Page: 711-740 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.31

NEURO-RIGHTS: LEGAL FRAMEWORKS AND CHALLENGES IN PROTECTING BRAIN DATA IN THE NEUROTECHNOLOGY ERA

Apurva Verma[1]

I. ABSTRACT

The rapid advancement of neurotechnology, from medical implants to consumer brain-computer interfaces (BCIs), presents unprecedented challenges to fundamental human rights. These technologies access, monitor, and even influence neural activity, generating "neurodata", highly sensitive information revealing an individual's thoughts, emotions, and mental states. This proliferation creates urgent threats to mental privacy, cognitive liberty, and mental integrity, rendering traditional data protection frameworks inadequate. This paper examines the emerging legal and ethical paradigm of "neurorights" designed to protect the human mind. It provides a conceptual foundation for cognitive liberty, mental privacy, and mental integrity. The research critically analyses and compares nascent global legal frameworks, contrasting Chile's pioneering constitutional amendments and the EU's robust, technology-neutral GDPR with the fragmented, state-level approach in the United States. Against this global backdrop, the paper evaluates India's preparedness. It identifies a significant "judicial-legislative gap": while India's Constitution, as interpreted in landmark cases like K.S. Puttaswamy v. Union of India, offers a strong implicit foundation for mental privacy, its statutory framework, mainly the Digital Personal Data Protection Act (DPDPA), 2023, critically fails to classify neurodata as sensitive. This omission, coupled with regulatory loopholes for consumer neuro-devices, leaves individuals vulnerable. The paper concludes by recommending a multi-pronged reform strategy for India, centred on amending the DPDPA, enacting a comprehensive standalone Neurotechnology Regulation Act, and establishing a specialised national oversight authority to safeguard cognitive freedom in the neurotechnology era.

[1] BBA LLB/2nd year/4th Semester Student at Symbiosis law school, NOIDA, (India). Email: apurva.verma@symlaw.edu.in

 (ISSN: 2583-7753)

II. KEYWORDS

Neurorights; Neurodata Protection; Cognitive Liberty; Mental Privacy; Digital Personal Data Protection Act, 2023

III. INTRODUCTION

Once restrained in the realm of science fiction, it is now steadily accelerating to the convergence of neuroscience, which has given rise to the field of neurotechnology.[2] Neurotechnology is a method used to access, monitor, analyse, manipulate and emulate the structure and function of the neural systems of natural human beings.[3] A significant turning point in medical and technological history was reached in January 2024 when Elon Musk's Neuralink[4] successfully implanted its first brain chip in a human subject.[5]

This era is marked by the development of methods and instruments that establish a direct connection between any electronic device and the human neural system.[6] It makes it possible to translate human thoughts into text and, in the form of bliss, often restores mobility to the paralysed, offers novel treatments for intractable neurological and psychiatric disorders such as Alzheimer's, Parkinson's and depression, enhancing human well-being. [7] Additionally, it is anticipated that the global market for wireless brain sensors will more than double by 2030, reaching $362 million, primarily due to hospital demand and academic research, highlighting the growing importance of these technologies globally.[8]

---

[2] Yuliya Sychikova, *The State of NeuroTech: Unlocking Minds & New Markets*, DataRoot Labs (Oct. 17, 2023), https://datarootlabs.com/blog/the-state-of-neurotech-unlocking-minds-and-new-markets.
[3] OECD, *Neurotechnology Toolkit: Implementing the OECD Recommendation on Responsible Innovation in Neurotechnology* (Apr. 2024), https://www.neuron-eranet.eu/wp-content/uploads/neurotech-toolkit-implementing-OECD-Recommendation.pdf.
[4] Elon Musk's Neuralink Implants Brain Chip in First Human, Reuters (reuters.com).
[5]Kamal Kumar, The Dawn of Neurotechnology and its Legal Challenges, SCC Times (0ct. 17,2025) , https://www.scconline.com/blog/post/2025/10/17/the-dawn-of-neurotechnology-and-its-legal-challenges/#:~:text=fundamental%20concerns%20about%20mental%20privacy%2C%20cognitive%20liberty%2C%20and%20the%20very%20essence%20of%20human%20autonomy.
[6] Philipp Kellmeyer, 'Neurorights': A Human Rights–Based Approach for Governing Neurotechnology, 412 Cambridge Univ. Press (2022).
[7] Lyric A. Jorgenson et al., The BRAIN Initiative: Developing Technology to Catalyse Neuroscience Discovery, 370 PHIL. TRANSACTIONS ROYAL SOC'Y B BIOL. SCI. (2015).
[8] Matej Mikulic, Wireless brain sensors market distribution worldwide in 2020 and 2030, by end user, Statista, (Feb. 21, 2025).

With applications spanning from advanced medical diagnostics and treatment to cognitive therapeutics and consumer-grade Brain Computer Interfaces (BCIs), these technologies generate highly sensitive and intimate brain data, which is referred to as neurodata. Such neurodata can reveal thoughts, emotions, perceptions, memories, preferences, and mental states, making it among the most personal and private forms of information, endangering the privacy of the persons.[9] The same technologies that work as a boon can also be used for surveillance, manipulation and control. This contrast can create a complex policy landscape, where innovation should tactfully handle the imperative protection of fundamental human rights.[10] In the present scenario, the proliferation of consumer neurotechnology devices, from wellness headbands to gaming interfaces, is collecting vast datasets of neural information with almost zero regulatory oversight.[11]

To combat threats posed by neurotechnology, a new approach known as "neurorights" has emerged. These are characterised as natural, social, legal, or ethical principles of entitlement and freedom that pertain to a person's cerebral and mental domain. [12]

A. Research Objectives

1. To examine the conceptual foundations of neurorights, including cognitive liberty, mental privacy, and mental integrity, within contemporary human rights jurisprudence.
2. To critically analyse global regulatory approaches toward neurodata protection, particularly in Chile, the European Union, and the United States.
3. To evaluate the adequacy of India's existing constitutional and statutory framework in addressing challenges posed by neurotechnology.
4. To identify regulatory gaps in the Digital Personal Data Protection Act, 2023 and related statutes concerning neurodata governance.

[9] Kellmeyer, supra note 3, at 414.
[10] Rafael Yuste, *It's Time for Neuro-Rights*, Horizons: J. Int'l Rel. & Sustainable Dev., Winter 2021, Issue No. 18 https://www.cirsd.org/en/horizons/horizons-winter-2021-issue-no-18/its-time-for-neuro--rights.
[11] Dias., supra note 6.
[12] Dias, supra note 6.

5. To propose a structured reform roadmap for establishing a comprehensive neurorights framework in India.

B. Research Questions

1. Does India's current statutory framework adequately protect neurodata generated by emerging neurotechnologies?
2. Can constitutional protections under Articles 19 and 21 sufficiently safeguard mental privacy and cognitive liberty in the absence of dedicated neurorights legislation?
3. How do international models, particularly Chile's constitutional amendment and the EU's GDPR framework, address neurodata differently from India?
4. What legislative and institutional reforms are necessary to ensure effective protection of neurorights in India?

C. Research Hypotheses

1. The existing constitutional protections under Articles 19 and 21 provide a foundational basis for neurorights but remain insufficient without explicit statutory recognition of neurodata as a distinct and sensitive category of information.
2. India's Digital Personal Data Protection Act, 2023 fails to adequately safeguard neurodata due to the absence of express classification and enhanced consent standards.
3. A comparative analysis of global frameworks demonstrates that jurisdictions adopting explicit constitutional or statutory recognition of neurorights provide stronger safeguards than those relying solely on general data protection principles.

D. Research Methodology

This study adopts a doctrinal and comparative legal research methodology. The doctrinal component involves critical analysis of constitutional provisions, statutory

instruments, judicial precedents, and regulatory frameworks relevant to neurorights and data protection in India.

The comparative component evaluates international approaches, particularly constitutional reforms in Chile, the regulatory architecture of the European Union under the GDPR and AI Act, and the fragmented federal–state model in the United States.

Primary sources include constitutional texts, legislation, judicial decisions, and international recommendations. Secondary sources comprise scholarly articles, policy papers, and interdisciplinary research on neurotechnology ethics and governance. The study is analytical in nature and seeks to identify normative gaps and propose reform-oriented solutions.

E. Research Problem

This research paper examines the international impact of neurotechnology developments and critically analyses how various nations are preparing to tackle the new issues surrounding neurorights. It discusses legal, ethical, and policy frameworks across the globe. The research evaluates India's preparedness in this evolving domain, highlighting regulatory gaps and socio-legal issues in safeguarding mental privacy and cognitive freedom. By a comparative analysis of global strategies, the paper seeks to suggest legal reforms for India to safeguard neurorights amid rapid advances in neurotechnology successfully.

F. Literature Review

The scholarly discourse on neurorights has evolved rapidly in response to advances in neurotechnology. Marcello Ienca and Roberto Andorno's seminal work, *"Towards New Human Rights in the Neurotechnology Age"* (2017), laid the normative foundation for recognising rights such as cognitive liberty, mental privacy, and mental integrity as extensions of existing human rights principles. Their framework argues that traditional privacy doctrines are insufficient to address the unique intrusiveness of neurodata.

Rafael Yuste et al., in "*Four Ethical Priorities for Neurotechnologies and AI*" (Nature, 2017), emphasised the urgent need for proactive governance mechanisms to prevent misuse of brain-computer interfaces and AI-driven neural systems. They proposed safeguarding personal identity, agency, and mental autonomy as core regulatory priorities.

Subsequent scholarship has expanded upon these foundations, examining the adequacy of data protection regimes such as the GDPR in regulating neurodata and analysing Chile's pioneering constitutional amendment as a model of rights-based governance. Comparative legal studies highlight the growing tension between innovation-driven regulatory models and rights-centric frameworks.

In the Indian context, academic discourse remains limited and largely confined to privacy jurisprudence following *K.S. Puttaswamy v. Union of India*. While this jurisprudence provides a constitutional anchor for mental privacy, dedicated scholarship on statutory neurorights protection remains underdeveloped, thereby underscoring the necessity of the present study.

IV. CONCEPTUAL FOUNDATIONS OF NEURORIGHTS

Neurorights encompass cognitive liberty, mental privacy, and mental integrity, aiming to preserve human dignity and freedom of thought in an era where brain function can be analysed and manipulated. The normative articulation of these rights has been most prominently developed in the work of Marcello Ienca and Roberto Andorno, who argue for the recognition of new human rights tailored to the neurotechnology age.[13]

Cognitive liberty, regarded as the foundational pillar of neurorights, refers to an individual's fundamental right to exercise sovereign control over their own mental processes, free from external coercion or manipulation. It includes both the freedom from non-consensual intrusion into neural activity and the freedom to voluntarily use

[13] Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Neurotechnology Age' (2017) 13(3) *Life Sciences, Society and Policy* 5.

neurotechnology for self-directed cognitive enhancement.[14] It includes both a negative freedom and a positive freedom: -

- **Negative Liberty -** It is the right to freedom from external, unconsented intrusion into one's mental processes. It is the right not to allow the use of neurotechnology for monitoring, manipulating, or modifying one's mind. This is protective mainly, preventing the individual from being coerced and manipulated.[15]
- **Positive Liberty -** This is the ability to have the freedom to use neurotechnology to change or improve one's own emotional and cognitive states. It supports the autonomy of an individual to have control over his own mental life, including deciding to seek cognitive improvement.[16]

This dualism creates complexity in regulating neurotechnology. A framework that does no more than shield against harm (negative liberty) without also considering the right to self-improvement (positive liberty) would be inadequate and might unnecessarily suppress innovation and individual freedom.

Mental privacy denotes the protection of a person's inner thoughts, emotions, memories, and cognitive processes from unauthorised access, storage, or inference. It extends beyond conventional informational privacy by safeguarding neural data that constitutes the forum internum of the individual.[17] It extends beyond the concept of data privacy, as it is related not just to information about a person but to their very neural activity that constitutes their inner life.[18] The UN Special Rapporteur for the right to privacy has highlighted the significance of this notion, pointing to the unprecedented degree of insight into a person's identity that can be gained from

[14] Nita A Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[15] Sjors Ligthart et al., *Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights'*, 32 Cambridge Q. of Healthcare Ethics 461 (2023).
[16] Id.
[17] Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Neurotechnology Age' (2017) 13(3) *Life Sciences, Society and Policy* 5.
[18] Beth Do et al., Privacy and the Rise of "Neurorights" in Latin America, Future of Privacy Forum (Mar. 20, 2024), https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/.

neurodata.[19] Likewise, UNESCO's International Bioethics Committee (IBC) has named mental privacy as a significant issue, acknowledging that the capacity to read brain function could represent a deep "affront to privacy of thought.". [20]Mental privacy is then envisioned as the last frontier of privacy, protecting the sanctity of the *forum internum* in a world where it is fast becoming technologically accessible.[21]

Mental integrity refers to the right to preserve the continuity, authenticity, and wholeness of one's mental life against non-consensual alteration or technological interference.[22] The most likely threat to mental integrity involves neurotechnology that circumvents an individual's rational control in a way that leads to a feeling of alienation from one's own mental states. [23] It has been established as a firm basis in the existing legal framework. Article 3 of the European Union Charter of Fundamental Rights unequivocally guarantees the "right to the integrity of the person," which it defines as encompassing both "physical and mental integrity."[24]

A central need for a separate framework of neurorights is due to neurodata represents a fundamentally distinct category of information, rendering conventional data protection frameworks like the Digital Personal Data Protection Act, 2023 or the EU's General Data Protection Regulation (GDPR), inadequate.[25] Neurodata refers to data collected from devices that monitor an individual's neural activity, which can then be used to infer cognitive functions.[26] While existing laws may cover neurodata under

[19] Office of the United Nations High Commissioner for Human Rights, *UN Expert Calls for Regulation of Neurotechnologies to Protect Right to Privacy*, UN Press Release (Mar. 12, 2025), https://www.ohchr.org/en/press-releases/2025/03/un-expert-calls-regulation-neurotechnologies-protect-right-privacy.
[20] UNESCO, Ethics of Neurotechnology, https://www.unesco.org/en/ethics-neurotech.
[21] UNESCO, *Report of the International Bioethics Committee (IBC) on the Ethical Issues of Neurotechnology*, U.N. Doc., (2021), https://unesdoc.unesco.org/ark:/48223/pf0000378724
[22] Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Neurotechnology Age' (2017) 13(3) *Life Sciences, Society and Policy* 5.
[23] Kellmeyer, supra note 3, at 418.
[24] Panel for the Future of Science and Technology (STOA), *The Protection of Mental Privacy in the Area of Neuroscience: Societal, Legal and Ethical Challenges* (July 2024), https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf.
[25] Kellmeyer, Supra note 3, at 417.
[26] Rafael Yuste et al., *Four Ethical Priorities for Neurotechnologies and AI*, Nature (2017).

broad definitions of "personal data" or "biometric data," they would have failed to capture its unique nature and the unprecedented risks it poses. [27]

V. OVERVIEW OF GLOBAL LEGAL FRAMEWORKS

The global regulatory response to neurotechnology reflects a growing recognition of the need to safeguard neurorights while balancing progressive scientific innovation. Different jurisdictions have adopted varied approaches ranging from constitutional reform to statutory reform.

1. **Latin American nations** - Constitutional amendment paths have been taken, showing the strong inclination towards human rights jurisprudence.
    - **Chile –** In 2021, it became the first country in the world to amend its constitution to address the challenges posed by neurotechnology.[28] Article 19 of the Chilean Constitution was amended to explicitly protect "mental integrity" and "neural data," providing the strongest possible legal and symbolic safeguard against potential misuse.[29] In the landmark judgement of 2023, the Chilean Supreme Court case Girardi v. Emotiv was the world's first judicial decision on neurorights, showcasing the direct effect of Chile's 2021 constitutional reform, safeguarding mental integrity and neural information. The Court ruled that Emotiv's holding of anonymised brain data without express consent infringed this right, ordering the erasure of all data stored. Rejecting anonymisation as a defence mechanism, it stressed that secondary use necessitates express, informed consent.[30]
    - **Brazil –** Several initiatives are underway reflecting a multi-facet approach. These include debate for amendment to the federal constitution to safeguard "mental integrity" and a bill that would modify Brazil's General Data Protection Law (LGPD) to categorically make neurodata an independent

[27] TrustArc, *Neurotechnology Privacy: Safeguarding the Next Frontier of Data* (2025), https://trustarc.com/resource/neurotechnology-privacy-safeguarding-the-next-frontier-of-data/
[28] Beth, supra note 16, at "Chile: The first country to protect "mental integrity" in its Constitution".
[29] Carlos Amunategui Perello, Neurorights.: The World's First Court Case, 28 INTELL. PROP. & TECH. L. J. 123 (Spring 2024).
[30] Hunter T. Carter, *Neural Rights: Landmark Ruling*, AFS Int'l (Oct. 18, 2023), https://www.afslaw.com/perspectives/news/neural-rights-landmark-ruling.

type of "sensitive data.". In December 2023, the state of Rio Grande do Sul amended its own constitution to encompass neurorights as a constitutional principle, marking a significant milestone.[31]

- **Mexico –** Lawmakers are considering constitutional reform seeking to enshrine individual identity and mental integrity protections as constitutional rights.[32]
- **Argentina –** The proposed bills seek to create a bicameral committee to create a holistic neurorights framework. [33]

2. **European Union** - In contrast to the Latin American approach of legislating new specific rights, the European Union has adopted a model that leverages the existing EU's technologically neutral legal framework to govern neurotechnology. Lawmakers believe that their sufficient to accommodate the challenges posed by new technologies.[34]
    - **General Data Protection Regulation (GDPR) –** The cornerstone of the EU's approach is the GDPR, which is regarded as the most comprehensive data protection law. The GDPR does not explicitly define "neurodata." However, its broad definition of personal data under Article 4(1) may encompass information relating to the physical, physiological, or mental identity of a natural person. More significantly, Article 9 of the GDPR classifies data concerning health, biometric data, and genetic data as "special categories of personal data," the processing of which is prohibited by default unless specific conditions are met.[35] Neurodata, depending on its nature and use, may therefore fall within the scope of Article 9, triggering heightened consent and compliance obligations. Furthermore, the processing of such sensitive data on a large scale would raise the need to conduct a Data Protection Impact Assessment (DPIA) under Article 35,[36] forcing

[31] Joseph A. Tomain, Ninth Amendment Neurorights, 100 IND. L.J. 1959 (Summer 2025).
[32] Id.
[33] Id.
[34] Centre for Future Generations (CFG), *Mapping neurotech governance: An overview of European regulations and international frameworks* (Sept. 2025), https://cfg.eu/neurotech-governance-map/.
[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1, art 9.
[36] GDPR, *supra* note 33, art. 35.

organisations to systematically identify and mitigate privacy risks before launching a product. [37]

- **The EU Artificial Intelligence Act –** It established a risk-based approach to regulate products and services that incorporate artificial intelligence. It explicitly acknowledges the potential of BCIs for manipulative purposes, directly referencing the risk of neurotechnology.[38] This act includes an AI system that establishes a "subliminal technique beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm". [39]
- **Medical Device Regulation –** It imposes a stringent requirement for clinical validation, safety, and post-market surveillance, ensuring a high degree of performance and patient safety. Primarily, it focuses on physical safety rather than data ethics; it adds specific regulations for high-risk applications. [40]

3. **United States** – It opted for fragmented and different laws for the federal and state levels. Absence of a comprehensive law leads to significant gaps in the regulation of neurotechnology. [41]At the federal level, existing laws provide only narrow, sector-specific protections that fail to cover the majority of neurotechnology applications.[42]
    - **The Health Insurance Portability and Accountability Act (HIPAA)-** The primary federal law governing health information. However, its scope is

[37] Nicholas Martin et al., *THE DATA PROTECTION IMPACT ASSESSMENT ACCORDING TO ARTICLE 35 GDPR,* Fraunhofer Institute, (Mar. 2025), https://publica-rest.fraunhofer.de/server/api/core/bitstreams/e6b91341-71f4-409b-8446-03432231a0d0/content.
[38] Centre for Future Generations, *Mapping neurotech governance* (Sept. 29, 2025), https://cfg.eu/neurotech-governance-map/.
[39] VeraSafe Data Protection Blog, *Mental Privacy in Neurotech and the Growing Risk for Organizations,* VeraSafe (Aug. 22, 2025), Mental Privacy in Neurotech and the Growing Risk for Organizations
[40] Cornelia Kutterer & Anamaria Corca, *Neurotech & EU Regulation: Innovation Meets Rights*, CONSIDERATI, (Apr. 30, 2025), https://www.considerati.com/publications/neurotechnology-in-the-eu-balancing-innovation-with-rights-based-regulation/.
[41] Kristina Iliopoulos & Nancy L. Perkins, Neural Data Privacy Regulation: *What Laws Exist and What Is Anticipated?,* Arnold&Porter, *(July 22, 2025), Neural Data Privacy Regulation: What Laws Exist and What Is Anticipated? | Advisories | Arnold & Porter*
[42] Tomain, supra note 28, at 1961.

narrowly limited to "covered entities" such as healthcare providers, health plans, and healthcare clearinghouses and their business associates. [43]This framework effectively regulates neurodata collected in a clinical context but offers no protection for data generated directly by neurotechnology devices, such as wellness headbands, meditation aids, or VR gaming headsets, which fall outside its purview. [44]

- **The Federal Trade Commission (FTC) Act-** It has the authority to take enforcement action against companies engaging in "unfair or deceptive acts or practices" under Section 5 of the FTC Act. [45]This could be used to prosecute neurotech companies that make fake claims about their privacy practices or misuse consumer data in ways that cause substantial harm. However, it does not establish a proactive regulatory framework with clear rules for consent, data minimisation, or user rights, leaving companies without clear guidance and consumers without outright protection. [46] These gaps in federal law have created a need for legislative action at the state level, mandating different regulatory models, therefore leading to an inconsistent legal framework.

4. **Colorado-** In 2024, Colorado became the first U.S. state to explicitly protect neurodata by enacting Senate Bill 24-222, which amended the Colorado Privacy Act (CPA) to include "neural data" within the definition of sensitive data.[47] This amendment is significant because the processing of sensitive data under the CPA requires prior, affirmative (opt-in) consent from consumers, thereby

[43] U.S. Dep't of Health & Human Servs., Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[44] VeraSafe, supra note 38, at "Are Existing Privacy Laws Sufficient?".
[45] Lena Zinne et al., A New Era of Privacy Enforcement: Lessons for Digital Health Players, SheppardMullin, (Sep. 11, 2025), https://www.sheppardhealthlaw.com/2025/09/articles/privacy-and-data-security/a-new-era-of-privacy-enforcement-lessons-for-digital-health-players/.
[46] PROTECTING AMERICA's CONSUMERS, Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule, FEDERAL TRADE COMMISSION, (Aug. 2024), https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach.
[47] Colorado Senate Bill 24-222 (2024), amending the Colorado Privacy Act, Colo Rev Stat § 6-1-1303.

extending enhanced statutory safeguards to neurodata collected by private entities.[48]

5. **California-** Also, California amended its California Consumer Privacy Act (CCPA) to add "neurodata" to its definition of "sensitive personal information". However, the CCPA provides significantly weaker protection regulations as it doesn't require upfront consent from the consumers, giving them a limited right to opt out of the use and disclosure of their sensitive data for purposes other than their required need. [49]

This difference in Colorado's opt-in model and California's opt-out model, along with different definitions of what constitutes "neural data," creates significant compliance challenges for companies operating nationwide. [50]

VI. THE ROLE OF INTERNATIONAL ORGANISATIONS

Against these stringent legislative models are non-binding principles, recommendations, and best practices developed by international organisations. These frameworks, though not directly enforceable, play a crucial role in shaping global norms and guiding the formation of national policies and corporate ethics.

1. **The Organisation for Economic Co-operation and Development (OECD) -** In 2019, the OECD Council adopted the responsible recommendation in Neurotechnology, the first international standard in this domain.[51] The Recommendation is based on nine core principles designed to guide governments and innovators:
   - Promote responsible innovation.
   - Prioritise safety assessment.
   - Promote inclusivity.
   - Foster scientific collaboration.

[48] Perkins, supra note 40, at "California and Colorado Enactments".
[49] Id.
[50] Jameson Spivack, *The "Neural Data" Goldilocks Problem: Defining "Neural Data" in U.S. State Privacy Laws, FUTURE OF PRIVACY FORUM*, (Aug. 12, 2025).
[51] GeeksforGeeks, OECD | Full Form, Objectives, Organisational Structure and Functions (Dec. 29, 2023), https://www.geeksforgeeks.org/general-knowledge/oecd-full-form-objectives-organisational-structure-and-functions/.

- Enable societal deliberation.
- Enable the capacity of oversight and advisory bodies.
- Safeguard personal brain data and other information.
- Promote cultures of stewardship and trust.
- Anticipate and monitor potential unintended use and/or misuse. [52]

VII. INDIA'S CURRENT LEGAL AND REGULATORY LANDSCAPE

India lacks explicit legislation on neurotechnology, yet its constitutional jurisprudence, as interpreted by the Supreme Court, provides a robust foundation for its recognition. [53]

1. **Article 21 –** It states that "No person shall be deprived of his life or personal liberty except according to procedure established by law".[54] Over the years, through judicial precedents Supreme Court has transformed this provision from a mere guarantee against arbitrary executive action into a rich repository of positive rights.[55] The broad interpretation of "life" has been held to mean a life of dignity, not mere animal existence, and "personal liberty" has been broadened to encompass a wide array of rights essential for a fulfilling life, including the right to privacy, autonomy, and mental peace. It incorporates various rights, providing a constitutional edge necessary to protect claims arising from technological advancements, including those posed by neurotechnology.[56] In *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, the nine-judge Bench unanimously affirmed the right to privacy as a fundamental right intrinsic to life and personal liberty under Article 21. Justice D.Y. Chandrachud's plurality opinion is particularly significant, as it articulated the doctrine of informational

[52] Testbook, OECD Full Form: Learn its Full Form, Objectives and Functions, https://testbook.com/full-form/oecd-full-form.
[53] The Dawn of Neurotechnology and its Legal Challenges, SCC Online Blog (Oct. 16, 2025), https://www.scconline.com/blog/post/2025/10/17/the-dawn-of-neurotechnology-and-its-legal-challenges/.
[54] M. Aishwarya Lakshmi, Neurotechnology and the Law: Should Thoughts Be Protected as Fundamental Rights?, Lawful Legal (July 10, 2025)
[55] Susmit Mukherjee, Securing Neuro-Privacy: An Argument for Recognition and Practical Regulation, Vidhi Centre for Legal Policy (Sept. 16, 2025), https://vidhilegalpolicy.in/blog/securing-neuro-privacy/.
[56] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

self-determination and recognised privacy as encompassing control over the dissemination and use of personal information. This reasoning is directly relevant to neurodata, which represents the most intimate form of informational identity.[57] This landmark judgment provides the direct constitutional basis for neuro-rights in India through several key principles:

- **Information Privacy:** The Court recognised an individual's right to safeguard their personal information. This principle must logically and necessarily extend to neurodata. If an individual has a right to control their demographic or financial data, that right must extend with even greater force to the data collected by their own brain, which is the most intimate and personal information that can exist.[58]
- **Self-Determination:** Building on informational privacy, the Court upheld the right to make independent decisions regarding one's private life and to determine for themselves what information crosses the boundary from the private to the public sphere. Neurotechnology that can read unexpressed thoughts or subconscious preferences directly challenges this right by potentially extracting information that an individual has not chosen to share, thereby infringing upon their decisional autonomy.[59]
- **The Inviolability of the Mind:** Crucially, the Puttaswamy judgment explicitly stated that the mind is an "inseparable element of an individual's personality" and that its inviolability is core to the right to privacy. This judicial recognition of the sanctity of the mental sphere provides a direct and powerful constitutional anchor for the right to mental privacy, establishing the mind as a protected space free from unwarranted intrusion.[60] In *Selvi v State of Karnataka* AIR 2010 SC 1974, the Supreme Court ruled that the compulsory administration of narco-analysis, polygraph examinations, and the Brain Electrical Activation Profile (BEAP) test

[57] Gokul. B, NEUROTECH AND THE INDIAN CONSTITUTION, Record Of Law (Aug. 29, 2025).
[58] Kumar, supra note 3, at "Neurotechnology and its constitutional implications".
[59] Somdyuti Das & Rajdeep Ghosh, *Neuro-Rights in India: A Legal Framework for the Future*, 6(1) Bennett J. Legal Stud. 109 (Apr. 2025).
[60] *Id.*

violated the right against self-incrimination under Article 20(3) and the right to personal liberty under Article 21. The Court did not directly adjudicate upon the Brain Electrical Oscillation Signature (BEOS) technique, which, although related, is a distinct methodology developed separately and has arisen in trial court proceedings. Under Article 20(3) [61] and the right to personal liberty under Article 21[62]. This puts a formidable constitutional barrier against the coercive use of any neurotechnology, whether for criminal investigation or other state purposes, without the free and informed consent of an individual.

2. **Article 19(1)(a)[63] –** It guarantees the right to freedom of speech and expression. It expands to protect a wide range of expression; therefore, this article also covers a robust foundation for cognitive liberty. As neurotechnology advances, particularly in fields capable of accessing, manipulating, or surveilling brain data, any infringement on freedom of thought becomes a direct infringement of this constitutional right. [64]
3. **Article 51A(h)[65] -** It mandates every citizen "to develop scientific temper, humanism and the spirit of inquiry and reform." This duty not only encourages society to embrace technological progress in neurotechnology and related fields but also expects responsible use and ethical oversight. It signals the government's and society's shared responsibility to ensure innovation does not outpace the protection of individual rights, like mental privacy. [66]

VIII. REGULATING PRIVATE ACTORS IN THE NEUROTECH SPHERE

Since fundamental rights under the constitution are enforced against the state, a crucial piece of the constitutional question arises: whether these rights can be enforced

[61] Constitution of India, Art. 20 (3).
[62] Constitution of India, Art. 21.
[63] Constitution of India, Art. 19(1)(a).
[64] Sinchana M.R. & R.S. Sanjanaa, *Right to cognitive liberty in a Transhumanism Era: A Case for Integration within Indian Legal Framework*, NUALS Law J. Blog (June 29, 2023).
[65] Constitution of India, Art. 51 A(h).
[66] Dr.P.Ramesh, Scientific Temper in Indian Education System - A Historical Perspective, 20(12) **Neuroquantology** 4669 (Dec. 2022),

against private companies, which are at the forefront of developing and deploying neurotechnology? The Supreme Court's (2023) decision in Kaushal Kishore v. State of Uttar Pradesh challenged this notion, with the majority holding that fundamental rights under Articles 19 and 21 can also be enforced against private persons and entities. [67]

The implication of this ruling for neuro-rights is profound. It suggests that a neurotechnology company, such as Neuralink or a manufacturer of a consumer BCI headset, could be directly held accountable under the Constitution for violating an individual's right to mental privacy. However, this judgment has been criticised for its "unsound reasoning" and represents a departure from settled jurisprudence, making its application uncertain. [68]While the judiciary has been remarkably progressive in expanding rights to meet new technological challenges, the legislature has remained reactive. [69]

IX. STATUTORY GAPS IN THE INDIAN FRAMEWORK

Despite having a strong constitutional foundation for neuro-rights, India has not specifically legislated a comprehensive statutory framework to protect neuro-rights. Existing laws were designed for a different technological era and are ill-equipped to handle the unique challenges posed by neurotechnology.

1. **The Digital Personal Data Protection Act, 2023 (DPDPA)** - is a statutory framework that safeguards personal data. However, it hasn't included neurodata in its definition of "sensitive personal data," which provides higher standards of protection, including the need for explicit consent for processing. By aiming for a broad, principle-based framework, the law fails to recognise the qualitative difference between neurodata and other forms of personal information. [70] Beyond the DPDPA, other related statutes like the Information

[67] *Kaushal Kishore v. State of Uttar Pradesh*, (2023) SCC OnLine SC 123.
[68] Das, supra note 60, at 45.
[69] Shubham Kumar, "*Judicial Activism and Technology Rights in India*," 12 Indian Law Journal, 112, 134 (2024)
[70] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act*, 2023, § 3(n) (India).

Technology Act, 2000, Medical Device Rules,2017 and the Mental Healthcare Act, 2017 also fall short of providing adequate protection.

2. **Information Technology Act, 2000 -** The IT Act and its associated rules, such as the Sensitive Personal Data or Information (SPDI) Rules of 2011, are the precursors to the DPDPA. They are fundamentally outdated and were designed to govern conventional digital data and cybersecurity threats. Their definitions and scope are too narrow to interpret or regulate the complex challenges posed by subconscious data collection and cognitive manipulation inherent in neurotechnology. [71]
3. **Medical Device Rules, 2017** - The regulation of neurotechnology hardware is governed by the Central Drugs Standard Control Organisation (CDSCO) under the Medical Devices Rules. While clinical devices like medical-grade EEG machines are classified and require regulatory approval, a critical loophole exists for the burgeoning consumer neurotechnology market. Devices marketed for non-medical purposes like "wellness," "meditation," or "gaming" can completely sidestep these stringent regulations, as long as they do not make explicit medical claims. This creates an artificial and dangerous regulatory boundary. An EEG is an EEG, regardless of its marketing. The data it collects is identical in nature and sensitivity. This regulatory gap exposes a large number of consumers to a risk of their sensitive neurodata being easily accessible to marketers without consumers' consent. [72]
4. **Mental Healthcare Act, 2017** - The scope of this Act is restricted to the context of mental healthcare, despite the fact that it is essential for defending the rights of people with mental health conditions and emphasises concepts like autonomy and consent. The broad range of non-clinical uses of neurotechnology in consumer markets, education, and workplaces cannot be covered by it. [73]

[71] Information Technology Act, 2000, § 43A; Sensitive Personal Data or Information Rules, 2011 (India).
[72] Medical Device Rules, 2017, Schedule VI (India); Vidhilegalpolicy.in, *Securing Neuro-Privacy* (2025).
[73] Mental Healthcare Act, 2017, § 3(1), (India).

This "judicial-legislative gap" means that while a constitutional remedy might exist in theory, it remains abstract, uncertain, and largely inaccessible to the average citizen. This underscores the absolute necessity for a proactive, multi-layered legislative and institutional reform is urgently required to secure the final frontier of human freedom.[74]

X. THE ADMISSIBILITY OF NEURO-EVIDENCE

The Indian Evidence Act of 1872 governs the use of neurotechnology in the Indian legal system, which presents both legal and scientific difficulties, especially when it comes to gathering evidence. Such methods, particularly the use of Brain Electrical Oscillation Signature (BEOS) profiling, have a contentious past in India.

In *State of Maharashtra v Aditi Sharma*, Sessions Court No 508/2007, Pune (decided 12 June 2008), the accused was convicted by the Sessions Court, with the judgment partly relying on results derived from a BEOS test. The decision generated substantial controversy concerning the scientific validity and evidentiary reliability of such techniques. Subsequently, the conviction was subject to challenge, and the accused was released on bail, reflecting the unsettled legal and scientific status of neuro-evidentiary methods in India.[75]This history has created significant judicial scepticism. This position was further solidified by the Supreme Court's decision in Selvi v. State of Karnataka, which was based on the fundamental constitutional principle that forcing an accused person to submit to such a test is a violation of their rights under Articles 20(3) and 21 rather than on the validity of the technology. [76]Therefore, it would still be unconstitutional in India to require the use of a neuro-evidentiary technique in a criminal investigation, even if it were proven to be 100% accurate. In the Indian legal system, this establishes a high bar for the admissibility of neuro-

[74] Shweta Bajaj, *Regulating Neural Data: Challenges and Opportunities in India*, 12 Asian Journal of Law and Technology, 2, 203-232 (2025).
[75] S*tate of Maharashtra v. Sharma*, (2008) Cr. L.J. 1628 (Bom); see also Anjali Pai, "*Brain Fingerprinting in India: Scientific Validity and Legal Challenges*," Indian J. of Forensic Med. & Toxicology (2018).
[76] Supra note 62.

evidence, emphasising the importance of constitutional rights over technological prowess.[77]

XI. CHALLENGES IN PROTECTING NEURODATA IN INDIA

The legislative gaps in India's legal system have resulted in a number of significant ethical and practical issues that threaten the fundamental basis of individual autonomy. This disparity illustrates why a simple extension of the existing laws is insufficient to maintain mental integrity and why a new paradigm is required.

1. **Reassessing the Concept of Informed Consent –** The ethical and legal frameworks that regulate data and medical procedures have historically depended on the idea of "informed consent." But when it comes to neurotechnology, this model is essentially flawed. For a number of reasons, the typical "click-wrap" consent form, in which users accept long terms and conditions they hardly ever read or comprehend, is completely insufficient. [78]
2. **The Ambiguity of Ownership and Control –** Who owns a person's neurodata is a fundamental question in Indian law that has not yet been resolved. In the absence of a clear statutory provision, ownership is typically determined by contract law, specifically the terms of service or user agreements provided by neurotechnology companies. These contracts are always written to give the business extensive, perpetual, and frequently exclusive rights to gather, use, analyse, and make money off of the user's neural data. The most private parts of a person's identity, their neural patterns and cognitive processes, are essentially turned into a corporate asset by this default legal arrangement, which can be bought and used like any other resource[79]
3. **The Dual Threat of Corporate and State Surveillance –** This lack of legal protection, coupled with a lack of clarity regarding ownership, thus creates a fertile ground for two major threats to cognitive liberty.

[77] G. Manjunath & V. Jayanth, *Legal Challenges in Adopting Neuro-Evidence in India*, 12 Indian Law Review, 3 (2024).
[78] Nita Farahany et al., *Recognizing Neuroprivacy as a Legal Right in the Age of Brain-Computer Interfaces*, 70 Stan. L. Rev. 889 (2018).
[79] Goering, supra note 6, at 832.

- **Commercial Exploitation:** Neural data represents the final frontier of what Shoshana Zuboff has termed "surveillance capitalism," a system in which human experience is translated into behavioural data for prediction and commercial profit.[80] In the neurotechnology context, firms may deploy neural data for highly sophisticated forms of neuromarketing, analysing subconscious responses to stimuli in order to shape consumer behaviour with unprecedented precision. Such practices risk enabling the construction of granular psychological profiles capable of predicting not merely purchasing habits, but political inclinations, emotional vulnerabilities, and intimate cognitive patterns, thereby intensifying concerns regarding autonomy and mental self-determination.
- **State and Employer Surveillance:** The possibility of abuse is not confined to commerce. Employers in the workplace might use neuro-monitoring devices to monitor employee attention, engagement, or levels of stress as a means of creating an environment of constant cognitive surveillance and pressure to perform. The state could also be tempted to employ such technologies as a form of "thought policing," monitoring citizens for dissenting thoughts or even pre-criminal intent, a dystopian prospect that is already being pursued in some authoritarian states.[81]

4. **Cognitive Manipulation and Algorithmic Bias -** The most profound and existential threat posed by neurotechnology is not merely a function of reading from the brain but its emerging capacity to write to it. This raises the spectre of cognitive manipulation-a process that threatens the very idea of free will and personal identity.
    - **Erosion of Psychological Continuity:** "Smart" BCIs and neuro-stimulation devices are being developed with the capability to "nudge"

[80] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
[81] Elizabeth E. Joh, *The New Surveillance: Policing, Data, and Protecting the Public Interest*, 57 Wm. & Mary L. Rev. 1567 (2016).

users' decisions, enhance certain moods, or suppress others, often based on their past neural data. While potentially beneficial for therapeutic purposes, this technology could also be used to subtly influence choices and preferences over time. The cumulative effect of these micro-interventions could gradually alter a person's personality, beliefs, and core identity without a single, identifiable moment of harm. This is not a traditional privacy breach; it is a slow-motion violation of the right to psychological continuity. Current legal frameworks, which are designed to address discrete events of harm, are completely unequipped to recognise or remedy this insidious form of cognitive manipulation.[82]

- **Algorithmic Bias:** The algorithms that interpret complex neural data are not neutral. They are trained on datasets, which can reflect existing social biases. This creates a significant risk that neurotechnology might be used to discriminate against individuals. For instance, such a biased algorithm, when used in hiring, may incorrectly flag the neural patterns of a candidate as indicative of low focus or high anxiety, leading to unfair discrimination. Its use in the criminal justice system could see certain groups being labelled as high-risk and erode the principle of equality before the law.[83]

XII. COMPARATIVE ANALYSIS BETWEEN INDIA AND THE GLOBAL FRAMEWORK

The legal framework for neural data protection in India originates from constitutional privacy rights under Article 21 and landmark cases like Puttaswamy, which built a strong but implicit protection for mental privacy and cognitive liberty. [84]However, India's primary data protection statute, the Digital Personal Data Protection Act, 2023, fails to even recognise neural data as a sensitive category. Therefore, it creates

[82] Hannah Maslen et al., *Brainjacking: Implant Security and the Ethics of Neurosecurity*, 20 Neuroethics 1 (2018).
[83] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 3-5 (2018).
[84] Supra note 56.

ambiguous standards for consent and insufficient safeguards for neurotechnology[85]. In contrast, while Chile acknowledges neural data at a constitutional level and a proposed bill on neuro-rights requires free, informed, and explicit consent with dedicated oversight, India has no specific statute or authority that deals exclusively with neurodata.

Similarly, in the U.S., protection afforded to neural data is inconsistent and provided through variable state laws like California's CCPA and Colorado's CPA, while the EU's GDPR has comprehensive protection for neural data by categorising it as special category data, requiring explicit consent, and enforcing stringent restrictions on processing. [86]Against this backdrop, several regulatory gaps mark the current system in India, particularly for consumer neurodevices falling outside of medical device rules, thus raising an imperative need for a separate neurorights legislation that could define neural data, bolster consent mechanisms, increase transparency, and establish dedicated oversight to balance innovation with protection of fundamental rights.

Aspect	**India**	**Chile**	**USA (State-level)**	**European Union**
Legal Status	Implicit Constitutional Protection	Explicit Constitutional Protection	Statutory Protection	Statutory Protection
Primary Legal Instrument	Constitution (Article 21), interpreted via *Puttaswamy* & *Selvi*	Constitutional Amendment (Article 19) & proposed Neuro-rights Bill	State Privacy Laws (e.g., California's CCPA, Colorado's CPA)	General Data Protection Regulation (GDPR)

[85] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act*, 2023, § 3(n) (India).
[86] California Consumer Privacy Act (Cal. Civ. Code §§1798.100 et seq.); Colorado Privacy Act, Colo. Rev. Stat. §§6-1-1301 et seq.; GDPR, Regulation (EU) 2016/679, Art. 9.

Definition of Neural Data	Not defined in statute.	Explicitly protected as part of "mental integrity" and "brain activity."	Explicitly defined as "sensitive personal information" in some state laws.	Not explicitly defined, but covered under "health data" or "biometric data" (Article 9).
Consent Standard	Unclear for neural data; standard consent under DPDPA.	Requires free, informed, and explicit consent.	Varies by state: Opt-in (Colorado) or Opt-out of use/sharing (California).	Explicit consent is required for processing special category data.
Key Prohibitions	No specific statutory prohibitions.	Protection of free will, personal identity, and mental privacy.	Limitations on the sale and sharing of sensitive data.	General prohibition on processing special category data, with limited exceptions.
Oversight Body	None specific. Data Protection Board of India has general remit.	Institute of Public Health (initially proposed, limited to healthcare).	Federal Trade Commission (FTC) & State Attorneys General.	National Data Protection Authorities (DPAs).

XIII. RECOMMENDATIONS AND LEGAL REFORMS FOR INDIA

What is needed to bridge the dangerous chasm between India's constitutional promise and its statutory reality is a proactive, multi-stage, multi-faceted reform strategy. This roadmap puts forward a "three-legged stool" approach: combining immediate statutory amendment, comprehensive new legislation, and robust institutional oversight in building a stable, effective neuro-rights framework.

1. **Amending the DPDPA, 2023 -** The most immediate and critical vulnerability is within the Digital Personal Data Protection Act, 2023 itself. This can be addressed with a focused and quick parliamentary amendment.[87]
   Parliament should explicitly include "Neural Data" in the list of "Sensitive Personal Data." Such a change would bring brain data squarely under the Act's most strict protections, including requirements for explicit, purpose-specific consent for its collection and processing.
2. **Enacting a Comprehensive Neurotechnology Regulation Act -** In the medium term, India must move beyond data protection and enact a standalone, comprehensive law dedicated to the governance of neurotechnology. This Neurotechnology Regulation Act would address the "technology and rights" problem directly, drawing inspiration from the rights-based approach of Chile and the high standards of the EU. The key pillars of this Act should include:[88]
   - The Right to Mental Privacy
   - The Right to Cognitive Liberty
   - The Right to Psychological Continuity (protecting personal identity from unauthorised alteration)
   - The Right to Agency (protecting free will from technological manipulation).

[87] Ministry of Electronics and Information Technology, DPDPA Amendment Proposal (2025).
[88] Carlos Silva & Priya Nair, *Global Neurotechnology Governance Models*, Int'l J. Health L., 20(3), 317-342 (2024).

3. **Establishing a National Neuroethics and Technology Authority (NETA) -** No amount of legislation can succeed without an efficient enforcing authority. In an attempt to resolve the issue of "enforcement and expertise," the Neurotechnology Regulation Act should create a new, independent regulatory authority, the National Neuroethics and Technology Authority, or NETA. A generalist body such as the Data Protection Board of India or the CDSCO could not provide the specialised, interdisciplinary capacity demanded by this complex field. The mandate of NETA should include:[89]

   - **Licensing and Auditing -** NETA would be responsible for licensing all neurotechnology devices and services operating in India and conducting regular audits to ensure compliance with safety and ethical standards.
   - **Guideline Development -** The authority would be tasked with developing and continuously updating detailed ethical guidelines for neurotechnology research and application. This process must involve mandatory consultation with a diverse group of experts from neuroscience, law, ethics, computer science, and civil society, mirroring the successful expert-led process in Chile.
   - **Enforcement and Adjudication -** NETA would have the power to investigate public complaints, conduct suo motu inquiries into potential violations, and impose significant penalties, including the revocation of licenses.
   - **Public Education -** A key function of NETA would be to promote public awareness and education about neurotechnology, its benefits, its risks, and the rights of citizens, thereby empowering individuals to make informed choices.

[89] Shweta Bajaj, *Establishing Neurotechnology Regulatory Authority*, Asian J. L. & Tech., 12(2), 203-232 (2025).

XIV. CONCLUSION

The incredible pace of progress at the intersection of neuroscience and technology precipitates a critical juncture for humanity, illuminating both unprecedented opportunities and one of the most profound threats to the essence of human identity-the human mind. As this paper has contended, neurotechnology's power to access, interpret, and even manipulate neural activity engenders vulnerabilities that prior legal regimes, designed to address other eras and other needs, are poorly positioned to address. Data harvested from our brains is more than strictly personal; it is internal, forming the very substrate of our thoughts, emotions, and sense of self.[90]

Through our comparative analysis, we show a world scrambling for a response. Chile has been at the vanguard with a rights-based approach by constitutionally entrenching mental integrity. The European Union uses its wide-reaching GDPR to classify neurodata as sensitive "health data" and requires explicit consent for its use. The United States, by contrast, provides a patchwork of state-level protections that generate legal uncertainty.[91]

India is in a precarious position, marked by a "judicial-legislative gap." The Supreme Court has been progressive, with judgments such as K.S. Puttaswamy and Selvi creating a strong constitutional foundation to protect mental privacy and cognitive liberty as key aspects of Article 21. This judicial promise, however, stands in striking contrast to a statutory void. The Digital Personal Data Protection Act, 2023, is a significant squandered opportunity: neurodata is not treated as "sensitive personal data" and thus receives minimal protection. This legislative inertia is dangerously compounded by regulatory loopholes that permit consumer-grade "wellness" and "gaming" neuro-devices to circumvent scrutiny applicable to medical technology despite collecting identically sensitive data. This gap exposes Indian citizens to the twin dangers of ubiquitous surveillance capitalism and cognitive manipulation. Bridging this chasm between constitutional right and statutory reality requires a

[90] Das, supra note 60, at 48.
[91] Niyati Singh Bais, *Decoding the Brain, Encoding the Law: A Study on Neuro-Technology and Law*, 5(4) Indian J. of Integrated Research in Law, 32-40 (2025)

proactive, three-pronged reform: The Parliament must immediately amend the DPDPA to expressly include "neural data" as sensitive information. Medium-term, the country needs to enact a comprehensive, standalone Neurotechnology Regulation Act codifying specific neurorights such as rights to mental privacy, cognitive liberty, and psychological continuity. And lastly, this framework needs to be under guarded by an expert, independent body with the specialised mandate to license, audit, and oversee this complex field. Protecting the mind is not an impediment to innovation; it is the essential prerequisite for ensuring that this powerful new chapter in human technology ultimately serves, rather than subverts, human dignity and freedom.

XV. REFERENCES

A. Cases

1. *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1 (Supreme Court of India).
2. *Selvi v State of Karnataka* (2010) 7 SCC 263.
3. *Kaushal Kishore v State of Uttar Pradesh* (2023) SCC OnLine SC 289.
4. *State of Maharashtra v Aditi Sharma* Sessions Case No 508/2007 (Sessions Court, Pune, 12 June 2008).
5. *Girardi v Emotiv Inc* (Supreme Court of Chile, 2023).

B. Legislation and Statutory Instruments

1. India

- Constitution of India, 1950, arts 19, 20(3), 21, 51A(h).
- Digital Personal Data Protection Act 2023 (India).
- Information Technology Act 2000 (India).
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India).
- Medical Devices Rules 2017 (India).
- Mental Healthcare Act 2017 (India).
- Indian Evidence Act 1872 (India).

2. Chile

- Constitución Política de la República de Chile, art 19 (as amended 2021 – protection of mental integrity and neural data).

3. European Union

- Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 3.
- Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
- Regulation (EU) 2024/1689 (Artificial Intelligence Act).
- Regulation (EU) 2017/745 on Medical Devices.

4. United States

- Health Insurance Portability and Accountability Act 1996 (HIPAA).
- Federal Trade Commission Act 1914, 15 USC §§ 41–58.
- Colorado Privacy Act 2021 (as amended by Senate Bill 24-222, 2024).
- California Consumer Privacy Act 2018 (as amended).

5. International Instruments and Soft Law

- OECD, *Recommendation on Responsible Innovation in Neurotechnology* (OECD/LEGAL/0457, 2019).
- UN Special Rapporteur on the Right to Privacy, Reports to the Human Rights Council (various years).
- UNESCO International Bioethics Committee (IBC), Reports on Neurotechnology and Human Rights.

C. Books and Journal Articles

1. Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13(5) *Life Sciences, Society and Policy* 5.

2. Rafael Yuste and others, 'Four Ethical Priorities for Neurotechnologies and AI' (2017) 551 *Nature* 159.

3. Nita A Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St Martin's Press 2023).

4. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).