Legal Protection against Digital Personal Identity Fraud in South Africa

Murdoch Watney
University of Johannesburg, South Africa

mwatney@uj.ac.za

Abstract: As digital transformation accelerates worldwide, personal identity authentication has become a global issue. In South Africa digital personal identity has become central to how individuals interact with government services, financial institutions, and online platforms. Digital identity refers to the authentication of users through personal attributes such as biometric data, voice, image, and behavioural patterns. While these systems offer efficiency and accessibility, they also introduce significant threats. Increasingly, digital personal identity is being cloned, manipulated, or misused through techniques like deepfakes, voice cloning, and biometric spoofing. The discussion examines whether South African law adequately protects individuals against the misuse of digital personal identity, particularly in the context of fraud. While financial gain is a common motive, misuse may also result in reputational harm, privacy violations, and unauthorised commercial exploitation. The analysis considers the legal framework governing digital personality fraud under the Protection of Personal Information Act (POPIA), the Cybercrimes Act, the Consumer Protection Act (CPA), and the common law remedy of *actio iniuriarum*, within the framework of constitutional rights to dignity and privacy. Comparative insights from Denmark, Tennessee (United States), the European Union, and the United Kingdom help contextualise South Africa's approach. The discussion argues that while South African law provides substantive protection, enforcement remains challenging due to technological complexity, evidentiary burdens, and limited institutional capacity. Strengthening technical expertise, public awareness, and regulatory enforcement is essential to ensure meaningful protection for digital citizens. Drawing on global approaches, the discussion proposes targeted legal reforms to enhance accountability and safeguard digital personal identity against fraud.

Keywords: Digital personal identity, Personality rights, Digital identity fraud, Digital personal identity authentication, South African legal framework governing digital identity fraud

1. Introduction

South Africa is rapidly digitising its public and private sectors. Citizens increasingly access government services, financial platforms, and personal technologies through biometric and digital authentication systems. This transformation has elevated digital personal identity which is the electronic representation of unique traits such as fingerprints, voice, and facial features as a cornerstone of modern life. Yet, as authentication becomes more seamless, the risks of personal identity misuse grow. Technologies like deepfakes, voice cloning, and biometric spoofing have enabled sophisticated forms of impersonation, often resulting in fraud, reputational harm, or privacy violations.

These abuses raise urgent questions about the adequacy of South African law in protecting digital citizens. While cybersecurity frameworks address technical, legal, and human behavioural components, they may not be sufficient to protect digital personal identity. This is because digital identity misuse, especially through AI-driven impersonation, raises deeper legal questions about autonomy, dignity, and expressive control.

Despite its growing role in authentication and fraud prevention, digital personal identity has not received the focused legal attention it demands. The legal system must respond not only to cybersecurity threats, but also to infringements of personality rights, which protect the core attributes of personhood. Watney's (2024) analysis of cyber fraud within the South African cybersecurity legal framework, focused primarily on the criminalisation of online deception and data breaches. However, the specific vulnerability of digital personal identity as a legally protected facet of personhood remains underexplored. The discussion builds on that foundation by examining fraud through the lens of personal identity misuse and evaluating the adequacy of legal protection for digital citizens.

The discussion examines whether South African law provides effective protection against fraud arising from the misuse of digital identity, and considers how global models, such as Denmark's proposed likeness-as-property regime and the Tennessee ELVIS Act, may inform potential reform.

2. Background to the Discussion: Defining key Concepts

Before evaluating the legal framework, it is essential to define the key concepts that underpin digital identity and its misuse.

2.1 Personality Rights vs Personal Identity

Personality rights in South African law protect the legal rights that arise from being a person such as dignity, privacy, identity, and reputation. These rights are afforded to individuals over aspects of their personal identity that express their personhood such as their name, image, voice, likeness, and reputation (Neethling, 2005). They protect:

- Image from being used without consent;
- Voice from being cloned;
- Reputation from being harmed; and
- Privacy from being invaded.

In this context, personal identity is not a separate legal category, but rather the content protected by personality rights. These rights are rooted in Roman-Dutch common law, where they were traditionally applied to protect individuals in the physical world from unauthorised use or exploitation of their identity (Neethling, 2005). The court in *Grütter v Lombard* confirmed the existence of personality rights in common law and found that the unauthorised use of a person's image in advertising infringed his right to dignity and identity. This case illustrates how the misuse of personal identity such as one's image or likeness constitutes a violation of personality rights.

2.2 Digital Personal Identity

With the rise of digital technologies, these rights have migrated online.

There is not a single or general definition of digital identity (Robles-Carrillo, 2024). Digital identity refers to the data and attributes used to authenticate an individual online. The authentication data consists of biometric data such as fingerprints and facial recognition, voice and image, as well as personal identifiers such as ID numbers, and behavioural patterns (Robles-Carrillo, 2024). These elements are increasingly used to verify identity in banking, healthcare, education, and government services. However, when cloned or manipulated, they can be weaponised to commit fraud.

A person's identity is not only expressed through physical presence but also through digital representations including biometric data, voice recordings, photographs, and even AI-generated likenesses. Just as a person's image could be misused in a newspaper advertisement decades ago, it can now be cloned, manipulated, and distributed across digital platforms without consent. However, drawing an analogue between the physical and electronic mediums is complex, as the electronic medium presents challenges that do not exist in the physical realm. Some of these challenges are:

- Security and privacy: Unlike physical documents, electronic data can be intercepted, duplicated, or altered remotely. Ensuring confidentiality and integrity requires for example sophisticated encryption and access controls.
- Authenticity and trust: In the physical world, signatures, seals, and paper trails help verify authenticity. Authenticity online is established through digital signatures, certificates, and blockchain-like technologies which are powerful but not always easily understood.
- Permanence vs. ephemerality: Physical media often have a tangible permanence. Electronic data, while easily duplicated, can be deleted, corrupted, or lost due to system failures or cyberattacks.

2.3 Misuse of Digital Identity

Misuse of digital identity refers to the unauthorised or deceptive use of a person's digital attributes such as biometric data, voice, image, or personal identifiers to impersonate, manipulate, or defraud others, often resulting in financial, reputational, or privacy-related harm. This misuse may occur through technological manipulation, such as deepfakes and biometric spoofing, or through human manipulation, such as social engineering.

The online environment amplifies the risk of misuse**.** Digital content is easily copied, altered, and disseminated at scale, often without the subject's knowledge. Technologies such as deepfakes and voice cloning make it possible to impersonate someone with alarming realism, leading to reputational harm, privacy violations, and even financial fraud.

Personality rights must therefore be understood as continuing protections that apply both offline and online. Although the legal principles remain the same, the medium and magnitude of harm differ. In the digital age, the

misuse of personality rights is not only easier but also more difficult to detect and remedy, raising urgent questions about enforcement, consent, and accountability.

2.4 Cybersecurity Threats and Risks

There is not a universal definition for cybersecurity. Cybersecurity is defined as "the practice of protecting systems, networks and data from digital threats. It involves strategies, tools and frameworks designed to safeguard sensitive information and ensure the integrity of digital operations" (Yassar et al, 2025). The cybersecurity legal landscape is shaped by the imperative to identify digital threats and assess the likelihood of those threats materialising into harm.

Effective cybersecurity requires a holistic framework that integrates three interdependent components: technical**,** legal, and human. The technical component encompasses encryption, firewalls, biometric authentication, and intrusion detection systems designed to prevent unauthorised access and data breaches. The legal component involves statutory and regulatory instruments that establish rights, duties, and enforcement mechanisms for data protection and cyber resilience. The human component addresses behavioural vulnerabilities, including social engineering, insider threats, and the need for digital literacy and ethical awareness. A robust cybersecurity framework must account for all three dimensions, recognising that technological safeguards alone are insufficient without legal accountability and informed human conduct. In South Africa, this tripartite approach is essential to mitigate the misuse of digital identities and ensure institutional and individual resilience against evolving cyber threats.

In the context of digital identity, key threats include biometric spoofing, deepfake impersonation, voice cloning used in scams, and data breaches exposing identity profiles. These threats are exacerbated by the permanence of biometric data as unlike passwords, fingerprints cannot be changed once compromised.

2.5 Cybercrime and Cyber Fraud

The South African National Cybersecurity Policy Framework (NCPF) defines cybercrime as: "Criminal and other offences that are committed through the use of cyberspace or information and communication technologies (ICTs), including the internet, mobile devices, and computer systems". Under the NCPF cybercrime explicitly includes the misuse of digital identities.

Section 8 of the Cybercrimes Act defines cyber fraud "when a person unlawfully and with the intent to defraud makes a misrepresentation by means of data or a computer program, or through any interference with data or a computer program, which causes actual or potential prejudice to another".

Digital identity misuse enables various forms of fraud, such as:

- Impersonation

This involves using deepfakes, voice clones, or stolen credentials to pose as someone else. For example, a cloned voice may be used to authorise a bank transfer, or a deepfake video may impersonate a CEO to manipulate stock prices. Deepfake technology uses artificial intelligence (AI) to manipulate audio and visual data. It can mimic voices, replicate faces, and fabricate entire personas. This enables the creation of synthetic versions of individuals without their knowledge or consent, deceiving the public and undermining trust (Mashinini, 2025). AI-generated deepfake challenges core legal principles such as consent, privacy, intellectual property, and criminal liability

- Biometric spoofing

Biometric spoofing refers to faking fingerprints, facial scans, or iris patterns to gain access to devices or systems. This form of fraud is particularly serious because biometric data is immutable.

- Social engineering

Social engineering involves manipulating individuals into revealing sensitive information or performing actions. One example is Business Email Compromise (BEC), where the threat actor impersonates executives or vendors to trick employees into transferring funds. Deepfakes and voice cloning are increasingly used to enhance credibility in these scams.

- Data manipulation

This includes altering or fabricating identity data to deceive systems, such as creating fake ID profiles or modifying biometric records.

3. South African Legal Framework Governing Digital Identity Fraud

Having defined key concepts**,** the South African legal framework governing digital personal identity fraud is explored.

It is important to distinguish between general legislation such as the Protection of Personal Information Act 4 of 2013 (POPIA), the Consumer Protection Act 68 of 1998 (CPA), and the Cybercrimes Act and industry-specific regulation**,** namely the Joint Standard 2 of 2024 (Joint Standard 2)**.**

POPIA, CPA, and the Cybercrimes Act apply broadly across sectors and are designed to protect all individuals in South Africa, regardless of the context in which their personal information is processed or their consumer rights are engaged. These statutes establish foundational rights and obligations relating to privacy, data protection, fraud prevention, and fair commercial conduct. By contrast, the Joint Standard 2 applies specifically to financial institutions regulated under the Financial Sector Regulation Act. It imposes cybersecurity and cyber resilience obligations tailored to the operational risks of the financial sector. While it complements POPIA by reinforcing the duty to protect biometric and identity-related data, its scope is limited to regulated entities such as banks, insurers, and pension funds. It does not create general rights for individuals, but rather sets technical and governance standards for institutional compliance.

3.1 Constitutional Rights

The Constitution guarantees the right to dignity in section 10, privacy in section 14, and bodily integrity in section 12. These rights underpin the legal protection of digital identity. Unauthorised use of a person's image or voice may violate these rights, especially when used to deceive or defraud.

South Africa's commitment to the United Nations Sustainable Development Goals (UN SDG) with specific reference to UN SDG 16 further supports the need for strong legal frameworks to protect individuals from exploitation and promote justice and accountability.

3.2 Protection of Personal Information (POPIA)

POPIA applies to any person or entity that processes personal information in South Africa, across all sectors. It gives effect to the constitutional right to privacy by regulating how personal information which includes identity-related data is collected, stored, and used. POPIA is therefore about data governance and privacy. Under POPIA and the EU GDPR, biometric data is classified as special personal information because of its sensitivity and potential for misuse

POPIA defines personal information broadly to include:

- Biometric data;
- Photographs;
- Voice recordings;
- Identity numbers; and
- Any data that can identify a person directly or indirectly.

Under POPIA:

- Consent is required before processing personal information (section 11);
- Purpose limitation ensures data is used only for its intended function (section 13); and
- Security safeguards must be in place to prevent unauthorised access or misuse (section 19).

In digital identity misuse, POPIA is triggered when:

- A person's biometric or identity data is cloned, shared, or manipulated without consent; and
- A company fails to secure personal data.

When someone's image, voice, or biometric data is cloned or manipulated without consent, it may constitute both a violation of personality rights and unlawful processing under POPIA.

3.3 Consumer Protection Act (CPA)

The CPA applies to commercial transactions where a person buys, uses, or is affected by a product or service. It protects consumers from unfair, misleading, or deceptive conduct in the supply of goods and services. CPA is therefore about market fairness and consumer rights.

In digital identity misuse, CPA is triggered when:

- A cloned voice is used to authorise a fraudulent purchase.
- A consumer is misled by a fake endorsement or impersonation in advertising.
- A service provider misuses identity data in a way that affects the consumer's transaction.

3.4 Cybercrimes Act

The Cybercrimes Act criminalises unlawful access to data, cyber fraud, identity theft, and cyber extortion. It provides a framework for prosecuting digital identity misuse, especially when biometric data or cloned media is used to deceive systems or individuals (Watney, 2024).

3.5 Joint Standard on Cybersecurity and Cyber Resilience(Joint Standard 2)

The Joint Standard 2 was issued by the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (PA)**,** this standard requires financial institutions to implement robust cybersecurity measures. While not directly focused on digital identity, it reinforces the duty to protect biometric and personal data used in authentication.

In conclusion: While both POPIA and the CPA may be relevant in cases of digital identity misuse, they operate in distinct legal domains. POPIA governs the lawful processing and protection of personal information, focusing on consent, privacy, and data security. The CPA, by contrast, applies to transactions between suppliers and consumers in a commercial context. In fraud scenarios involving digital identity, POPIA may be invoked where personal data is misused without consent, while the CPA applies where such misuse results in consumer harm within a business context.

The Joint Standard 2 plays a critical role in regulating the security of digital identity systems, particularly where biometric authentication is used. It requires financial institutions to implement governance frameworks, risk assessments, and incident response plans to prevent unauthorised access, data breaches, and identity-based fraud. In cases where a financial institution fails to secure biometric login systems or allows impersonation through cloned voice or image data, it may be in breach of both POPIA and the Joint Standard 2. The Standard 2 complements POPIA by reinforcing the technical and organisational safeguards required to protect personal information, and it intersects with the CPA when identity misuse results in consumer harm during financial transactions. The Joint Standard 2 therefore forms part of a layered regulatory approach to digital identity protection, especially in high-risk sectors where fraud and impersonation are prevalent.

4. Legal Liability and Enforcement Challenges Under the South African law

Having outlined the legal framework governing digital identity protection in paragraph 4, the following section examines its practical application regarding liability and the challenges associated with enforcing liability.

4.1 Criminal Liability

Digital identity misuse may constitute a cybercrime under the Cybercrimes Act which criminalises offences such as identity theft, cyber fraud, and unauthorised access to data. These offences require proof of intent to deceive and actual or potential prejudice. However, prosecution is often hindered by practical challenges. Perpetrators frequently operate anonymously or across borders, using encrypted platforms, spoofed IP addresses, and false digital credentials, making them difficult to trace. Even when a suspect is identified, gathering admissible digital evidence demands specialised forensic expertise and strict chain-of-custody protocols.

Law enforcement agencies may lack the technical capacity or resources to investigate complex cyber offences, particularly those involving biometric spoofing or deepfake impersonation. In addition, prosecutorial discretion and systemic backlog in the criminal justice system may result in delays or de-prioritisation of cybercrime cases especially where the financial loss is modest or the victim is an individual. While the legal framework exists, the practical enforcement of criminal liability remains uneven. These challenges underscore the need for enhanced digital forensic capacity, cross-border cooperation, and public-private partnerships to strengthen cybercrime prosecution in South Africa.

4.2 Civil Liability

Where biometric data is processed without consent, victims may seek redress under the POPIA. Available remedies include:

- Lodging a complaint with the Information Regulator.
- Seeking civil damages under section 99.

- Requesting correction or deletion of unlawfully processed data.

Victims may also pursue common law claims for infringement of personality rights, including unauthorised use of image or voice, defamation, invasion of privacy, or misrepresentation. These claims are typically brought through the *actio iniuriarum,* a delictual action that protects non-patrimonial interests such as dignity, identity, and autonomy. Damages may encompass financial loss, emotional distress, and reputational harm.

Despite these remedies, enforcement remains fraught with difficulty. Identifying perpetrators in cyber-related cases is notoriously complex, particularly when anonymity, spoofing, or foreign servers are involved. In some instances, victims may consider holding third parties such as banks or service providers liable for failing to implement adequate safeguards, especially where biometric authentication systems are compromised. Yet this route is equally challenging as proving negligence or breach of statutory duty requires expert evidence, and institutions may rely on contractual disclaimers or demonstrate compliance with regulatory standards.

Moreover, civil litigation in South Africa is time-consuming and costly. Thus, although the legal framework offers substantive remedies, the real-world enforcement of civil liability remains uncertain particularly for ordinary individuals without access to legal resources or technical expertise.

Against the backdrop of substantive legal protection and practical enforcement challenges, the following section examines how selected foreign jurisdictions have approached the regulation of digital identity misuse, offering comparative insights that may inform South Africa's evolving legal response to digital personal identity fraud.

5. Comparative Analysis

While this discussion focuses on South Africa's legal framework, the challenges of digital personal identity misuse are global in scope. Jurisdictions across the globe are grappling with the legal implications of digital identity misuse, particularly in the context of artificial intelligence and biometric technologies. In light of the enforcement challenges facing South African law, it is instructive to examine how other jurisdictions have responded to the misuse of digital personal identity.

5.1 Global Approaches to Digital Identity Protection

Global approaches to digital identity protection reflect distinct legal philosophies. The UK's *Economic Crime and Corporate Transparency Act* offers a valuable institutional liability approach that merits consideration in South Africa's context. It's*"* failure to prevent fraud" (FTPFP) offence shifts the emphasis from the method of identity misuse to the responsibility of organisations to implement reasonable fraud prevention measures. The FTPF offence is not about digital identity authentication *per se* but about corporate accountability for fraud. This approach is particularly relevant in South Africa's context, where digital identity fraud often occurs within institutional systems that lack robust safeguards.

While the approaches vary, a comparative analysis reveals the following models:

- Statutory personality rights model

The Ensuring Likeness Voice and Image Security (ELVIS) Act, passed in 2024 by Tennessee, US is an example of a statutory personality rights model. It is the first-of-its-kind state law offering protections for an individual's voice and likeness against unauthorized clones and fakes generated using artificial intelligence (AI) (Auerbach, 2025).

The ELVIS Act represents a targeted statutory intervention aimed primarily at performers and public figures against commercial exploitation (Auerbach, 2025). It criminalises and civilly penalises the unauthorised use of a person's voice and likeness, including AI-generated impersonations. Although limited in geographic scope and focused on commercial exploitation, the Act affirms the principle that digital identity misuse constitutes a legal harm. It offers a statutory remedy rooted in personality rights, reinforcing the idea that individuals should control how their identity is used in digital spaces.

- Intellectual property model

Denmark proposes a bill that will grant its citizens copyright to their face, body, and voice. The proposed bill is the first in Europe to give citizens the legal right to ask platforms like Facebook, Instagram, and TikTok to take down fake digital versions of themselves online (Podadera, 2025; Woods, 2025).

The aim of the proposed bill is to:

- Give individuals ownership over their face, voice, and expressions.

- Allow them to license or restrict use like a copyrighted work.
- Provide legal remedies even when no financial loss is proven.

Denmark's proposed legislation represents a proactive shift in how digital identity is protected. Rather than relying solely on privacy-based frameworks like the EU GDPR which regulate how personal data is processed, Denmark reframes likeness (including voice, face, and expressions) as a proprietary right. This gives individuals affirmative control over their digital personal identity, allowing them to demand removal of deepfake content and sue for damages without needing to prove data harm or breach (Podadera, 2025**)**. It moves beyond enforcement of privacy violations and toward ownership-based protection, where the mere unauthorised use of one's likeness is actionable. This model empowers individuals to act swiftly and decisively against misuse, especially in commercial or reputational contexts.

- Hybrid constitutional–statutory model

South Africa's framework is more layered. The Constitution guarantees the rights to privacy and dignity, which underpins the protection of digital identity. POPIA operationalises these rights by regulating the processing of personal and biometric data, while the Cybercrimes Act criminalises identity theft, fraud, and unauthorised access. However, unlike Denmark's proposed IP model or the ELVIS Act's statutory clarity, South Africa has yet to codify digital personality rights explicitly.

5.2 Concluding Observations

While many jurisdictions possess foundational legal frameworks for data protection and identity rights, the rapid evolution of AI-driven fraud has exposed substantive gaps in how digital identity misuse is regulated. Denmark and Tennessee have responded not merely by strengthening enforcement, but by reimagining the legal basis for personal identity protection.

Denmark's proposal to treat a person's likeness including voice, face, and expressions as a form of intellectual property reflects a shift from privacy-based regulation to proprietary control, offering individuals direct remedies against deepfake misuse (Woods, 2025). Although this approach borrows from copyright logic, it does not equate a voice or likeness with a creative work; rather, it creates a *sui generis* right tailored to digital identity. The Denmark approach is novel but it does not automatically mean that other EU member countries will follow suit. Some EU member states may resist this model, arguing that the GDPR already protects biometric data and that extending copyright-like control to likeness may undermine freedom of expression and complicate enforcement. Denmark's proposal to treat likeness as intellectual property may also raise concerns about legal coherence and overreach.

The tension between technological innovation and legal doctrine reflects a broader challenge, namely safeguarding digital identity without overhauling foundational legal principles. Jurisdictions have responded in varied ways. Denmark proposes a likeness-as-property regime applicable to all individuals, while Tennessee's ELVIS Act focuses on protecting performers from AI-driven impersonation in commercial settings.

These developments suggest that legal innovation, and not just enforcement, may be necessary to meet the challenges posed by emerging technologies. South Africa, while equipped with constitutional and statutory protections, may need to consider whether its current framework sufficiently anticipates the risks of digital identity manipulation and whether clearer codification of personality rights in the digital realm is warranted. The goal is not to follow global trends blindly, but to build a coherent, resilient framework that protects digital citizens in practice.

6. Recommendations

Drawing on these insights, the following recommendations aim to strengthen South Africa's legal and institutional response to digital identity misuse, with a focus on fraud prevention, victim redress, and regulatory reform (Mashinini, 2025):

6.1 Enhance Institutional Capacity

- Invest in specialised digital forensic units within law enforcement to improve investigation and evidence-gathering in cybercrime cases.
- Expand the technical expertise and resources of the Information Regulator to ensure effective enforcement of POPIA, especially in biometric data cases.

Improve Legal Clarity and Accessibility

- Develop statutory guidance or judicial practice notes on the application of personality rights to digital identity misuse, including deepfakes and voice cloning.
- Promote public legal education on digital identity rights and available remedies, especially for vulnerable and digitally active users.

6.2 Strengthen Cross-Border and Public-Private Cooperation

- Establish formal cooperation mechanisms with international cybercrime units and digital platforms to trace perpetrators and preserve evidence across jurisdictions.
- Encourage partnerships between government, financial institutions, and tech companies to develop shared standards for biometric authentication and fraud prevention.

6.3 Consider Legislative Reform

- Explore the feasibility of introducing statutory personality rights for digital identity, drawing on models like the Tennessee ELVIS Act and Denmark's likeness-as-property proposal.
- Review the Cybercrimes Act and POPIA to ensure they adequately address emerging threats such as AI-generated impersonation and biometric spoofing.

6.4 Promote Victim-Centred Remedies

- Simplify access to civil remedies for victims of digital identity misuse, including streamlined procedures for POPIA complaints and small claims for non-patrimonial harm.
- Support alternative dispute resolution mechanisms that are affordable, accessible, and tailored to digital harms.

6.5 Introduce Institutional Liability for Failure to Prevent Fraud

- Drawing on the UK's Economic Crime and Corporate Transparency Act, South Africa should consider introducing a statutory offence for failure to prevent fraud**.** This approach shifts liability to organisations that benefit from fraudulent conduct committed by employees or agents, unless they can demonstrate that reasonable fraud prevention procedures were in place. Such a provision would incentivise banks, service providers, and digital platforms to adopt robust identity verification systems and internal controls, thereby reducing opportunities for digital identity misuse. It would also align South Africa's enforcement strategy with global trends in corporate accountability.

7. Conclusion

Digital personal identity has become a cornerstone of modern life, yet its misuse presents complex legal, ethical, and practical challenges. The focus of the research is not solely on the consequence of digital identity misuse such as fraud but on the protection of digital personal identity as an extension of personality rights.

South Africa's legal framework anchored in constitutional rights and comprising POPIA, the Cybercrimes Act, and common law personality rights offers substantive avenues for protection. The court's decision in *Grütter v Lombard* affirms the right to control one's identity, but adapting these principles to digital threats remains a pressing challenge. Victims of digital personal identity misuse, particularly in cases involving cyberfraud, continue to face significant barriers to redress due to technological complexity, evidentiary burdens, and institutional constraints.

Comparative approaches from Denmark, Tennessee, the UK, and the EU illustrate that legal systems can respond to digital identity threats through varied mechanisms, including proprietary control, statutory personality rights, and institutional accountability. These approaches offer valuable insights for South Africa as it seeks to strengthen its liability frameworks and respond to emerging risks such as AI-driven impersonation.

To ensure meaningful protection for digital citizens against digital personal identity fraud, South Africa should enhance its technical capacity, clarify the legal status of digital personal identity, and consider targeted legislative reforms. Measures such as introducing corporate liability for failure to prevent fraud, and exploring statutory personality rights, could help close enforcement gaps and align South Africa's legal response with global best practices.

Ultimately, protecting digital personal identity is not only a cybersecurity imperative, but it is also part of a global effort to safeguard dignity, identity, and trust in the digital age.

AI Declaration: I acknowledge the use of Microsoft Copilot as an assistive tool during my research. The final work reflects my own analysis, argumentation, and interpretation of the subject matter.

Ethics Statement: No ethical clearance was required.

References

Auerbach, B.C. (2024) "Trailblazing Tennessee Legislation – the ELVIS Act", [online], https://www.outsidegc.com/blog/trailblazing-tennessee-legislation-the-elvis-act.

Consumer Protection Act 68 of 1998.

Constitution of South Africa of 1996.

Cybercrimes Act 19 of 2020.

Economic Crime and Corporate Transparency Act (ECCTA). (2024) https://assets.publishing.service.gov.uk/media/67f8ef1845705eb1a1513f35/Failure+to+Prevent+Fraud+Guidance+-+English+Language+v1.6.pdf.

Ensuring Likeness Voice and Image Security (ELVIS) Act of 2024.

Grütter v Lombard 2007 (4) SA 89 (SCA), [online], https://www.saflii.org/za/cases/ZASCA/2007/2.html.

Joint Standard on Cybersecurity and Cyber Resilience Requirements 2 of 2024

Mashinini, N. (2025) "Deepfakes and South African law: remedies on paper, gaps in practice", [online], https://theconversation.com/deepfakes-and-south-african-law-remedies-on-paper-gaps-in-practice-263850.

National Cybersecurity Policy Framework (NCPF) of 2015.

Neetling, J. (2005) "Personality rights: a comparative overview", *The Comparative and International Law Journal of Southern Africa*, Vol. 38, No. 2 2005**.**

Podadera, S.D. (2025), "The first step towards fighting AI Abuse? Denmark Grants Citizens The Copyright to Their Face, Body and Voice", [online], https://www.remotestaff.com.au/blog/denmark-ai-face-copyright-law/.

Protection of Personal Information Act 4 of 2013.

United Nations Sustainable Development Goals, [online], https://sdgs.un.org/goals.

Robles-Carrillo, M. (2024) "Digital identity: an approach to its nature, concept, and functionalities", [online], https://digibug.ugr.es/bitstream/handle/10481/94868/Robles_Carrillo_Digital%20Identity.pdf?sequence=1&isAllowed=y.

Watney, M.M. (2024**)** "Exploring cyber fraud within the South African cybersecurity legal framework" [online]; https://www.researchgate.net/publication/381651578.

Woods, C. Denmark proposes copyright laws to protect against deepfakes", [online] https://lsj.com.au/articles/denmark-proposes-copyright-laws-to-protect-against-deepfakes/.

Yassar et al. (2025) "What is cybersecurity?", (2025) [online], https://www.techtarget.com/searchsecurity/definition/cybersecurity.