

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3
2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Mental Privacy under Article 21: Constitutional Limits on Neurotechnological Data Extraction in India

TANISH DAHUJA*

ABSTRACT

The emergence of consumer and commercial neurotechnologies capable of extracting, processing, and inferring cognitive data from neural signals presents Indian constitutional privacy jurisprudence with a challenge that existing doctrine is structurally ill-equipped to address. While the nine-judge bench in Justice K.S. Puttaswamy (Retd.) v. Union of India established privacy as a fundamental right under Article 21 of the Constitution, recognizing informational privacy, decisional autonomy, and dignity as its interlocking dimensions, the framework was elaborated against a background of conventional data collection. Neurotechnological systems, including electroencephalographic wearables, affective computing interfaces, cognitive analytics platforms, and neural biometric systems, operate at a constitutively different register: they access cognitive states before their expression, generate probabilistic inferences about mental processes from physiological signals, and collapse the conventional distinction between information a person possesses and information that is constructed from her neural activity. This paper argues that neurodata occupies a constitutionally distinct category from ordinary personal data because its extraction compromises not merely informational privacy but the pre-expressive substrate of decisional autonomy itself. Critically examining the Digital Personal Data Protection Act, 2023, the paper identifies structural deficiencies in neurodata classification, inferred data governance, and consent architecture that render the statute inadequate as a governance framework. Drawing selectively on Chile's 2021 constitutional neurorights amendment and the EU Artificial Intelligence Act's restrictions on cognitively intrusive systems, the paper argues that the Puttaswamy framework, properly extended, can accommodate a doctrine of mental privacy within Article 21 without requiring entirely new constitutional language. A tripartite constitutional standard is proposed: cognitive integrity protection, a doctrine of inferential restraint, and heightened proportionality review for neurotechnological intrusions. This framework reflects the constitutional values of dignity, autonomy, and mental self-determination already embedded in India's privacy jurisprudence, and is capable of governing the specific constitutional harm that neurodata extraction poses.

* Author is an Advocate at Punjab and Haryana High Court, India.

Keywords: Article 21; neurotechnology; mental privacy; neurodata; informational privacy; decisional autonomy; DPDP Act 2023; cognitive integrity

I. INTRODUCTION

India's constitutional privacy jurisprudence underwent a structural transformation in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹ where a unanimous nine-judge bench held privacy to be a fundamental right inhering in Article 21 of the Constitution of India. The judgment consolidated and extended doctrinal developments spanning several decades,² recognizing privacy as a multi-dimensional right encompassing bodily integrity, informational autonomy, and the freedom to make intimate choices without state surveillance or compulsion. Its significance for the constitutional governance of emerging data technologies has been widely recognized in subsequent jurisprudence and scholarship. Yet the specific constitutional problem posed by neurotechnological data extraction, a problem that is both practically immediate and doctrinally novel, has received insufficient analytical attention.

Neurotechnological systems present a challenge to existing privacy doctrine that differs not merely in degree but in constitutional kind. Conventional data collection, however pervasive, extracts information that a person has already expressed through behavior, communication, or transaction. Neurotechnological systems, including electroencephalographic wearables, emotion recognition interfaces, cognitive analytics platforms, and neural biometric authentication tools, operate differently: they extract physiological signals from the brain and body and, through computational inference, generate data representing cognitive and affective states that the subject has never communicated and may not consciously recognize. The Supreme Court's holding in *Selvi v. State of Karnataka*³ that non-consensual extraction of mental information through scientific techniques violates Article 21 illuminates the constitutional principle at stake, but its application has not yet been extended to the civilian neurotechnological contexts that now make its doctrinal development practically urgent.

The constitutional difficulty is this: the *Puttaswamy* framework's informational privacy strand protects data that a person possesses and may disclose; but neurodata is constructed from physiological signals by the operator's systems: it is generated *about* a person rather than collected *from* her. The decisional autonomy strand protects the right to make intimate choices

¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter *Puttaswamy*].

² For the doctrinal lineage of constitutional privacy prior to *Puttaswamy*, see *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India); *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India); *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

³ *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India) [hereinafter *Selvi*].

without interference; but neurodata extraction operates at a prior stage, accessing the cognitive substrate from which choices emerge before those choices have formed. Existing doctrine, calibrated to the protection of expressive information and formed choices, is architecturally inadequate for the pre-expressive domain that neurotechnology penetrates. This inadequacy is compounded by the structural deficiencies of India's primary data governance statute, the Digital Personal Data Protection Act, 2023,⁴ which contains no classification framework for neurophysiological data and no governance architecture for cognitively inferred data.

This paper proceeds as follows. Section II defines neurodata for constitutional purposes and identifies its constitutionally significant characteristics. Section III examines the Article 21 jurisprudential architecture and argues that mental privacy is already latent within it. Section IV demonstrates the structural failure of existing informational privacy doctrine to address neurodata. Section V critically evaluates the Digital Personal Data Protection Act, 2023. Section VI surveys comparative developments selectively. Section VII proposes a doctrinal framework for mental privacy under Article 21. Section VIII concludes.

II. NEUROTECHNOLOGICAL DATA EXTRACTION: RELEVANT CATEGORIES AND CONSTITUTIONAL SIGNIFICANCE

For constitutional purposes, neurodata may be defined as data derived from neural, neurophysiological, or neuropsychological processes, whether extracted directly from brain activity or inferred through computational analysis of physiological proxies. This definition encompasses technologies presently deployed in commercial, educational, and employment contexts: consumer-grade electroencephalographic wearables monitoring attention and stress levels; emotion recognition and affective computing systems analyzing facial musculature and vocal patterns; cognitive analytics platforms assessing mental workload; and neural biometric systems used for authentication and continuous identity verification.⁵ Each of these categories generates data that its operators may use to construct assessments of a subject's cognitive and affective states, often without the subject's meaningful awareness of the inferences being generated.

Two characteristics render neurodata constitutionally distinct from ordinary personal data. First, neurodata has an inherently inferential dimension: contemporary neural signal processing relies on machine learning models to translate raw physiological signals into actionable cognitive

⁴ Digital Personal Data Protection Act, No. 22 of 2023 (India) [hereinafter DPDP Act].

⁵ NITA A. FARAHANY, *THE BATTLE FOR YOUR BRAIN: DEFENDING THE RIGHT TO THINK FREELY IN THE AGE OF NEUROTECHNOLOGY* 8–18 (St. Martin's Press 2023) [hereinafter FARAHANY].

assessments. The inferences so generated are not records of existing information; they are probabilistic constructions that produce cognitive profiles from neural patterns. The relationship between the source signal and the inferred cognitive state is mediated by opaque algorithmic processes that the subject cannot observe, verify, or contest.⁶ Second, neurodata has an asymmetric extraction structure: the subject typically cannot know what cognitive states have been inferred from her neural signals, cannot verify the accuracy of those inferences, and cannot meaningfully contest them in contexts where institutional power asymmetry forecloses any practical opt-out. This asymmetry is structural, not contingent; it reflects the fundamental epistemic gap between the operator's signal processing capacity and the subject's awareness of what is being generated from her physiological signals.

The constitutional significance of these characteristics lies in their relationship to the interests that Article 21 privacy protects. The inferential dimension means that neurodata extraction cannot be governed purely through consent to source data collection; consent to wear an EEG device does not constitute informed consent to the full range of cognitive inferences the operator's algorithms may subsequently generate. The asymmetric extraction structure means that the consent model underlying both constitutional privacy doctrine and existing statutory frameworks cannot operate as an adequate safeguard where the subject lacks the epistemic resources to understand what she is consenting to. Both characteristics have direct implications for how constitutional scrutiny must be calibrated to address the specific constitutional harms that neurotechnological extraction inflicts.⁷

III. ARTICLE 21 AND THE CONSTITUTIONAL ARCHITECTURE OF MENTAL PRIVACY

A. The Puttaswamy Framework

The *Puttaswamy* judgment is the necessary starting point for any constitutional analysis of privacy in India. The nine-judge bench converged on several foundational propositions: privacy is a fundamental right under Article 21; it encompasses both negative rights against intrusion and positive dimensions protecting individual autonomy; it protects informational interests as well as the individual's capacity for intimate choice; and it is grounded in the constitutional values of dignity, liberty, and autonomy.⁸ The judgment resolved decades of doctrinal uncertainty and established the constitutional framework within which all privacy claims must

⁶ Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Neurotechnology Age*, 13 LIFE SCIS. SOC'Y & POL'Y 5 (2017).

⁷ Puttaswamy, *supra* note 1. For the informational privacy strand's doctrinal antecedents, see *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (India).

⁸ Puttaswamy, *supra* note 1.

now be evaluated.

Justice Chandrachud's concurring opinion articulated what has become the most analytically influential framework within the judgment: a tripartite conception of privacy encompassing privacy of the person (bodily integrity), informational privacy (the right to control personal data), and the privacy of choice (decisional autonomy in intimate matters).⁹ This structure provides the constitutional raw material from which a doctrine of mental privacy can be constructed, though its application to neurotechnology requires doctrinal extension beyond the contexts initially contemplated. Crucially, the informational privacy strand as developed in *Puttaswamy* is not merely a data-protection right; it is a constitutional interest in controlling the narrative of one's own identity, specifically the right to determine for oneself what information about oneself is communicated to others, and on what terms. This formulation carries immediate significance for the present argument: a right to determine what information is communicated about oneself necessarily presupposes a domain of information that is the subject's own to disclose or withhold. Neurotechnological extraction challenges this presupposition not by appropriating information the subject has already formed but by constructing intimate data from her physiological signals without awaiting any communicative act on her part.¹⁰

B. Decisional Autonomy and the Pre-Expressive Domain

The decisional autonomy strand of *Puttaswamy*, that is, the right to make choices about intimate aspects of one's life without state compulsion or surveillance, has been elaborated in subsequent jurisprudence, most notably *Navtej Singh Johar v. Union of India*¹¹ and *Common Cause (A Regd. Society) v. Union of India*.¹² The constitutional logic is that certain domains of personal choice are so constitutive of individual identity that state interference requires compelling justification; autonomy is protected not merely because choices are valuable in themselves but because the capacity to form and act upon choices is a precondition of constitutional personhood.

Neurodata extraction poses a threat to this dimension of Article 21 that existing doctrine does not reach: it intrudes upon cognition before choices have been formed. A constitutional framework that protects only formed choices, meaning choices that have crystallized into expression or action, cannot protect the cognitive processes from which choices emerge. This matters constitutionally because manipulation of the pre-expressive cognitive domain can

⁹ Puttaswamy, *supra* note 1.

¹⁰ FARAHANY, *supra* note 5, at 43–56. See also Rafael Yuste & Sara Goering, *Four Ethical Priorities for Neurotechnologies and AI*, 551 NATURE 159, 160 (2017).

¹¹ Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (India).

¹² Common Cause (A Regd. Society) v. Union of India, (2018) 5 SCC 1 (India).

compromise the deliberative autonomy that constitutional privacy is designed to preserve. An entity possessing neurodata-derived knowledge of a person's attentional vulnerabilities, emotional triggers, and cognitive patterns can shape her deliberative environment in ways that circumvent rather than engage her autonomous agency. This is not merely a privacy harm in the conventional sense; it is an autonomy harm that reaches the core constitutional value that Article 21 protects.¹³

C. Bodily Integrity and the Selvi Principle

The bodily integrity dimension of Article 21 privacy, recognized in *Puttaswamy* and established in cases including *Suchita Srivastava v. Chandigarh Administration*,¹⁴ extends constitutional protection directly to neural signal extraction. Neural signals are biological data generated by the body; their extraction through wearable devices, affective computing systems, or biometric neural scanning involves a form of bodily access that engages Article 21's integrity protections.

The Supreme Court's decision in *Selvi v. State of Karnataka*¹⁵ is the most significant Indian authority on the constitutional limits of mental data extraction. The Court held that narcoanalysis, polygraph testing, and Brain Electrical Oscillation Signature profiling administered without consent violate both Article 20(3) and Article 21. The constitutional reasoning extends beyond its immediate procedural context: the Court held that these techniques extract mental content without voluntary cooperation, and that the constitutional bar applies to information generated from cognitive processes regardless of whether that generation is achieved through chemical, physiological, or computational means. The right to mental privacy, meaning the individual's right to control what is generated from and communicated about her cognitive states, was recognized as a protected constitutional interest.¹⁶

Selvi's reasoning is a doctrinal resource that has been underutilized in privacy scholarship. The judgment's constitutional logic does not confine itself to criminal proceedings; it reflects a broader principle that the mental domain of an individual constitutes a constitutionally protected space into which access requires either voluntary consent or justification meeting Article 21's requirements. Extending *Selvi*'s principle to civilian neurotechnological contexts, including workplace monitoring, consumer wellness applications, and educational assessment platforms,

¹³ FARAHANY, *supra* note 5, at 45–56.

¹⁴ *Suchita Srivastava v. Chandigarh Administration*, (2009) 9 SCC 1 (India). On the purposive construction of Article 21 generally, see *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

¹⁵ *Selvi*, (2010) 7 SCC 263. Brain Electrical Oscillation Signature (BEOS) profiling involves passive EEG recording correlated with memory-evoked neural responses; the Court held that neither polygraph testing, narcoanalysis, nor BEOS profiling may be administered without the subject's consent.

¹⁶ *Id.*

does not require doctrinal innovation. It requires only the recognition that the constitutional protection of the mental domain applies wherever the structural conditions of non-consensual cognitive extraction exist, regardless of whether the extracting actor is the state in a criminal investigation or a private entity in a commercial relationship.¹⁷

D. Dignity and Constitutional Personhood

The dignity strand of Article 21, articulated in *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*¹⁸ and affirmed throughout *Puttaswamy*, grounds the right to privacy in the constitutional recognition of personhood. If dignity protects the right to live as a free and self-determining person rather than as an object of external control, then the domain of conscious mental life, the space within which persons form intentions, develop preferences, and constitute their identities, must fall within its protective scope. Neurotechnological extraction that enables others to access, profile, and exploit an individual's cognitive processes without her meaningful consent treats her inner life as a resource available for extraction rather than as a constitutionally protected dimension of her personhood. The argument is structural, not sentimental: dignity under Article 21 protects the conditions necessary for autonomous agency, and the pre-expressive mental domain is the constitutive site of such agency.

It bears noting that the dignity argument developed here does not depend on establishing that consciousness or cognitive life is uniquely sacred in some metaphysical sense. The constitutional argument is narrower: since the *Puttaswamy* Court recognized privacy as essential to dignity because it protects the individual's capacity to develop and project her own sense of identity, and since identity is constituted through cognitive processes, through the formation of preferences, the development of commitments, and the deliberative exercise of practical reason, it follows that constitutional protection for dignity extends to the cognitive domain from which identity emerges. The mental domain is not simply a further category of sensitive data; it is the constitutional precondition for the very subjecthood that Article 21's dignity clause is designed to protect. This conclusion does not require any departure from the framework elaborated in *Puttaswamy*¹⁹; it is an application of that framework to a constitutional challenge the Court did not yet confront.

¹⁷ Selvi, *supra* note 3.

¹⁸ *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608 (India).

¹⁹ *Puttaswamy*, *supra* note 1.

IV. THE STRUCTURAL FAILURE OF EXISTING PRIVACY DOCTRINE

A. The Inferential Privacy Problem

The structural inadequacy of informational privacy doctrine in addressing neurodata lies in what may be termed the inferential privacy problem. Existing frameworks, constitutional and statutory alike, operate on a model of information disclosure: privacy is infringed when identifiable information about a person is collected, processed, or shared without consent. The implicit presupposition is that the information extracted pre-exists its extraction as a record of something the person has expressed, done, or communicated. The subject's right is conceived as a right to control information that she already possesses.²⁰

Neurodata disrupts this model at a constitutive level. When an affective computing platform infers from a job applicant's facial micro-expressions and vocal pitch that she is experiencing anxiety or cognitive deception, it is not collecting information she has disclosed. It is constructing a cognitive profile through algorithmic analysis of physiological signals the subject generated without intentional communication.²¹ The subject may not know this inference has been made, cannot verify its accuracy, and almost certainly cannot contest its use in hiring decisions that affect her materially. Informational privacy doctrine, designed to protect against the unauthorized use of information a person already possesses about herself, offers no analytical traction here because the constitutional harm operates not at the level of unauthorized disclosure but at the level of unauthorized construction of intimate cognitive data about her.

A corollary of the inferential privacy problem is an ontological one: neurodata is not merely more intimate than ordinary personal data; it is different in kind. Ordinary personal data is derived from a person's actions, transactions, communications, or records, data that however sensitive reflects what she has already done or said. Neurodata, by contrast, is derived from what she *is* neurologically and cognitively at a given moment. It reaches below the threshold of intentional expression to access cognitive states that are prior to and formative of any deliberate act. This is why the *Puttaswamy* framework's model of informational privacy, built on the analogy of a person who holds information about herself and may choose to release or retain it, cannot, without significant extension, govern the extraction of data that exists only because an external system has interrogated her physiology. The constitutional gap is not merely technical; it is structural, inhering in the model of privacy that existing doctrine assumes.²²

²⁰ Puttaswamy, *supra* note 1.

²¹ FARAHANY, *supra* note 5, at 43–56.

²² FARAHANY, *supra* note 5.

B. Consent Architecture and Epistemic Asymmetry

The consent model underlying constitutional privacy doctrine and the Digital Personal Data Protection Act's governance architecture²³ presupposes a subject who can identify what data is being collected, understand its implications, and make an informed choice about processing. In neurotechnological contexts, this presupposition fails structurally. The opacity and complexity of neural signal processing algorithms render the "informed" component of consent deficient: an individual consenting to wear an EEG monitoring device for workplace productivity cannot foresee, and is typically not informed about, the full range of cognitive inferences the operator's machine learning models will generate from her neural signals.²⁴ The consent obtained is, at best, consent to source data collection; it is not and cannot be consent to the inferences subsequently constructed from that data.

Second, the voluntariness of consent is structurally compromised wherever institutional power asymmetry exists. An employee asked to wear cognitive monitoring technology during working hours, a student required to submit to attention-tracking software in examination conditions, or an insurance applicant whose neurodata affects actuarial risk assessment cannot meaningfully be said to give free consent. The structural coerciveness of these relationships, combined with the absence of meaningful opt-out alternatives, negates the voluntariness premise on which consent-based governance rests. The constitutional significance of this structural failure extends beyond the regulatory framework to the constitutional status of consent as a basis for neurotechnological intrusion.²⁵

A further dimension of the consent architecture problem concerns the temporal structure of neurotechnological extraction. Conventional data collection typically occurs at discrete, identifiable moments (a form submission, a transaction, or a login) that create natural occasions for consent solicitation. Continuous neurotechnological monitoring, by contrast, generates data streams across extended time periods during which consent would need to be continuously operative rather than merely initially given. The "once-off" or "per-purpose" consent models contemplated by the DPDP Act are structurally unsuited to governing data extraction that occurs continuously over hours or days of workplace monitoring or consumer device use. Designing a consent architecture that is capable of governing continuous neural signal processing, one that remains meaningfully operative rather than degenerating into a formality, requires specific

²³ DPDP Act, *supra* note 4, § 6(1)–(3).

²⁴ Ienca & Andorno, *supra* note 6, at 7–9.

²⁵ Ienca & Andorno, *supra* note 6, at 7–9.

regulatory innovation that the Act's current framework does not provide.²⁶

C. The Manipulation Problem and Autonomous Deliberation

Neurodata extraction raises a constitutional concern that transcends privacy in its informational or decisional dimensions: it creates the technical capacity for cognitive manipulation that operates below the threshold of deliberate awareness. The *Puttaswamy* framework's autonomy strand protects the right to make intimate choices without external compulsion.²⁷ But cognitive profiling systems that generate detailed models of attentional vulnerabilities, emotional triggers, and deliberative patterns from neurodata create instruments of behavioral influence that circumvent deliberate choice rather than coerce it, shaping the conditions of deliberation rather than overriding its outcomes. The constitutional question of whether neurotechnologically-enabled cognitive manipulation by private actors implicates Article 21's autonomy protections remains unresolved in Indian courts. The argument that it does is both doctrinally available and practically necessary: Article 21 protects not merely the freedom to choose but the integrity of the deliberative conditions from which choice emerges, and cognitive profiling that systematically compromises those conditions constitutes an autonomy harm of constitutional significance.

V. THE DPDP ACT, 2023: STRUCTURAL DEFICIENCIES

A. The Neurodata Classification Gap

The Digital Personal Data Protection Act, 2023, defines "personal data" as any data about an individual who is identifiable by or in relation to such data.²⁸ The Act contemplates a category of "sensitive personal data" to be specified through subordinate legislation, but as enacted it does not classify neurophysiological data, cognitively inferred data, or neural biometric data among the categories warranting heightened protection. Biometric data, though recognized as sensitive in pre-existing regulatory instruments, receives no special treatment for its neurological subset. This classification gap has direct constitutional implications: neurodata's capacity to reveal intimate cognitive and affective information through inferential processing places it at a level of sensitivity that is categorically greater than conventional biometric data.

The pre-legislative history of India's data protection framework makes this gap conspicuous. The Srikrishna Committee Report of 2018 proposed that biometric and genetic data receive

²⁶ DPDP Act, *supra* note 4.

²⁷ Puttaswamy, *supra* note 1.

²⁸ DPDP Act, *supra* note 4, § 2(t) (defining "personal data" as "any data about an individual who is identifiable by or in relation to such data").

special protection on the basis of their capacity to reveal intimate characteristics and their potential for harmful misuse.²⁹ The analytical logic supporting special treatment for neurophysiological and cognitively inferred data is at least as compelling as that supporting protection for biometric or genetic data: neurodata's inferential capacity reaches into the mental domain in a manner that no other category of personal data can replicate, revealing cognitive characteristics, emotional vulnerabilities, and mental states that are more intimate and more consequential than the biometric identifiers the Committee sought to protect. The absence of neurodata from the Act's classification framework represents a structural failure that subordinate legislation must address as a matter of constitutional necessity.

B. Inferred Data and the Governance Architecture

A more fundamental structural deficiency concerns the Act's treatment of data generated through inferential processing. The Act's consent requirements and purpose limitation principles apply to the collection and processing of personal data,³⁰ but they do not clearly govern data that is generated through algorithmic inference from lawfully collected source data. When a behavioral analytics platform generates a cognitive vulnerability profile from EEG data collected under a workplace productivity monitoring consent, the consent obtained for source data collection does not automatically extend to the cognitive inferences subsequently generated. The Act provides no mechanism specifically governing this inferential processing or imposing any requirements on the construction of cognitive profiles from neural signals.

This gap is constitutionally significant because cognitive inferences derived from neurodata may be more intimate and more consequential than the source data from which they are derived.³¹ An individual's raw EEG signal, taken in isolation, may be relatively uninformative; the detailed cognitive profile inferred from that signal by a sophisticated machine learning model may reveal attentional deficits, emotional instabilities, and deliberative vulnerabilities that no direct communication from the subject would disclose. The Act's failure to govern this inferential dimension means that the most constitutionally sensitive aspect of neurotechnological extraction, specifically the construction of intimate cognitive representations from physiological signals, falls entirely outside its regulatory architecture.

This gap acquires greater constitutional urgency given the trajectory of commercial

²⁹ JUSTICE B.N. SRIKRISHNA COMM., MIN. OF ELEC. & INFO. TECH., A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS 22–25 (2018). The Committee proposed biometric and genetic data as sensitive categories warranting heightened protection; the DPDP Act adopted a narrower, framework-based approach, deferring specific classification to subordinate legislation.

³⁰ DPDP Act, *supra* note 4, §§ 4, 6, 9.

³¹ FARAHANY, *supra* note 5, at 87–99.

neurotechnology development. The market for consumer EEG devices, workplace cognitive analytics, and affective computing platforms is expanding, and the inferential models operators deploy are becoming progressively more granular and more intimate in their outputs.³² A data governance framework adequate for conventional personal data collection is not adequate for neural signal processing; the constitutional requirements identified in this analysis cannot be satisfied without specific statutory provisions that address the distinctive structure of neurotechnological harm.³³

C. Consent Architecture and Significant Data Fiduciaries

The Act's consent-based framework, with heightened obligations for significant data fiduciaries,³⁴ reflects sound data governance principles but is inadequate for the structural features of neurotechnological platforms. The Act does not address the epistemic asymmetries that compromise voluntary and informed consent in contexts of neural signal processing; it does not require specific disclosure of the inferential processing methodologies applied to neural source data; and it contains no provision analogous to the GDPR's restrictions on significant automated decision-making that produces legal or similar effects on data subjects.³⁵ The resulting framework formally satisfies data protection requirements while permitting precisely the kind of cognitively invasive processing that constitutional doctrine requires to be subjected to heightened scrutiny.

VI. COMPARATIVE CONSTITUTIONAL AND REGULATORY APPROACHES

Chile's 2021 constitutional amendment to Article 19 of its Political Constitution, being the first constitutional recognition of neurorights worldwide, protects mental integrity against unjustified or non-consensual augmentation, diminishment, or interference with cognitive processes.³⁶ The amendment is instructive in two respects. It demonstrates that the constitutional protection of cognitive processes is a legally implementable category rather than a speculative aspiration. And it reveals the limitations of rights-articulation strategies in isolation: constitutional language alone does not generate workable doctrinal standards or enforcement mechanisms. The organic expansion of Article 21 to accommodate new constitutional interests, as demonstrated by *Puttaswamy* itself, provides a more institutionally

³² FARAHANY, *supra* note 5, at 87–99.

³³ DPDP Act, *supra* note 4.

³⁴ DPDP Act, *supra* note 4, §§ 10–11.

³⁵ Council Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (imposing restrictions on solely automated processing that produces legal or similarly significant effects on data subjects).

³⁶ Constitución Política de la República de Chile [C.P.] art. 19, núm. 1 (as amended 2021) (Chile). The amendment introduced explicit constitutional protection for “mental integrity” against non-consensual neurotechnological interference, making Chile the first state to constitutionalize neurorights.

coherent pathway for the Indian constitutional context than formal textual amendment.

The European Union's Artificial Intelligence Act³⁷ is more directly relevant to the regulatory dimension. Article 5's prohibition on AI systems deploying subliminal techniques affecting persons without their awareness, and the Act's classification of emotion recognition and biometric categorization systems as high-risk applications requiring specific transparency and oversight obligations, reflect a regulatory judgment that cognitively intrusive AI systems cannot be adequately governed through standard data protection architecture. The Act also illustrates the importance of ex ante regulatory design: its prohibitions operate prospectively on system deployment rather than reactively on demonstrated harm, addressing the constitutional injury before it is inflicted.

The neurorights framework advanced by Ienca and Andorno, encompassing cognitive liberty, mental privacy, mental integrity, and psychological continuity, has shaped both Chilean and EU approaches.³⁸ For Indian constitutional purposes, its analytical value lies not in its specific rights articulations but in its precise identification of the discrete constitutional interests that neurodata extraction implicates. These interests, namely cognitive autonomy, mental non-disclosure, and protection against cognitive manipulation, are already latent within the *Puttaswamy* framework's dignity and autonomy foundations. The comparative lesson is less about importing new rights categories than about recognizing that Indian constitutional jurisprudence already possesses the doctrinal resources to address these interests if appropriately developed.

The GDPR's classification of biometric data processed for unique identification as special category data subject to heightened processing restrictions³⁹ provides a regulatory analogue for neurodata classification. The underlying principle, that data capable of generating intimate inferences about a person warrants protection beyond what standard consent mechanisms provide, applies with equal or greater force to neurophysiological data and cognitively inferred data. The EU framework also illustrates the operational feasibility of special category regimes with distinct consent thresholds and use restrictions, a model that the DPDP Act's subordinate legislative framework could incorporate specifically for neurodata.

³⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L) (EU) [hereinafter EU AI Act]. Article 5 prohibits AI systems deploying subliminal techniques affecting persons without awareness; Article 50 imposes transparency obligations on emotion-recognition systems.

³⁸ Ienca & Andorno, *supra* note 6.

³⁹ GDPR, *supra* note 24, art. 9 (designating biometric data processed for unique identification as "special category data" subject to prohibition absent explicit consent or other prescribed ground).

VII. TOWARDS A CONSTITUTIONAL FRAMEWORK FOR MENTAL PRIVACY

A. Mental Privacy as a Distinct Article 21 Interest

The analysis in the preceding sections supports the recognition of mental privacy as a distinct, named constitutional interest within the Article 21 framework. Mental privacy, as proposed here, protects the pre-expressive cognitive domain, the space within which individuals form thoughts, develop intentions, and constitute their inner lives, from external access, extraction, and exploitation without adequate justification. As a constitutional interest, it is distinct from informational privacy because it protects not merely information the subject possesses but the cognitive substrate from which information and choices emerge; and it is distinct from decisional autonomy because it operates at a prior stage, protecting the conditions under which autonomous deliberation is possible rather than the deliberated choices themselves.⁴⁰

The constitutional foundation for this interest is already present in existing doctrine. Justice Chandrachud's recognition in *Puttaswamy* that privacy encompasses the right to determine what to disclose⁴¹ extends naturally to the pre-expressive domain: the right to determine what to disclose necessarily encompasses the right not to have undisclosed cognitive states accessed without consent. The *Selvi* holding that non-consensual mental extraction violates Article 21⁴² confirms that the constitutional protection of the mental domain is not a novel proposition; its generalization from the criminal investigation context to civilian neurotechnological contexts is the doctrinal task that the present analysis undertakes. No new constitutional language is required; what is required is the recognition that existing doctrine, properly applied, already covers the constitutional ground.

B. Cognitive Integrity as a Constitutional Standard

The second element of the proposed framework is the constitutional standard of cognitive integrity: the right not to have one's neural processes deliberately monitored, altered, or exploited without justification satisfying heightened constitutional scrutiny.⁴³ Cognitive integrity has two dimensions. Negatively, it prohibits neurotechnological intrusions that compromise the individual's capacity for autonomous cognitive functioning, including systems that exploit neural signals to influence behavior below the threshold of deliberate awareness. Positively, it requires that any actor seeking to access or process neurodata, whether state or

⁴⁰ *Puttaswamy*, *supra* note 1.

⁴¹ *Puttaswamy*, *supra* note 1.

⁴² *Selvi*, (2010) 7 SCC 263.

⁴³ FARAHANY, *supra* note 5, at 145–170 (arguing for “cognitive liberty” as the foundational constitutional value for neurotechnology governance).

private, must demonstrate a compelling interest, narrow tailoring of means, and procedural safeguards that actively protect the subject's deliberative capacity. This standard is not a new fundamental right; it is the application of existing Article 21 doctrine to the specific constitutional challenge that neural signal extraction poses.

C. Heightened Proportionality Review

The *Puttaswamy* framework endorsed a four-part proportionality test for constitutional review of privacy intrusions: legitimate aim, rational nexus, necessity in means, and proportionality *stricto sensu*.⁴⁴ For neurotechnological intrusions, the cognitive intimacy of neurodata justifies applying this framework at heightened stringency at each stage. The legitimate aim requirement should be construed strictly: commercial productivity monitoring, behavioral targeting, and actuarial risk assessment cannot constitute sufficient constitutional justification for the extraction of intimate cognitive data. The necessity requirement should demand not merely that the measure is effective but that no less cognitively invasive alternative could achieve the same aim. The proportionality balance must weight the cognitive intimacy of the intrusion heavily against the asserted benefit, recognizing that the constitutional value of mental privacy, as the substrate of autonomous personhood, is categorically greater than that of ordinary personal data.

Two implications follow for the operation of heightened proportionality review in neurotechnological contexts. First, a state interest in security or law enforcement, however weighty in other surveillance contexts, cannot automatically justify neurotechnological cognitive extraction; the heightened intimacy of the mental domain requires a correspondingly heightened demonstration of necessity that security-based justifications will rarely satisfy. Second, and of greater immediate practical relevance, private actors deploying neurotechnological systems in employment or consumer contexts cannot invoke legitimate business purposes, including workforce efficiency, user personalization, or actuarial accuracy, as constitutionally adequate justifications for cognitive extraction. The proportionality analysis under heightened scrutiny requires that the asserted benefit be of sufficient constitutional weight to justify intrusion into a domain that Article 21 treats as constitutively connected to personhood.⁴⁵

D. Inferential Restraint and Cognitive Profiling

The fourth doctrinal element is a principle of inferential restraint: cognitive inferences generated

⁴⁴ *Puttaswamy*, *supra* note 1. See also *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India) (applying proportionality analysis to internet access restrictions under Article 19).

⁴⁵ *Puttaswamy*, *supra* note 1 (Chandrachud, J., concurring). See also *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

from neurodata are constitutionally governed even where the source data was lawfully collected. Cognitive profiling, meaning the construction of detailed models of an individual's mental characteristics, emotional vulnerabilities, and deliberative patterns from neural signals, should attract categorical prohibition in institutional power contexts (employment, education, insurance) and heightened proportionality scrutiny in all other contexts.⁴⁶ The constitutional basis lies in the relationship between cognitive profiling and deliberative autonomy: a profile of sufficient granularity creates the technical capacity for behavioral manipulation that circumvents autonomous deliberation rather than engaging it. Constitutional protection of autonomous agency is rendered illusory if the conditions of deliberation can be systematically shaped through knowledge extracted from the subject's neural activity.

E. Statutory Implementation

At the statutory level, the constitutional framework proposed above requires three specific reforms to the Digital Personal Data Protection Act, 2023. First, neurophysiological data and cognitively inferred data derived from neural signals should be designated as sensitive personal data, with correspondingly heightened consent requirements, processing restrictions, and purpose limitations. Second, a provision specifically governing inferential processing should require separate, granular consent for cognitive inferences generated from neural source data, accompanied by rights to explanation and contestation. Third, a sector-specific prohibition on neurotechnological cognitive profiling in employment and educational contexts should be enacted, modeled on the European Union's approach to high-risk AI system designations.⁴⁷ These reforms would operationalize the constitutional framework within the statutory architecture and provide the practical enforcement mechanisms through which mental privacy doctrine can be given effect in the contexts where neurotechnological extraction poses the greatest constitutional risk.

VIII. CONCLUSION

The constitutional analysis in this paper has argued from a specific doctrinal observation: neurodata is constitutionally distinct from ordinary personal data because its extraction compromises not merely informational privacy but the pre-expressive substrate of decisional autonomy. The *Puttaswamy* framework, while providing the necessary constitutional foundation, requires doctrinal recalibration to address this specific challenge. Mental privacy is

⁴⁶ OECD, Recommendation of the Council on Responsible Innovation in Neurotechnology (Dec. 11, 2019) (recommending that member states adopt safeguards for neurotechnology including informed consent, data minimization, and non-discrimination principles).

⁴⁷ EU AI Act, *supra* note 26, arts. 5, 6, Annex III; GDPR, *supra* note 24, art. 9.

already latent within Article 21 jurisprudence: in the decisional autonomy strand of *Puttaswamy*, the bodily integrity dimensions of privacy, the dignity foundations of the right, and the *Selvi*⁴⁸ Court's recognition that the mental domain constitutes a constitutionally protected space. What is required is the recognition of these latent elements and the construction from them of a framework adequate to the constitutional challenge neurotechnology poses.

The Digital Personal Data Protection Act, 2023, as presently enacted, is structurally inadequate to govern neurotechnological data extraction. Its classification framework, consent architecture, and absence of inferential data governance leave the most constitutionally sensitive dimension of neurodata processing unregulated. Statutory reform is constitutionally necessary, but it cannot substitute for judicial recognition of mental privacy as a distinct Article 21 interest: without that constitutional foundation, statutory protections for neurodata will rest on policy discretion rather than principled constitutional requirement and will be vulnerable to legislative dilution. The framework proposed in this paper, comprising mental privacy as a distinct Article 21 interest, cognitive integrity as a constitutional standard, heightened proportionality review, and a doctrine of inferential restraint, builds on existing constitutional materials rather than importing foreign rights categories. Its contribution to Indian constitutional scholarship lies in demonstrating that the architecture of Article 21, properly applied to the specific constitutional challenge that neurodata poses, is sufficient to protect cognitive selfhood without requiring the language of the Constitution to change.

The broader implication is methodological. The challenge neurotechnology poses to constitutional privacy doctrine is the most acute instance of a general problem: constitutional frameworks calibrated to one technological environment being required to govern another. The *Puttaswamy* Court's recognition that fundamental rights speak to emerging conditions, specifically that they are not frozen in the technological assumptions of their moment of articulation, provides the jurisprudential basis for the doctrinal development this paper advocates. Mental privacy is not an exotic doctrinal innovation; it is the application of that recognition to the specific domain of cognitive life. The question for Indian constitutional adjudication is not whether Article 21 can protect the mental domain, but whether courts and legislators will recognize, with the urgency that emerging neurotechnological deployment demands, that it must.⁴⁹

⁴⁸ *Selvi*, *supra* note 3.

⁴⁹ *Puttaswamy*, *supra* note 1.