakness*

The second finding is that institutional fragmentation constitutes a systemic weakness within South Africa's cybersecurity governance architecture. Cybercrime investigation, intelligence gathering, regulatory oversight and incident response are dispersed across multiple institutions, including the South African Police Service (SAPS), the Directorate for Priority Crime Investigation (DPCI), the National Prosecuting Authority (NPA), the State Security Agency (SSA), the Information Regulator and the Cybersecurity Hub.[936]

This dispersion of mandates has resulted in overlapping responsibilities, unclear lines of accountability and coordination failures during significant cyber incidents.[937] In practice, uncertainty often arises regarding which institution has lead responsibility for incident response, evidence preservation and engagement with private-sector entities.[938] Such ambiguity delays response times, undermines evidentiary integrity and weakens public confidence in state capacity.

Oversight reports have repeatedly identified deficiencies in cyber-risk management, outdated ICT infrastructure and weak internal controls across public institutions.[939] These findings reinforce the conclusion that institutional fragmentation is not merely an administrative inconvenience, but a structural impediment to effective cybersecurity enforcement.

---

935 NPA Annual Report 2023/2024; Snail and Musoni, 'Overview of Cybercrime Law' 320-322; Mabunda, 'The South African Legislative Response' 40–45; Mabeka and Cassim, 'Interpreting the Provisions of the Cybercrimes Act' 22–23.

936 NCPF.

937 Stewart 'Understanding South African Cybersecurity Law' (2025).

938 Stewart 'Understanding South African Cybersecurity Law' (2025).

939 Auditor-General of South Africa, *Consolidated General Report on National and Provincial Audit Outcomes 2022–2023* (Republic of South Africa, 2023).

Comparative analysis demonstrates that jurisdictions with integrated governance architectures, such as the EU under NIS2 and the US under the CISA model, achieve superior outcomes by centralising coordination authority while retaining sector-specific expertise.[940] South Africa's current architecture lacks an equivalently empowered coordinating node, resulting in a reactive rather than strategic cybersecurity posture.

2.3 *Enforcement deficits and the legitimacy of Cybercrime law*

The third finding concerns the relationship between enforcement effectiveness and the legitimacy of cybercrime law. Criminalisation assumes deterrence only where there is a credible likelihood of detection and sanction. Persistently low prosecution and conviction rates for cybercrime therefore undermine both the practical and normative authority of the Cybercrimes Act.[941]

Where victims perceive that reporting cybercrime yields little prospect of redress, under-reporting increases and reliance on informal or private risk-management strategies becomes more common. This dynamic disproportionately disadvantages individuals, small businesses and vulnerable data subjects who lack the resources to absorb cyber losses independently. Over time, enforcement deficits erode public trust in the criminal justice system and weaken compliance incentives.

The research confirms that enforcement capacity is not a peripheral concern, but a central determinant of whether cybersecurity law operates as an effective regulatory instrument or merely as symbolic legislation.

2.4 *POPIA's preventative contribution and its structural limits*

The fourth finding is that the POPIA has made a meaningful contribution to cybersecurity through its preventative orientation.[942] Section 19 of POPIA obliges responsible parties to implement appropriate technical and organisational measures to

940 Directive (EU) 2022/2555 (NIS 2 Directive); Cybersecurity and Infrastructure Security Agency Act of 2018 (United States).
941 NPA Annual Report 2023/2024; INTERPOL, African Cyberthreat Assessment Report (2023).
942 POPIA.

safeguard personal information, thereby promoting baseline cyber-security practices across both public and private sectors.[943]

However, POPIA's contribution is inherently limited by its regulatory design. POPIA was not intended to function as a cybercrime statute, and its enforcement mechanisms focus on compliance and administrative accountability rather than criminal investigation and prosecution.[944] As a result, POPIA is unable to compensate for deficiencies in digital-forensics capacity, investigative expertise or international cooperation. While POPIA strengthens organisational resilience and risk management, it operates alongside, rather than in place of effective criminal enforcement mechanisms.

2.5 *Deficits in International cybercrime cooperation*

The fifth finding is that South Africa's limited integration into international cybercrime cooperation frameworks constitutes a critical strategic weakness. Cybercrime is inherently transnational, with perpetrators, infrastructure and digital evidence frequently dispersed across multiple jurisdictions. Effective enforcement therefore depends on rapid and reliable cross-border cooperation.

South Africa's sustained non-ratification of the Budapest Convention on Cybercrime and its Second Additional Protocol, deprives domestic authorities of access to expedited data-preservation procedures, the 24/7 contact network and direct cooperation channels essential for time-sensitive investigations such as ransomware and business email compromise.[945]

This significantly constrains investigative effectiveness and limits South Africa's ability to respond to cybercrime at the speed required by contemporary threat environments.

943 POPIA, s 19.
944 POPIA, s 39.
945 Budapest Convention; Council of Europe, Second Additional Protocol to the Convention on Cybercrime (2021).

3 Recommendations

The research suggests that legislative reform should therefore be targeted and purposive, aimed at enabling existing statutes to function as an integrated enforcement framework rather than introducing additional layers of regulation. This section advances four interrelated legislative reform priorities. In doing so, it recognises that measures directed at the full operationalisation of existing statutory mechanisms and the facilitation of effective coordination and cross-border cooperation warrant earlier attention, as they directly affect enforcement capability. Other reforms, while no less significant, are appropriately understood as complementary and sequential within a broader, integrated reform agenda.

3.1 *Ratification of the Budapest Convention on Cybercrime*

The first legislative reform priority concerns the ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention) and its Second Additional Protocol.[946] Ratification would not require a fundamental restructuring of South Africa's substantive cybercrime law. The Cybercrimes Act already reflects substantial normative alignment with the Convention's offence catalogue, including provisions addressing unlawful access, data interference, system interference and cyber-enabled fraud.[947]

The principal value of ratification lies not in offence creation, but in operational cooperation. The Budapest Convention provides mechanisms for expedited preservation of stored computer data, partial disclosure of traffic data, mutual legal assistance procedures tailored to digital evidence, and a continuously available 24/7 network for urgent cooperation.[948] These mechanisms are essential in time-sensitive investigations such as those concerning ransomware, business email compromise and distributed denial-of-service attacks, where digital evidence may be altered or destroyed within hours.

---

946 Budapest Convention; Council of Europe, Second Additional Protocol to the Convention on Cybercrime (2021).

947 Cybercrimes Act.

948 Budapest Convention arts 16–17, 35.

South Africa's continued non-ratification deprives law-enforcement authorities of access to these tools and forces reliance on slower, traditional mutual legal assistance processes that are ill-suited to the velocity of cybercrime.[949] This gap undermines investigative effectiveness and weakens South Africa's credibility as a regional leader in cybersecurity enforcement.[950] Accordingly, ratification would represent a low-cost, high-impact reform that directly addresses one of the most significant structural weaknesses identified in this dissertation.

3.2 *Harmonisation of Cybercrime-related legislation*

The second reform priority is legislative harmonisation. South Africa's cybersecurity framework is dispersed across multiple statutes, POPIA, ECTA, RICA and the Cybercrimes Act, each enacted in response to different technological and policy concerns.[951] While this incremental development is understandable, it has produced overlapping mandates, inconsistent terminology and uncertainty regarding procedural interfaces.

Harmonisation does not necessitate the consolidation of all cyber-related provisions into a single statute, nor does it entail the redefinition of concepts already articulated in existing instruments such as ECTA and RICA. Rather, Parliament should pursue a structured harmonisation process aimed at clarifying how these existing definitions operate across statutes in the context of cybercrime investigation and enforcement. This includes aligning the application of established concepts such as "data", "interception" and "electronic communication" across POPIA, RICA, ECTA and the Cybercrimes Act, and clarifying the legal interfaces between investigative powers under the Cybercrimes Act, interception authorisations under RICA, and data-protection obligations under POPIA. In addition, harmonisation should address operative concepts that are relied upon but not expressly defined, most notably the notion of "lawful

949 Mabunda, 'The South African legislative response'.
950 SADC Parliamentary Forum, Model Law on Computer Crime and Cybercrime (2012).
951 Snail and Musoni, 'Overview of Cybercrime Law' 320-322.

authority", which plays a central role in determining the legality of access, interception and disclosure of data across these instruments.

For purposes of legislative coherence, "lawful authority" could be defined as follows:

"'Lawful authority' means permission or consent, or other legally recognised authorisation, relating to data or electronic communications in the possession or control of a data subject, data holder, responsible party or operator, granted in terms of an applicable law of the Republic, and exercised in accordance with constitutionally compliant procedures, including any required judicial or statutory oversight, for the purposes of access, interception, preservation, seizure, disclosure or processing of such data or communications."

Doctrinal clarity is particularly important where encryption, compelled assistance and access to stored data are concerned. Uncertainty in these areas risks inhibiting lawful investigations while simultaneously exposing the state to constitutional challenge. Legislative harmonisation would therefore enhance legal certainty for investigators, prosecutors, service providers and courts, reducing reliance on ad hoc interpretation and improving enforcement consistency.

3.3 *Full operationalisation of the Cybercrimes Act*

The third reform priority is the full operationalisation of the Cybercrimes Act. The enforcement deficiencies identified in this study stem primarily from the partial commencement and incomplete operationalisation of the Cybercrimes Act, rather than from gaps in the substantive offence provisions themselves.[952] In this context, reform is required to bring existing statutory mechanisms into full effect through regulation, designation and procedural clarification, rather than to amend or expand the offence framework.

Full operationalisation requires three complementary measures. First, the outstanding regulatory, directive and designation-based measures contemplated by the

[952] Proclamation R 42 GG 45562 (30 November 2021).

Cybercrimes Act must be finalised. This includes those required to give practical effect to data-preservation procedures, international cooperation mechanisms, service provider reporting obligations, and the designation and operation of competent authorities under the Act. Where statutory mechanisms depend on institutional designation, reporting structures or procedural guidance, delay in implementation renders the underlying provisions legally inert.

Second, Parliament should require the development of binding operational directives and standard operating procedures for agencies responsible for enforcing the Act, particularly the SAPS, the DPCI and the NPA. Without such guidance, enforcement practice remains inconsistent and overly dependent on individual capacity rather than institutional process.[953]

Third, the Act's international cooperation mechanisms should be aligned with Budapest Convention standards, even prior to formal ratification. This includes ensuring that South Africa's designated points of contact are adequately staffed, technically competent and continuously available. Legislative oversight should focus on whether these mechanisms function in practice, not merely whether they exist on paper.

3.4 *Digital evidence, cloud data and procedural reform*

A further legislative gap identified by this research concerns the treatment of digital evidence, particularly in cloud-based and transnational environments. South Africa lacks a unified statutory framework governing the preservation, seizure, transfer and admissibility of digital evidence. In the absence of a unified statutory framework governing digital evidence, courts are required to rely on general evidentiary principles and ad hoc procedural adaptations, resulting in uncertainty, inconsistency and fragmented judicial approaches to the admissibility and evaluation of electronic evidence.[954]

---

953 NPA Annual Report 2023/2024.

954 Criminal Procedure Act 51 of 1977; *S v Ndiki* 2008 (2) SACR 252 (C); D van der Merwe and others, *Information and Communications Technology Law* (3rd edn, LexisNexis 2022).

The Cybercrimes Act addresses certain aspects of evidence, including data preservation and search and seizure, but does not comprehensively regulate chain of custody, integrity verification, metadata handling or access to cloud-stored data held by foreign service providers. As digital infrastructure increasingly migrates to distributed cloud environments, these gaps become more pronounced.

Legislative reform should therefore prioritise the development of a coherent digital-evidence regime, either through amendments to the Criminal Procedure Act or through a dedicated Digital Evidence Code of Practice. Such a framework should address minimum standards for evidence preservation, authentication, forensic imaging and cross-border data access, while remaining consistent with constitutional safeguards and POPIA's data-protection principles.[955]

By clarifying procedural expectations and evidentiary standards, legislative reform in this area would strengthen prosecutorial success rates and enhance judicial confidence in digital evidence, thereby directly addressing the enforcement deficits identified in this study.

4 Institutional and policy recommendations

While legislative reform is a necessary component of strengthening South Africa's cybersecurity framework, it is insufficient on its own. As demonstrated in this study, the principal weaknesses undermining the efficacy of South Africa's cybercrime regime arise from institutional fragmentation, capacity deficits and weak operational coordination. Effective cybersecurity governance therefore requires targeted institutional and policy interventions designed to translate statutory authority into sustained enforcement capability.

4.1 *Strengthening Cybercrime investigation and prosecution capacity*

The first institutional priority is the development of specialised cybercrime capacity within the SAPS, the DPCI and the NPA. Cybercrime investigations increasingly require

955 POPIA, s 19; Criminal Procedure Act.

expertise in digital forensics, malware analysis, cryptocurrency tracing, cloud-based evidence collection and cross-border data access.[956] Generalist investigative models are ill-suited to these demands.

This research confirms that specialist capacity remains concentrated in a small number of units, with limited reach across provinces and local jurisdictions. As a result, investigative quality varies significantly, and complex cyber-enabled cases are often deprioritised or inadequately prepared for prosecution.[957] Sustained investment is therefore required to expand dedicated cybercrime units, supported by ring-fenced funding for forensic tools, secure evidence environments and continuous technical training.

Prosecutorial capacity must be developed in parallel. Cybercrime cases frequently involve complex evidentiary issues relating to data integrity, attribution and chain of custody. Without prosecutors who are both legally and technically competent, even well-investigated cases risk collapse at trial.[958] Institutional reform should therefore include the creation of specialist cybercrime prosecution teams within the NPA, supported by structured collaboration with investigators from the earliest stages of case development.

4.2 *Clarifying institutional mandates and national coordination*

A second institutional reform priority is the clarification of mandates and the strengthening of national coordination mechanisms. South Africa's cybersecurity governance landscape remains characterised by overlapping responsibilities distributed across multiple institutions, including SAPS, the DPCI, the SSA, the Information Regulator, sector-specific regulators and the Cybersecurity Hub.[959]

---

956 Naidoo, 'The Effectiveness of Detection and Prosecution' 20; Mpuru and Kgoale, 'Recognizing the Evolving Cybercrime Threats'; Venter, 'Ransomware Threats'; INTERPOL, African Cyberthreat Assessment Report (2023).

957 Auditor-General Consolidated General Report 2022–2023.

958 NPA Annual Report 2023/2024.

959 NCPF.

This fragmentation has produced uncertainty regarding leadership during significant cyber incidents, weakened information-sharing and delayed response times.[960] Institutional reform should therefore prioritise the establishment of a clearly defined national coordination architecture. One option is to elevate the Cybersecurity Hub into a statutorily empowered national Computer Security Incident Response Team (CSIRT), with explicit authority to coordinate incident reporting, threat intelligence sharing and cross-sector response.[961]

Clear coordination does not require the centralisation of all cyber functions, but it does require unambiguous leadership, formalised reporting channels and enforceable cooperation obligations.

Such reforms would directly address the governance deficits identified in section 5.2 of this chapter and align South Africa more closely with international best practice.

4.3 *Enhancing public–private cooperation and information sharing*

Given that much of South Africa's critical digital infrastructure is privately owned, effective cybersecurity governance cannot be achieved through state action alone. Banks, telecommunications providers, cloud service providers and technology firms play a central role in both preventing and responding to cyber incidents.[962]

Institutional reform should therefore include the development of structured public–private cooperation mechanisms. This includes mandatory incident-reporting thresholds for critical sectors, standardised information-sharing protocols and legal safeguards to encourage voluntary disclosure without disproportionate liability exposure. International experience demonstrates that timely information sharing significantly enhances national situational awareness and response capability.[963]

---

960 Polity, 'SAA Cyber Incident and Cybersecurity Law'.

961 NCPF; Cybersecurity Hub (South Africa), 'About Us' <https://www.cybersecurityhub.gov.za/about-us\> accessed 16 October 2025.

962 POPIA, s 19.

963 Directive (EU) 2022/2555 (NIS2 Directive).

Such cooperation must be grounded in clear legal frameworks that balance cybersecurity objectives with data-protection and confidentiality obligations. POPIA provides an important baseline, but additional guidance is required to clarify how personal data may be lawfully shared for cybersecurity and law-enforcement purposes.

4.4 *Adapting institutional capacity to emerging technologies*

The final institutional recommendation concerns preparedness for emerging technologies. Recent developments in cybercrime are characterised by increased automation and scalability, allowing criminal conduct to be replicated rapidly across multiple targets and jurisdictions. These developments challenge enforcement models that rely on reactive investigation and individualised attribution, reinforcing the need for regulatory and institutional frameworks capable of responding to volume, velocity and cross-border complexity.[964]

Institutional reform must therefore recognise the growing importance of human–machine collaboration in cybersecurity enforcement. This includes the adoption of AI-assisted analytics for threat detection, network monitoring and forensic triage, while retaining human oversight to ensure accountability and constitutional compliance.

The expansion of cloud computing and Software-as-a-Service platforms further complicates enforcement by dispersing data across multiple jurisdictions. Institutional capacity must evolve accordingly, incorporating cloud-forensics expertise and cross-border investigative coordination. Without such adaptation, enforcement mechanisms risk becoming obsolete in the face of rapidly evolving threat environments.

5 Concluding reflections

This dissertation has critically examined the development and efficacy of South Africa's cybersecurity laws in combating cybercrime within a constitutional, institutional and comparative framework. It has demonstrated that South Africa has made significant progress in developing a modern and rights-conscious legislative architecture through

964 IOL Business Report, 'Cyber Security in 2026'.

instruments such as the Cybercrimes Act, the Electronic Communications and Transactions Act, the Regulation of Interception of Communications and Provision of Communication-Related Information Act, the Protection of Personal Information Act and the National Cybersecurity Policy Framework. However, the central contribution of this study lies in its finding that the principal impediments to effective cybersecurity governance in South Africa are no longer primarily legislative, but structural and operational in nature. Fragmented institutional mandates, partial operationalisation of key statutory mechanisms, limited investigative and prosecutorial capacity, and weak integration into international cooperation frameworks have resulted in a persistent gap between legal design and enforcement reality. From a constitutional perspective, this gap is significant. This is clear as cybercrime directly threatens fundamental rights while the expansion of cyber-policing and surveillance powers simultaneously raises concerns relating to proportionality, oversight and accountability under section 7(2) of the Constitution.[965]

The study further demonstrates that cyber resilience cannot be achieved through law in isolation, but requires the convergence of legislative clarity, institutional competence, technological expertise and effective international cooperation. Comparative experience from the European Union and the United States illustrates that cybersecurity effectiveness depends on governance models capable of translating legal norms into coordinated operational practice, highlighting the strategic cost of South Africa's continued exclusion from key international cybercrime cooperation mechanisms in an inherently transnational threat environment. Ultimately, this dissertation concludes that cybersecurity constitutes a core governance challenge with profound implications for constitutional democracy, economic security and public trust, and that addressing the deficiencies identified in this study is crucial in order to strengthen cybercrime enforcement and to uphold the constitutional promise in an increasingly digital society.

965 Constitution, ss 7(2), 14, 16, 32; *AmaBhungane*.

Bibliography

Books

Bradford A, *The Brussels Effect*

Bradford A, *The Brussels Effect: How the European Union Rules the World* (OUP 2020)

Burns and Burger-Smidt, *A Commentary on the Protection of Personal Information Act*

Burns Y and A Burger-Smidt A, *A Commentary on the Protection of Personal Information Act* (LexisNexis Durban 2023)

Ehiane and others *Cybercrime and Challenges in South Africa*

Ehiane and others *Cybercrime and Challenges in South Africa* (Palgrave Macmillan 2023)

Papadopoulos and Snail *Cyberlaw @ SA*

Papadopoulos S and Snail S *Cyberlaw @ SA: The Law of the Internet in South Africa* (4th edn, Van Schaik 2021)

Shinder and Cross, Scene of the Cybercrime

Debra Littlejohn Shinder and Michael Cross, Scene of the Cybercrime (2nd edn, Elsevier 2008)

Tikk, Tikk and Schatz, *Evolution of Global Cybersecurity Norms (2020)*

Tikk J, Tikk E and Schatz T, 'The Evolution of Global Cybersecurity Norms in the Digital Age' in Eneken Tikk and Mika Kerttunen (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020)

van der Merwe and others *Information and Communications Technology Law*

van der Merwe and others *Information and Communications Technology Law* (1st edn, LexisNexis 2008)

van der Merwe and others *Information and Communications Technology Law*

van der Merwe and others *Information and Communications Technology Law* (3rd edn, LexisNexis 2022)

Von dem Bussche and Voigt *EU GDPR: A Practical Guide*

Von dem Bussche A and Voigt P *The EU General Data Protection Regulation (GDPR)* (2nd edn Springer 2024)

Constitution

Constitution of the Republic of South Africa, 1996

Legislation

Banks Act 94 of 1990

Child Justice Act 75 of 2008

Computer Evidence Act 57 of 1983

Correctional Services Act 111 of 1998

Criminal Law Amendment Act 105 of 1997

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Criminal Procedure Act 51 of 1977

Critical Infrastructure Protection Act 8 of 2019

Cybercrimes Act No. 19 of 2020

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Financial Intelligence Centre Act 38 of 2001

Financial Sector Regulation Act 9 of 2017

Independent Communications Authority of South Africa Act 13 of 2000

Insurance Act 18 of 2017

National Key Points Act 102 of 1980 (repealed)

National Prosecuting Authority Act 32 of 1998

Protection of Personal Information Act 4 of 2013

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

South African Police Service Act 68 of 1995

Case law

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services [2021] ZACC 3

Boudewyn Homburg de Vries Smuts N.O and Others v MEC for Department of Economic Affairs and Others (1199/2021) [2022] ZAECGHC 35 (26 July 2022)

Buchler v Minister of SAPS N.O. and Others (6310/2022) [2023] ZAFSHC 1 (5 January 2023)

De Jager v Netcare Limited and Others (42041/16) [2025] ZAGPPHC 141

FirstRand Bank Limited v Ayob and Another 045157/2023) [2025] ZAGPPHC 350 (15 April 2025)

FirstRand Bank Limited t/a Wesbank v Govendor [2023] ZAGPJHC 610

Fourie v Van der Spuy and De Jongh Inc. and Others (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019)

Gerber v PSG Wealth Financial Planning (Pty) Ltd (36447/2021) [2023] ZAGPJHC 270 (23 March 2023)

Global & Local Investments Advisors (Pty) Ltd v Fouché (SCA) (unreported case no 71/2019, 18-3-2020)

Hartog v Daly and Others (A5012/2022) [2023] ZAGPJHC 40; [2023] 2 All SA 156 (GJ) (24 January 2023)

Hattingh v S (A307/2015) [2016] ZAWCHC 199

Hawarden v Edward Nathan Sonnenbergs Inc (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ); 2023 (4) SA 152 (GJ)

Heroldt v Wills [2022] ZAGPJHC 341

Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC).

Lester Connock Commemoration Fund v Brough Capital (Pty) Ltd and Another (28646/2020) [2023] ZAGPJHC 1329; 2024 (2) SA 486 (GJ) (16 November 2023)

Mgoqi v S [2020] ZAECGHC 33

Momentum Metropolitan Life Limited v Lavender Hill Trading 544 CC and Another (19204/23) [2025] ZAWCHC 99

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

Ndlovu v S (CA&R14/2016) 2016 ZAECBHC 12. 12

Okundu v S [2016] ZAECGHC 131

R v Douvenga (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported)

S v Berend Howard unreported case no 41/258/02, Johannesburg Regional Magistrates Court

S v Lucky Majangandile Erasmus and Felix Unathi Pupu (2023)

S v Tandwa and Others 538/06) [2007] ZASCA 34; 2008 (1) SACR 613 (SCA) (28 March 2007)

Salzmann v S (755/18) [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200 (SCA)

Smuts N.O. and Others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism and Others (1199/2021) [2022] ZAECMKHC 42 (26 July 2022)

South African Airways Soc v BDFM Publishers (Pty) Ltd and Others (2015/33205) [2015] ZAGPJHC 293; [2016] 1 All SA 860 (GJ); 2016 (2) SA 561 (GJ) (17 December 2015)

Thint (Pty) Ltd v National Director of Public Prosecutions and Others; *Zuma and Another v National Director of Public Prosecutions and Others* (CCT 89/07; CCT 91/07) [2008] ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC); 2008 (12) BCLR 1197 (CC) (31 July 2008)

Regional instruments

Commission Implementing Decision (EU) 2023/1795 (Data Privacy Framework) [2023] OJ L 231/118

> Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework (notified under document C(2023)4745) [2023] OJ L 231/118

Convention on Cybercrime

> Convention on Cybercrime (ETS No. 185) (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 (Convention on Cybercrime)

Directive (EU) 2022/2555, NIS 2 Directive on Measures for a High Common Level of Cybersecurity across the Union [2022] OJ L333/80

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80

EU Charter of Fundamental Rights

Charter of Fundamental Rights of the European Union [2012] OJ C 326/02

European Commission, EU Cybersecurity Strategy for the Digital Decade

Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final (16 December 2020) CELEX 52020JC0018

ISO 27032

International Organization for Standardization, ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity (International Organization for Standardization 2012)

Malabo Convention

African Union, African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023) 29560 Treaty No 0048

Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) [2016] OJ L119/1

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2019/881, Cybersecurity Act on ENISA and ICT Certification [2019] OJ L151/15

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification [2019] OJ L151/15

Regulation (EU) 2022/2065

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1

Regulation (EU) 2022/2554

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1 (DORA)

Regulation (EU) 2023/1543 (e-Evidence Regulation)

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118

Regulation (EU) 2024/2847 (Cyber Resilience Act)

Regulation (EU) 2024/2847 (Cyber Resilience Act) [2024] OJ L 2847, arts 2 and 6 and Annex I. European Commission, Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and

Amending Regulation (EU) 2019/1020 COM (2022) 454 final, 15 September 2022

Second Additional Protocol to the Convention on Cybercrime

Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (ETS No 189, 2021)

Foreign legislation

Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018 Pub L 115-141 132 Stat 348

Computer Fraud and Abuse Act 1986 18 USC § 1030

Cybersecurity and Infrastructure Security Agency Act of 2018, Pub L No 115-278, 132 Stat 4168

Cybersecurity Information Sharing Act of 2015, 6 USC §§ 1501–1510

Gramm-Leach-Bliley Act, Pub L No 106–102, 113 Stat 1338 (1999)

Federal Information Security Modernization Act of 2014 (FISMA), 44 USC § 3551 et seq

Health Insurance Portability and Accountability Act 1996 (HIPAA) Pub L 104-191 110 Stat 1936

National Defense Authorization Act 2021 Pub L 116-283 134 Stat 3388

Stored Communications Act of 1986, 18 USC §§ 2701–2713

Foreign cases

Data Protection Commissioner v Facebook Ireland Ltd and Schrems (C-311/18) EU:C:2020:559

Schrems v Data Protection Commissioner (C-362/14) EU:C:2015:650

Weltimmo s r o v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14) EU:C:2015:639

Journal articles

Almeida, ‘A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks’

Almeida F, ‘A Comparative Analysis of EU-Based Cybersecurity Skills Frameworks’ (2023) 13(7) Education Sciences 730 https://doi.org/10.3390/educsci13070730

Bester and Arendse, ‘Measuring Cybersecurity Awareness’

Bester K and Arendse DE, ‘Measuring Cybersecurity Awareness in a South African Military Sample’ (2024) 52(1) Scientia Militaria: South African Journal of Military Studies 5–33 https://doi.org/10.5787/52-1-1445

Cachalia and Klaaren, ‘Towards a Public Law Perspective’

Cachalia F and Klaaren J, ‘Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization’ (2024) 68 Journal of African Law 89

Cassim, ‘Addressing the Challenges Posed by Cybercrime’

Cassim F, ‘Addressing the Challenges Posed by Cybercrime: A South African Perspective’ (2010) 5(3) Journal of International Commercial Law and Technology 155

Cassim, ‘Addressing the Growing Spectre of Cyber Crime in Africa’

Cassim, F ‘Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures adopted by South Africa and Other Regional Role Players’ 44 (1) (2011) The Comparative and International Law Journal of Southern Africa 123

Chitimira and Ncube, 'Regulation of AI and 5G'

Chitimira H and Ncube P, 'The Regulation of Artificial Intelligence and 5G Technology to Combat Cybercrime in South African Banks' (2021) 24 Potchefstroom Electronic Law Journal 1

Coetzee, ‘Cross-Border Data Flows and the Protection of Personal Information Act’

Coetzee J, ‘Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision’ (2024) PER/PELJ vol 27, no 1, 1,10, DOI 10.17159/1727-3781/2024/v27i0a15234

du Toit, 'Search Warrant Provisions of the Cybercrimes Act'

du Toit P, ‘The Search Warrant Provisions of the Cybercrimes Act and Their Relationship with the Criminal Procedure Act’ (2023) 43(4) Obiter 764

Ezeji, Olutola and Bello, 'Cyber-related Crime in South Africa'

Ezeji CL, Olutola AA and Bello PO, ‘Cyber-related Crime in South Africa: Extent and Perspectives of State’s Role players’ (2018) 31(3) Acta Criminologica: Southern African Journal of Criminology Special Edition: Cybercrime 93

Fahey, ‘The Evolution of EU–US Cybersecurity Law and Policy’

Fahey E, ‘The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence’ (2024) 46 Journal of European Integration 1073–1088 https://doi.org/10.1080/07036337.2024.2411240

Farrand and Carrapico, ‘Digital Sovereignty and Taking Back Control’

Farrand B and Carrapico H, ‘Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity’ (2022) 31 European Security 435

Fonseca and van Wyk, ‘Cybersecurity in South Africa’

Fonseca RS and van Wyk JA, ‘Cybersecurity in South Africa: Status, Governance, and Prospects’ in Scott N Romaniuk and Mary Manjikian (eds), Routledge Companion to Global Cyber-Security Strategy (Routledge 2021) 591

Grynwajc, ‘US v EU: A Comparative Approach to Cybersecurity’

Grynwajc S, ‘US v EU: A Comparative Approach to Cybersecurity’ (2013) Revue européenne de droit de la consommation et de la concurrence

Gcaza and others, ‘A General Morphological Analysis’

Gcaza N and others, ‘A General Morphological Analysis: Delineating a CyberSecurity Culture’(2017) 25(3) Information and Computer Security 271

Hamman & Papadopoulos ‘Direct marketing and spam via electronic communications’

Hamman B & Papadopoulos S ‘Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa’ (2014) De Jure 42

Henten and others, 'Cybersecurity Institutions'

Henten A, Windekilde I and Falch M, ‘Cybersecurity Institutions in the EU and the US’ (SSRN working paper, 7 June 2024) <http://dx.doi.org/10.2139/ssrn.4954365> accessed 7 January 2026

Jones B, ‘Is POPIA Bad Business for South Africa? Comparing the GDPR and POPIA’

Jones B, ‘Is POPIA Bad Business for South Africa? Comparing the GDPR and POPIA’ (2022)10 Penn State Journal of Law and International Affairs 1

Kandeh, Futcher and Botha, ‘Enforcement of the Protection of personal Information’

Kandeh A, Futcher A and Botha R, ‘Enforcement of the Protection of personal Information (POPI) Act: Perspective of Data Management Professionals’ (2020) 22(1) South African Journal of Information Management 1

Khan and Mkuzangwe, ‘Advancing Cybersecurity Capabilities’

Khan ZC and Mkuzangwe NNP, ‘Advancing Cybersecurity Capabilities for South African Organisations through R&D’ Council for Scientific and Industrial Research, Pretoria, South Africa 1

Lötter, 'Comparative Critique of the Cybercrimes Act'

Lötter C, ‘A Comparative Critique of the Cybercrimes Act 19 of 2020: Positioning South Africa vis-à-vis Australia’ (2025) 28 PER / PELJ 2

Mabeka, 'Cybercrimes Act and Civil Proceedings'

Mabeka NQ, 'The Cybercrimes Act 19 of 2020, Section 7 versus Civil Proceedings' (2024) 38(2) Speculum Juris 419

Mabeka, ‘The Prevalence of Cybercrimes and Hacking Incidents’

Mabeka NQ, ‘The Prevalence of Cybercrimes and Hacking Incidents and Their Impact on the Confidentiality of Documents in Civil Proceedings’ (2024) 28 Law, Democracy & Development 50

Mabeka and Cassim, ‘Interpreting the Provisions of the Cybercrimes Act'

Mabeka NQ and Cassim F, ‘Interpreting the Provisions of the Cybercrimes Act 19 of 2020 in the Context of Civil Procedure: A Future Journey’ (2023) 44(1) Obiter 19

Mabunda, 'Cyberfraud or Offline Fraud'

Mabunda S, ‘Is it Cyberfraud or Good Ol’ Offline Fraud: A Look at Section 8 of the South African Cybercrimes Bill’ (2018) 2 Journal of Anti-Corruption Law 58

Matsaung and Masiloane, ‘The Role of Cyber Intelligence in Policing Cybercrime in South Africa’

Matsaung P and Masiloane DT, ‘The Role of Cyber Intelligence in Policing Cybercrime in South Africa: Insights from Law Enforcement Officers’ (2025) 34(2) African Security Review 152

Malahleka, 'The Problem of Trans-Border Information Flows’

Malahleka M, 'The Problem of Trans-Border Information Flows in the Protection of Personal Information' (2024) 27 Potchefstroom Electronic Law Journal 1

Maluleke, 'Exploring Cybercrime in Africa'

Maluleke W, ‘Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa’ (2023) 6(6) International Journal of Social Science Research and Review (IJSSRR) 223

Madnick, Huang and Madnick, ‘The Evolution of Global Cybersecurity’

Madnick B, Huang K and Madnick S, ‘The Evolution of Global Cybersecurity Norms in the Digital Age: A Longitudinal Study of the Cybersecurity Norm Development Process’ (2024) 33 Information Security Journal: A Global Perspective 204

Mbonye, Moodley and Nyika, ‘Examining the applicability’

Mbonye V, Moodley M and Nyika F, ‘Examining the applicability of the Protection f Personal Information Act in AI-driven environments’ (2024) 26(1) SAJIM 1

Mpuru and Kgoale, ‘Recognizing the Evolving Cybercrime Threats’

Mpuru L and Kgoale C, ‘Recognizing the Evolving Cybercrime Threats in South Africa’ (2025) African Security https://doi.org/10.1080/19392206.2025.2515302

Musoni and others, ‘Global Approaches to Digital Sovereignty’

Musoni M, Karkare P, Teevan C and Domingo E, ‘Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy’

(ECDPM Discussion Paper No 344, Maastricht, May 2023) <https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf> accessed 19 January 2026

Naude and Papadopoulos, ‘Data Protection in South Africa’

Naude A and Papadopoulos S, ‘Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)’ (2016) THRHR 57

Ngcece, Mkhize and Majola, ‘Exploring Responses to Cybercrime in South Africa:

Ngcece S, Mkhize S and Majola K, ‘Exploring Responses to Cybercrime in South Africa: The South African Police Services (SAPS) Perspectives’ (2025) Journal of Cyberspace Studies 1 https://doi.org/10.22059/jcss.2025.395262.1149

Nyambuya and Gopal, ‘The Influence of South Africa’s’

Nyambuya VP and Gopal ND, ‘The Influence of South Africa’s democratic Principles on its Cybersecurity Framework and Cyber Threat Response’ (2024) 3 (2) Journal of BRICS Studies 55

Olorunlana, ‘The U.S. Role in Shaping Global Cybersecurity Norms’

Olorunlana T, ‘The U.S. Role in Shaping Global Cybersecurity Norms’ (2024) 1(4) International Journal of Science, Architecture, Technology, and Environment 217

Orji, 'AU Convention on Cybersecurity '

Orji UJ, ‘The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?’ (2018) 12(2) Masaryk University Journal of Law and Technology 91

Pieterse, 'Cyber Threat Landscape in South Africa'

Pieterse H, ‘The Cyber Threat Landscape in South Africa: A 10-Year Review’ (2012) 28 African Journal of Information and Communication (AJIC) 23

Ramluckan, 'International Humanitarian Law and Cyber Environment'

Ramluckan T, ‘International Humanitarian Law and its Applicability to the South African Cyber Environment’ (2020) 19(3) Journal of Information Warfare 102

Ramluckan, Van Niekerk and Leenen, ‘Research Challenges for Cybersecurity’

Ramluckan T, van Niekerk B and Leenen L, ‘Research Challenges for Cybersecurity and Cyberwarfare: A South African Perspective’ (paper presented at the 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal, July 2019) <https://researchspace.ukzn.ac.za/> accessed 16 July 2025

Roos ‘The European Union’s General Data Protection Regulation (GDPR)’

Roos A ‘The European Union’s General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected ‘Content Principles” (2020) CILSA 53 (3)

Sekati, 'Extradition and Extra-territorial Jurisdiction'

Sekati P, ‘Assessing the Effectiveness of Extradition and the Enforcement of Extra-territorial Jurisdiction in Addressing Trans-national Cybercrimes’ (2022) 55(1) Comparative and International Law Journal of Southern Africa 17

Snail, 'Convergence of Cybercrime and Data Protection Laws'

Snail S, ‘The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013’ (2022) 43(3) Obiter 536

Snail, ‘Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities’

Snail S, ‘Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities’ (2009) 1 Journal of Information, Law & Technology (JILT) 1

Snail and Musoni, 'Overview of Cybercrime Law'

Snail S and Musoni M, ‘An Overview of Cybercrime Law in South Africa’ (2023) 4 International Cybersecurity Law Review 299

Snider, Shandler, Zandani and Canetti, 'Cyberattacks and Cybersecurity Policies'

Snider K, Shandler R, Zandani S and Canetti D, ‘Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies’ (2021) 7(1) Journal of Cybersecurity 1

Srinivas, Das and Kumar, ’Government Regulations in Cybersecurity’

Srinivas J, Das AK and Kumar K, ‘Government Regulations in Cybersecurity: Framework, standards and Recommendations’ (2019) Future Generation Computer Systems https://doi.org/10.1016/j.future.2018.09.063

Swales ‘Protection of Personal Information’

Swales L, ‘Protection of Personal Information: South Africa’s Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)’ (2016) 28 South African Mercantile Law Journal 49

Sutherland, 'Governance of Cybersecurity'

Sutherland E, ‘Governance of Cybersecurity – The Case of South Africa’ (2017) 20 African Journal of Information and Communication (AJIC) 83

Teichmann F and Sergi B, ‘The EU Cyber Resilience Act’

Teichmann F and Sergi B, ‘The EU Cyber Resilience Act: Hybrid Governance, Compliance, and Cybersecurity Regulation in the Digital Ecosystem’ (2025) 61 Computer Law & Security Review 105354 https://doi.org/10.1016/j.clsr.2025.105354 6-8

Timcke, Gaffley and Rens, 'The centrality of cybersecurity’

Timcke S, Gaffley M and Rens A, 'The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa’s Transnet' (2023) 32 The African Journal of Information and Communication 1 https://doi.org/10.23962/ajic.i32.16949

van der Merwe, ‘The Cybercrimes Act 19 of 2020: A Silver Bullet?’

van der Merwe, ‘The Cybercrimes Act 19 of 2020: A Silver Bullet?’ (2024) 5(1) South African Law Journal Digital 45 <https://www.lawjournal.digital/jour/article/view/313/107> accessed 16 October 2025

Watney, ‘Admissibility of Electronic Evidence in Criminal Proceedings’

Watney M, ‘Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position’ (2009) 1 Journal of Information, Law & Technology (JILT) 1

Watney, 'South Africa’s Cybersecurity Legal Framework'

Watney M, ‘Exploring South Africa’s Cybersecurity Legal Framework Regulating Information Confidentiality, Integrity, and Availability’ (2024) 19(1) Proceedings of the 19th International Conference on Cyber Warfare and Security 430

On-line resources

Adinga, 'POPIA Compliance in Cloud ERP’

Adinga, 'POPIA Compliance in Cloud ERP: A Complete Guide to Data Protection in the Cloud' (19 August 2025) <https://adinga.co.za/popia-compliance-in-cloud-erp-adinga-cloud-erp/> accessed 17 October 2025

Allen, 'South Africa Lays Down the Law on Cybercrime'

Allen K, 'South Africa Lays Down the Law on Cybercrime' (ISS, 9 June 2021) <https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime> accessed 1 April 2025

AGSA, ‘PFMA 2022-23 Audit Outcomes Report (2023)’

Auditor-General of South Africa (AGSA), ‘Consolidated General Report on National and Provincial Government Audit Outcomes 2022-23’ (AGSA, 2023) <https://www.agsa.co.za/Portals/0/Reports/PFMA/2022-23/Updates/PFMA%20Report%202022-23%20FINAL%20INTERACTIVE%20PDF.pdf> accessed 21 October 2025

Auditor-General South Africa, 'Government Information Systems Management'

Auditor-General South Africa, 'Government Information Systems Management' (2023–24) <https://pfma-2023-24.agsareports.co.za/pages/government-information-systems-management> accessed 16 October 2025

Auditor-General South Africa, ‘Public Finance Management Act Report 2022/23 (2023)’

Auditor-General South Africa, ‘Public Finance Management Act Report 2022/23 (2023)’ <https://www.agsa.co.za/Reporting/PFMAReports/PFMA2022-23.aspx> accessed 17 October 2025

Barlow, ‘What Makes SA a Target for Cyber Crime, What Actions Can Be Taken?’

Barlow E, ‘What Makes SA a Target for Cyber Crime, What Actions Can Be Taken?’ (ITWEB, 23 May 2023) <https://www.itweb.co.za/article/what-makes-sa-a-target-for-cyber-crime-what-actions-can-be-taken/Pero37Z34ydMQb6m> accessed 25 March 2025

Bhagattjee, Govuza and Seban, ‘Cybercrime in South Africa – Attorneys Fall Victim to Cyber Fraud’

Bhagattjee P, Govuza A and Seban L, ‘Cybercrime in South Africa – Attorneys Fall Victim to Cyber Fraud’ (Cliffe Dekker Hofmeyr, 18 Feb 2020) <https://www.cliffedekkerhofmeyr.com/news/publications/2020/technology/tmt-alert-18-february-cybercrime-in-south-africa-attorneys-fall-victim-to-cyber-fraud.html> accessed 6 May 2025

Buchan and Devanny, ‘South Africa’s Cyber Strategy Under Ramaphosa’

Buchan R and Devanny J, South Africa’s Cyber Strategy Under Ramaphosa: Limited

Progress, Low Priority (Carnegie Endowment for International Peace 2024) <https://carnegie-production-assets.s3.amazonaws.com/static/files/Buchan_Devanny_South_Africa_Cyber_Strategy.pdf> accessed 15 October 2025

CISA, ‘Joint Cyber Defense Collaborative Charter (2021)’

Cybersecurity and Infrastructure Security Agency (CISA), ‘Joint Cyber Defense Collaborative: Unifying Cyber Defense Planning and Operations’ (CISA, August 2021) <https://nsarchive.gwu.edu/sites/default/files/documents/qytieo-agiyf/04.pdf> accessed 21 October 2025

CISA, ‘Secure by Design’

Cybersecurity and Infrastructure Security Agency (CISA), ‘Secure by Design (2023)’ <https://www.cisa.gov/securebydesign> accessed 22 October 2025

CISA, ‘Strategic Intent (US Department of Homeland Security 2019)’

Cybersecurity and Infrastructure Security Agency (CISA), ‘CISA Strategic Intent: Defend Today, Secure Tomorrow (CISA, August 2019)’ <https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf> accessed 19 October 2025

CoE, ‘CyberSouth’

Council of Europe, ‘CyberSouth: Cooperation on Cybercrime in the Southern Neighbourhood Region’ <https://www.coe.int/en/web/cybercrime/cybersouth> accessed 21 October 2025

Council Conclusions (Cyber Diplomacy Toolbox) ST 10474/17

Council of the European Union, Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”) (19 June 2017) ST 10474/17 <https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf> accessed 30 November 2025

Council of Europe, ‘Integrating Cybercrime Issues into National Judicial Training Curricula’

Council of Europe, ‘Integrating Cybercrime Issues into National Judicial Training Curricula’ <https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/glacy-integrating-cybercrime-issues-into-national-judicial-training-curricula> accessed 20 October 2025

Crisanto, Pelegrini and Prenio, ‘Banks Cyber Security’

Crisanto JC, Pelegrini JU and Prenio J, ‘Banks Cyber Security A Second Generation of Regulatory Approaches, FSI Insights No 50’ (Bank for International Settlements, 12 June 2023) <https://www.bis.org/fsi/publ/insights50.pdf> accessed 18 September 2025

CRS, Cybersecurity: Deterrence Policy (R47011, 2022)

Congressional Research Service, Cybersecurity: Deterrence Policy (Report R47011, 18 January 2022) <https://crsreports.congress.gov/product/pdf/R/R47011> accessed 26 November 2025

CSIR, ‘National Cybersecurity Survey Report’

Council for Scientific and Industrial Research (CSIR), National Cybersecurity Survey Report (2024) <https://researchspace.csir.co.za> accessed 18 October 2025

Cybersecurity and Infrastructure Security Agency, ‘Critical Infrastructure Overview (2023)’

Cybersecurity and Infrastructure Security Agency (CISA), CISA Releases 2023 Year in Review Showcasing Efforts to Protect Critical Infrastructure (17 January 2024) <https://www.cisa.gov/news-events/news/cisa-releases-2023-year-review-showcasing-efforts-protect-critical-infrastructure> accessed 20 October 2025

Cybercrime Awareness and Skills for Law Enforcement, ‘Cybil Portal’

Cybercrime Awareness and Skills for Law Enforcement, ‘Cybil Portal’ <https://cybilportal.org/projects/cybercrime-awareness-and-skills-for-law-enforcement-providing-specialist-cybercrime-investigation-skills/> accessed 20 October 2025

Cybercrime Operations Desk, ‘INTERPOL African Cyberthreat Assessment Report’

Cybercrime Operations Desk, ‘INTERPOL African Cyberthreat Assessment Report 2024: Outlook by the African Cybercrime Operations Desk’ (3rd edn, INTERPOL April 2024) <https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf> accessed 18 March 2025

Cybersecurity Hub, ‘Homepage’

Cybersecurity Hub, ‘Homepage’ <https://www.cybersecurityhub.gov.za/> accessed 17 October 2025

C3SA, Home Page (UCT)

Cybersecurity Capacity Centre for Southern Africa (C3SA), Home Page (University of Cape Town) <https://c3sa.uct.ac.za/> accessed 20 October 2025

DCDT, 'Annual Report 2023/24 (2024)'

Department of Communications and Digital Technologies, Annual Report 2023/24 (Government of South Africa, 2024) <https://www.gov.za/sites/default/files/gcis_document/202501/dcdt-2023-24-annual-report.pdf> accessed 20 November 2025

DCDT, 'Cybersecurity Hub Project (South African Government)'

Department of Communications and Digital Technologies, Cybersecurity Hub Project (South African Government) <https://www.dcdt.gov.za/cybersecurity-hub-project.html> accessed 27 October 2025

Department of Communications and Digital Technologies, 'National Digital and Future Skills Strategy (2020)'

Department of Communications and Digital Technologies, 'National Digital and Future Skills Strategy South Africa' (Government Gazette, General Notice 513, No 43730, 23 September 2020) <https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf> accessed 13 October 2025

Department of Justice and Constitutional Development (South Africa), 'Minister Lamola Welcomes Commencement of the Cybercrimes Act'

Department of Justice and Constitutional Development (South Africa), Minister Lamola Welcomes Commencement of the Cybercrimes Act, 2020 (1 December 2021) <https://www.justice.gov.za/m_statements/2021/20211201-ms-CybercrimesAct_Min.html> accessed 2 November 2025

DHS, 'Official Website'

US Department of Homeland Security, Official Website <https://www.dhs.gov/> accessed 5 December 2025

Digital School of Marketing, 'Navigating POPIA and GDPR in Cybersecurity compliance'

Digital School of Marketing, 'Navigating POPIA and GDPR in Cybersecurity compliance' (Digital School of Marketing, 20 August 2025) <https://digitalschoolofmarketing.co.za/cyber-security-blog/navigating-popia-and-gdpr-in-cybersecurity-compliance/> accessed 5 September 2025

Duja Consulting, ‘Cyber Fraud Meets Forensics’

Duja Consulting, ‘Cyber Fraud Meets Forensics: Auditing in a Digital Threat Landscape’ (Duja Consulting Blog, 3 September 2025) <https://www.duja.co.za/cyber-fraud-meets-forensics-auditing-in-a-digital-threat-landscape/> accessed 18 September 2025

Duncan, ‘RICA Erodes Your Right to Privacy’

Duncan J, ‘RICA Erodes Your Right to Privacy’ (TechCentral, 28 November 2014) <http://www.techcentral.co.za/rica-erodes-your-right-to-privacy/52973> accessed 5 August 2025

Defenceweb, ‘South Africa in Top Five Countries Affected by Cybercrime in 2022’

Defenceweb, ‘South Africa in Top Five Countries Affected by Cybercrime in 2022’ (Defenceweb, 28 April 2023) <https://www.defenceweb.co.za/cyber-defence/south-africa-in-top-five-countries-affected-by-cybercrime-in-2022/> accessed 10 March 2025

Econorisk, 'Cybercrime in South Africa' (Econorisk, 2025)

Econorisk, 'Cybercrime in South Africa' (Econorisk, 2025) <https://econorisk.co.za/cybercrime-in-south-africa/> accessed 16 October 2025

ECSO, ‘Cybersecurity Skills Framework (2021)’

European Cyber Security Organisation (ECSO), ‘European Cyber Security Organisation (Digital Skills & Jobs Platform)’ <https://digital-skills-jobs.europa.eu/en/organisations/european-cyber-security-organisation> accessed 19 October 2025

ENISA, ‘Challenges in NIS 2 Implementation (2023)’

NquiringMinds CyberNews, ENISA identifies compliance challenges for critical infrastructure sectors under NIS2 Directive (28 October 2024) <https://nquiringminds.com/cybernews/enisa-identifies-compliance-challenges-for-critical-infrastructure-sectors-under-nis2-directive/> accessed 25 October 2025

ENISA, ‘Cybersecurity Certification Framework’

European Union Agency for Cybersecurity (ENISA), ‘Cybersecurity Certification Framework’ <https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework> accessed 17 October 2025

ENISA, ‘CyCLONe: Cyber Crisis Liaison Organisation Network (2022)’

European Cyber Security Organisation (ECSO), ‘ENISA tests the operating procedures for the EU Cyber Crisis Liaison Organisation Network’ (13 October 2021) <https://ecs-org.eu/enisa-tests-the-operating-procedures-for-the-eu-cyber-crisis-liaison-organisation-network/> accessed 22 October 2025

ENISA, ‘EU Cybersecurity Policy Overview (2023)’

European Union Agency for Cybersecurity (ENISA), ‘State of Cybersecurity in the EU’ <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu> accessed 20 October 2025

ENISA, 'European Cybersecurity Skills Framework (2022)'

European Union Agency for Cybersecurity (ENISA), 'European Cybersecurity Skills Framework (ECSF)' <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf> accessed 25 October 2025

ENISA, ‘Joint Cyber Capacity Report (2024)’

European Union Agency for Cybersecurity (ENISA), ‘2024 Report on the State of Cybersecurity in the Union’ (3 December 2024) <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> accessed 21 October 2025

ENISA, ‘Technical Guidance on Security Measures (2022)’

European Union Agency for Cybersecurity (ENISA), ‘Guideline on Security Measures under the European Electronic Communications Code (EECC) (2022)’ <https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc> accessed 18 October 2025

Eurojust

Eurojust, ‘About Eurojust’ <https://www.eurojust.europa.eu/> accessed 20 October 2025

European Commission, ‘Shaping Europe’s Digital Future (2020)’

European Commission, Shaping Europe’s Digital Future (Communication) COM(2020) <https://eufordigital.eu/library/shaping-europes-digital-future/> accessed 25 October 2025

European Commission, ‘2030 Digital Compass’ COM(2021) 118

European Commission, ‘2030 Digital Compass: the European Way for the Digital Decade’ (Commission Communication COM(2021)118 final, 9

March 2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118> accessed 25 October 2025 Europol, ‘European Cybercrime Centre (EC3)’

Europol, ‘European Cybercrime Centre (EC3)’ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> accessed 20 October 2025

Europol, ‘European Cybercrime Centre (EC3): Operational Mandate (2013)’

Europol, EC3: Opening of the European Cybercrime Centre (3 January 2013) <https://www.europol.europa.eu/media-press/newsroom/news/ec3-opening-of-european-cybercrime-centre-0> accessed 23 October 2025

Executive Order 13636 ‘Improving Critical Infrastructure Cybersecurity’

Executive Order 13636 ‘Improving Critical Infrastructure Cybersecurity’ (12 February 2013) <https://www.govinfo.gov/content/pkg/DCPD-201300091/pdf/DCPD-201300091.pdf accessed> 12 November 2025

Executive Order 14028, ‘Improving the Nation’s Cybersecurity’

Executive Order 14028, Improving the Nation’s Cybersecurity (12 May 2021) DCPD-202100401, 86 Fed Reg 26633 (May 12 2021) <https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf> accessed 12 November 2025

EY, ‘Top 10 Risks in Telecommunications’

EY, ‘Top 10 Risks in Telecommunications’ (EY Global, January 2025) <https://www.ey.com/en_za/insights/telecommunications/top-10-risks-for-telecommunications> accessed 18 September 2025

Fairbridges Wertheim Becker, 'The Appeal Court Has Overturned a Recent Cyber Crime Ruling’

Fairbridges Wertheim Becker, 'The Appeal Court Has Overturned a Recent Cyber Crime Ruling: What Are the Implications for Companies Under the POPI Act?' (Fairbridges Wertheim Becker, 2025) <https://fwblaw.co.za/the-appeal-court-has-overturned-a-recent-cyber-crime-ruling-what-are-the-implications-for-companies-under-the-popi-act/> accessed 17 October 2025

FBI IC3, ‘2024 Internet Crime Report (2024)’

Federal Bureau of Investigation, ‘Internet Crime Complaint Center (IC3), 2024 Internet Crime Report (2024)’ <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf> accessed 23 October 2025

Federal Bureau of Investigation

Federal Bureau of Investigation (FBI), Cyber (FBI, 2026) <https://www.fbi.gov/investigate/cyber> accessed 10 January 2026.

FSCA & PA, ‘Joint Standard 2: Cybersecurity and Cyber Resilience (2024)’

Financial Sector Conduct Authority and Prudential Authority, Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience (17 May 2024) <https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2024/joint-comms-2-of-2024/Joint%20Communication%202%20of%202024%20-%20Publication%20of%20the%20Joint%20Standard%20-%20Cybersecurity%20and%20cyber%20resilience.pdf> accessed 22 October 2025

GAO, ‘Actions Needed to Address Cybersecurity Risks Facing the Electric Grid (GAO-19-332, 2019)’

United States Government Accountability Office, ‘Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks

Facing the Electric Grid, (GAO Report GAO-19-332, 25 September 2019) <https://www.gao.gov/products/gao-19-332> accessed 21 October 2025

Giordano, ‘Schrems II and Modern Multinational Information Security Practice’

Scott M Giordano, ‘The Impact of Schrems II on the Modern Multinational Information Security Practice Part 1: The Potential Disruption to International Commerce’ (30 November 2021) ISACA Journal <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/the-impact-of-schrems-ii-on-the-modern-multinational-information-security-practice-part-1> accessed 19 January 2026

Gavaza, 'Concern grows about criminal use of unregistered SIM cards'

Gavaza M, 'Concern grows about criminal use of unregistered SIM cards' (BusinessLIVE, 13 February 2025) <https://www.businesslive.co.za/bd/national/2025-02-13-concern-grows-about-criminal-use-of-unregistered-sim-cards/> accessed 5 September 2025

Government of South Africa, ‘Media Statement: ICASA Publishes Findings Document’

Government of South Africa, Media Statement: ICASA Publishes Findings Document and Position Paper on Cybersecurity (3 April 2019) <https://www.gov.za/news/media-statements/icasa-publishes-findings-document-and-position-paper-cybersecurity-03-apr> accessed 8 August 2025

High-Level Panel Report on the SSA, Reform of the State Security Agency (2019)

High-Level Review Panel on the State Security Agency (South African Government, March 2019) <https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf> accessed 10 January 2026

ICASA, ‘Findings Document’

Independent Communications Authority of South Africa, Findings Document and Position Paper on ICASA's Roles and Responsibilities on Cybersecurity Matters (Government Gazette No 42319, Notice No 198 of 15 March 2019) <https://www.icasa.org.za/news/2019/findings-and-position-on-icasas-roles-and-responsibilities-on-cybersecurity-matters> accessed 8 August 2025

ICASA, Strategic Plan 2025–2030'

Independent Communications Authority of South Africa, ICASA Strategic Plan 2025–2030 (ICASA, 2025) <https://www.icasa.org.za/strategic-plan-2025-2030> accessed 25 November 2025

IISS, 'Cyber Capabilities and National Power: Volume II (2023)'

International Institute for Strategic Studies, 'Cyber Capabilities and National Power: A Net Assessment, Volume II (IISS, September 2023)' <https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/> accessed 30 November 2025

ImmuniWeb, 'South Africa Protection of Personal Information Act (POPIA) Compliance'

ImmuniWeb, 'South Africa Protection of Personal Information Act (POPIA) Compliance' (ImmuniWeb, 8 July 2025) <https://www.immuniweb.com/compliance/south-africa-protection-of-personal-information-act-popia-compliance/> accessed 20 October 2025

Information Regulator, 'Enforcement Notice: Dis-Chem Pharmacies Limited'

Information Regulator, 'Enforcement Notice: Dis-Chem Pharmacies Limited (5 February 2024)' <https://inforegulator.org.za/wp-content/uploads/2020/07/DIS-CHEM-ENFORCEMENT-NOTICE.pdf> accessed 16 October 2025

Information Regulator, 'Enforcement Notice: DOJCD Matter'

Information Regulator, Enforcement Notice: DOJCD Matter (9 May 2023) <https://inforegulator.org.za/wp-

content/uploads/2020/07/ENFORCEMENT-NOTICE-DOJCD-MATTER-090523.pdf> accessed 16 October 2025

Information Regulator, ‘Annual Report 2022/2023 (2023) (accessed 5 December 2025)’

Information Regulator (South Africa), Information Regulator Annual Report 2022/2023 (2023) <https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023_25_Approved-by-Members_Final90.pdf> accessed 5 December 2025

Information Regulator of South Africa, ‘Information Regulator Shares outcomes’

Information Regulator of South Africa, ‘Media Statement: Information Regulator Shares outcomes of Complaints Investigated and Assessments Conducted in relation to PAIA and POPIA’ (5 April 2023) <https://inforegulator.org.za/wp-content/uploads/2020/07/pdf-Final-Version_MEDIA-BRIEFING-OF-INFORMATION-REGULATOR-ON-OUTCOMES-OF-RECEIVED-COMPLAINTS-003.pdf> accessed 11 September 2025

IntelWatch, ‘Submission on RICA Bill’

IntelWatch, ‘Submission on RICA Bill’ (IntelWatch, 6 October 2023) <https://intelwatch.org.za/wp-content/uploads/2023/10/231006-Intelwatch-RICA-Bill-Submission.pdf> accessed 8 August 2025

INTERPOL, 'African Cyberthreat Assessment Report'

INTERPOL, 'African Cyberthreat Assessment Report' (INTERPOL, October 2021) <https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf> accessed 1 March 2025

INTERPOL, ‘Africa Cyberthreat Assessment Report 2025’

INTERPOL, ‘Africa Cyberthreat Assessment Report 2025’ (INTERPOL, May 2025)

<https://www.interpol.int/en/content/download/23094/file/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf> accessed 10 March 2025

INTERPOL, ‘Capacity Building’

INTERPOL, ‘Capacity Building’ <https://www.interpol.int/en/How-we-work/Capacity-building> accessed 20 October 2025

ITLawCo, 'Critical Infrastructure Protection Act 8 of 2019 (CIPA)’

ITLawCo, 'Critical Infrastructure Protection Act 8 of 2019 (CIPA)' (ITLawCo, 20 November 019) <https://itlawco.com/critical-infrastructure-protection-act-8-of-2019-cipa/> accessed 6 August 2025

ITU, ‘SADC Model Law on Cybercrime (2012)’

International Telecommunication Union, ‘Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law’ (HIPSSA Project, 2012) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf> accessed 25 October 2025

ITWeb, ‘Hands Off Cyber Security’

ITWeb, ‘Hands Off Cyber Security, ICASA Told’ (ITWeb, 20 March 2019) <https://www.itweb.co.za/article/hands-off-cyber-security-icasa-told/VgZeyqJA3ewMdjX9> accessed 8 August 2025

JMR Software, 'Regulatory Compliance in South Africa’

JMR Software, 'Regulatory Compliance in South Africa: The Role of POPIA and PAM' (TechCentral, 19 March 2025) <https://techcentral.co.za/regulatory-compliance-popia-jmr-software/261044/> accessed 17 October 2025

KelaCyber, ‘How Banks Use Threat Intelligence’

KelaCyber, ‘How Banks Use Threat Intelligence’ (KelaCyber Blog) <https://www.kelacyber.com/blog/how-banks-use-threat-intelligence/> accessed 18 September 2025

Khan, 'Strengthening RICA'

Khan F, 'Strengthening RICA: A Necessary Overhaul for Privacy and Security'(ProtectionWeb, 27 January 2025) <https://www.protectionweb.co.za/opinion-and-analysis/strengthening-rica-a-necessary-overhaul-for-privacy-and-security/> accessed 6 September 2025

Lisinski, 'End-to-End Encryption: A South African Perspective'

Lisinski R, 'End-to-End Encryption: A South African Perspective' (Fluxmans, 3 November 2016) <https://fluxmans.com/article/end-end-encryption-south-african-perspective-ryszard-lisinski> accessed 6 September 2025

Luck, 'RICA: Walking a fine line between crime prevention

Luck R, 'RICA: Walking a fine line between crime prevention and protection of rights' (De Rebus, 2014) <https://www.derebus.org.za/rica-walking-fine-line-crime-prevention-protection-rights/> accessed 5 September 2025

Meyer Attorneys, 'POPIA Breach Notification'

Meyer Attorneys, 'POPIA Breach Notification' <https://meyerattorneys.co.za/2025/09/03/popia-breach-notification/> accessed 17 October 2025

Michalsons Attorneys, 'Complying with RICA a guide'

Michalsons Attorneys, 'Complying with RICA a guide' (6 July 2015) <https://www.michalsons.com/blog/complying-with-rica/1157> accessed 6 September 2025

Michalsons Attorneys, 'South Africa Considers Establishing a Cyber Commissioner'

Michalsons Attorneys, 'South Africa Considers Establishing a Cyber Commissioner' (Michalsons, 3 March 2025) <https://www.michalsons.com/blog/south-africa-considers-establishing-a-cyber-commissioner/61846> accessed 16 October 2025

Mpahlwa, 'How Can South Africa Combat the Growing Threat of Cybercrime?'

Mpahlwa M, 'How Can South Africa Combat the Growing Threat of Cybercrime?' (De Rebus, 1 March 2025) <https://www.derebus.org.za/how-can-south-africa-combat-the-growing-threat-of-cybercrime/> accessed 16 October 2025

Mzekandaba, 'Cyber Crimes' Annual Impact on SA Estimated at R22bn'

Mzekandaba S, 'Cyber Crimes' Annual Impact on SA Estimated at R22bn' (ITWeb, 16 October 2023) <https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m> accessed 3 April 2025

National Cybersecurity Strategy, 'White House, March 2023'

National Cybersecurity Strategy (White House, March 2023) <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> accessed 11 November 2025

National Institute of Standards and Technology, 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST SP 800–181 rev 1, 2020)'

National Institute of Standards and Technology (NIST), 'NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181, August 2017)' <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf> accessed 20 December 2025

National Institute of Standards and Technology, ‘Recommendation for Key Management: Part 1 – General (NIST SP 800-57 Rev 5, 2020)’

National Institute of Standards and Technology (NIST), ‘Recommendation for Key Management: Part 1 – General (NIST Special Publication 800-57 Part 1 Revision 5, May 2020)’ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf> accessed 19 October 2025

National Prosecuting Authority, ‘Annual Report 2023/24 (2024)’

National Prosecuting Authority, ‘Annual Report 2023/24 (2024)’

<https://www.npa.gov.za/sites/default/files/uploads/NPA%202024%20Annual%20Report_web_2.pdf> accessed 16 October 2025

National Security Agency

National Security Agency (NSA), About NSA <https://www.nsa.gov/> accessed 27 October 2025

NIST, ‘Cybersecurity Framework 2.0 (February 2024)’

NIST, ‘Cybersecurity Framework 2.0 (February 2024)’ <https://www.nist.gov/cyberframework> accessed 12 November 2025

NIST, ‘Cybersecurity Framework 2.0 Mappings to International Standards (2024)’

NIST, Cybersecurity Framework 2.0 Mappings to International Standards (2024) <https://www.nist.gov/cyberframework/international> accessed 12 November 2025

NIST, ‘SP 800-53 Rev 5: Security and Privacy Controls (2020)’

National Institute of Standards and Technology (NIST), ‘Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations’ (US Department of Commerce, September 2020) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> accessed 15 November 2025

Office of the National Cyber Director, ‘About the Office of the National Cyber Director’

Office of the National Cyber Director (ONCD), ‘About the Office of the National Cyber Director’ <https://www.whitehouse.gov/oncd/> accessed 29 October 2025

Panchia, ‘Command line to control room’

Panchia Y, ‘Command line to control room: SA’s infrastructure vulnerable to cyberattacks’ Daily Maverick, 17 July 2025) <https://www.dailymaverick.co.za/article/2025-07-17-command-line-to-control-room-sas-infrastructure-vulnerable-to-cyberattacks/> accessed 7 August 2025

Parliament, ‘ATC No 109—2025 (4 July 2025)’

Parliament of the Republic of South Africa, Announcements, Tablings and Committee Reports, No 109—2025, Second Session, Seventh Parliament, Friday, 4 July 2025 (Parliament of South Africa, 4 July 2025) <https://www.parliament.gov.za/storage/app/media/Docs/atc/01ls62wggb37zgmru4dzdjdosupvrgduih.pdf > accessed 18 October 2025

Parliamentary Monitoring Group (PMG), ‘Committee Question 27090’

Parliamentary Monitoring Group (PMG), ‘Committee Question 27090’ (PMG) <https://www.pmg.org.za/committee-question/27090/> accessed 18 October 2025

Parliamentary Question No 3964 (South Africa 2023)

Parliament of the Republic of South Africa, ‘Parliamentary Question No 3964 (Internal Question Paper 45-2023): Written Reply’ (18 December 2023) <https://static.pmg.org.za/RNW3964-2023-12-18.pdf> accessed 23 October 2025

PMG, ‘Portfolio Committee Report on GCIS and MDDA Performance’

Parliamentary Monitoring Group, ‘ATC231025: Report of the Portfolio Committee on Communications and Digital Technologies on the 2022/23

Third and Fourth Quarter Performance and Expenditure Reports of Government Communication and Information System (GCIS) and the Media Development and Diversity Agency (MDDA) (24 October 2023)' <https://pmg.org.za/tabled-committee-report/5522/> accessed 15 October 2025

PPM Attorneys, 'A Breakdown of the RICA Bill'

PPM Attorneys, 'A Breakdown of the RICA Bill' (PPM Attorneys, 5 September 2023) <https://www.ppmattorneys.co.za/breakdown-of-rica-bill/> accessed 5 September 2025

Ransomware Task Force, 'Combating Ransomware (2021)'

Ransomware Task Force (Institute for Security and Technology), 'Combating Ransomware: A Comprehensive Framework for Action – Key Recommendations from the Ransomware Task Force (September 2021)' <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf> accessed 18 November 2025

Republic of South Africa, 'Minister Assures the Public of Government's Work on Cyber Security'

Republic of South Africa, 'Minister Khumbudzo Ntshavheni Assures the Public of Government's Work on Cyber Security' (Media statement, 6 May 2021) <https://www.gov.za/news/media-statements/minister-khumbudzo-ntshavheni-assures-public-governments-work-cyber-security> accessed 17 October 2025

SABRIC, 'Annual Crime Statistics 2021'

South African Banking Risk Information Centre (SABRIC), 'Annual Crime Statistics 2021 (2024)' <https://www.sabric.co.za/wp-content/uploads/2024/11/SABRIC-Annual-Crime-Stats-2021.pdf> accessed 17 October 2025

Sadeeh, 'Cyber Resilience Framework in South Africa'

Sadeeh A, ‘Cyber Resilience Framework in South Africa’ (Inside Telecom, 02 December 2022) <https://insidetelecom.com/cyber-resilience-framework-cyber-governance-in-south-africa/> accessed 15 March 2025

Shingange, 'A Review of South Africa’s National Cybersecurity Policy Framework: Progress and Challenges After Nearly a Decade'

Shingange G, 'A Review of South Africa’s National Cybersecurity Policy Framework: Progress and Challenges After Nearly a Decade' (Institute for Defence, Security and Intelligence, 26 July 2024) <https://idsi.org.za/2024/07/26/a-review-of-south-africas-national-cybersecurity-policy-framework-progress-and-challenges-after-nearly-a-decade/> accessed 17 March 2025

Smith, ‘RSAWEB Victim of Cyberattack as wave of Ransomware Attempts Hits SA’

Smith C, 'RSAWEB Victim of Cyberattack as Wave of Ransomware Attempts Hits SA in Past Week' (News24, 6 February 2023) <https://www.news24.com/News24/rsaweb-victim-of-cyberattack-as-wave-of-ransomware-attempts-hits-sa-in-past-week-20230206> accessed 5 March 2025

Snail, ‘Legal Intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cybercrimes Act 19 of 2020’

Snail S, ‘Legal Intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cybercrimes Act 19 of 2020’ (Community Manager, 15 June 2021) <https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/> accessed 19 March 2025

South African Banking Risk Information Centre (SABRIC), ‘Annual Crime Statistics 2023’

South African Banking Risk Information Centre (SABRIC), ‘Annual Crime Statistics 2023’ (SABRIC, 2024) <https://www.sabric.co.za/media/vjyn5f4d/sabric-annual-crime-stats-2023-2.pdf> accessed 8 March 2025

South African Government, ‘National Data and Cloud Policy’

South African Government, ‘Electronic Communications Act: National Data and Cloud Policy’ (Government Gazette No. 50741, 31 May 2024) <https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf accessed> 20 October 2025

South African Police Service, 'Annual Report 2023/24'

South African Police Service, 'Annual Report 2023/24' (2024) <https://www.gov.za/sites/default/files/gcis_document/202411/sapsannual-report2023-24.pdf> accessed 16 October 2025

Stanger J, 'Cybersecurity Paradigm Shifts: Insights from Tech Leadership'

Stanger J, 'Cybersecurity Paradigm Shifts: Insights from Tech Leadership' (CompTIA, 16 October 2024) <https://www.comptia.org/en/blog/cybersecurity-paradigm-shifts-insights-from-tech-leadership/> accessed 6 August 2025

State Security Agency, ‘CSIRT’

State Security Agency, ‘CSIRT’ <https://www.ssa.gov.za/CSIRT accessed> 17 October 2025

Stewart ‘Understanding South African Cybersecurity Law’ (2025)

Stewart K, ‘Understanding South African Cybersecurity Law in the Context of the Recent SAA Cyber Incident’ (Polity, 31 July 2025) <https://www.polity.org.za/article/understanding-south-african-cybersecurity-law-in-the-context-of-the-recent-saa-cyber-incident-2025-07-31> accessed 18 November 2025

The Right to Privacy in South Africa, '(Joint Submission to the UN Human Rights Committee, 2017)'

The Right to Privacy in South Africa, '(Joint Submission to the UN Human Rights Committee, 2017)'<https://upr-info.org/sites/default/files/documents/2017-04/js15_upr27_zaf_e_main.pdf> accessed 6 September 2025

Thompson, 'The Digital Revolution'

Thompson R, 'The Digital Revolution: How Technology is Changing the Way We Communicate and Interact' (Visual Life, 9 June 2023) <https://rikithompson.ds.lib.uw.edu/visuallife/the-digital-revolution-how-technology-is-changing-the-way-we-communicate-and-interact/> accessed 1 March 2025

Thompson Davy, 'Exclusive: Failure to RICA mobile SIM cards may be rampant'

Thompson Davy K, 'Exclusive: Failure to RICA mobile SIM cards may be rampant'(BusinessLIVE, 26 September 2023) <https://www.businesslive.co.za/bd/national/2023-09-26-exclusive-failure-to-rica-mobile-sim-cards-may-be-rampant/> accessed 5 September 2025

Tinonetsana, 'Policy Postdoctoral Fellow, National Research Foundation'

Tinonetsana F, Policy Postdoctoral Fellow, National Research Foundation; Postdoctoral Fellow, Durban University of Technology (2025) <https://hsrc.ac.za/wp-content/uploads/2025/06/Faith-Tinonetsane-PB.pdf> accessed 5 August 2025

UNICRI, 'Access to Justice in the Digital Age (2025)'

United Nations Interregional Crime and Justice Research Institute (UNICRI), Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa (June 2025) <https://www.unicri.org/Publication-

Access-Justice-Digital-Age-Empowering-Victims-Africa> accessed 25 October 2025

United States Cyber Command

United States Cyber Command (USCYBERCOM), About USCYBERCOM <https://www.cybercom.mil/> accessed 30 October 2025

United States Cyber Command, Vision and Strategy (2020)

United States Cyber Command (USCYBERCOM), Mission & Vision <https://www.cybercom.mil/About/Mission-and-Vision/#:~:text=Mission%20&%20Vision,and%20assure%20access%20to%20cyberspace.> accessed 03 January 2026

US Department of State, 'International Cyberspace and Digital Policy Strategy (2024)'

United States Department of State, 'United States International Cyberspace and Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future (May 2024)' <https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf> accessed 10 January 2026

Venter, 'Ransomware Threats'

Venter Z, 'Ransomware Threats: How AI Can Help Combat Cybercrime' (Independent Online, 26 June 2025) <https://iol.co.za/news/education/2025-06-26-ransomware-threats-how-ai-can-help-combat-cybercrime/> accessed 17 October 2025

Webber Wenzel, 'The Cybercrimes Act Becomes Partially Operational'

Webber Wenzel, 'The Cybercrimes Act Becomes Partially Operational' (Webber Wenzel, 1 December 2021) <https://www.webberwentzel.com/News/Pages/the-cybercrimes-act-becomes-partially-operational.aspx accessed> 16 March 2025

Werksmans Attorneys, ‘POPIA and RICA: Acronyms and Privacy’

Werksmans Attorneys, ‘POPIA and RICA: Acronyms and Privacy’ (Werksmans Legal Update, 3 July 2023) <https://www.werksmans.com/legal-updates-and-opinions/popia-and-rica-acronyms-and-privacy/> accessed 8 August 2025

World Economic Forum, Advancing Cyber Resilience

World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards (World Economic Forum 2017) <https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf> accessed 6 April 2026

World Economic Forum, ‘The Global Risks Report 2022’

World Economic Forum, ‘The Global Risks Report 2022’ (WEF, 11 January 2022) <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf> accessed 10 March 2025

Wray, FBI Budget Request for FY 2022

Wray C, Statement: Federal Bureau of Investigation Budget Request for Fiscal Year 2022 (speech presented to the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington DC, 23 June 2021) <https://www.fbi.gov/news/speeches-and-testimony/federal-bureau-of-investigation-budget-request-for-fiscal-year-2022-062321> accessed 11 November 2025

Others

Cybercrimes and Cybersecurity Bill 2017

Cybercrimes and Cybersecurity Bill [B 6–2017]

CISA

Cybersecurity and Infrastructure Security Agency (CISA)

DCDT, National Cybersecurity Policy Framework (2017)

Department of Communications and Digital Technologies, National Cybersecurity Policy Framework (NCPF) (DTPS, 2017)

FSCA and Prudential Authority, Guidance Note on Cybersecurity Risk Management (2021)

Financial Sector Conduct Authority and Prudential Authority, Guidance Note on Cybersecurity Risk Management for Financial Institutions (FSCA, 2021)

FSCA, Insurance Sector Cyber Risk Management Framework (2020)

Financial Sector Conduct Authority, Insurance Sector Cyber Risk Management Framework (FSCA, 2020)

Gonçalves and Serfontein, 'Systemic Approaches'

Gonçalves D and Serfontein D, Systemic Approaches to Critical Infrastructure Risk and Security Capabilities (CSIR Report, November 2022)

ICASA, Electronic Communications and Network Security Guidelines (2020)

Independent Communications Authority of South Africa, Electronic Communications and Network Security Guidelines (ICASA, 2020)

Joint Standard 2 of 2024

Prudential Authority and Financial Sector Conduct Authority, Joint Standard 2 of 2024: Cyber Security and Cyber Resilience Requirements (2024)

Malatji M and others, Cyber Governance in the Water Sector (2022)

Malatji M and others, Cyber Governance in the Water Sector: Volume 1 – Water and Sanitation Cybersecurity Legislative and Policy Environment

(Water Research Commission Report No 3060/1/22, University of Johannesburg 2022)

National Cybersecurity Policy Framework

State Security Agency, National Cybersecurity Policy Framework (Government Gazette No 39475, 4 December 2015)

NIST, Cybersecurity Framework

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1, 2018)

Proclamation R 42 of 2021 (Cybercrimes Act commencement)

Proclamation R 42 of 30 November 2021, Commencement of Certain Provisions of the Cybercrimes Act 19 of 2020 (GG 45526, 30 November 2021)

RICA Amendment Bill 2023 (GG 48976)

Department of Justice and Constitutional Development, RICA Amendment Bill 2023 (GG 48976, 2023)

SAPS Draft SOPs (2024)

South African Police Service (SAPS), Draft SAPS Standard Operating Procedures under Section 26 of the Cybercrimes Act (2024)

SARB, Operational Risk and Cybersecurity Guidelines (2021)

South African Reserve Bank, Operational Risk and Cybersecurity Guidelines (SARB, 2021)

Theses

Bote, ‘The South African National Cyber Security Policy Framework’

Bote D, ‘The South African National Cyber Security Policy Framework: A Critical Analysis’ (MA thesis, North-West University 2019)

Chigada, ‘Towards an Aligned South African National Cybersecurity Policy Framework’

Chigada J, ‘Towards an Aligned South African National Cybersecurity Policy Framework’ (Ph.D. Thesis, University of Cape Town 2023)

Mabunda, ‘The South African legislative response’

Mabunda S, ‘The South African legislative response to cybercrime’ (Doctoral Thesis, University of Western Cape 2021)

Naidoo, ‘The Effectiveness of Detection and Prosecution’

Naidoo S, ‘The Effectiveness of Detection and Prosecution of Cybercrime Threats Against Companies in South Africa’ (LLM by coursework and research report, University of the Witwatersrand 2023)

Ntsaluba, ‘Cybersecurity Policy and Legislation in South Africa’

Ntsaluba N, ‘Cybersecurity Policy and Legislation in South Africa’ (LLM thesis, University of Pretoria 2017)

Sekgololo, ‘The State of Cybersecurity in South Africa’

Sekgololo MJ, ‘The State of Cybersecurity in South Africa, 2010–2019’ (MA dissertation, University of Johannesburg 2021)

Yusuf A, ‘Employees’ Cybersecurity Awareness’

Yusuf A, ‘Employees’ Cybersecurity Awareness and Behaviour in South African Higher Education Institutions’ (MIT dissertation, University of Pretoria 2024)