

Beyond Data Privacy: The Case For Mental Privacy And Neuro-Rights

Oltre la privacy dei dati: Il caso della privacy mentale e dei diritti neurologici

[MIRNA ELIZABETH GONZÁLEZ BARRERA](#) 

Professor and Researcher
University of Guadalajara

[JERSAIN ZADAMING LIAMAS COVARRUBIAS](#) 

Professor and Researcher
University of Guadalajara

Abstract

This article contends that neurotechnology governance should operationalize existing rights rather than create new “neurorights.” Drawing on EU, Chilean, and U.S. developments and international soft law, and on U.S. First/Fourth/Fifth Amendment tensions, it proposes a capability-based framework that defines protected objects (neurodata, neuro-inference, neuro-effect), presumes their sensitivity, tiers duties by what systems can reveal or modulate, embeds a Neuro-Privacy Impact Assessment at design, heightens safeguards in coercive settings (treating compelled decoding as presumptively testimonial), sets evidentiary gatekeeping, and forbids deceptive neuromodulation. The result is actionable guidance without new constitutional text.

L'articolo aderisce alla tesi secondo cui sarebbe preferibile rendere effettive e operative le tutele già esistenti, invece di creare nuovi “neuro-diritti”. Alla luce degli sviluppi in UE, Cile e USA e del soft law internazionale, e delle tensioni con Primo/Quarto/Quinto Emendamento, propone un quadro “capability-based” che definisce gli oggetti protetti (neurodata, neuro-inference, neuro-effect), ne presume la sensibilità, calibra gli obblighi in base a ciò che i sistemi rivelano/modulano, integra una Neuro-Privacy Impact Assessment in fase di design, rafforza le garanzie in contesti coercitivi (decodifica coattiva come testimoniale), fissa criteri probatori e vieta neuromodulazione ingannevole.



© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.

This contribution is licensed under a Creative Commons Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Keywords: neuroscience; neurotechnologies; neuro-rights; cognitive liberty; mental privacy; brain-computer interfaces; legal frameworks.

Summary: [1. Introduction](#) - [2. Neuroscience and Neurotechnologies.](#) - [3. Towards a Neuro-Rights Era.](#) - [4. The intersection between privacy and neuro-rights](#) - [5. The Paradox of privacy in the era of neuro-rights](#) - [6. Lawmaking, Governance, and Enforceable Norms on Neuro-Rights](#) - [7. Findings and Critical Discussion](#) - [8. From Principles to Practice: An Operational Framework for Mental Privacy and Neurorights](#) - [9. Conclusions](#)

1. Introduction.

The convergence of neuroscience and emerging neurotechnologies has profoundly reshaped how we understand cognition, behavior, and decision-making. Advances in electroencephalography (EEG), functional magnetic resonance imaging (fMRI), and positron emission tomography (PET), together with neurostimulation, brain-computer interfaces (BCIs), and psychoactive interventions, have expanded diagnostic and therapeutic horizons while posing unprecedented ethical and legal challenges. Beyond correlating brain activity with behavior, contemporary tools enable real-time observation, decoding, and even modulation of cognitive processes. That shift exposes novel vulnerabilities, pressures existing constitutional, and privacy frameworks to address risks that were previously theoretical.

Legislative and policy experiments now unfolding across jurisdictions make the stakes concrete. Chile has constitutionalized core neurorights, Spain has articulated influential soft-law parameters, and several Latin American systems - from Mexico to Brazil - are advancing bills and constitutional reforms that target mental integrity and the processing of neural data. Taken together, these developments suggest that classical data-privacy paradigms do not fully capture the inviolability of thought and that a distinct focus on mental privacy is needed to protect inner cognitive processes from extraction and manipulation.

Anchored in the Italian privacy tradition shaped by Cesare Massimo Bianca, this article takes that work as its doctrinal touchstone and extends Bianca's move from *riservatezza* (privacy) to the broader protection of personal data as control over the informational dimension of the person.¹ In that lineage, mental privacy is not mere secrecy but governance of what is decoded or modulated about one's cognitive life; accordingly, the analysis that follows treats neurodata, neuro-inference, and neuro-effect as protected objects and tiers obligations by capability rather than by sectoral label. Echoing Bianca's insistence on the effectiveness of consent and responsibility, the framework presumes the sensitivity of brain-related signals and inferences, embeds cognition-specific impact assessment at design time, and binds both public bodies and digital platforms, today's de facto authorities, to rules that make consent meaningful and accountability real. Read in this way, Bianca's privacy

¹ CM Bianca and FD Busnelli, La protezione dei dati personali: Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy") (Cedam 2007) 2200

principles supply the normative spine for the operational standards developed in Sections 5–8, including heightened safeguards in coercive settings and evidentiary gatekeeping for forensic uses.

At the same time, ethical and philosophical analyses of cognitive liberty have highlighted how “brain-reading” and “mind-reading” tools can be deployed to exploit technological asymmetries.² Unauthorized access to neural data or the manipulation of cognitive states threatens autonomy and may entrench coercion, discrimination, and power imbalances. Against that backdrop, debate persists over whether neurorights should stand alone or be treated as derivatives of existing guarantees of privacy, autonomy, and freedom of thought. As Mollo has argued, early interventions in design and regulation are essential to ensure that neuroethologies promote well-being without eroding human dignity.³

This article responds to that debate with a comparative and normative argument. It maps how current instruments, constitutional provisions, statutory regimes, and international guidance, already protect interests commonly grouped as neurorights, and it shows where those protections fail when confronted with consumer neurotech and AI-driven inference. Building on that analysis, the article advances a capability-based operational framework that renders mental privacy, cognitive liberty, and mental integrity administrable without inventing new, free-standing rights. The framework defines the protected objects (neurodata, neuro-inference, neuro-effect), presumes their sensitivity, tiers obligations by what systems can reveal or modulate rather than how they are marketed, embeds cognition-specific impact assessment at design time, and draws bright lines for coercive and quasi-coercive contexts, evidentiary gatekeeping, and deceptive neuromodulation. Section 2 surveys the scientific and technical background; Section 3 situates neurorights within human-rights doctrine; Section 4 examines First, Fourth, and Fifth Amendment pressures; Section 5 reframes authentication and the paradoxes of privacy in a neurotech era; Section 6 compares legislative, governance, and hard-law approaches; Section 7 distills the faults and gaps; Section 8 sets out the operational framework; and Section 9 concludes with implications for regulators, courts, and industry. The central claim is that law can already make its promises “bite” where cognition is at stake—if we align capability, context, and accountability.

2. Neuroscience and Neurotechnologies

Neuroscience is an interdisciplinary field that integrates biology, psychology, engineering, and other disciplines to study the brain and its role in generating thoughts, actions, and cognitive experiences. Over the years, technological advances have revolutionized our understanding of the nervous system,

²S Guida, ‘Affrontare il potere della neurotecnologia: il neuromarketing tra azzardo morale, impatti sulla personalità dell’utente e tutela dei neurodiritti’ (2023) EJPLT Observatory <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1806/1291>

³ AA Mollo, ‘La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici’ (2021) 1 EJPLT <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1326>

unveiling the mechanisms underlying neural activity. Neurotechnology, a rapidly expanding branch of neuroscience, bridges the nervous system and technology, enabling both the observation and manipulation of brain functions. Techniques such as electroencephalography (EEG), functional magnetic resonance imaging (fMRI), and brain-computer interfaces (BCIs) have significantly transformed neuroscience by making brain processes observable and interactive.⁴

Neuroscience has deepened our understanding of the brain by revealing the physical mechanisms that drive the stimulus-thought-behavior (STB) sequence, offering critical insights for fields such as law and cognitive science. Traditional approaches to behavior primarily focused on observable stimuli and responses, constrained by the inability to examine the brain's internal processes in detail. However, technological advancements, including brain imaging and neurochemical analysis, have made it possible to study the neural processes underlying thought, transforming it from an abstract concept into an observable and measurable phenomenon.⁵

The emergence of new neuroscience-based technologies has reshaped how we understand and interact with the human mind. While traditional neuroscience focused on observing and interpreting brain activity, a new wave of neurotechnologies now enables the direct monitoring and manipulation of cognitive processes. This shift has profound implications for mental autonomy, raising pressing legal and ethical questions that existing frameworks struggle to address.⁶

The rapid advancement of neurotechnologies has introduced groundbreaking innovations that significantly enhance our ability to study and interact with the human brain. Brain imaging techniques such as EEG and fMRI provide detailed structural and functional insights into neural activity, facilitating advances in diagnostics and research. Additionally, neurostimulation technologies such as transcranial magnetic stimulation (TMS) and deep brain stimulation (DBS) have revolutionized the treatment of neurological and psychiatric disorders by directly modulating brain activity. Furthermore, psychoactive drugs and neurostimulation techniques are being explored for their potential in cognitive enhancement, offering the possibility to improve memory, focus, and other cognitive capacities. These technological developments underscore the transformative potential of neurotechnologies in expanding human capabilities and addressing complex medical challenges, while also necessitating careful ethical and regulatory oversight to maximize their benefits and mitigate potential risks.⁷

⁴ MF Álamos, L Kausel, C Baselga-Garriga, P. Ramos, F. Aboitiz, X Uribe-Etxebarria and R Yuste, 'A technocratic oath' in P López-Silva and L Valera (eds), *Protecting the mind: Challenges in law, neuroprotection and neurorights* (Springer 2022) 163 - 174.

⁵OR Goodenoug and M Tucker, 'Why neuroscience matters for law' in A D'Aloia and MC Errigo (eds), *Neuroscience and law: Complicated crossings and new perspectives* (Springer Nature Switzerland AG 2020) 51-68.

⁶ MJ Blitz, 'Freedom of thought and the structure of American constitutional rights' in MJ Blitz, JC Bublitz and JC Moriarty (eds), *The Law and Ethics of Freedom of Thought, 1: Neuroscience, Autonomy and Individual Rights* (Palgrave Macmillan 2021) 125 - 126.

⁷ P Sommaggio and M Mazzocca, 'Cognitive liberty and human rights' in A D'Aloia and MC Errigo (eds), *Neuroscience and law: Complicated crossings and new perspectives* (Springer Nature Switzerland AG 2020) 96 - 99.

One particularly controversial application of neurotechnology is lie detection. The development of deception detection methods has evolved from traditional physiological measures to advanced neuroimaging techniques. Early methods, such as the polygraph, relied on monitoring physiological responses like heart rate and sweat secretion to infer dishonesty, though these methods were often criticized for their unreliability and susceptibility to false positives. The introduction of alternative techniques, such as the Guilty Knowledge Test (GKT), sought to identify recognition of crime-related information rather than deception itself, yet these approaches also faced challenges, including susceptibility to countermeasures and experimental limitations. With the advent of neuroimaging technologies like EEG and fMRI, lie detection has entered a new phase, offering potentially more accurate and sophisticated methods.⁸ By observing neural activity associated with recognition and deception, these techniques promise to address some of the shortcomings of earlier methods. However, their integration into law enforcement and judicial proceedings raises significant ethical and privacy concerns, as these technologies become increasingly invasive and capable of accessing mental states that were previously considered private.

Building on recent forensic scholarship, Stocchi cautions that many of these applications remain at a pre-paradigmatic stage, with limited external validity and no stable consensus on core constructs; consequently, routine claims of “objective” and “quantifiable” results are frequently unwarranted, and strict gatekeeping is advisable before admission in criminal proceedings. He also highlights methodological fragilities, susceptibility to countermeasures, small and non-representative samples, and proprietary protocols that impede independent replication, and a problematic slippage from laboratory “recognition” measures to juridical notions of “guilt,” introducing potential normative bias in fact-finding.⁹

While these technologies offer groundbreaking benefits in medicine and research, as Salardi argues, neurotechnologies can be an “important ally” within a comprehensive public-health approach to mental health, yet their growing pervasiveness reframes the balance between power and liberty, even in democratic, market-based contexts, given direct-to-consumer pathways and non-clinical uses. She urges a differentiated assessment of invasive versus non-invasive modalities and a structured risk taxonomy, alongside regulatory measures that embed privacy-by-design and privacy-by-default, basic technical/ethical literacy for patients and citizens, and robust public engagement as the preferred route to legitimate, rights-anchored governance.¹⁰ They also introduce unprecedented risks to privacy and autonomy. The growing ability to decode, influence, or extract cognitive data raises pressing legal concerns that traditional privacy laws may not fully address. This challenge has given rise to the emerging concept of neuro-rights.

⁸ MJ Blitz, *Searching minds by scanning brains: Neuroscience technology and constitutional privacy protection* (Palgrave Macmillan 2017) 45 - 49.

⁹ F Stocchi, *Neuroscienze e applicazioni in ambito forense: profili filosofici ed etico-giuridici* (Giappichelli 2025) 121-163.

¹⁰ S Salardi, *Neurotecnologie tra potere e libertà: Medicina, etica, discriminazioni di genere* (CEDAM-Wolters Kluwer 2024) 66-107.

Advancements in neurotechnologies, including brain-imaging techniques such as fMRI, positron emission tomography (PET) scans, and EEG, have profoundly transformed our understanding of brain function,¹¹ offering unprecedented insights into mental events.¹² These tools not only enable the observation of neural processes¹³ but also open the door to novel applications such as "mind-reading" and "brain-reading".¹⁴ While these terms are often used interchangeably, they refer to different aspects of cognitive analysis: "mind-reading" involves interpreting unspoken thoughts, whereas "brain-reading" focuses on analyzing the brain's responses to specific stimuli. These capabilities hold potential for diagnostics, research, and even interpersonal communication,¹⁵ with applications ranging from brain-controlled virtual environments to real-time cognitive assessments.¹⁶

However, the ability to access mental contents¹⁷ raises serious concerns regarding mental privacy.¹⁸ The use of neuroimaging to reveal thoughts, intentions, or psychological states challenges traditional notions of individual autonomy and legal protections under constitutional frameworks. Courts and scholars continue to debate whether such practices constitute an unacceptable intrusion, with some arguing that they amount to a form of cognitive search, akin to the legal doctrine of searching an "extended mind".¹⁹ This concept suggests that mental processes, when mediated by technology, should be recognized as part of a protected cognitive domain, deserving legal safeguards similar to those applied to physical property.

Moreover, the potential for cognitive manipulation²⁰ through these technologies presents significant ethical dilemmas. By influencing thought patterns or monitoring cognitive responses, neurotechnologies could compromise an individual's ability to freely form and control their ideas. Such risks highlight the need to address issues of mental sovereignty, ensuring individuals retain full control over their thoughts and cognitive processes.

In this context, the concept of Cognitive Liberty (CL)²¹ has emerged as a fundamental principle for safeguarding individuals' rights against unauthorized access or influence over their minds. This framework advocates for a balanced approach to neurotechnology, ensuring that scientific and technological progress aligns with fundamental ethical and legal protections. As neurotechnologies continue to evolve, these discussions remain crucial in shaping policies that uphold both innovation and the preservation of fundamental human rights.

¹¹MJ Blitz, 'Freedom of thought and the structure of American constitutional rights' (n 6) 103-151.

¹² MJ Blitz, *Searching minds by scanning brains* (n 8) 1-144

¹³ Ibid 1-144

¹⁴ Ibid 1-144

¹⁵ MJ Blitz, 'Freedom of thought and the structure of American constitutional rights' (n 6) 103-151

¹⁶ MJ Blitz, *Searching minds by scanning brains* (n 8) 1-144

¹⁷A Lavazza, 'Technology Against Technology: A Case for Embedding Limits in Neurodevices to Protect Our Freedom of Thought' in Blitz MJ, Bublitz JC and Moriarty JC (eds), *The Law and Ethics of Freedom of Thought, Volume 1: Neuroscience, Autonomy and Individual Rights* (Palgrave Macmillan 2021) 259 - 289, 263.

¹⁸A Wajnerman and P López-Silva, 'Mental privacy and neuroprotection: An open debate' in P López-Silva and L Valera (eds), *Protecting the mind* (Springer 2022) 185 - 202, 150 - 152.

¹⁹ MJ Blitz, *Searching minds by scanning brains* (n 8) 1-144

²⁰ MJ Blitz, 'Freedom of thought and the structure of American constitutional rights' (n 6) 103-151

²¹P Sommaggio and M Mazzocca, 'Cognitive liberty and human rights' (n 7) 95 - 111, 95 - 96.

3. Towards a Neuro-Rights Era

Human rights are fundamental and inalienable entitlements inherent to every individual, regardless of nationality, ethnicity, gender, language, religion, or any other distinguishing characteristic. Grounded in the inherent dignity of the human person, which is the source of human rights rather than their product—these rights encompass civil, political, economic, social, and cultural guarantees, ensuring fundamental freedoms such as the right to life, liberty, freedom of expression, and protection from torture or slavery.²² In recent years, the advancement of neurotechnologies, particularly artificial intelligence (AI) and brain-computer interfaces (BCIs), has raised pressing ethical and legal questions, leading to the conceptualization of neurorights. These proposed rights aim to protect individuals from the risks associated with neurotechnological interventions, specifically those that allow access, interpretation, or manipulation of brain activity. The primary focus of neurorights is to safeguard mental privacy, cognitive liberty, and personal identity from unauthorized interference.²³ The view that human dignity is the foundation from which human rights derive is developed in contemporary doctrine under the “human dignity approach.”²⁴

While existing human rights frameworks offer protections relevant to emerging technologies, such as the right to privacy, non-discrimination, and data protection, the rapid evolution of neurotechnology challenges whether these safeguards sufficiently address the unique risks posed to the human mind. Scholars debate whether neurorights should be recognized as derivative rights, meaning they extend pre-existing human rights, or as stand-alone rights that establish novel normative protections.²⁵ The derivation approach suggests that existing rights, such as freedom of thought and privacy, can be expanded to cover neurotechnological risks, maintaining legal coherence and avoiding redundancy. However, proponents of stand-alone neurorights argue that neurotechnologies enable cognitive interference beyond the scope of current legal frameworks, necessitating explicit recognition of rights that protect mental integrity and autonomy.²⁶ This debate underscores the broader challenge of ensuring that human rights frameworks remain adaptable to technological advancements while avoiding speculative overreach or unnecessary fragmentation.

Legal frameworks have often conceptualized human agency through a dualistic lens that separates mind from brain. Contemporary neuroscience rejects that split, viewing mental processes as direct manifestations of neural activity.²⁷ In that light, traditional legal concepts—belief, intent, consent—long treated as purely “mental” constructs are better understood as brain states

²² United Nations, Human Rights (2023) <https://www.un.org/en/global-issues/human-rights>

²³ F Gilbert and I Russo, ‘Neurorights: The land of speculative ethics and alarming claims?’ (2024) 15 *AJOB Neurosci*, 113 - 115.

²⁴ P Tiedemann, *Philosophical Foundation of Human Rights* (2nd ed, Springer 2023) 65 - 140

²⁵ T Istace, ‘Establishing neurorights: New rights versus derived rights’ (2025) 17 *J Hum Rights Pract*, 121-133

²⁶ *Ibid* 135–136.

²⁷ PA Alces, *Trialectic: The confluence of law, neuroscience and morality* (The University of Chicago Press 2023), 56-57

shaped by neural configurations in context. This shift is especially salient as neurotechnologies increasingly decode and modulate such states, reinforcing the mind–brain continuity.

Actions such as inferring an individual's mental state through neuroimaging²⁸ or other intrusive technologies raise acute ethical and legal concerns, particularly for mental privacy.²⁹ While law enforcement routinely collects observable physiological data (e.g., breathalyzers) to gauge impairment, tools that can extract unspoken thoughts or intentions invite a different level of scrutiny. Courts may need to distinguish the collection of outward physiological measures from access to private cognitive content.³⁰ That distinction becomes pivotal as methods evolve from analyzing stimulus-bound neural responses (brain-reading) to deciphering self-generated thoughts (mind-reading). The latter creates serious self-incrimination risks by exposing inner experience without explicit consent, challenging traditional Fourth and Fifth Amendment protections.³¹

The growing exploitation of emotions and cognitive states by AI-driven neurotechnologies further highlights the fragility of mental autonomy in the digital age.³² Platforms mine behavioral traces—facial expression, voice, gaze to detect states such as anxiety or stress. Even when framed as personalization, the same pipelines can be used to steer choices. For example, targeting vulnerable users with overpriced or unnecessary products at moments of susceptibility erodes autonomous decision-making. Nor is the risk confined to markets: public authorities may deploy neurotechnologies to reshape cognition, including through the forcible administration of neuroactive substances to alter behavior.³³

Neurotechnologies that interface with human cognition therefore warrant a recalibration of existing human rights protections. While some scholars urge recognition of stand-alone neurorights, others favor integrating them as derivative rights within freedom of thought, privacy, and non-discrimination frameworks.³⁴ ³⁵ The derivation approach offers a coherent legal basis for addressing novel risks while preserving doctrinal continuity.

A key derivative neuroright is cognitive liberty, which extends freedom of thought to cover new forms of cognitive interference and manipulation.³⁶ ³⁷ It safeguards an individual's authority over their own mental processes,

²⁸MJ Blitz, *Searching minds by scanning brains* (n 8).

²⁹P Sommaggio and M Mazzocca, '*Cognitive liberty and human rights*' (n 7) 95–111.

³⁰A Lavazza, 'Technology Against Technology: A Case for Embedding Limits in Neurodevices to Protect Our Freedom of Thought' (n 17) 259 - 289.

³¹N Farahany, 'Searching Secrets' (2012) 160 U Penn L Rev 1239 https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1057&context=penn_law_review

³²K Grisse, 'Recommender systems, manipulation and private autonomy: How European civil law regulates and should regulate recommender systems for the benefit of private autonomy' in S Genovesi, K Kaesling and S Robbins (eds), *Recommender systems: Legal and ethical issues* (Springer Nature Switzerland AG 2023) 101-128, 115.

³³MJ Blitz, 'Freedom of thought and the structure of American constitutional rights' (n 6).

³⁴M Ienca and R Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) 13 Life Sci Soc Policy 5

³⁵T Istace, 'Establishing neurorights: New rights versus derived rights' (n 25) 121.

³⁶RG Boire, 'On cognitive liberty' (2000) 1 Journ of Cognitive Liberties 7 <https://www.cognitiveliberty.org/on-cognitive-liberty-boire/>

³⁷W Sententia, 'Neuroethical considerations: Cognitive liberty and converging technologies for improving human cognition' (2004) 1013 Ann NY Acad Sci 221

protecting against coerced alteration.³⁸ Unlike traditional freedom of thought, which has been linked primarily to freedom of speech,³⁹ cognitive liberty also addresses non-verbal influences, including pharmacological interventions and digital neurotechnologies.⁴⁰

Similarly, mental privacy, a subcategory of the right to privacy, has become central as tools capable of decoding brain activity proliferate.^{41 42} It protects against the unauthorized extraction, recording, or analysis of neural data, ensuring control over inner cognitive experience.^{43 44} Additionally, intellectual privacy complements these protections by shielding thought processes from unwarranted surveillance or cognitive profiling.⁴⁵

The right to silence, traditionally tied to protections against self-incrimination, takes on new significance in the era of forensic neurotechnology.⁴⁶ With advances in brain imaging and cognitive decoding, authorities may attempt to extract incriminating content directly from the brain, sidestepping established safeguards.⁴⁷ To forestall that outcome, scholars argue the right to silence must encompass neural data so individuals retain control over their inner cognitive states.⁴⁸

Additionally, the right to mental integrity bars unauthorized cognitive interference—whether covert neuromodulation, neurostimulation, or AI-driven nudging—and is especially salient where states contemplate compulsory psychosurgery or cognitive enhancement for criminal rehabilitation.^{49 50}

Recognizing neurorights within existing human-rights frameworks thus supplies a coherent, adaptable response to neurotechnology's challenges. By specifying how freedom of thought, privacy, and cognitive autonomy apply at the mind–brain interface, the law can adapt without fragmenting the system of rights.⁵¹ As neuroscience advances, the need for clear legal boundaries around mental privacy, cognitive liberty, and intellectual autonomy will only grow; future frameworks should prioritize human dignity and cognitive sovereignty so that progress does not come at the expense of mental freedom.

³⁸ N Farahany, 'Searching Secrets' (n 31) 160 U Penn L Rev 1239.

³⁹ Ashcroft v Free Speech Coalition 535 US 234 (2002).
<https://supreme.justia.com/cases/federal/us/535/234/>

⁴⁰ A Kolber, 'Clarifying the debate over therapeutic forgetting' (2007) 7 Am J Bioethics 25

⁴¹ N Farahany, 'Searching Secrets' (n 31) 160 U Penn L Rev 1239.

⁴² J Cohen, 'Examined lives: Informational privacy and the subject as object' (1996) 52 Stanford L Rev 983

⁴³ M Gazzaniga, *The ethical brain* (Dana Press 2005) 201

⁴⁴ M Ienca and R Andorno, 'Towards new human rights' (n 34) 5

⁴⁵ N Farahany, 'Incriminating thoughts' (2012) 64 Stanford L Rev 351
<https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2012/03/Farahany-64-Stan-L-Rev-351.pdf>

⁴⁶ N Farahany, 'Searching Secrets' (n 31) 160 U Penn L Rev 1239.

⁴⁷ Ibid.

⁴⁸ A Lavazza, 'Technology Against Technology: A Case for Embedding Limits in Neurodevices to Protect Our Freedom of Thought' (n 17) 259–289.

⁴⁹ M Ienca and R Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (n 34) 13 Life Sci Soc Policy 5.

⁵⁰ A Lavazza, 'Technology Against Technology: A Case for Embedding Limits in Neurodevices to Protect Our Freedom of Thought' (n 17) 259–289.

⁵¹ T Istace, 'Establishing neurorights: New rights versus derived rights' (n 25).

4. The intersection between privacy and neuro-rights.

Neurotechnologies challenge existing constitutional protections in ways that require a reconsideration of fundamental rights. Three key areas of concern emerge: freedom of thought and expression (First Amendment), protection against unreasonable searches (Fourth Amendment), and safeguards against self-incrimination (Fifth Amendment).

a. *The First Amendment and neuro-rights.*

The intersection between the First Amendment and neuro-rights presents complex legal and ethical considerations regarding cognitive liberty and mental privacy. The First Amendment has traditionally been understood as safeguarding freedom of speech, but it also encompasses the freedom of thought, which is essential for meaningful self-expression.⁵² Courts have occasionally recognized this connection, as seen in *Doe v. City of Lafayette*,⁵³ where the Seventh Circuit Court of Appeals emphasized that government action punishing an individual for mere thought would contravene First Amendment protections. Similarly, the Supreme Court in *Stanley v. Georgia*⁵⁴ suggested that the First Amendment could extend to protect against mental manipulation. These precedents indicate that cognitive liberty, the right to control one's own mind, could be implicitly protected under First Amendment jurisprudence.

However, the advent of neurotechnologies challenges the existing legal framework. Advances in neuroimaging and brain-computer interfaces (BCIs) raise concerns about government and corporate surveillance of neural data. Scholars argue that the First Amendment may serve as a "backstop" for cognitive privacy where Fourth and Fifth Amendment protections fall short.⁵⁵⁵⁶ For instance, if government agencies were to compel individuals to disclose brain activity through functional MRI (fMRI) scans, it could constitute an unconstitutional intrusion into thought processes, much like how compelled speech is restricted under the First Amendment.⁵⁷ The implications extend to private entities as well. Employers or technology companies could potentially impose conditions requiring individuals to consent to neural monitoring, thereby coercing cognitive disclosures in exchange for employment or access to digital services.⁵⁸ This raises fundamental questions about whether the First Amendment should be interpreted to limit such private encroachments on mental autonomy.

⁵² N Richards, 'Intellectual Privacy' (2008) 87 Texas L Rev 387 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108268

⁵³ *Doe v City of Lafayette*, 377 F3d 757 (7th Cir 2004) <https://casetext.com/case/doe-v-city-of-lafayette-ind>

⁵⁴ *Stanley v Georgia*, 394 US 557 (1969) <https://supreme.justia.com/cases/federal/us/394/557/>

⁵⁵ MJ Blitz, *Searching minds by scanning brains* (n 8).

⁵⁶ DJ Solove, *The Future of Reputation Gossip, Rumor and Privacy on the Internet* (Yale University Press 2007) 247

⁵⁷ A Kolber, 'The Experiential Future of the Law' (2010) 60 Emory L J 586 <https://scholarlycommons.law.emory.edu/elj/vol60/iss3/1/>

⁵⁸ F Niker, G Felsen, SK Nagel and PB Reiner, 'Autonomy, evidence-responsiveness, and the ethics of influence' in MJ Blitz and JC Bublitz (eds), *The law and ethics of freedom of thought*, Volume 1 (Palgrave Macmillan 2021) 105-124

Additionally, courts have recognized that freedom of thought is integral to intellectual privacy. Richards⁵⁹ argues that just as the First Amendment protects the "marketplace of ideas" it must also safeguard the "workshops where ideas are crafted", namely, the cognitive processes underlying free expression. Pustilnik⁶⁰ further contends that compelled neuroimaging should be considered a search of "private information within a space of presumed privacy" and thus be subject to stringent constitutional scrutiny. The parallels with *Kyllo v. United States*⁶¹ are evident; just as thermal imaging was deemed an unconstitutional search when used to detect activity inside a home, neuroimaging technologies capable of revealing thoughts or cognitive patterns should likewise be considered unconstitutional intrusions under the First Amendment and the Fourth Amendment.^{62 63} The core issue remains whether individuals can be compelled, either by the state or private actors, to expose their cognitive processes against their will.

In light of these concerns, a robust First Amendment framework addressing neuro-rights must evolve. While individuals have the right to voluntarily modify their cognitive states through reading, media consumption, or even brain stimulation, the legal system must delineate between voluntary cognitive alterations and coercive neuro-interventions.^{64 65} Courts may need to establish clear jurisprudence distinguishing between protected cognitive autonomy and impermissible intrusions into neural activity. The debate over whether individuals can consent to cognitive surveillance in commercial settings remains contentious. Some argue that a strong First Amendment doctrine should allow individuals the freedom to share or commercialize their mental processes, while others advocate for government intervention to prevent undue influence or exploitation.^{66 67} Ultimately, the recognition of neuro-rights under the First Amendment could reshape constitutional protections to accommodate emerging neurotechnologies and ensure that cognitive liberty remains a fundamental right in the digital age.

b. The Fourth Amendment and neuro-rights.

The Fourth Amendment to the United States Constitution provides a fundamental safeguard against unreasonable searches and seizures,

⁵⁹N Richards, 'Intellectual Privacy' (n 52) 87 Texas L Rev 387.

⁶⁰AC Pustilnik, 'Neurotechnologies at the intersection of criminal procedure and constitution law' in S Richardson and J Parry (eds), *The constitution and the future of criminal law* (Cambridge University Press 2013) 109-134

⁶¹ *Kyllo v United States*, 533 US 27 (2001) <https://supreme.justia.com/cases/federal/us/533/27/>

⁶²AC Pustilnik, 'Neurotechnologies at the intersection of criminal procedure and constitution law' (n 60), 109-134

⁶³ *Kyllo v United States*, 533 US 27 (2001) <https://supreme.justia.com/cases/federal/us/533/27/>

⁶⁴ MJ Blitz, 'Freedom of Thought for the Extended Mind: Cognitive Enhancement and the Constitution' (2010) 57 William & Mary L Rev 1050 <https://scholarship.law.okcu.edu/work/ns/f74599e1-6606-4cde-86a2-0f677c5cd2cc>

⁶⁵AS Jwa, 'Regulating the use of cognitive enhancement: An analytic framework' (2019) 12 Neuroethics 293

⁶⁶ RH Thaler and CR Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (Yale University Press 2009) 293

⁶⁷ JC Bublitz, 'Cognitive Liberty or the International Human Right to Freedom of Thought' in J Clausen and N Levy (eds), *Springer Handbook of Neuroethics* (Springer 2015) 1309 - 1334

reinforcing the principle that individuals have a right to privacy in their persons, houses, papers, and effects. Traditionally, the legal framework surrounding this amendment has revolved around physical intrusions and the expectation of privacy in tangible and digital spaces.⁶⁸ However, advancements in neuroscience and neurotechnology introduce unprecedented challenges, particularly concerning the protection of brain activity and cognitive processes. As governments and private entities explore the potential of neuroimaging and brain-computer interfaces (BCIs), questions arise regarding whether and how neural data should be shielded under the Fourth Amendment.⁶⁹

The intersection of neuro-rights, a set of emerging legal principles advocating for the protection of mental privacy, cognitive liberty, and personal identity, complicates traditional Fourth Amendment analyses.⁷⁰ Historically, jurisprudence has held that individuals forfeit privacy protections over information voluntarily disclosed to third parties. This third-party doctrine, established in *Smith v. Maryland*⁷¹ and *United States v. Miller*,⁷² suggests that once data is shared with an external entity, the Fourth Amendment no longer protects it. If applied to neural data, this precedent could allow law enforcement or corporations to access cognitive patterns, emotional states, or even subconscious reactions recorded through neurotechnology, without requiring a warrant.⁷³ Such an interpretation poses significant ethical and legal concerns, as neurodata is deeply tied to individual autonomy and self-determination.

Furthermore, the doctrine of abandonment, wherein privacy rights are forfeited over discarded personal effects, raises additional complexities when applied to neural data. In *California v. Greenwood*,⁷⁴ the Supreme Court ruled that once an individual discards trash on the curb, they lose any reasonable expectation of privacy in its contents. Courts have similarly deemed metadata and behavioral patterns as publicly accessible information.⁷⁵ If neural activity were classified similarly, individuals could lose control over their most intimate thoughts and emotions simply by interacting with neuro-enabled devices. Scholars argue that this would create a paradox: while legal protections exist for thoughts expressed in diaries or online searches, direct neural recordings could be accessed with fewer safeguards, despite their inherently private nature.⁷⁶

To address these concerns, some legal scholars advocate for extending heightened Fourth Amendment protections to neural data, similar to how *Riley*

⁶⁸ OS Kerr, 'Applying the Fourth Amendment to the Internet: A General Approach' (2010) 62 Stanford L Rev 1005 <http://www.jstor.org/stable/40649623>

⁶⁹ N Farahany, 'Searching Secrets' (n 31) 160 U Penn L Rev 1239.

⁷⁰ M Ienca and R Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (n 34) 13 Life Sci Soc Policy 5.

⁷¹ *Smith v Maryland*, 442 US 735 (1979) <https://supreme.justia.com/cases/federal/us/442/735/>

⁷² *United States v Miller*, 425 US 435 (1976) <https://supreme.justia.com/cases/federal/us/425/435/>

⁷³ S Henderson, 'The Timely Demise of the Fourth Amendment Third Party Doctrine' (2011) 96 Iowa L Rev Bull 39 https://digitalcommons.law.ou.edu/fac_articles/176/

⁷⁴ *California v Greenwood*, 486 US 35 (1988) <https://supreme.justia.com/cases/federal/us/486/35/>

⁷⁵ C Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (University of Chicago Press 2007) 274

⁷⁶ J Bambauer, 'Is Data Speech?' (2015) 66 Stanford L Rev 57 https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/01/66_Stan._L_Rev_57_Bambauer.pdf

v. California⁷⁷ reinforced privacy rights for smartphone content. In *Riley*, the Supreme Court ruled that law enforcement must obtain a warrant before searching the contents of a mobile device, recognizing that the vast amount of personal data stored on smartphones requires stronger constitutional safeguards. Courts could adopt a similar framework for neuroimaging data, requiring a warrant based on probable cause for any law enforcement access, as neural activity, like biometric or genetic data, contains uniquely sensitive information.⁷⁸ Additionally, the First Amendment, which protects freedom of thought and expression, could serve as a basis for limiting government and corporate interference in mental privacy.⁷⁹ This approach would ensure that individuals retain control over their cognitive processes, reinforcing the fundamental legal principle that the mind remains an inviolable domain.

As neurotechnology advances and integrates into daily life, the legal system must confront these pressing issues. The evolution of Fourth Amendment jurisprudence will determine whether neural privacy is adequately safeguarded or whether existing doctrines will allow unprecedented intrusions into the human mind. The recognition of neuro-rights as an extension of constitutional protections may serve as a necessary legal frontier in preserving cognitive liberty in the digital age.

c. The Fifth Amendment and neuro-rights.

The increasing capabilities of neurotechnology raise critical constitutional questions, particularly regarding the scope of the Fifth Amendment's privilege against self-incrimination. Traditionally, the Fifth Amendment prevents individuals from being compelled to provide testimonial evidence that could be used against them in a criminal proceeding.⁸⁰ However, the emergence of neuroimaging techniques capable of extracting cognitive data challenges the foundational testimonial-physical dichotomy in self-incrimination jurisprudence.⁸¹ If the government is prohibited from compelling an individual to verbalize self-incriminating information, it follows that the same protection should extend to the involuntary extraction of mental content via neuroimaging or brain scans.⁸²

A pivotal question in this debate is whether compelled neuroimaging constitutes "testimonial" evidence under the Fifth Amendment. The Supreme Court's decision in *Schmerber v. California*⁸³ established that the privilege against self-incrimination applies to "communications or testimony" but does not extend to "real or physical evidence." This distinction has been used to

⁷⁷ *Riley v. California*, 573 US 373 (2014) <https://supreme.justia.com/cases/federal/us/573/373/>

⁷⁸ DJ Solove, *The Future of Reputation Gossip, Rumor and Privacy on the Internet* (n 56) 247

⁷⁹ MJ Blitz, *'Freedom of Thought for the Extended Mind: Cognitive Enhancement and the Constitution'* (n 64) 1049-1118

⁸⁰ *Schmerber v. California*, 384 US 757 (1966) <https://supreme.justia.com/cases/federal/us/384/757/>

⁸¹ D Fox, *'The right to silence as protecting mental control'* (2009) 42 *Akron L Rev* 5 <https://ideaexchange.uakron.edu/akronlawreview/vol42/iss3/5>

⁸² N Farahany, *'Searching Secrets'* (n 31) 160 *U Penn L Rev* 1239.

⁸³ *Schmerber v. California* (n 79).

justify compelling fingerprints, blood samples, and handwriting exemplars.⁸⁴ However, neuroimaging challenges this framework because it directly accesses cognitive processes rather than merely identifying physical characteristics.⁸⁶ If the state were to compel brain fingerprinting to determine whether an individual recognizes specific crime-related images, the evidence would rely on the subject's mental state rather than purely physiological responses, thus falling within the testimonial category.⁸⁷

The application of the Fifth Amendment to neurotechnology is further complicated by the "cruel trilemma" rationale, which holds that individuals should not be forced to choose between self-accusation, perjury, or contempt.⁸⁸ Unlike physical evidence, neuroimaging inherently implicates the accused's cognitive autonomy, as it extracts knowledge that the individual would otherwise have the constitutional right to withhold.⁸⁹ This aligns with the broader concept of "cognitive liberty," which some scholars argue should be recognized as a fundamental right to protect individuals from undue governmental intrusion into their mental processes.⁹⁰

Furthermore, the jurisprudence surrounding the right to silence suggests that an individual should have control over their thoughts and mental privacy. The right to remain silent, as protected in *Miranda v. Arizona*,⁹¹ prevents coercive government tactics that compel individuals to disclose incriminating thoughts. If law enforcement were allowed to circumvent this right through neuroimaging, it would erode the very foundation of the Fifth Amendment by enabling authorities to access internal cognitive states without consent.⁹² Thus, if the government is prohibited from forcing verbal confessions, it should equally be barred from compelling an individual to produce brain-based responses that reveal their knowledge or intent.⁹³

In conclusion, as neuroscience advances, constitutional law must evolve to address the implications of neuro-rights under the Fifth Amendment. The testimonial-physical dichotomy, which has long guided self-incrimination jurisprudence, may be inadequate to protect individuals from involuntary cognitive extraction. Recognizing cognitive liberty within the scope of the Fifth Amendment would provide necessary legal safeguards against the potential misuse of neurotechnology, ensuring that mental privacy remains a protected constitutional right.

⁸⁴ *Gilbert v California*, 388 US 263 (1967) <https://supreme.justia.com/cases/federal/us/388/263/>

⁸⁵ *United States v Wade*, 388 US 218 (1967) <https://supreme.justia.com/cases/federal/us/388/218/>

⁸⁶ MS Pardo and D Patterson, 'Minds, brains, and norms' (2011) 4 *Neuroethics* 179

⁸⁷ *Ibid.*

⁸⁸ *Murphy v Waterfront Comm'n*, 378 US 52 (1964) <https://supreme.justia.com/cases/federal/us/378/52/>

⁸⁹ N Farahany, 'Searching Secrets' (n 31) 160 *U Penn L Rev* 1239.

⁹⁰ W Sententia, 'Neuroethical considerations: Cognitive liberty and converging technologies for improving human cognition' (n 37).

⁹¹ *Miranda v Arizona* 384 US 436 (1966). <https://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/fifth-amendment-activities/miranda-v-arizona/facts-and-case-summary-miranda-v-arizona>

⁹² DJ Solove, *The Future of Reputation Gossip, Rumor and Privacy on the Internet* (n 55).

⁹³ D Fox, 'The right to silence as protecting mental control' (n 80).

5. The Paradox of privacy in the era of neuro-rights.

Privacy has traditionally been categorized into four main types: information privacy, communication privacy, bodily privacy, and territorial privacy, each addressing different dimensions of personal autonomy and data protection.⁹⁴ However, recent technological advancements, particularly in artificial intelligence and neurotechnology, have introduced a new dimension: mental privacy. This emerging concept pertains to the protection of individuals' thoughts, emotions, and cognitive processes from unauthorized access, manipulation, or surveillance. As brain-computer interfaces and neuroimaging techniques become more sophisticated, the legal and ethical implications of mental privacy warrant urgent scholarly attention to ensure the preservation of cognitive freedom and individual autonomy in the digital age. Read through Bianca's lens, the paradox is not secrecy versus disclosure but the governance of informational control over the person, which mental privacy must now preserve against decoding and modulation.⁹⁵

Authentication mechanisms serve as the foundation of secure access control in computing systems by verifying user identities and preventing unauthorized access. These mechanisms can be categorized into four main types: knowledge-based authentication (Type I), which relies on something the user knows, such as passwords, PINs, and security questions; possession-based authentication (Type II), which involves something the user has, including smart cards, security tokens, or one-time passwords (OTPs); inherence-based authentication (Type III), which is based on something the user is, such as biometric factors like fingerprints, facial recognition, or voice patterns; and location-based authentication (Type IV), which validates a user's identity based on their geographical position, using GPS coordinates, IP addresses, or network proximity. Organizations increasingly adopt multi-factor authentication (MFA), which combines two or more of these authentication types to enhance security and mitigate risks associated with single-factor authentication. The evolution of authentication methods continues, incorporating behavioral analytics and artificial intelligence to create adaptive and risk-based authentication frameworks that respond dynamically to emerging cybersecurity threats.⁹⁶

As technology advances toward direct brain-computer interfaces and neuro-authentication methods, the concept of mental privacy is becoming a crucial legal and ethical issue. While biometric authentication is currently regarded as a rigid and secure approach, its legal and ethical limitations indicate a future where passwords may emerge as the strongest authentication factor. Unlike biometric identifiers, which can be compelled without violating self-incrimination protections, passwords remain protected under the Fifth Amendment because they are testimonial in nature and reside solely within an individual's mind.⁹⁷ This distinction is particularly important in the era of neuro-rights, where the extraction of cognitive data could lead to unprecedented

⁹⁴A Tang, *Privacy in practice: Establish and operationalize a holistic data privacy program* (CRC Press 2023) 471

⁹⁵CM Bianca and DS Busnelli (eds), *La protezione dei dati personali* (n 1).

⁹⁶D Dasgupta, A Roy and A Nag, *Advances in user authentication* (Springer International Publishing 2017) 360

⁹⁷JL Grama, *Legal and privacy issues in information security* (3rd edn, Jones & Bartlett Learning 2022) 552

forms of surveillance and coercion. As Carter⁹⁸ provocatively notes, if information must be extracted, surely brain scanning is more humane than torture. However, such a notion raises serious constitutional and human rights concerns, as it challenges the core principles of privacy, autonomy, and free will.

Legal precedents have demonstrated the significance of this distinction. The Apple v. FBI case⁹⁹ serves as a key example of the growing tension between privacy and security in digital spaces. In that case, Apple refused to comply with a court order requiring it to create a backdoor to bypass iPhone encryption, arguing that such an action would set a dangerous precedent for future government access to private information. If biometric authentication mechanisms, such as facial recognition or fingerprint scanning, can be legally compelled, the risk of extending this principle to future neuro-authentication technologies is evident.¹⁰⁰ The argument that "locked drawers can be forced open but our inner thoughts will, by their very nature, remain hidden until we reveal them"¹⁰¹ highlights the fundamental role of passwords in preserving cognitive liberty. Unlike physical evidence, thoughts and passwords exist solely within the mind, making them one of the few authentication factors that remain legally defensible.

Given these concerns, the protection of mental privacy must be reinforced through constitutional and statutory safeguards. The First Amendment protects freedom of thought and expression, preventing compelled ideological disclosures. The Fourth Amendment protects against unreasonable searches and seizures, raising questions about whether law enforcement could gain access to neuro-authentication data without a warrant. Most importantly, the Fifth Amendment's protection against self-incrimination ensures that individuals cannot be compelled to disclose passwords or passcodes, a safeguard that does not extend to biometric authentication.¹⁰² This evolving legal landscape suggests that as neuro-rights become more prominent, authentication frameworks must prioritize mechanisms that uphold individual autonomy and cognitive freedom.

However, this does not negate the necessity of robust security measures. Multi-Factor Authentication (MFA) remains essential, as it integrates multiple authentication layers to mitigate risks associated with single-factor authentication. The challenge moving forward is to design authentication systems that balance security, convenience, and the inviolability of mental privacy. In this context, passwords, despite their vulnerabilities, may become the most ethically sound and legally protected authentication factor. Future policies must therefore ensure that mental privacy remains safeguarded, not only under existing constitutional provisions but also through new regulatory frameworks that anticipate the ethical dilemmas posed by emerging neurotechnologies.

⁹⁸ R Carter, 'Neurotelepathy: The rise of mind-reading machines' (Science Focus, 25 September 2015) <http://www.sciencefocus.com/feature/mind-reading/neurotelepathy-rise-mind-reading-machines>

⁹⁹ Apple v FBI, in the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant (U.S. Dist Ct for the Central Dist of California 2016) <https://epic.org/documents/apple-v-fbi-2/>

¹⁰⁰ Ibid.

¹⁰¹ MJ Blitz, Searching minds by scanning brains (n 8).

¹⁰² JL Grama, Legal and privacy issues in information security (n 97).

6. Lawmaking, Governance, and Enforceable Norms on Neuro-Rights

Recent advances in neurotechnology have spurred complex ethical, legal, and social debates, underscoring the need for enforceable norms that safeguard mental privacy, cognitive liberty, and personal autonomy. This section examines three interrelated dimensions of regulation. First, it surveys legislative proposals and draft bills that establish the foundational legal framework for neurorights. Second, it analyses multilevel governance and policy initiatives that coordinate efforts across national, regional, and international levels to align scientific innovation with robust protective measures. Third, it explores hard-law approaches—legislation, constitutional reforms, and judicial decisions—that embed neurorights within binding legal structures. Taken together, this framework offers a roadmap for addressing the challenges and opportunities presented by emerging neurotechnologies.

The analysis adopts a purposive comparative design to map how different legal orders are beginning to protect interests often framed as “neurorights”. Jurisdictions were selected on four grounds: (i) salience of legal change (early constitutional or statutory measures specifically addressing neurotechnology: Chile; state-level innovation in the United States: Colorado); (ii) regulatory generality with direct neurotech implications (the European Union’s binding acquis on privacy/data, AI, product safety, and cybersecurity—treated at Union level rather than via Member States to avoid duplication); (iii) evidence of judicial enforcement (early case law applying constitutional or statutory guarantees to neurotech: Chile); and (iv) policy leadership (national programmes and international soft law that shape standards and expectations: Israel, Korea, OECD, UNESCO, the Inter-American system, RIPD, Parlatino). The comparison proceeds along six axes: (1) legal status (soft law versus binding constitutional, legislative, and case-law instruments); (2) protected interests (mental privacy, cognitive liberty, mental integrity, identity); (3) treatment of brain-related data (recognition as personal/special-category/sensitive data and lawful bases, including consent); (4) risk-management and governance duties (impact assessments, data-protection-by-design, human oversight, transparency, auditing); (5) enforcement and remedies (supervisory authorities, constitutional actions, private rights of action); and (6) sectoral triggers (medical devices/health, employment/education, law enforcement/public security, online platforms).

a. Legislative Proposals and Draft Bills on Neuro-Rights

Recent years have witnessed a surge in legislative initiatives worldwide seeking to address the ethical, legal, and societal implications of neurotechnologies. These proposals generally emphasize the protection of mental privacy, cognitive liberty, and personal autonomy while promoting scientific innovation under robust regulatory frameworks. Below is an overview of key draft bills and legislative efforts in various jurisdictions:

In Chile, a landmark proposal introduced in October 2020 aims to create a comprehensive legal framework for neuro-rights, highlighting the importance of mental privacy, personal identity, and equitable access to cognitive enhancement. This initiative draws significantly on the work of scholars such as Rafael Yuste and the recommendations of the Morningside Group, underscoring the need for preemptive measures against unauthorized interventions through brain-computer interfaces.¹⁰³

In Mexico, multiple proposals underscore the national push for constitutional and statutory reforms on neuro-rights. Federal Deputy María Eugenia Hernández Pérez introduced an amendment to Article 4 of the Political Constitution, explicitly guaranteeing physical and mental integrity and prohibiting any authority or private entity from compromising an individual's mental privacy or self-determination.¹⁰⁴ Simultaneously, a legislative initiative from the LXV Legislature advocates reforms to Article 73, Fraction XVII, broadening congressional authority to regulate emerging technologies, such as AI and neurotechnologies, in response to concerns over privacy, algorithmic bias, and potential misuse of neural data.¹⁰⁵ In 2024, Senator Alejandra Lagunes Soto Ruíz proposed the General Law of Neuroderechos and Neurotechnologies, envisioning an ethical and operational framework for ensuring informed consent, stringent cybersecurity standards, and equitable access in key sectors like healthcare and education.¹⁰⁶ Further reinforcing this trend, in February 2025, Senator Agustín Dorantes Lámbarri introduced a constitutional reform initiative mandating the creation of a National Agency of Artificial Intelligence and Cybersecurity to safeguard neurodata and cerebral activity against privacy breaches and discriminatory practices.¹⁰⁷

¹⁰³ G Girardi, C Goic, F Chahuán, J A Coloma and A De Urresti, *Proyecto de ley sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías* (Senado, legislatura 368, 7 October 2020) <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=14385&prmbOLETIN=13828-19> accessed 6 April 2025

¹⁰⁴ M E Hernández Pérez, *Iniciativa con proyecto de decreto por la que se adiciona un noveno párrafo y se recorren los subsecuentes del Artículo 4º; de la Constitución Política de los Estados Unidos Mexicanos* (Cámara de Diputados LXV Legislatura, Palacio Legislativo de San Lázaro, 1 August 2023) https://sil.gobernacion.gob.mx/Archivos/Documentos/2023/08/asun_4588906_20230808_1690903141.pdf accessed 8 April 2025

¹⁰⁵ A Lagunes Soto Ruíz, X Gálvez Ruíz, J C Ramírez Marín, G Madero Muñoz and M A Mancera Espinoza, *Iniciativa con proyecto de decreto por el que se reforma la fracción XVII, al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de inteligencia artificial, ciberseguridad y neuroderechos* (Senado de la República del H. Congreso de la Unión, LXV Legislatura, H. Congreso de la Unión, 20 September 2023) https://infosen.senado.gob.mx/sqsp/gaceta/65/3/2023-09-26-1/assets/documentos/Ini_PVEM_diversos_senadores_art_73_CPEUM.pdf accessed 7 April 2025

¹⁰⁶ A Lagunes Soto Ruíz, *Iniciativa con proyecto de decreto por el que se expide la Ley General de Neuroderechos y Neurotecnologías y se reforman y adicionan diversas disposiciones en materia de neuroderechos y neurotecnologías* (Comisión Permanente del H. Congreso de la Unión, LXV Legislatura, H. Congreso de la Unión, 17 July 2024) https://infosen.senado.gob.mx/sqsp/gaceta/65/3/2024-07-17-1/assets/documentos/Ini_PVEM_Sen_Alejandra_Lagunes_Neuroderechos_Neurotecnologias.pdf accessed 8 April 2025

¹⁰⁷ A Dorantes Lámbarri, *Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de ciberseguridad, inteligencia artificial, cibertecnologías, neurotecnologías y neuroderechos* (Senado de la República, LXVI Legislatura, Salón de Sesiones del Senado de la República, 5 February 2025) https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/02/asun_4832468_20250206_1738863808.pdf accessed 8 April 2025

In Brazil, the Proposed Constitutional Amendment No. 29 of 2023 seeks to enshrine explicit protections for mental integrity and algorithmic transparency, requiring that technological development uphold human dignity and adopt transparent algorithmic practices.¹⁰⁸ Additionally, Bill PL 522/2022 proposes an amendment to Brazil's General Data Protection Law (LGPD), classifying "neural data" derived from neuroimaging techniques as sensitive personal data. This bill places strict consent requirements on the processing of such information and prohibits neurotechnology uses that may harm psychological integrity.¹⁰⁹

In Costa Rica, a proposed reform to Law No. 8968 aims to expand the definition of biometric data to include neural information obtained through brain scans and other neuroimaging methods. By requiring "reasoned consent" for processing such data, the initiative seeks to protect individual dignity and encourage transparency and accountability in neurotechnology applications.¹¹⁰

In Colombia, legislators have introduced amendments to the nation's data protection law to regulate the processing of neurodata in the context of artificial intelligence and emerging neurotechnologies. The statutory project proposes dedicated provisions for defining "neurodata" and mandates stricter obligations around consent, processing limitations, and secure handling of highly sensitive brain-related information.¹¹¹

In Argentina, Bill 2446/23 of 2023 proposes creating a bicameral committee to draft legislative instruments that protect neurorights, with a mandate to address cognitive freedom, data confidentiality, and algorithmic biases.¹¹² Another measure, also referred to under Bill 2446/23 but introduced in 2022, seeks to amend the Federal Code of Civil Procedure by allowing evidence from neurotechnologies under judicial oversight and explicit informed consent, ensuring mental integrity and privacy are not compromised.¹¹³

Finally, in Uruguay, a proposal titled "*Actividad Cerebral y Neuronal de las Personas*" seeks to classify neural and brain data as sensitive information. This amendment underscores the urgency of extending the highest standards of

¹⁰⁸ R Rodrigues and others, *Proposta de Emenda à Constituição n° 29, de 2023* (Senado Federal, Gabinete do Senador Randolfe Rodrigues, 2023) <https://www25.senado.leg.br/web/atividade/materias/-/materia/158095> accessed 8 April 2025

¹⁰⁹ C H Gaguim, PL 522/2022 Inteiro teor – Projeto de Lei (Câmara dos Deputados, 9 March 2022) <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524> accessed 6 April 2025

¹¹⁰ Expediente 23667, *Ley de protección de la persona frente al tratamiento de sus datos neurales y biométricos – Proyecto de Ley* (Asamblea Legislativa, Comisión de Ciencia, Tecnología y Educación, 30 March 2023) <https://delfino.cr/asamblea/proyecto/23667> accessed 8 April 2025

¹¹¹ HR Carrascal Rojas and others, *Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales* (Comisión Primera Constitucional Permanente, Cámara – Proyecto No 156/2023C, radicación 22 August 2023; Senado, Legislatura 2023–2024, Gaceta N° 1188 de 2023) <https://www.camara.gov.co/proteccion-de-datos-personales> accessed 8 April 2025

¹¹² CM Doñate, 1983/2023 – *Proyecto de Ley de Creación de la Comisión Bicameral Especial para la Redacción de Propuestas Legislativas que Tiendan a la Protección Integral de los Neuroderechos* (Honorable Senado de la Nación Argentina, Version Preliminar) <https://www.senado.gob.ar/parlamentario/parlamentaria/476927/downloadPdf> accessed 8 April 2025

¹¹³ H Cámara de Diputados de la Nación Argentina, Proyecto de Ley: El Senado y la Honorable Cámara de Diputados de la Nación sancionan con fuerza de ley – Artículo 1°.- Modifíquese el artículo 134 del Código Procesal Penal Federal de la Nación y sus modificatorias, el que quedará redactado de la siguiente manera: <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/0339-D-2022.pdf> accessed 8 April 2025

data protection to neural information, thereby reinforcing privacy and individual autonomy.¹¹⁴

Together, these initiatives reflect a growing consensus on the urgent need for legal standards tailored to the unique challenges posed by neurotechnologies. By recognizing neural data as particularly sensitive and demanding explicit consent and rigorous oversight, these legislative proposals contribute to the broader discussion on how best to balance innovation with the protection of mental privacy and cognitive liberty in an era of rapid scientific progress.

b. Multilevel Governance and Policy Initiatives on Neurorights

Multilevel governance initiatives on neurorights have proliferated across national, regional, and international arenas, reflecting a growing consensus on the need for coordinated strategies to regulate neurotechnologies. These initiatives range from targeted national programs designed to accelerate brain research and innovation, to international frameworks promoting responsible development, ethical guidelines, and legal safeguards. Collectively, they underscore the imperative of aligning scientific progress with protections for cognitive liberty, mental privacy, and human dignity.

At the national level, countries such as Israel and Korea have developed high-profile programs that aim to establish themselves as global leaders in neurotechnology.

- Israel Brain Technologies (IBT) is a non-profit organization envisioned by former President Shimon Peres, focused on accelerating the commercialization of brain-related innovations by supporting entrepreneurs, building collaborative research networks, and serving as a hub of expertise on emerging neurotechnologies.¹¹⁵
- The Korea Brain Initiative, announced in 2016, constitutes a decade-long strategic plan led by the Ministry of Science, ICT, and Future Planning. It targets breakthroughs in multidisciplinary research, merging physical, digital, and biological sciences, while fostering robust training programs and resource-sharing pipelines. By emphasizing brain mapping, AI-driven computational approaches, and precision medicine, Korea seeks to shape the fourth industrial revolution through neuroscience and neurotechnology.¹¹⁶

¹¹⁴ R Goñi Reyes, ACTIVIDAD CEREBRAL Y NEURONAL DE LAS PERSONAS. Se adiciona a la categoría de dato sensible (Proyecto de Ley, Asunto No 163406, Cámara Representantes, 2 July 2024, Carpeta/Año 4393/2024, Comisión: Constitución, Códigos, Legislación General y Administración [CRR]) <https://parlamento.gub.uy/documentosyleyes/ficha-asunto/163406> accessed 8 April 2025

¹¹⁵ Israel Brain Technologies (IBT), About IBT (BrainTech 2019) <https://braintech.kenes.com/about-ibt/> accessed 8 April 2025

¹¹⁶ Korea Brain Research Institute, Korea Brain Initiative – Executive Summary https://www.kbri.re.kr/new/pages_eng/sub/page.html?mc=3186 accessed 8 April 2025

In Europe, Spain's Carta de Derechos Digitales provides a pivotal legal framework guiding the use of neurotechnologies, particularly in employment contexts. It delineates conditions and safeguards for integrating neurotechnologies into the workplace to ensure personal control over identity and decision-making sovereignty, emphasizing confidentiality, security, and the non-discriminatory use of brain-related data.¹¹⁷ Similarly, the BRAIN Initiative launched by President Obama in the United States exemplifies a large-scale research effort to revolutionize our understanding of neural circuits, with the potential to influence global policy directions on neurotechnology development.¹¹⁸

At the international level, several notable organizations have issued guiding principles or recommendations on neurorights:

- The OECD Council adopted Recommendation OECD/LEGAL/0457 on Responsible Innovation in Neurotechnology, urging governments and innovators to prioritize safety, respect for human rights, and stakeholder engagement in neurotechnology research and applications.¹¹⁹
- UNESCO has published two significant documents addressing the ethical dimensions of emerging technologies: the 2021 Recommendation on the Ethics of Artificial Intelligence, which underscores the importance of preventing discrimination and protecting privacy in AI and related fields,¹²⁰ and the 2022 report "Ethical Issues of Neurotechnology," highlighting potential risks to mental privacy, cognitive liberty, and social justice.¹²¹

Efforts within the Inter-American system illustrate the region's commitment to creating enforceable legal standards that protect mental autonomy:

- The Inter-American Juridical Committee issued a Declaration on Neuroscience, Neurotechnologies and Human Rights in August 2021, calling for robust regulatory frameworks to safeguard individual dignity, emotional integrity, and equitable access to neurotechnologies.¹²²

¹¹⁷ Gobierno de España, Charter of Digital Rights (Ministerio de Asuntos Económicos y Transformación Digital 2021) https://derechodigital.pre.red.es/documentos/CartaDerechosDigitales_04_ENG.pdf

¹¹⁸ About the BRAIN Initiative – The Initiative Kicks Off (Obama White House Archives, 2 April 2013) <https://obamawhitehouse.archives.gov/BRAIN> accessed 8 April 2025

¹¹⁹ Recommendation of the Council on Responsible Innovation in Neurotechnology (OECD Legal Instruments, OECD/LEGAL/0457, Adopted 11 December 2019, C(2019)159/REV1, C/M(2019)17) <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0457> accessed 8 April 2025

¹²⁰ UNESCO [72613], Recommendation on the Ethics of Artificial Intelligence (UNESCO, SHS/BIO/PI/2021/1, 2022) <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 8 April 2025

¹²¹ Comité Internacional de Bioética, Ethical issues of neurotechnology: report, adopted in December 2021 (2022) <https://doi.org/10.54678/ONKB6229> accessed 8 April 2025

¹²² Inter-American Juridical Committee, Declaration of the Inter-American Juridical Committee on Neuroscience, Neurotechnologies and Human Rights: New Legal Challenges for the Americas (99th Regular Session OEA/Ser. Q, CJI/DEC. 01 (XCIX-O/21), 11 August 2021) https://www.oas.org/en/sla/iajc/docs/CJI-DEC_01_XCIX-O-21_ENG.pdf accessed 8 April 2025

- The subsequent Inter-American Declaration of Principles regarding Neuroscience, Neurotechnologies, and Human Rights, adopted in March 2023, reiterates the urgency of integrating international standards to govern neurotechnological applications, underscoring non-discrimination and equitable innovation.¹²³

Regional data protection bodies have also joined the conversation. In September 2023, the Ibero-American Data Protection Network (RIPD) updated its internal regulations to form dedicated working groups on neurodata and digital health, aligning its stance on neuro-rights with recent Inter-American declarations and reaffirming its commitment to cross-border coordination.¹²⁴ Likewise, the Latin American and Caribbean Parliament (Parlatino) has drafted a Model Law on Neuro-rights, proposing foundational legal safeguards for mental privacy, identity, and access to cognitive enhancement tools, thereby illustrating a proactive legislative model that can be adapted by individual nations.¹²⁵

Collectively, these policy and governance initiatives illustrate an emerging global consensus on the dual imperative of fostering cutting-edge neuroscience research while instituting robust ethical and legal protections. By situating neurorights within broader discussions of data governance, digital rights, and human dignity, they lay the groundwork for comprehensive, multi-stakeholder collaboration aimed at ensuring that neurotechnological progress enhances individual well-being without compromising cognitive autonomy.

c. Hard Law Approaches: Legislation, Constitutional Reforms, and Judicial Decisions

Recent advancements in neurotechnology have prompted legislatures and courts worldwide to adopt binding legal measures that go beyond soft law instruments. These “hard law” approaches underscore the growing recognition that cognitive liberty and mental privacy warrant robust protection under enforceable statutes, constitutional provisions, and judicial rulings.

The EU’s binding *acquis* already protects interests often framed as ‘neurorights’. The Charter of Fundamental Rights enshrines human dignity and respect for physical and mental integrity (art 3(1)), alongside privacy and data protection (arts 7–8), which together ground claims to mental privacy.¹²⁶ The GDPR treats brain-related information as personal data; where neural signals

¹²³ Inter-American Juridical Committee, Inter-American Declaration of Principles regarding Neuroscience, Neurotechnologies, and Human Rights (102nd Regular Session OEA/Ser. Q, CJI/RES. 281 (CII-O/23) corr.1, Rio de Janeiro, Brazil, 9 March 2023, Original: Spanish) https://www.oas.org/en/sla/iajc/docs/CJI-RES_281_CII-O-23_corr1_ENG.pdf accessed 8 April 2025

¹²⁴ Declaración Final del Encuentro de la Red Iberoamericana con motivo del XX Aniversario de la RIPD (Sesión cerrada) (Reunión presencial celebrada en La Antigua (Guatemala) 25 September 2023) <https://www.redipd.org/sites/default/files/2023-10/declaracion-encuentro-xx-aniversario-ripd.pdf> accessed 8 April 2025

¹²⁵ Ley Modelo de Neuroderechos para América Latina y El Caribe (CTEC-PARLATINO, Sede Permanente, Panamá, 26 November 2022) <https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf> accessed 8 April 2025

¹²⁶ Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 1, 3(1), 7–8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2012_326_R_0391_01

or derived inferences reveal health status or are processed for biometric identification, they fall within special categories and face strict processing conditions (including explicit consent or limited public-interest bases), plus data-protection-by-design, DPIAs, and safeguards against solely automated decisions with legal effects.¹²⁷ For police and criminal justice contexts, the Law Enforcement Directive imposes comparable constraints on sensitive biometric and health data.¹²⁸ Sector-specific regulation also matters: neurotechnology that qualifies as a medical device must meet safety, performance and post-market surveillance duties under the MDR;¹²⁹ and horizontal cybersecurity obligations under NIS2 extend risk-management and incident-notification requirements to operators whose systems process neurodata.¹³⁰ In the wider European system, the Council of Europe's Oviedo Convention protects physical and mental integrity in biomedicine¹³¹, and the modernised Convention 108+ updates pan-European data-protection standards that encompass biometric and health data.¹³²

The EU Artificial Intelligence Act sets horizontal, binding rules for AI and directly touches neurotechnology that embeds AI. Depending on function and context, such systems may be prohibited (eg manipulative AI that materially distorts behaviour or certain emotion-inference uses) or high-risk (eg AI safety components of medical devices; biometric and emotion-recognition systems in workplace/education), which triggers strict duties on risk management, data governance, testing, transparency, logging, human oversight, robustness and cybersecurity, alongside staged application dates (with bans applying first).¹³³ Downstream digital legislation also matters. The Digital Services Act imposes transparency and systemic-risk duties (notably for very large platforms) relevant where tools infer emotions or cognitive states from user signals;¹³⁴ the Digital Markets Act constrains "gatekeepers" from combining personal data across services without valid opt-in, limiting exploitative cross-context use of

¹²⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1, arts 4(13)–(15), 9(1), 22, 25, 35; recitals 26, 35. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

¹²⁸ Directive (EU) 2016/680 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 by competent authorities [2016] OJ L119/89. <https://eur-lex.europa.eu/eli/dir/2016/680/oj>

¹²⁹ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] OJ L117/1. <https://eur-lex.europa.eu/eli/reg/2017/745/oj>

¹³⁰ 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 (NIS2) [2022] OJ L333/80. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

¹³¹ Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Oviedo Convention). <https://www.coe.int/en/web/human-rights-and-biomedicine/oviedo-convention>

¹³² Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+, CETS No 223, 2018). <https://rm.coe.int/16808ac918>

¹³³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) OJ L, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

¹³⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

neurodata;¹³⁵ and the Data Governance Act creates trusted data-intermediary and “data altruism” frameworks that can structure cross-border sharing of sensitive neurodata for research under safeguards.¹³⁶ At the level of principles, the European Declaration on Digital Rights and Principles anchors a human-centric approach—privacy, dignity, transparency and freedom from manipulative practices—that supports neurorights-consistent interpretation of the acquis.¹³⁷

In Chile, the 2021 constitutional amendment, known as Ley 21.383, represents a global first in explicitly safeguarding mental integrity and neurodata.¹³⁸ Article 19 of Chile’s Constitution was modified to stipulate that scientific and technological development must serve people while respecting life and the physical and mental integrity of individuals. Significantly, the law establishes mandatory protections for any use of neurotechnologies that access cerebral activity or data derived therefrom, thereby setting a precedent for how national constitutions can enshrine neurorights. This constitutional enshrinement has subsequently shaped both statutory regulation and jurisprudence on neurorights within Chile.

In the United States, the state of Colorado has taken pioneering steps to expand privacy protections for neural data. Bill HB24-1058, titled “Protect Privacy of Biological Data,” amends the Colorado Privacy Act by categorizing biological data, including “neural data”, as sensitive personal information.¹³⁹ The measure underwent a legislative timeline beginning with its introduction on January 10, 2024, approval in committee on February 9, and formal adoption by the Colorado Legislature on March 26. Governor approval followed on April 17, 2024, and the new law is slated to take effect on August 7, 2024. This timeline reflects how state legislatures are responding to the evolving demands of neurotechnology and highlights the importance of requiring explicit consent and robust safeguards for processing neural data in commercial and governmental contexts.

Also in Chile, the Supreme Court’s August 9, 2023 judgment serves as one of the first high-level judicial interpretations of neuro-rights enforcement.¹⁴⁰ The case involved a constitutional protection action against Emotiv Inc. concerning its “Insight” device, a non-invasive neurotechnology used for self-quantification. The plaintiffs argued that insufficient data protections constituted a breach of Chile’s constitutional guarantees related to physical

¹³⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1. <https://eur-lex.europa.eu/eli/reg/2022/1925/oj>

¹³⁶ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act) [2022] OJ L152/1. <https://eur-lex.europa.eu/eli/reg/2022/868/oj>

¹³⁷ European Declaration on Digital Rights and Principles for the Digital Decade [2022] OJ C23/1. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>

¹³⁸ Gobierno de Chile, Constitución Política de la República de Chile (2024) https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf

¹³⁹ Protect Privacy of Biological Data: Concerning protecting the privacy of individuals’ biological data, and, in connection therewith, protecting the privacy of neural data and expanding the scope of the “Colorado Privacy Act” accordingly (House Bill 24-1058, 2024 Regular Session, approved 17 April 2024, effective 7 August 2024) <https://leg.colorado.gov/bills/hb24-1058> accessed 8 April 2025

¹⁴⁰ Sentencia [Folio N° 217225-2023, Rol N° 105.065-2023] (Tercera Sala de la Corte Suprema de Chile, Santiago, 9 agosto 2023) <https://www.diariojudicial.com/uploads/0000053479-original.pdf> accessed 8 April 2025

and mental integrity. The Court recognized the risks posed by unauthorized data collection, potential re-identification of users, and inadequate security measures, thus compelling regulators to adopt stricter oversight of commercial neurotech devices. This decision not only vindicates constitutional provisions but also clarifies the legal basis for adjudicating alleged violations of neurorights, strengthening the role of courts in upholding mental privacy.

Collectively, these legislative and judicial actions illustrate how binding legal frameworks can reinforce cognitive liberty and mental privacy through constitutional, statutory, and case law mechanisms. By imposing explicit obligations on technology providers and recognizing the enforceability of neurorights claims, these developments herald a shifting legal landscape in which safeguarding mental integrity assumes a central position in public law and policy.

7. Findings and Critical Discussion

The analysis shows three regulatory postures now co-existing in the governance of neurotechnology: a rights-anchored constitutional model (Chile), a data-protection-centric model with sectoral overlays (the European Union), and targeted statutory innovation (for example, Colorado). Each secures parts of what current discourse groups under neurorights, yet their fit and sufficiency diverge once applied to consumer-grade devices, high-confidence inferences drawn from brain-adjacent signals, and coercive or quasi-coercive settings such as the workplace, education, and criminal justice.

A first tension concerns whether neurorights should be recognised as stand-alone guarantees or as derivatives of existing rights. Chile's constitutional amendment offers powerful symbolic and doctrinal anchoring for mental integrity and neurodata, but it leaves implementation questions largely to subsequent legislation and courts: which actors owe which duties, and with what remedies? By contrast, the EU's derivative approach, Charter rights on dignity, integrity, privacy and data protection, operationalised through the GDPR and sectoral instruments, yields concrete obligations (data-protection-by-design, impact assessments, safety and post-market duties). Yet protection can be under-inclusive where intrusive cognitive inferences are not classified as special-category data because the controller disclaims medical or biometric purpose. This functional gap suggests the need for a rebuttable presumption that neural signals and high-confidence cognitive inferences are special-category data irrespective of declared purpose, with the burden on controllers to justify any derogation.

A second fault line is coverage of non-medical, direct-to-consumer neurotechnology. Much of this market is framed as wellness or productivity, potentially falling outside stringent medical-device regimes while still enabling decoding of affect, attention, or recognition. The EU's horizontal AI Act partially addresses this through prohibitions and high-risk duties, and the Digital Services/Markets Acts constrain manipulative uses and cross-context data combination; nevertheless, borderline classification remains a vector of regulatory arbitrage. A more coherent approach would align product-safety, AI,

and data-protection triggers around capabilities and foreseeable inferences rather than sectoral labels, coupled with market-surveillance powers to reclassify products as evidence on real-world use emerges.

Third, manipulation and emotion inference sit at the edge of existing frameworks. The AI Act's prohibition on systems that materially distort behaviour, and its limits on certain emotion-recognition uses in the workplace and education, mark genuine progress. But the material distortion threshold and context-specific carve-outs risk leaving commercial nudge-by-design architectures intact, especially where inference pipelines draw on multimodal signals that include brain-adjacent or neurotech-derived data. Here, the DSA's systemic-risk duties for very large platforms provide a complementary lever, yet effective mitigation will likely require clearer rules on dark patterns and on the admissibility of neuro-derived inferences in personalisation, scoring, and eligibility determinations.

Fourth, criminal-justice and forensic contexts expose unresolved questions about mental privacy, self-incrimination, and compelled access to neural signals. The EU Law Enforcement Directive imports many GDPR-style safeguards but was not drafted with brain-decoding in mind; likewise, Chile's constitutional guarantees now meet early judicial testing. Courts will need to decide whether compelled neuroimaging is properly characterised as accessing testimonial content, how consent operates under custody or power imbalances, and what exceptions, if any, could survive strict necessity and proportionality review. Without authoritative guidance, there is a risk of fragmented practice and technological drift.

Fifth, enforcement and remedies will determine whether paper rights travel into practice. Data-protection authorities, market-surveillance bodies, health-product regulators, and courts each hold pieces of the enforcement puzzle, but coordination is uneven. The Chilean *recurso de protección* shows how constitutional process can generate rapid relief, while EU private enforcement remains limited by standing and collective-redress frictions. A credible regime for neurotechnology should combine proactive duties (design, risk governance, auditability), *ex post* controls (recall, withdrawal, fines), and meaningful individual remedies (access, objection, deletion, contestation of automated outcomes), with clear allocation of responsibility across complex supply chains.

Finally, the comparative mapping points to a constructive synthesis. The EU model demonstrates how derivative rights, when given operational bite through horizontal and sectoral legislation, can discipline real systems at scale; Chile's constitutional approach supplies a clear normative north star that facilitates principled adjudication; and targeted statutes such as Colorado's can close definitional and sensitivity gaps for neural data in consumer contexts. Pulling these strands together suggests a forward path: adopt capability-based definitions of neurodata and neuro-inferences; treat them as presumptively sensitive with strict lawful-basis and purpose-limitation controls; require on-device or privacy-preserving processing by default for decoding functions; prohibit employer or educational mandates for neural monitoring absent tightly drawn necessity tests; hard-ban covert neuromodulation and deceptive interfaces; and create auditable, sandboxed pathways for bona fide clinical and accessibility uses under independent oversight. Such measures would reduce

the present mismatch between what technology can reveal or influence and what the law currently anticipates, without fragmenting the general system of fundamental rights.

In short, the problem is not the absence of norms but their misalignment with capability, context, and enforcement. A neurorights-consistent reading of existing instruments, shored up by targeted clarifications where genuinely novel risks arise, offers the most legally coherent and administrable path to safeguarding mental privacy, cognitive liberty, and mental integrity as neurotechnology moves from laboratories to everyday life.

8. From Principles to Practice: An Operational Framework for Mental Privacy and Neurorights

The preceding analysis shows that contemporary instruments already protect interests commonly grouped as “neurorights,” even if they do so unevenly. What is missing is not another declaration but a workable method for applying those interests to systems that decode, infer, or influence cognition. The central claim here is that neurorights can be made both administrable and innovation-compatible through a capability-based operational framework that rides on top of existing law. Rather than multiplying free-standing rights, the proposal gives concrete content to mental privacy, cognitive liberty, and mental integrity across product design, data governance, evidence law, and enforcement. This capability-based method operationalizes Bianca’s privacy principles, effective consent and responsibility anchored in control over the informational dimension of the person, for neurodata, neuro-inference, and neuro-effect.¹⁴¹

Any practicable regime must begin by clarifying the protected object. I use three linked notions that map onto the comparative materials in section 6 while closing gaps exposed by consumer-grade devices and AI inference pipelines. “Neurodata” covers signals captured directly from the nervous system together with brain-adjacent biosignals when used with the capability to reveal cognitive states with non-trivial reliability; this includes EEG streams, implanted-device telemetry, and pupillometry or micro-expressions when combined for cognitive decoding, as well as model embeddings trained on such inputs. “Neuro-inference” denotes outputs—attention, recognition, intent, affect, belief attribution—generated from neurodata or from multimodal data in which the neuro component is material to the output. “Neuro-effect” designates any technical action designed to modulate cognitive states, from TMS protocols and closed-loop stimulation to interface features engineered to induce attentional or affective shifts. Framed in this way, classification turns on capability and foreseeable use, not on sector labels or the controller’s purpose statement, thereby reducing the classification arbitrage surfaced in section 6(c).

With the protected object in view, mental privacy needs a presumption that bites in practice: neurodata and high-confidence neuro-inferences should be treated as presumptively sensitive. Controllers who wish to process them must

¹⁴¹ CM Bianca and FD Busnelli (eds), *La protezione dei dati personali* (n 1) 2200

satisfy narrowed lawful-basis pathways—explicit and unbundled consent insulated from detriment; a tightly drawn, statutory public-interest ground; or a clinical/assistive exception subject to independent oversight. Where a controller asserts that an inference is merely “well-being analytics,” the burden lies with that controller to rebut sensitivity through evidence about model performance, error profiles, population drift, and downstream use. This approach gives operational teeth to the derivative-rights architecture of the EU acquis while avoiding the need to invent new rights from whole cloth.

Coercive and quasi-coercive contexts require special treatment because they bring the concerns in sections 3–4 into sharpest focus. Whenever neurodata, neuro-inferences, or neuro-effects are sought or imposed in criminal procedure, immigration screening, employment, or education, two presumptions should govern. First, access that reveals—or materially risks revealing—internally held content such as recognition, intent, or belief is properly characterised as testimonial and is therefore presumptively barred, extending the right to silence to neural decoding. Second, even where testimonial concerns are not triggered, any use must satisfy strict necessity and proportionality with narrow scope, independent authorisation, and robust rights to contestation. Consent obtained under dependency should be treated as suspect unless a genuine, no-detriment alternative exists. Reliability must not be assumed: pre-deployment validation on representative populations, public error-rate disclosure, and adversarial testing are prerequisites, not afterthoughts, and individuals must have access to expert assistance to challenge outputs.

Much of the current mismatch between risk and regulation arises because classification follows marketing rather than capability. Systems should therefore be tiered by what they can infer or modulate. A device that enables high-confidence mind- or brain-reading belongs in the strictest tier regardless of “wellness” branding; adding an AI component that performs emotion or intent inference elevates tiering automatically. Tiering then triggers obligations already familiar to regulators—risk management, data governance, robustness, human oversight—but calibrated to cognitive impact. The result is to avoid both under-inclusion (wellness BCIs that function as *de facto* diagnostic tools) and over-breadth (benign biofeedback with no realistic decoding capability).

Rights travel into practice only if they are built into design. To that end, a Neuro-Privacy Impact Assessment should be layered onto existing DPIAs and AI risk-management processes. The assessment must force early confrontation with cognition-specific harms: which cognitive states can be revealed or influenced; in what contexts are harms plausible; what is the foreseeable error profile across sub-populations; which privacy-preserving techniques—on-device computation, secure enclaves, federated learning, differential privacy—are feasible; how will models and stimulation protocols be audited, rolled back, or sunsetted if harms surface? Three default rules give these duties purchase: process on device whenever feasible; retain only derived metrics strictly necessary for the user-facing function (no raw-signal retention by default); and maintain tamper-evident provenance logs linking outputs to model version, parameters, and input path to enable meaningful contestation.

A further line must be drawn around manipulation. Where interfaces are intentionally designed to steer cognition covertly, neurorights collapse into consumer protection unless a bright line is articulated. Deceptive neuromodulation and covert optimisation for cognitive susceptibility should be prohibited outside clinically supervised therapy or bona fide accessibility use. In commercial settings, optimisation that relies on neuro- must be disclosed, must be opt-in, and must be categorically inferences excluded from eligibility, pricing, and disciplinary decisions. Platforms should be barred from combining neuro-inferences with profiling for consequential outcomes unless a specific statutory regime permits it under strict safeguards.

Evidence law must reflect the reliability and testimonial concerns developed in sections 2–4. Neuro-inferences should be inadmissible to prove mental states absent a concrete showing that the construct measured has forensic validity beyond the laboratory, that individual-level error and base-rate problems have been addressed, and that probative value outweighs the chilling effect on mental privacy. Even then, derivative-use limits should prevent such inferences from seeding investigative fishing expeditions or underwriting compelled follow-on testing.

Enforcement architecture will determine whether the foregoing is more than aspiration. Competence should be allocated along existing lines—data-protection authorities for processing and lawful-basis questions; product-safety and market-surveillance bodies for capability-based tiering; health regulators for clinical neurotech; and courts for testimonial and coercion issues - while ensuring coordinated action. Remedies should include injunctive relief; exclusion of unlawfully obtained neuro-evidence; algorithmic disgorgement for models trained on illegally processed neurodata; recall for deceptive neuromodulation; statutory damages for dignitary harms; and collective redress where chilling effects are diffuse.

Finally, the framework must preserve space for research, therapy, and accessibility. It does so by coupling strict necessity with independent oversight and participant control. Time-limited sandboxes should operate with transparent protocols, ethical recruitment, and public reporting of adverse events, so that learning accrues to the system rather than remaining proprietary. In this way, the proposal is not anti-innovation; it is pro-accountability.

What this adds is straightforward. The comparative materials in section 6 established where the law stands; this chapter specifies how to use it. It resolves the stand-alone versus derivative impasse by giving derivative rights operational bite through capability-based definitions and a presumption of sensitivity; it supplies justiciable standards for coercive contexts and admissibility that speak to the hardest cases rather than merely listing instruments; and it offers design-time duties and enforcement tools that regulators can incorporate into guidance or rulemaking without waiting for new constitutional text. Neurorights thus become governable not by proclamation, but by aligning capability, context, and accountability as neurotechnology moves from the laboratory into ordinary life.

9. Conclusions

This article contends that the urgent task in neurotechnology governance is not to mint new, free-standing rights, but to render existing guarantees operable against systems that decode, infer, or influence cognition. Building on the comparative analysis in Section 6 and the critical discussion in Section 7, Section 8 set out a capability-based framework that gives concrete content to mental privacy, cognitive liberty, and mental integrity. It defines protected objects (neurodata, neuro-inference, neuro-effect), presumes their sensitivity, tiers obligations by what systems can reveal or modulate rather than how they are marketed, embeds cognition-specific impact assessment into design, and draws bright lines against deceptive neuromodulation and coerced neural access.

The comparative mapping shows that legal orders already contain the building blocks for such a framework, even if they deploy them unevenly. The European Union's derivative-rights architecture—privacy and data protection operationalised through horizontal and sectoral instruments—supplies enforceable duties at scale; Chile's constitutional amendment provides a clear normative anchor and a vehicle for principled adjudication; and targeted statutes such as Colorado's close definitional gaps around neural data in consumer contexts. Taken together, these models point to a workable synthesis: treat neuro-capabilities as presumptively sensitive; align product-safety, AI, and data-protection triggers to capability and foreseeable inference; and ensure that coercive or quasi-coercive contexts activate heightened testimonial and proportionality controls.

The policy implications are immediate. Regulators need not await new constitutional text to act. Data-protection authorities can clarify that neural signals and high-confidence cognitive inferences are ordinarily special-category/sensitive data; product-safety and market-surveillance bodies can reclassify "wellness" devices whose real-world capabilities cross diagnostic or decoding thresholds; health regulators can require cognition-specific validation and post-market surveillance for closed-loop systems; and courts can treat compelled decoding of recognition, intent, or belief as presumptively testimonial, subject to strict necessity and proportionality. Evidence law can demand construct validity beyond the laboratory and guard against derivative use that chills mental privacy. These measures do not expand the catalogue of rights; they operationalise the ones we already have.

Two limitations of the present study warrant emphasis. First, the framework is normative and doctrinal rather than empirical; it does not measure how the proposed presumptions and tiering rules perform in practice across populations or devices. Second, several hinges of the analysis—what counts as a "high-confidence" cognitive inference, how to calibrate the testimonial character of compelled decoding, how to audit neuromodulatory interfaces—require sustained, interdisciplinary work. Future research should develop reference metrics and audit protocols for cognitive inference, test reliability and base-rate behaviour in diverse cohorts, and evaluate the comparative effectiveness of on-device and privacy-preserving pipelines under operational constraints.

The core claim is conceptual and administrable: mental privacy and cognitive liberty can be safeguarded by aligning capability, context, and accountability. When classification follows what a system can reveal or influence, when coercive settings trigger heightened standards, and when design-time duties and evidentiary gatekeeping are made explicit, neurorights become governable without fragmenting the general system of fundamental rights. Protecting the conditions under which thought is formed is a precondition for self-government; the law can meet that demand now by making its existing promises bite where cognition is at stake.