Before the mind is touched: What Chile's neurorights mean for South Africa's legal and ethical framework

W M Botes,[1,2] LLM (Intellectual Property Law), LLD (Biotechnology Law); **T Naidoo,**[2] LLM (Medical Law)

[1] *Department of Psychology, Pestilli Neuroscience Lab, University of Texas at Austin, Tex., USA*
[2] *School of Law, University of KwaZulu-Natal, Durban, South Africa*

Corresponding author: *T Naidoo (218035912@stu.ukzn.ac.za)*

This article examines what Chile's neurorights reforms may mean for South Africa (SA)'s legal and ethical framework. Chile is the first country to adopt an explicit constitutional and legislative response to neurotechnology, including protection for brain activity and information derived from it. Using Chile as a comparative lens, the article argues that SA does not necessarily require an immediate *sui generis* constitutional amendment to address neurorights-type concerns. Rather, existing constitutional protections for dignity, privacy, bodily and psychological integrity, freedom of thought and informed consent are already normatively receptive to many of the harms posed by emerging neurotechnologies. The more urgent challenge lies in timing; SA law remains largely reactive, often offering remedies only after intrusion, extraction or misuse has already occurred. The article therefore contends that protection should move upstream through proactive, risk-sensitive procedural reform and anticipatory governance, particularly in high-risk contexts involving coercion, asymmetrical power or intimate mental inference. It further argues that a neurotechnology-sensitive interpretation of existing rights, informed by local constitutional doctrine, neuroethics, and SA concerns around dignity, vulnerability and relational personhood, provides a more coherent and contextually appropriate path than immediate constitutional transplantation. The article concludes by outlining the general contours of *ex ante* safeguards for neurotechnology in SA while leaving open the possibility that more explicit neurorights protections may become necessary if existing doctrines prove systematically under-protective.

Keywords: neurorights, neurotechnology, mental privacy, cognitive liberty, neurodata, South African constitutional law, Chile, data protection

S Afr J Bioethics Law 2026;19(1):e4772. https://doi.org/10.7196/SAJBL.2026.v19i1.4772

Why mental privacy now matters in South Africa

Emerging technologies are rapidly reshaping how public and private entities interact with personal data in South Africa (SA), including sensitive biometric and neuro-inference technologies.[1,2] Police and law enforcement increasingly deploy artificial intelligence (AI)-enabled tools for identification and surveillance. For example, the South African Police Service (SAPS) uses applications that integrate fingerprint, facial and iris recognition against the national identity system to verify millions of identities in near real time, supporting investigations and case file management.[3] Predictive policing and automated surveillance systems, such as licence plate recognition networks like Vumacam, illustrate how data-driven tools are already embedded in public safety strategies.[4] Mobile and contactless biometric verification tools, including face and fingerprint scanning systems, are also increasingly being used within SA's broader public sector identity verification ecosystem, often in connection with the ongoing digital identity modernisation efforts of the Department of Home Affairs.[5]

At the same time, wearable and wellness technologies that collect and infer physiological and psychological data are becoming ubiquitous.[6] AI-powered health wearables like the Samsung Galaxy Ring, available in SA, track stress, sleep, heart rate, and other markers tied to physical and mental wellbeing.[7] Globally accessible electroencephalogram (EEG) headsets, such as the Muse brain activity band, and consumer EEG devices, such as the Emotiv Insight, illustrate how neural sensing is moving into the mainstream, enabling users to monitor relaxation or cognitive states outside clinical settings.[8] Digital and AI-based mental health applications are also widely used locally. Apps such as Wysa and Woebot, which guide users through cognitive behavioural therapy techniques using natural language interactions and mood tracking, have gained popularity in SA as accessible mental health support tools.[9,10]

Yet SA law typically responds *after* data collection or harm has occurred, treating evidentiary admissibility or privacy breaches as retrospective issues rather than preventing intrusion into mental life in the first place. Once sensitive mental data are accessed or inferred, the harm to dignity, autonomy and privacy cannot be undone even if evidence is later excluded. This raises a critical question: what can SA learn from Chile's proactive neurorights approach without copying its Constitution?

Although this article is primarily a comparative constitutional and doctrinal analysis, the questions raised by neurorights are not solely legal. They also emerge from a broader neuroethical debate concerning cognitive liberty, mental privacy, mental integrity, and the protection of agency in the face of increasingly sophisticated neurotechnologies. Foundational scholarship by Ienca and Andorno[11] together with the influential ethical framing offered by Yuste *et al.*[12]

has argued that existing legal and ethical frameworks may be strained by technologies capable of inferring, decoding or influencing mental states, thereby raising concerns that extend beyond conventional data protection to the conditions of autonomous thought itself. More recent governance-orientated work, including Ienca *et al.*,[13] further supports the view that neural data and neurotechnological interventions raise distinctive normative concerns that cannot be fully captured by ordinary privacy or medical law frameworks alone. These concerns are also increasingly reflected in contemporary public-facing neuroethics discourse, including Farahany's *The Battle for Your Brain*.[14] In the SA context, however, such debates must additionally be read through local normative lenses, including dignity, vulnerability, relational autonomy, and, where appropriate, *ubuntu*-informed approaches to personhood and social responsibility. The argument advanced here therefore remains primarily doctrinal. Still, it is informed by broader neuroethical debates that help illuminate why neural data and neurotechnological interventions may warrant heightened normative and legal scrutiny.

Chile's constitutional model of neurorights

Chile became the first country in the world to constitutionalise neurorights through a targeted amendment adopted in October 2021. This reform was not driven solely by lawyers, but emerged from a close alliance among neuroscientists, ethicists and policy-makers.[15] A central figure was neuroscientist Rafael Yuste, one of the original authors of the global 'neurorights' proposal, who worked directly with Chilean legislators. The political moment also mattered because after mass protests in 2019, Chile entered a period of intense constitutional reflection, creating space for innovative rights-based responses to emerging technologies.

The amendment was adopted through Law No. 21.383 and inserted into Article 19(1) of the Chilean Constitution, which protects fundamental rights. In translation, the new clause provides that:

> 'Scientific and technological development shall be at the service of people and shall be carried out with respect for life and physical and psychic integrity. The law shall regulate the requirements, conditions, and restrictions for its use by people and must especially protect cerebral activity, as well as the information derived from it.'[16]

This wording does two important things. First, it frames science and technology as constitutionally limited by human dignity and mental integrity. Second, it gives special status to 'cerebral activity' and 'information derived from it', elevating brain data to a constitutionally protected category. The practical effect is that the Chilean Parliament is now under a constitutional duty to adopt detailed legislation regulating neurotechnology, and any law or practice that undermines mental integrity can be struck down by the courts.

Chile's neurorights reforms should also be situated within a constitutional culture that is not politically neutral. Chile's post-dictatorship constitutional discourse has been deeply shaped by historical experiences of state overreach, including torture, surveillance, and violations of bodily and psychological integrity under the Pinochet regime (see, generally, Collins,[17] Loveman,[18] and Chilean constitutional jurisprudence and inter-American human rights materials recognising the protection of physical and psychological integrity in the post-authoritarian context). While there is no evidence that the neurorights amendment was conceived as a direct response to dictatorship-era practices, the constitutional language protecting 'physical and psychic integrity' and affording special protection to 'cerebral activity' and 'information derived from it' is nevertheless resonant within a broader Latin American human rights tradition that has long treated psychological coercion, dignity, and limits on state power as matters of constitutional significance. Read in that context, Chile's neurorights framework can be understood not merely as anticipatory governance of emerging neurotechnologies, but as emerging within a constitutional order already acutely attentive to forms of domination that threaten mental autonomy, the integrity of thought, and the conditions of personhood.

Implementation is currently unfolding through proposed neuroprotection legislation, often referred to as Chile's Neuroprotection or Neurotechnology Bill.[19] While still developing, this framework aims to regulate the certification of neurotechnology devices, set conditions for lawful data use, and establish oversight mechanisms to protect mental privacy and cognitive liberty. In parallel, Chilean regulators have already begun acting under the constitutional amendment itself. In the landmark case of *Girardi v Emotiv*,[20] the Chilean Supreme Court held that brainwave data collected by a consumer EEG device fell within the 'most intimate sphere of the person' and required heightened protection. The Court ordered the deletion of the data and required state authorities to prevent further sales of such devices unless they complied with the constitutional standard.[21] This decision shows the core effect of the Chilean model: courts can now intervene *before* or immediately after misuse, rather than waiting for harm to be remedied through later damages or the exclusion of evidence.

Chile's neurorights framework should not, however, be treated as a settled or unproblematic model. While *Girardi v Emotiv* is widely cited as an early and symbolically significant decision in the global neurorights debate, its practical effect and doctrinal reach remain contested. Likewise, Chile's constitutional amendment, although pioneering in expressly protecting 'cerebral activity' and 'information derived from it', has been criticised for its brain-centric framing and uncertain boundaries, and the difficulty of translating constitutional symbolism into workable regulatory design. Chilean scholarship has accordingly raised important questions about whether the amendment and proposed implementing framework provide sufficiently coherent or adaptable protection across the wider continuum of neurotechnologies, inferential systems and cognitive risks.[15,21,22] For present purposes, Chile is therefore best understood not as a fully mature template for transplantation, but as a valuable comparative experiment: one that powerfully surfaces the problem of anticipatory protection, while also illustrating the conceptual and institutional limits of early neurorights lawmaking.

This model matters for SA for three main reasons. First, it shifts legal protection to a point *before* intrusion. In Chile, neurotechnology cannot lawfully be used on people unless it complies with statutory conditions that give effect to the Constitution. This requirement means that the legality of interference with the mind is tested in advance, not only when evidence is challenged in court or when harm has already occurred.

Second, Chile recognises brain data as uniquely sensitive. By naming 'cerebral activity' and 'information derived from it' in the

Constitution, it signals that mental processes are not just another form of personal data. They deserve heightened protection because they relate directly to identity, autonomy, and freedom of thought. This constitutional recognition stands in contrast to systems that treat neural outputs as ordinary biometric or medical data.

Third, the Chilean model integrates constitutional rights with data and health law. Mental privacy is not left to ordinary data statutes alone. Still, it is anchored at the highest level of the legal system and then given effect through health law, consumer regulation, and data protection rules. This institutional design creates a layered system that protects mental integrity across medical, commercial and criminal contexts.

However, the Chilean model also has limitations for SA. Its wording is strongly brain centric. The Constitution requires that the law 'especially protect cerebral activity, as well as the information derived from it'.[16] This focus risks missing technologies that infer mental states indirectly, such as eye tracking, facial micro-expressions, voice stress analysis or attention-tracking software, which may reveal thoughts or recognition without directly scanning the brain.[16] A narrow reading of 'cerebral activity' could leave such tools outside the highest level of protection.

For SA, copying this wording into its own Constitution[23] would be both unlikely and unnecessary. A constitutional amendment is politically difficult and unnecessary, as the South African Bill of Rights already protects bodily and psychological integrity, privacy, and freedom of thought (sections 12(2), 14 and 15 of the Constitution). The problem is not the absence of rights, but the timing and clarity of their protection. Chile shows the value of acting before intrusion. SA can learn from this logic without copying Chile's constitutional text, by developing technology-neutral rules that protect mental content, whether accessed through the brain or through behavioural proxies, using ordinary legislative and procedural tools.

A technology-neutral understanding of neurorights

A doctrinally persuasive SA response to Chile's neurorights experiment should begin not by immediately constitutionalising a wholly novel and freestanding right, but by first clarifying the legal object that requires protection. In this respect, the operational definition of neurodata developed by Ray *et al*.[24] (Supplementary Box 1 in that article) is particularly useful, as it defines neurodata functionally and in data-centric terms as data derived directly or indirectly from the structure, activity or functional signals of the human nervous system, including raw recordings, processed signals and computationally derived representations that remain reasonably linkable to such activity or retain meaningful inferential or reconstructive capacity regarding neural, cognitive, emotional or behavioural states. This definition is doctrinally significant because it avoids an unduly narrow, device-specific conception of neural information and instead captures the full downstream realities of contemporary neurotechnology, including predictive outputs, inferred profiles and model artefacts in which neural traceability or meaningful inferential capacity persists.[25] Against that backdrop, Chile's constitutional reform is best understood not as conclusive proof that a *sui generis* right to mental privacy has already crystallised in comparative law, but rather as a constitutional signal that neurotechnological intervention and neurodata processing may implicate a qualitatively distinct dimension of personhood, autonomy and mental integrity deserving heightened protection. For SA, the stronger doctrinal route is therefore not the immediate recognition of an autonomous neuroright, but a principled, neurotechnology-sensitive interpretation of existing constitutional guarantees, particularly privacy, dignity, bodily and psychological integrity, freedom of thought and informed consent, supplemented by a clear operational category of neurodata that can trigger heightened duties of consent, purpose limitation, access restriction, proportionality, and governance of downstream inferential uses (see Yuste,[25] Jwa and Poldrack[26] and Eke *et al*.[27]). Such an approach remains faithful to SA's transformative constitutional method while avoiding premature rights inflation, yet still leaves open the possibility that, should existing rights prove systematically under-protective in the face of neural inference, cognitive profiling or behavioural manipulation, a more explicit *sui generis* protection for mental privacy may in future become normatively and doctrinally justified (see Yuste *et al*.[12] and Ienca *et al*.[13]). These authorities support the argument that existing rights may be interpreted expansively for now, while leaving open future doctrinal development if neurotechnological harms expose structural gaps.

SA's current framework: Strong rights, late protection

SA's constitutional order already contains the normative building blocks required to protect mental privacy and cognitive liberty. The difficulty is not a lack of rights, but that the legal system often activates protection too late, *after* intrusive collection has occurred. Neurotechnology and neuro-inference tools expose this timing weakness because once mental states are accessed, inferred or recorded, the intrusion cannot be reversed.

Constitutional anchors: Strong substantive rights

Four constitutional protections are particularly relevant to neurotechnology and mental privacy.

First, section 12(2) guarantees everyone the right to bodily and psychological integrity, including security in and control over one's body, and not to be subjected to medical or scientific experiments without informed consent. Even where neurotechnology is not framed as 'medical', the right is conceptually important; using devices to probe or shape cognition can constitute an interference with psychological integrity and self-control, particularly when applied coercively or under conditions of vulnerability (for example, during custodial interrogation).

Second, section 14 protects privacy, including the right not to have one's person or home searched, possessions seized, or communications infringed. Traditionally, this right is operationalised through search-and-seizure doctrine, warrants, and proportionality limits. Neurotechnology complicates this because it can generate 'private' information without entering a home or seizing a physical object. A device can infer recognition, stress, arousal or attention from physiological or behavioural signals, turning the body into a constant source of evidence.

Third, section 15 protects freedom of religion, belief and opinion. While not commonly litigated as a 'freedom of thought' clause in the

way some international instruments are, it provides a constitutional foothold for arguing that the state should not intrude into mental processes or attempt to extract mental content without strict safeguards. In neurotechnology debates, this right becomes relevant where the state deploys tools designed to access, predict or influence cognitive states, particularly when deployed coercively.

Fourth, section 35(5) provides that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if admission would render the trial unfair or otherwise be detrimental to the administration of justice. This is the key criminal procedure safeguard in practice. Yet it is also the clearest illustration of the 'late protection' problem: it is a remedial mechanism that is typically triggered only *after* the evidence has already been obtained, meaning that the intrusion into mental privacy and psychological integrity has already occurred.

In the SA context, the normative case for caution regarding neurorights is further strengthened by local bioethical traditions that emphasise relational personhood, vulnerability and dignity as socially embedded rather than purely individualistic concepts. *Ubuntu*-informed ethical reasoning, as developed, for example, by Metz,[28] does not displace constitutional rights analysis. Still, it does illuminate why neurotechnological interference with thought, emotion, memory or behavioural disposition may be especially troubling; such interventions do not affect only isolated individual choice. Still, they may disrupt the relational conditions through which personhood, agency and moral recognition are constituted. Read alongside the Constitution's protection of dignity, privacy and bodily and psychological integrity, and in conversation with calls for more contextually grounded African bioethics such as Behrens,[29] an African bioethical lens supports a more context-sensitive approach to neurotechnology governance, one attentive not only to autonomy in the liberal sense, but also to dependency, social vulnerability, structural inequality, and the possibility that neural data practices may reproduce forms of epistemic or technological domination. On this view, the SA response need not immediately constitutionalise a freestanding neuroright. Still, it should recognise that the ethical stakes of neurotechnology are heightened where interventions or inferences bear directly on the relational and social foundations of personhood.

This article does not seek to provide a comprehensive review of all SA writing on neurotechnology, privacy, or digital health regulation. Its contribution is narrower and more specific; it offers a comparative constitutional analysis of Chile's neurorights framework and asks what, if anything, SA constitutional doctrine can learn from it. The novelty of the argument lies not in the general observation that neurotechnologies may implicate rights to privacy, dignity, or bodily and psychological integrity, but in the claim that SA's existing constitutional architecture is already normatively receptive to neurorights-type concerns. At the same time, the more urgent legal challenge is procedural and institutional, namely, how to move protection 'upstream' through anticipatory governance, consent design and neurodata-sensitive regulatory safeguards before harm becomes constitutionally visible. To our knowledge, this specific combination of comparative constitutional analysis, SA doctrinal interpretation, and pre-emptive governance framing remains underdeveloped in the existing local literature.

How SA courts would analyse neurorights-type disputes

SA courts would be likely to analyse neurorights-type disputes through existing constitutional doctrine rather than by recognising a novel freestanding right. The primary doctrinal route would be section 14, interpreted as protection not only against physical searches but against unjustified access to intimate informational domains. SA privacy jurisprudence already recognises that privacy is not absolute but exists on a gradient, with the strongest protection attaching to the inner sanctum or intimate personal sphere. In *Bernstein v Bester*,[30] the Constitutional Court explained that the more closely information relates to personal identity, autonomy and intimacy, the more intense the constitutional protection becomes. That reasoning is directly adaptable to neurotechnology: mental data, whether derived from direct neural recording or reliable cognitive inference, should be understood as falling within the highest tier of informational privacy, because it concerns the most intimate layer of personhood, thought, recognition, emotion, attention and mental self-disclosure. This understanding is reinforced by *Mistry v Interim National Medical and Dental Council*[31] and *Investigating Directorate v Hyundai Motor Distributors*,[32] where the Court stressed that intrusive search powers must be narrowly construed and exercised under constitutionally adequate safeguards, especially through properly circumscribed warrants. In *Magajane v Chairperson, North West Gambling Board*,[33] the Court likewise held that warrantless inspections were unconstitutional where less restrictive means, notably prior judicial authorisation, were available. On this approach, compelled neuro-inference can plausibly be understood as a form of cognitive or informational search, even where no physical object is seized. The doctrinal implication is not that neurorights require recognition as a wholly new constitutional category, but that they sharpen and intensify the protection already afforded by the inner core of section 14 privacy.

Section 12(2) strengthens this analysis by applying to technologies that directly probe, record or shape cognition, because neurorights-type harms implicate not only privacy but also bodily and psychological integrity, agency, and control over one's person. This engagement of section 12(2) does not mean that all cognitive inference would be automatically unconstitutional, but reflects that the provision is triggered whenever the state or another actor uses a technology to penetrate, extract or materially influence mental processes in a manner that undermines a person's control over their own body or mind. Although SA jurisprudence on psychological integrity remains underdeveloped, the logic of bodily integrity cases is instructive. In *Minister of Safety and Security v Xaba*,[34] the Court treated compelled surgical extraction of evidence from a suspect's body as a constitutionally serious intrusion that could not be justified under ordinary investigative powers. By analogy, coercive neuro-inference or direct neural recording should be understood as constitutionally suspect where it compels access to mental content or substantially interferes with mental self-determination. Such interference would not necessarily be *per se* unconstitutional. Still, it should trigger rigorous scrutiny under section 36, requiring that it be lawful, necessary and scientifically reliable, and that less restrictive means be absent before the intrusion occurs.

Section 15 further supports this reading and should be understood as more than merely supplementary. The provision protects not

only religion and belief, but also conscience, thought and opinion, making it a plausible constitutional anchor for the protected inner mental sphere. Read together with section 39(1)(b), this provision allows interpretation in the light of international human rights law, which distinguishes between the protected inner domain of thought and conscience (*forum internum*) and the outward manifestation or expression of belief, which may be subject to limitation. Where neurotechnology penetrates or extracts mental content, such as recognition responses, emotional states or cognitive patterns, the constitutional concern is therefore not only informational privacy under section 14, but intrusion into this protected inner sphere itself.

In criminal proceedings, courts would most often encounter such issues through section 35(5), which governs the exclusion of evidence obtained in violation of constitutional rights. As the Supreme Court of Appeal explained in *S v Tandwa*,[35] this provision operates as a remedial mechanism triggered only after the evidence has already been obtained. For ordinary evidentiary violations, that may sometimes be sufficient. But where the intrusion concerns mental privacy or psychological integrity, reliance on exclusion alone is constitutionally problematic because the core harm has already occurred and cannot be undone. The difficulty is therefore not merely procedural. A framework that relies primarily on *post hoc* exclusion risks becoming constitutionally incoherent; it recognises the right, yet structurally permits its irreversible violation before the law intervenes. This is difficult to reconcile with the state's positive obligation under section 7(2) to respect, protect, promote and fulfil the rights in the Bill of Rights. In neurorights-type contexts, section 35(5) cannot be the primary safeguard; where intrusion into the mind is itself the completed violation, a remedial-only model may be constitutionally inadequate.

Statutory landscape: Partial safeguards, fragmented by context

SA's main statutory protections are meaningful but incomplete for neurodata and mental inference. The Protection of Personal Information Act 4 of 2013 (POPIA) provides a general framework for lawful processing.[36] For mental privacy, two features matter most. First, POPIA generally prohibits the processing of 'special personal information' unless an exception applies. This category includes, among other things, information concerning health and biometric information (section 26 read with the definitions and permitted grounds in sections 27 - 33). Neurodata is not explicitly listed, so it would need to be argued into existing categories, most plausibly as health-related or biometric-derived information, creating uncertainty. Second, POPIA contains provisions that limit its application where information is processed for law enforcement or litigation-related functions (sections 6(1)(c) - (d) and 37 – including exclusions for certain public bodies and exemptions where processing is necessary for the prevention, detection, investigation, prosecution and punishment of offences, and for the conduct of legal proceedings). In practical terms, these pathways create a risk that investigators can collect sensitive cognitive inference data first and then argue for its legality later. POPIA's structure is largely compliance orientated, containing conditions for lawful processing, purpose limitation, minimisation and safeguards. Still, it does not impose a universal requirement of *prior judicial authorisation* for the use of mental content inference tools in investigations.

The National Health Act 61 of 2003[37] (NHA) offers a clearer confidentiality rule, but only within healthcare settings. Section 14(1) provides that 'all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment, is confidential', and section 14(2) permits disclosure only in limited circumstances, including with the user's written consent, under a court order or law, or where non-disclosure poses a serious threat to public health or to the health/wellbeing of the user or others. These sections are highly relevant where neurodata originates clinically, for example, EEG or neuroimaging conducted for diagnostic purposes. However, its protection is *context bound* and does not govern neurodata collected outside a 'health establishment', such as by police, employers, schools, insurers, or consumer devices.

The Criminal Procedure Act 51 of 1977[38] (CPA) establishes the procedural architecture governing searches and seizures in chapter 2 (sections 19 - 36), with section 21 entrenching prior judicial authorisation on reasonable grounds as the primary *ex ante* control for intrusive investigations, subject only to narrowly circumscribed exceptions under section 22. Warrants and reasonableness principles operate as the traditional *ex ante* control for intrusive investigations. Yet neurotechnology often does not fit neatly into the physical search-and-seizure model. If police do not 'seize' a tangible object but instead generate cognitive inference data by recording eye movements, stress responses or neural signals, it is not always clear that current warrant practice will automatically treat this as requiring prior judicial scrutiny, particularly where the technology is framed as 'observation' or 'interview technique' rather than a search.

Existing SA criminal procedure offers some analogical guidance, but no settled answer, for neurocognitive investigative techniques. Cases involving bodily samples and forensic evidence show that courts have long recognised that the compelled extraction of information from the body implicates privacy and constitutional rights, even when it is treated as non-testimonial physical evidence. In *S v Orrie*,[39] for example, the involuntary taking of a blood sample for DNA profiling was recognised as an intrusion on privacy, albeit one that could in principle be justified in the criminal process. That line of authority is useful because it shows that the body may become a site of evidentiary extraction without collapsing the constitutional inquiry into ordinary observation. Yet neurotechnology remains distinguishable. Eye tracking, cognitive inference tools, affective analytics or neural monitoring may not require the seizure of a physical object or the extraction of a conventional bodily sample at all; they may instead generate evidence by interpreting behavioural, physiological or neural signals in real time. The CPA's existing search-and-seizure architecture, including section 21's warrant model, therefore provides only an imperfect fit; it helps illuminate the seriousness of compelled access to intimate information. Still, it does not clearly determine when technologically mediated inference about mental states should count as a search, an inspection, a forensic procedure, or something constitutionally more exceptional. That uncertainty is precisely why a more explicit *ex ante* framework is needed.

The timing problem: Legality tested after intrusion

These constitutional and statutory rules create strong normative constraints, but they frequently activate too late. In criminal

matters, section 35(5) exclusion is typically litigated at trial or during admissibility proceedings, after the data exist and after mental intrusion has occurred.[38] Even if evidence is excluded, the invasion of psychological integrity and privacy cannot be undone. Because POPIA is structured around processing conditions and includes exemptions relevant to investigations and proceedings,[36] it can be invoked by state actors to justify collection without the kind of advance authorisation that would be expected for other intrusive techniques. This situation creates a grey zone where neuro-inference tools might be used operationally before courts have had an opportunity to set boundaries. The NHA strongly protects clinical neurodata, but if the same category of data is generated outside the healthcare system, through consumer wearables, workplace monitoring or police-deployed devices, those confidentiality protections fall away, leaving POPIA and general constitutional review as the primary safeguards.

POPIA, law enforcement, and the timing problem: SA case studies

SA's data protection framework does not prohibit the use of personal information for law enforcement purposes. POPIA expressly allows processing where it is necessary to comply with a legal obligation or perform a public law duty, including for the prevention, detection, investigation and prosecution of offences.[36] Such procedures do include police investigations. If SAPS can show that processing is 'necessary' for investigation or prosecution, POPIA may permit collection and use even without the data subject's consent. Although such processing remains subject to POPIA's general conditions, such as lawfulness, minimality, purpose specification and security safeguards, POPIA does not require prior judicial authorisation for all highly intrusive forms of data collection, including those that access or infer mental states. Legal scrutiny often occurs only later, if an accused challenges the evidence at trial or if the Information Regulator intervenes after harm has already occurred. This structural feature deepens the 'late protection' problem: in other words, mental intrusion may occur first, with legal assessment only afterwards.

This timing weakness becomes clear in three realistic SA scenarios.

First, imagine that SAPS introduces eye tracking software during identity parades to record whether a suspect's gaze lingers longer on a particular photograph, which investigators treat as evidence of recognition. There is no statute requiring advance judicial authorisation for such cognitive inference techniques. Police could argue that this is behavioural or biometric evidence processed for law enforcement purposes and therefore permissible under POPIA. A court would be likely to assess legality only later, under section 35(5) of the Constitution,[23] when deciding whether to admit the evidence. By then, the intrusion into the suspect's mental life has already occurred, placing dignity, privacy, psychological integrity and fair-trial rights at risk.

Second, consider a patient who undergoes an EEG in a public hospital for epilepsy diagnosis. Police later request access to the EEG data during a robbery investigation. Under section 14 of the NHA,[37] the data are confidential and may be disclosed only with the patient's written consent or under a court order or law. This provides meaningful protection, but the NHA does not specify how narrow such an order must be, how long data may be kept, or whether secondary analysis is allowed. If access is granted without strict limits, misuse will again have to be challenged after the fact. Protection exists, but it is still structurally late.

Third, consider an SA company marketing a 'focus-enhancing' headset to schools or employers. The device tracks EEG-like signals or physiological proxies and claims to measure attention or stress. Data are processed under POPIA, which contains no specific mental privacy standard. If the company asserts a lawful basis and claims to meet POPIA's conditions, the system may be deployed, even on children or economically vulnerable workers. There is no independent verification of scientific reliability, no special consent standard for mental data, and no clear rule limiting secondary use. If harm occurs, users must complain later to the Information Regulator or go to court. Again, protection is reactive.

Across criminal justice, healthcare, and consumer markets, the same pattern appears. POPIA allows police access for investigative purposes; the NHA protects clinical data, but only within healthcare settings; and the CPA[38] focuses mainly on physical searches. None of these legal frameworks consistently requires that cognitive inference techniques be authorised and limited *before* they are used. This is the structural weakness that Chile's neurorights model exposes. Its importance lies not in its wording, but in its timing; protection is triggered before intrusion. SA can reach a similar point without constitutional amendment, but only by developing technology-neutral rules that require early, independent control whenever the state or private actors seek to access, infer or shape a person's mental life.

What SA can learn from Chile

The central lesson from Chile is simple: protection must occur *before* intrusion into the mind. Once thoughts, emotions, recognition responses, or cognitive patterns have been accessed or inferred, no later remedy can undo that invasion. Excluding evidence, awarding damages, or issuing compliance orders may acknowledge wrongdoing, but they cannot restore mental privacy. Chile's approach therefore treats interference with mental processes as something that must be controlled in advance, through clear legal conditions and independent oversight, rather than repaired afterwards.

SA already protects dignity, privacy, psychological integrity, freedom of thought, and fair-trial rights.[23] The problem is not substance but timing. These rights are usually triggered only after the mind has already been accessed.

SA can adopt Chile's proactive logic without constitutional change. A short statute, or targeted amendments to the CPA and POPIA, could introduce a technology-neutral rule that applies to any method that accesses, infers, predicts or shapes mental content, whether through brain scans or indirect proxies such as eye tracking, emotion detection or attention monitoring. For criminal justice, this framework should require prior judicial authorisation, proof of reliability and necessity, and narrow limits on device, protocol, duration and use, as well as full record-keeping with defined retention and deletion periods. This proposed framework would move control upstream, ensuring that courts set boundaries before intrusion occurs.

This proposed approach fits naturally into SA's institutional design. Courts already authorise intrusive searches and surveillance and can extend that authority to cognitive inference techniques. The South African Health Products Regulatory Authority (SAHPRA) can certify neurotechnology used in clinical or quasi-clinical contexts, and the Information Regulator can oversee data compliance, guided by heightened standards for mental data.

No constitutional amendment is needed. SA's Bill of Rights already sets out the values; what is missing is procedural timing. Building on the warrant tradition and rights-based criminal procedure, SA can protect mental privacy across policing, healthcare, education, workplaces and consumer markets by ensuring that when the mind is at stake, the law intervenes before intrusion occurs.

To avoid remaining purely aspirational, the SA reform agenda should be understood in institutionally modest but concrete terms.

First, prior judicial authorisation or comparably independent *ex ante* oversight should be reserved for high-risk or coercive contexts in which neurotechnologies are used to infer, monitor or influence mental states under conditions of asymmetrical power, most obviously in criminal investigations, custodial settings, compulsory psychiatric assessments, workplace monitoring or educational discipline, rather than for ordinary low-risk consumer or therapeutic uses. In such contexts, the threshold should be necessity, proportionality, scientific reliability, and the absence of less intrusive means, mirroring familiar constitutional limits on bodily searches and privacy intrusions.

Second, where neurotechnologies are deployed for clinical or quasi-clinical purposes, SAHPRA (or a specialised co-regulatory framework involving SAHPRA, research ethics structures, and information regulators) should assess not only conventional safety and efficacy, but also modality-specific inferential risk, downstream data governance, explainability of outputs, and whether the technology enables cognitive, affective or behavioural profiling beyond its stated therapeutic purpose.

Third, for non-clinical neurodata practices, SA law could adopt a risk-tiered governance model, drawing comparatively, though not mechanically, on Chile's implementing debates, under which higher-risk uses trigger enhanced consent, independent oversight, stricter purpose limitation, and heightened restrictions on secondary use or compelled disclosure.

Properly understood, the proposed reforms therefore amount not to a wholesale new regulatory code, but to a set of targeted upstream safeguards that make existing constitutional protections more operational before harm is normalised or retrospectively litigated.

Conclusion

Neurotechnology and cognitive inference tools are no longer futuristic risks. In SA, they already appear in different forms in policing, healthcare, education, workplaces and consumer markets. Although SA's Constitution strongly protects dignity, privacy, psychological integrity, freedom of thought and fair-trial rights, these protections are too often activated only after the mind has already been accessed. Chile's neurorights amendment shows that the critical issue is not the wording of rights, but the timing of their protection: the law must intervene *before* mental intrusion occurs, not merely respond afterwards.

SA does not need to copy Chile's constitutional text. Its Bill of Rights already provides the necessary normative foundation. What is required is a procedural shift through ordinary legislation to provide for technology-neutral rules requiring advance authorisation, reliability screening, a narrow scope and record-keeping whenever mental content is accessed or inferred. Such reforms can be built into existing institutions, drawing on SA's strong warrant tradition and rights-based criminal procedure.

This shift is also an ethical and policy imperative. Mental privacy is inseparable from dignity and autonomy. Without control over one's inner life, other freedoms lose meaning. The risks of intrusive technologies are not evenly distributed; vulnerable groups, suspects in custody, patients, children, workers, and economically dependent communities are more likely to be exposed without real choice. If left unregulated, neurotechnology may deepen inequality rather than advance human wellbeing.

Public trust in health and justice systems depends on the assurance that intimate mental information will not be extracted casually or secretly. Protecting mental privacy therefore supports both individual rights and institutional legitimacy. A proactive approach also aligns with African bioethics' emphasis on relational dignity by respecting people not as data sources, but as moral agents in the community. Acting before the mind is touched is not only a legal necessity, but also a moral obligation.

Declaration. The research for this study was done in partial fulfilment of the requirements for TN's PhD (Law) degree at the University of KwaZulu-Natal.
Acknowledgements. None.
Author contributions. Both authors contributed equally to the conceptualisation, research, writing, review and editing of this manuscript.
Funding. None.
Conflicts of interest. None.

1. Breckenridge K. The biometric state: The promise and peril of digital government in the new South Africa. J South Afr Stud 2005;31(2):267-282. https://doi.org/10.1080/03057070500109458/
2. Wodajo K. Societal and structural risks of biometric ID: Towards people's right to privacy. Sci Technol Soc 2024;29(4):614-631. https://doi.org/10.1177/09717218241281941
3. Darch C, Majikijela Y, Adams R, Rule S. AI, biometrics and securitisation in migration management: Policy options for South Africa. Policy Action Network, March 2020. https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData5_Migration_Elec.pdf (accessed 27 January 2026).
4. Oxford Institute of Technology and Justice. South Africa. https://www.techandjustice.bsg.ox.ac.uk/research/south-africa#:~:text=The%20system%20triggered%2014%2C255%20alerts,of%20interest%20for%20other%20cases (accessed 27 January 2026).
5. Hassan M. South Africa adopts ABIS solution to national identity program. M2SYS Blog, 10 July 2018. https://www.m2sys.com/blog/biometric-resources/south-africa-adopts-abis-solution-to-national-identity-program/#:~:text=The%20Home%20Affairs%20Department%20of,added%20in%20fiscal%202019%2D2020 (accessed 27 January 2026).
6. Mbekwa N, Adebesin F. Not missing a step: South Africans taking control of their personal wellbeing using wearable health devices. J Health Inform Afr 2019;6(2):11-18. https://doi.org/10.12856/JHIA-2019-v6-i2-224
7. Samsung. Introducing Galaxy Ring: Samsung's first smart ring. https://www.samsung.com/za/mobile-phone-buying-guide/introducing-samsung-galaxy-ring/#:~:text=Smart%20rings%20are%20innovative%20devices,of%20the%20Samsung%20Health%20app (accessed 27 January 2026).
8. Sawangjai P, Hompoonsup S, Leelaarporn P, Kongwudhikunakorn S, Wilaiprasitporn T. Consumer grade EEG measuring sensors as research tools: A review. IEEE Sens J 2019;20(8):3996-4024. https://doi.org/10.1109/JSEN.2019.2962874
9. Chipps W. South African university students' user experience of mobile applications for anxiety and depression. Master's thesis. Cape Town: Department of Psychology, Faculty of Humanities, University of Cape Town, 2024. http://hdl.handle.net/11427/40830 (accessed 14 April 2026).
10. Khan F, Kayser N, Madiba M. Enhancing student wellbeing and success through AI-driven mental-health support: A case study of AI mental-health chatbot implementation at a South African university. J Stud Aff Afr 2025;13(2). https://doi.org/10.24085/jsaa.v13i2.5983
11. Ienca M, Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. Life Sci Soc Policy 2017;13(1):5. https://doi.org/10.1186/s40504-017-0050-1

12. Yuste R, Goering S, Arcas, B, et al. Four ethical priorities for neurotechnologies and AI. Nature 2017;551(7679):159-163. https://doi.org/10.1038/551159a
13. Ienca M, Fins JJ, Jox RJ, et al. Towards a governance framework for brain data. Neuroethics 2022;15:20. https://doi.org/10.1007/s12152-022-09498-8
14. Farahany NA. The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology. New York: St Martin's Press, 2023.
15. López-Silva P, Madrid R. Neural data and neuroprotection in the Chilean Constitution Reform Bill: Critical considerations. In: López-Silva P, ed. Contextualizing Neuroprotection: Latin American Perspectives on the Impact of Neurotechnological Development in Life and Society. Cham, Switzerland: Springer Nature, 2025:161-176. https://doi.org/10.1007/978-3-031-96055-0_11
16. Diario Oficial República de Chile. Ley número 21.383: Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas. [This is the amended Chilean Constitution of 2021.] https://www.diariooficial.interior.gob.cl/edicionelectronica/index.php?date=25-10-2021&edition=43086-B&v=2 (accessed 27 January 2026).
17. Collins C. Post-transitional justice: Human rights trials in Chile and El Salvador. Latin Am Polit Soc 2011;53(4):211-215. https://doi.org/10.2307/41342356
18. Loveman B. Chile: The Legacy of Hispanic Capitalism. 3rd ed. Oxford: Oxford University Press, 2001.
19. Proyecto de Ley. Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías. Boletín 13828-19. [This the bill in the Chilean Congress that would regulate neurotechnologies and protect neurorights beyond the constitutional amendment.] https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmBOLETIN=13828-19&prmID=14385 (accessed 27 January 2026).
20. Girardi/Lavín v Emotiv Inc. Decision by the Chilean Supreme Court, 9 August 2023. https://derechocienciaytecnologia.uc.cl/wp-content/uploads/2024/02/CS-105065-2023.pdf (accessed 27 January 2026).
21. Cornejo-Plaza MI, Cippitani R, Pasquino V. Chilean Supreme Court ruling on the protection of brain activity: Neurorights, personal data protection, and neurodata. Front Psychol 2024;15:1330439. https://doi.org/10.3389/fpsyg.2024.1330439
22. Zúñiga-Fajuri A, Villavicencio Miranda L, Zaror Miralles D, Salas Venegas R. Neurorights in Chile: Between neuroscience and legal science. Dev Neuroethics Bioeth 2021;4:165-179. https://doi.org/10.1016/bs.dnb.2021.06.001
23. Constitution of the Republic of South Africa, 1996. https://www.justice.gov.za/constitution/SAConstitution-web-eng.pdf (accessed 14 April 2026).
24. Ray KL, Botes M, Collier M, et al. Global brain research in the era of national data sovereignty. Nature Neurosci 2026 (in press).
25. Yuste R. Advocating for neurodata privacy and neurotechnology regulation. Nature Protoc 2023;18(10):2869-2875. https://doi.org/10.1038/s41596-023-00873-0
26. Jwa AS, Poldrack RA. Addressing privacy risk in neuroscience data: From data protection to harm prevention. J Law Biosci 2022;9(2):lsac025 https://doi.org/10.1093/jlb/lsac025
27. Eke DO, Bernard A, Bjaalie JG, et al. International data governance for neuroscience. Neuron 2022;110(4):600-612. https://doi.org/10.1016/j.neuron.2021.11.017
28. Metz T. Ubuntu as a moral theory and human rights in South Africa. Afr Hum Rights Law J 2011;11(2):532-559. https://www.ahrlj.up.ac.za/images/ahrlj/2011/ahrlj_vol11_no2_2011_thadeus_metz.pdf (accessed 14 April 2026).
29. Behrens KG. Towards an indigenous African bioethics. S Afr J Bioethics Law 2013;6(1):32-35. https://www.academia.edu/3820857/Towards_an_Indigenous_African_Bioethics (accessed 14 April 2026).
30. Bernstein and Others v Bester NO and Others (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996).
31. Mistry v Interim National Medical and Dental Council and Others (CCT13/97) [1998] ZACC 10; 1998 (4) SA 1127 (CC); 1998 (7) BCLR 880 (CC) (29 May 1998).
32. Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others (CCT1/00) [2000] ZACC 12; 2000 (10) BCLR 1079 (CC); 2001 (1) SA 545 (CC); 2000 (2) SACR 349 (CC) (25 August 2000).
33. Magajane v Chairperson, North West Gambling Board (CCT49/05) [2006] ZACC 8; 2006 (10) BCLR 1133 (CC) ; 2006 (5) SA 250 ; 2006 (2) SACR 447 (8 June 2006).
34. Minister of Safety and Security v Xaba 2004 (1) SACR 149 (D).
35. S v Tandwa and Others (538/06) [2007] ZASCA 34; [2007] SCA 34 (RSA); 2008 (1) SACR 613 (SCA) (28 March 2007).
36. South Africa. Protection of Personal Information Act 4 of 2013. https://www.gov.za/documents/protection-personal-information-act (accessed 14 April 2026).
37. South Africa. National Health Act 61 of 2003. https://www.gov.za/documents/acts/national-health-act-61-2003-23-jul-2004 (accessed 14 April 2026).
38. South Africa. Criminal Procedure Act 51 of 1977. https://www.gov.za/documents/criminal-procedure-act-1977-26-mar-2015-1224 (accessed 14 April 2026).
39. S v Orrie and Another (SS 32/O3) [2003] ZAWCHC 63; 2004 (3) SA 584 (C); 2004 (1) SACR 162 (C) (21 November 2003).

Received 29 January 2026; accepted 7 April 2026.