Rooted in Tradition. Driven by Justice.

PEER-REVIEWED • OPEN ACCESS • MULTI-DISCIPLINARY LEGAL RESEARCH JOURNAL

THINKING IS NOT DATA YET: NEURAL PRIVACY, NEUROTECHNOLOGY AND THE SILENCE OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

VISHNU YADAV

Research Articles • MOS-00001 • Published 20 October 2026

ABSTRACT

For most of human history, the mind has been the one place that no law, employer or government could enter. Neurotechnology is changing that. Devices that record and interpret the electrical activity of the brain, once confined to hospitals and laboratories, are now sold as headbands for meditation, focus and sleep, and researchers have shown that brain recordings can be used to reconstruct the gist of what a person is hearing or imagining. The data these devices generate can reveal attention, fatigue, emotional states and, potentially, health conditions that the user has never disclosed to anyone. This paper asks whether Indian law is ready for this development. It examines the constitutional foundations of mental privacy in India, drawing on the Supreme Court's rulings on involuntary brain-based testing and on the fundamental right to privacy. It then analyses the Digital Personal Data Protection Act, 2023 and the Rules notified in November 2025, and finds that the Act, by abandoning the category of sensitive personal data that featured in earlier drafts, treats a brain recording no differently from an email address. Gaps in the regulation of medical devices, research and workplace monitoring compound the problem. A comparative study of Chile, the United States, the European Union and recent international instruments, including the 2025 UNESCO Recommendation on the Ethics of Neurotechnology, informs a set of proposals for recognising neural data as a specially protected category in Indian law.

KEYWORDS

Neural Data, Neurotechnology, Mental Privacy, Neurorights, DPDP Act 2023, Article 21, Cognitive Liberty, Sensitive Personal Data

VOLUME 1, ISSUE 1 (INAUGURAL ISSUE), OCTOBER TO DECEMBER 2026 • THEME: LABOUR, EMPLOYMENT & SOCIAL SECURITY LAW

Mos Legis Review, Vol. 1, Issue 1 (2026), pp. 1-15

Licensed under CC BY 4.0

THINKING IS NOT DATA YET: NEURAL PRIVACY, NEUROTECHNOLOGY AND THE SILENCE OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Vishnu Yadav
Ph.D. Scholar, Maharashtra National Law University, Nagpur

Abstract

For most of human history, the mind has been the one place that no law, employer or government could enter. Neurotechnology is changing that. Devices that record and interpret the electrical activity of the brain, once confined to hospitals and laboratories, are now sold as headbands for meditation, focus and sleep, and researchers have shown that brain recordings can be used to reconstruct the gist of what a person is hearing or imagining. The data these devices generate can reveal attention, fatigue, emotional states and, potentially, health conditions that the user has never disclosed to anyone. This paper asks whether Indian law is ready for this development. It examines the constitutional foundations of mental privacy in India, drawing on the Supreme Court's rulings on involuntary brain-based testing and on the fundamental right to privacy. It then analyses the Digital Personal Data Protection Act, 2023 and the Rules notified in November 2025, and finds that the Act, by abandoning the category of sensitive personal data that featured in earlier drafts, treats a brain recording no differently from an email address. Gaps in the regulation of medical devices, research and workplace monitoring compound the problem. A comparative study of Chile, the United States, the European Union and recent international instruments, including the 2025 UNESCO Recommendation on the Ethics of Neurotechnology, informs a set of proposals for recognising neural data as a specially protected category in Indian law.

Keywords

Neural Data, Neurotechnology, Mental Privacy, Neurorights, DPDP Act 2023, Article 21, Cognitive Liberty, Sensitive Personal Data

1. Introduction

Every legal system rests on certain assumptions that are so obvious they are rarely written down. One of them is that a person's thoughts are private by nature. The law can compel a witness to speak, search a home or read a letter, but it has never had to decide who may read a mind, because no one could. That assumption is now under strain. Neurotechnology, the family of devices and methods that record, interpret or alter the activity of the nervous system, has advanced to the point where brain signals can be collected outside clinical settings and analysed by algorithms capable of drawing inferences their wearers may not even be aware of.

In 2017, a group of neuroscientists, clinicians, ethicists and engineers warned in the journal *Nature* that the combination of neurotechnology and artificial intelligence would soon allow access to people's mental processes, and identified privacy and consent as the first of four ethical priorities requiring urgent attention.[1] Six years later, researchers reported that a decoder trained on brain recordings could reconstruct the meaning of continuous language that a participant was hearing or imagining, although the system required the participant's cooperation and extensive individual training.[2] Meanwhile, consumer devices that measure brain activity have entered the market for meditation, gaming, productivity and sleep. A 2024 study of thirty consumer neurotechnology companies found that almost all of them appeared to have access to the neural data of their users with no meaningful limits on that access.[3]

India has a large and young population of early technology adopters, a growing medical device industry and an ambitious digital economy. It also has a new data protection law. The Digital Personal Data Protection Act, 2023 (DPDP Act), together with the Rules notified in November 2025, will govern the processing of digital personal data in India for years to come. The central question of this paper is whether that law is adequate to protect the most intimate category of data that technology has yet produced. The paper argues that it is not, and that the problem lies less in what the Act says than in what it leaves unsaid.

Part 2 explains what neurotechnology is and what neural data can reveal. Part 3 sets out the case for treating mental privacy as a distinct interest. Part 4 traces its constitutional foundations in India, including the freedoms of thought and conscience. Part 5 analyses the DPDP Act and its Rules, and Part 6 examines sectoral gaps in medical device regulation, research ethics and the workplace. Part 7 surveys comparative and international developments, Part 8 offers recommendations and Part 9 concludes.

[1] Rafael Yuste, Sara Goering, et al., "Four Ethical Priorities for Neurotechnologies and AI" 551 *Nature* 159 (2017).
[2] Jerry Tang, Amanda LeBel, Shailee Jain and Alexander G. Huth, "Semantic Reconstruction of Continuous Language from Non-invasive Brain Recordings" 26 *Nature Neuroscience* 858 (2023).
[3] Neurorights Foundation, *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies* (Neurorights Foundation, New York, Apr. 2024).

2. Understanding Neurotechnology and Neural Data

2.1 From the Clinic to the Consumer

Neurotechnology is not new. Electroencephalography, which records electrical activity through electrodes placed on the scalp, has been used in medicine for about a century, and functional magnetic resonance imaging has transformed neuroscience research since the 1990s. Implanted devices that stimulate the brain are used to treat movement disorders, and brain-computer interfaces have allowed people with paralysis to control cursors and robotic limbs.

What has changed is the setting. Dry-electrode headbands, earbuds with sensors and lightweight headsets now allow brain signals to be collected at home, at work or in a classroom, without a clinician. These products are typically marketed for wellness rather than treatment, promising better focus, calmer minds or deeper sleep. Private investment in the sector has grown rapidly, and companies have begun testing implanted interfaces in human volunteers. As the devices become cheaper and more comfortable, the volume of neural data collected outside the regulated healthcare system will grow accordingly.

2.2 What Neural Data Can Reveal

Neural data is distinctive in three ways. First, it is largely involuntary. A person can choose what to type or say, but cannot easily control the electrical activity of the brain or the involuntary responses it produces to a stimulus. Second, it is rich in inference. Even relatively crude consumer signals can indicate attention, drowsiness, stress and emotional arousal, and when combined with other data and analysed by machine learning, they may point to neurological or psychiatric conditions. Third, its value grows over time. Data collected today for a meditation app may be reanalysed tomorrow with better algorithms to reveal information that neither the user nor the company anticipated at the time of collection.

It is important not to overstate current capabilities. Consumer devices cannot read specific thoughts, and the most striking decoding results depend on large laboratory scanners and the active cooperation of participants. But law must regulate for the trajectory of a technology, not only its present state. The history of data protection shows that information once thought harmless, such as location pings or browsing histories, became deeply revealing once it could be collected at scale and combined with other sources. There is every reason to expect the same of neural data.

2.3 The Promise of Neurotechnology

None of this is an argument against neurotechnology. Its medical promise is real and, for some patients, transformative. Brain-computer interfaces offer people with severe paralysis

the prospect of communicating and controlling devices again. Neurostimulation can relieve symptoms of movement disorders and is being studied for depression and other conditions that resist conventional treatment. Better monitoring may allow earlier detection of epilepsy, dementia and other neurological diseases, and could help address the heavy and often untreated burden of mental illness. For a country like India, where specialist neurological and psychiatric care is scarce outside major cities, affordable devices combined with remote analysis could extend diagnosis and care to many who now go without. The challenge for law is therefore not to choose between innovation and protection, but to design rules that allow the benefits to be realised while preventing the same technology from becoming an instrument of surveillance or manipulation. Clear rules can also support innovation by giving developers certainty and earning the public trust on which medical adoption depends.

3. Why Neural Data Is Different: The Case for Mental Privacy

3.1 The Emergence of Neurorights

In an influential article, Marcello Ienca and Roberto Andorno argued that existing human rights were not sufficient to address the challenges of neurotechnology and proposed four new rights: cognitive liberty, mental privacy, mental integrity and psychological continuity.[4] Mental privacy, in their account, protects individuals against the unauthorised collection and use of information about their brains, while mental integrity protects against harmful interference with neural processes. Rafael Yuste and his colleagues have pressed for these "neurorights" to be recognised in national constitutions and international law.[5]

The neurorights proposal has also attracted serious criticism. Jan Christoph Bublitz has argued that some of the proposed rights are vague or duplicate existing protections, and that the real task is to interpret and strengthen established rights such as privacy and freedom of thought rather than to multiply new ones.[6] Ienca himself has since clarified that neurorights are best understood as a specification of existing human rights in the context of neurotechnology rather than as entirely new entitlements.[7] This debate is directly relevant to India. As Part 4 shows, Indian constitutional law already contains the building blocks of mental privacy; what is missing is their translation into data protection law.

3.2 Cognitive Liberty

Nita Farahany has framed the issue in terms of cognitive liberty, the right to self-determination over one's brain and mental experiences. She argues that as brain-sensing

[4] Marcello Ienca and Roberto Andorno, "Towards New Human Rights in the Age of Neuroscience and Neurotechnology" 13 *Life Sciences, Society and Policy* 5 (2017).
[5] Rafael Yuste, Jared Genser and Stephanie Herrmann, "It's Time for Neuro-Rights" 18 *Horizons: Journal of International Relations and Sustainable Development* 154 (2021).
[6] Jan Christoph Bublitz, "Novel Neurorights: From Nonsense to Substance" 15 *Neuroethics* 7 (2022).
[7] Marcello Ienca, "On Neurorights" 15 *Frontiers in Human Neuroscience* 701258 (2021).

devices become integrated into everyday products and workplaces, the greatest threat is not dramatic mind-reading but the quiet normalisation of monitoring attention, fatigue and emotional states by employers, governments and companies.[8] Her analysis is useful because it moves the debate away from science fiction towards ordinary uses that are already technically feasible, such as monitoring the alertness of drivers and factory workers or measuring the engagement of students.

The common thread in this literature is that neural data is not merely another form of personal data. It sits closer to the self than almost any other information. A leaked password can be changed and a leaked address can be moved away from, but the patterns of one's brain cannot be replaced. This is the essential justification for special protection.

4. Constitutional Foundations of Mental Privacy in India

4.1 *Selvi* and the Inviolability of the Mind

The Indian Supreme Court confronted the intrusion of science into the mind long before consumer neurotechnology existed. In *Selvi v. State of Karnataka*, a three-judge bench considered the involuntary administration of narcoanalysis, polygraph examination and the Brain Electrical Activation Profile test, which measured the brain's responses to stimuli in an attempt to detect familiarity with details of a crime. The Court held that compelling a person to undergo any of these techniques violated the right against self-incrimination under Article 20(3) and was an unwarranted intrusion into personal liberty under Article 21.[9] It drew a clear line between the physical evidence that may be taken from a person's body and the contents of the mind, which the person alone may choose to reveal.

Selvi is the closest the Supreme Court has come to articulating a right to mental privacy, and its reasoning extends naturally to modern neurotechnology. If the State cannot compel a person to submit to a test that measures brain responses, it is difficult to see how a private company or employer could legitimately obtain comparable information through consent that is uninformed or coerced. The judgment also recognised the dangers of unreliable science being given the appearance of certainty, a warning that applies with equal force to algorithmic inferences drawn from brain signals.

4.2 Privacy as a Fundamental Right

The nine-judge bench in *K.S. Puttaswamy v. Union of India* recognised privacy as a fundamental right protected under Article 21 and Part III as a whole.[10] The judges identified several dimensions of privacy, including bodily privacy, informational privacy and the

[8] Nita A. Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press, New York, 2023).
[9] *Selvi v. State of Karnataka* (2010) 7 SCC 263.
[10] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

privacy of choice, and linked the right to dignity and autonomy. Neural data engages all three. It is derived from the body, it constitutes information about the person and it can reveal, and potentially influence, the choices a person makes. The Court also emphasised that the State has a positive obligation to protect privacy against non-State actors, which formed the constitutional basis for a data protection law in the first place.

The later Aadhaar judgment applied a proportionality test to the collection of biometric data by the State, upholding the core scheme while striking down several provisions that allowed excessive or unnecessary use.[11] The Court's attention to the special risks of biometric information offers a useful analogy. If fingerprints and iris scans warrant careful constitutional scrutiny, brain recordings, which can reveal far more about a person's inner life, warrant greater scrutiny still.

4.3 Autonomy and Self-Determination

In *Common Cause v. Union of India*, the Constitution Bench affirmed the right of individuals to make decisions about their own bodies and medical treatment, including through advance directives, as an aspect of dignity and autonomy under Article 21.[12] The emphasis on self-determination supports the idea of cognitive liberty. A person who decides what may be done to their body should equally be able to decide whether their brain activity may be recorded, analysed or influenced. Read together with *Selvi* and *Puttaswamy*, these decisions establish that mental privacy is not a foreign concept awaiting import into Indian law. It is already embedded in Articles 20(3) and 21.[13] The question is whether the statutory framework gives it practical effect. Constitutional rights operate primarily against the State, and their horizontal application to private companies remains limited and uncertain. Most neural data, however, is collected by private firms. Unless the protections recognised by the Supreme Court are carried into legislation that binds private data fiduciaries, mental privacy will remain strong in principle and weak in the places where it is most likely to be tested.

4.4 Freedom of Thought and Conscience

Two further guarantees deserve mention. Article 19(1)(a) protects freedom of speech and expression, and Article 25(1) guarantees to all persons freedom of conscience. Although these provisions are usually invoked in disputes about speech and religion, they rest on a deeper premise: that a person's inner life of belief, opinion and reflection belongs to that person. Freedom of expression would be hollow if the thoughts that precede expression could be monitored before a person chose to speak. Freedom of conscience would mean little if the processes through which conscience forms could be measured and nudged by others. In this

[11] *K.S. Puttaswamy v. Union of India* (2019) 1 SCC 1.
[12] *Common Cause v. Union of India* (2018) 5 SCC 1.
[13] The Constitution of India, arts. 19(1)(a), 20(3), 21 and 25(1).

sense, the Constitution protects not only what a person says and does, but also the inner space in which a person decides what to say and do. Neurotechnology that monitors or influences mental states engages that space directly, and any law permitting it must be tested against these guarantees as well as against Article 21.

5. Neural Data under the Digital Personal Data Protection Act, 2023

5.1 The Disappearance of Sensitive Personal Data

India's journey towards a data protection law began well before *Puttaswamy*. A Group of Experts chaired by Justice A.P. Shah proposed a set of national privacy principles in 2012.[14] The interim regime under the Information Technology Act, 2000 already distinguished sensitive personal data, which includes information relating to physical, physiological and mental health condition, medical records and biometric information, and imposed additional requirements on its collection.[15] After *Puttaswamy*, the committee chaired by Justice B.N. Srikrishna recommended a comprehensive law that would subject sensitive personal data, including health, genetic and biometric data, to stricter grounds of processing.[16] The Personal Data Protection Bill, 2019 retained a detailed category of sensitive personal data.[17]

The DPDP Act abandoned this approach. It defines personal data simply as any data about an individual who is identifiable by or in relation to such data, and applies largely uniform obligations to all of it.[18] The word "sensitivity" appears only as one of the factors the Central Government may consider when designating a Significant Data Fiduciary. The result is that, once the Act is fully in force, a brain recording collected by a wellness app will be governed by the same basic rules as a customer's email address. The Act also provides that the provision of the Information Technology Act on compensation for failure to protect sensitive data will be omitted, so that the existing category will disappear when the relevant part of the Act commences.

5.2 Consent and Legitimate Uses

The primary ground for processing under the DPDP Act is consent, which must be free, specific, informed, unconditional and unambiguous, given through a clear affirmative action and limited to data necessary for the specified purpose. On paper, this standard is demanding.

[14] Planning Commission, Government of India, *Report of the Group of Experts on Privacy* (Chaired by Justice A.P. Shah) (Oct. 2012).
[15] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 3.
[16] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, New Delhi, 2018).
[17] The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).
[18] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(t), 4, 6, 7, 8, 9, 10, 11, 12, 13, 17, 33 and 44.

In practice, consent to neurotechnology raises special difficulties. Users are unlikely to understand what can be inferred from their brain signals, and companies themselves may not know what future analysis will reveal. The Emotiv litigation in Chile, discussed in Part 7, shows how standard terms of service can be drafted to retain neural data for research and other purposes in ways the user never meaningfully considered.

The Act also permits processing without consent for certain "legitimate uses", including purposes of employment or those related to safeguarding the employer from loss or liability. This provision deserves close attention. An employer that equips workers with fatigue-monitoring headbands in the name of safety may claim that the processing falls within this ground, removing the need for consent altogether. Given the power imbalance in employment, the absence of any special restriction on neural monitoring at work is a significant gap.

5.3 Children, Exemptions and Inferences

The Act offers stronger protection for children. It requires verifiable parental consent and prohibits processing that is likely to cause any detrimental effect on a child's well-being, as well as tracking, behavioural monitoring and targeted advertising directed at children. These provisions would restrict the use of attention-monitoring devices on students, although the Central Government retains power to exempt particular classes of data fiduciaries or purposes. For adults, no comparable restriction exists.

The exemptions in the Act raise further concerns. The Central Government may exempt instrumentalities of the State from its provisions in the interests of sovereignty, security, public order and related grounds. In the context of neurotechnology, this would leave State use of brain-based methods subject only to constitutional limits such as those in *Selvi*, without the procedural safeguards a statute could provide.

Finally, the Act does not expressly regulate inferences. Much of the risk of neural data lies not in the raw signal but in what can be deduced from it about mood, health or susceptibility. Whether such inferences are personal data, and whether a person can demand their correction or erasure, is left to interpretation. The Rules notified in November 2025 provide detailed procedures for notices, consent managers, security safeguards and breach reporting, with most substantive obligations taking effect after an eighteen-month transition period.[19] They do not, however, create any special category for health, biometric or neural data. The silence of the statute is carried into its rules.

[19] The Digital Personal Data Protection Rules, 2025 (notified by the Ministry of Electronics and Information Technology, Nov. 2025).

5.4 The Rights of the Data Principal

The Act gives individuals the right to obtain a summary of their personal data and the processing activities undertaken with it, the right to correction and erasure, and the right to grievance redressal. These rights are valuable, but they were designed with conventional records in mind. Neural data is often processed into models, profiles and scores that are not easily separated from the underlying recordings. A user who withdraws consent and asks for erasure may find that the raw brain signals are deleted while the inferences drawn from them, or the algorithms trained on them, remain in use. The Chilean case discussed in Part 7 turned on exactly this kind of retention. Unless the law clarifies that erasure extends to derived data and inferences, the rights of the data principal may offer little real control over the most sensitive uses of neural information. The Act's reliance on the Data Protection Board as the principal forum for enforcement adds a practical concern: the Board will need technical expertise in neuroscience and machine learning to assess whether a company's claims about anonymisation or deletion are true.

6. Sectoral Gaps: Medical Devices, Research and the Workplace

6.1 The Medical Device Boundary

Devices intended for the diagnosis or treatment of disease are regulated in India under the Medical Devices Rules, 2017, framed under the Drugs and Cosmetics Act, 1940.[20] A clinical electroencephalography system or an implanted neurostimulator falls within this framework, which addresses safety, performance and quality. The boundary, however, is drawn by intended use. A consumer headband marketed for meditation or focus, and described by its manufacturer as not intended for medical purposes, may fall outside the regime entirely even if it collects the same type of signal. This is a familiar regulatory gap across jurisdictions, and it means that the most widely used neurotechnology products are likely to be the least regulated.

The medical device framework is also concerned with physical safety rather than data. Even for regulated devices, it does not prescribe how the neural data generated by a device should be stored, shared or used for secondary purposes. That task falls to data protection law, which, as shown above, does not distinguish neural data from other information.

6.2 Research Ethics and Mental Health Law

Research involving human participants in India is governed by the national ethical guidelines issued by the Indian Council of Medical Research, which require informed consent, ethics committee review and protection of confidentiality.[21] These guidelines provide important

[20] The Medical Devices Rules, 2017, framed under the Drugs and Cosmetics Act, 1940.
[21] Indian Council of Medical Research, *National Ethical Guidelines for Biomedical and Health Research Involving Human Participants* (ICMR, New Delhi, 2017).

safeguards for formal research studies, but they do not bind a technology company that collects neural data from customers and later uses it to train algorithms. The Mental Healthcare Act, 2017 guarantees persons with mental illness the right to confidentiality in respect of their mental health, treatment and physical healthcare,[22] but this protection is tied to the context of care. It does not reach a consumer app that infers anxiety or depression from brain signals outside any therapeutic relationship.

6.3 Neurotechnology at Work and in the Market

The workplace is where neurotechnology is most likely to be deployed without genuine choice. Fatigue monitoring for drivers and machine operators can be justified on safety grounds, but the same devices can measure attention and engagement across an entire workforce. Combined with the employment-related legitimate use under the DPDP Act, there is a real risk that brain monitoring could become a condition of employment in some sectors.

Consumer protection law offers some help. The Consumer Protection Act, 2019 prohibits unfair trade practices, including false or misleading representations about goods and services,[23] and the Central Consumer Protection Authority has issued guidelines against dark patterns that manipulate consumers into choices they did not intend.[24] These instruments can be used to challenge misleading claims about what a device does with brain data or consent flows designed to extract agreement. They are, however, reactive and general, and are no substitute for clear substantive rules on neural data.

6.4 Risks of Discrimination

A further concern is discrimination. If neural data or inferences drawn from it reach insurers, lenders or employers, they could be used to make decisions about people on the basis of predicted conditions or traits, such as a supposed tendency towards anxiety, inattention or cognitive decline. Such predictions may be inaccurate, and even when they are accurate they may penalise people for conditions they have never developed or that do not affect their ability to work. Indian law prohibits certain forms of discrimination on the basis of disability, but it does not specifically address decisions based on inferred mental characteristics drawn from brain data. Without clear limits on the purposes for which neural data may be used and shared, the risk is that a person's brain activity becomes a hidden factor in decisions about employment, insurance or credit, without the person ever knowing. A data protection law that restricted secondary uses of neural data and prohibited its use in such decisions would address this risk at its source.

[22] The Mental Healthcare Act, 2017 (Act 10 of 2017), s. 23.
[23] The Consumer Protection Act, 2019 (Act 35 of 2019), s. 2(47).
[24] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023* (Nov. 30, 2023).

7. Comparative and International Perspectives

7.1 Chile: Constitutional Neurorights in Action

Chile became the first country to protect brain activity expressly in its constitution. A 2021 amendment provides that scientific and technological development shall be at the service of people and shall respect life and physical and mental integrity, and requires the law to protect brain activity and the information derived from it.[25] The provision was soon tested. A former senator who had used a consumer headset sued its manufacturer, whose terms allowed it to retain users' brain data for research. In August 2023, the Supreme Court of Chile held that the company's storage of that data violated his rights to mental integrity and privacy, ordered its deletion and directed that the device not be sold in Chile until the relevant privacy practices were revised.[26] The case is significant because it rejected the argument that anonymised neural data could be used freely, and insisted on specific consent for research use.

7.2 The United States: State Neural Data Laws

In the United States, protection has come through State consumer privacy laws. In 2024, Colorado amended its privacy statute to treat neural data as sensitive data, requiring consent before collection or processing.[27] California followed later that year, adding neural data to the definition of sensitive personal information under its consumer privacy law.[28] These laws are modest in scope, but they demonstrate a workable legislative technique: rather than building an entirely new regime, they place neural data within the existing special category of sensitive data and attach stronger rules to it.

7.3 The European Union and Other Jurisdictions

The European Union's General Data Protection Regulation prohibits the processing of special categories of personal data, including health data and biometric data used for unique identification, unless specific conditions are met.[29] Neural data is not named, but much of it will qualify as health data and thus attract strong protection. More recently, the Artificial Intelligence Act prohibits the use of AI systems to infer the emotions of a person in the workplace and in educational institutions, except for medical or safety reasons.[30] This prohibition addresses precisely the kind of workplace and classroom monitoring that neurotechnology makes possible. Spain has gone further at the level of soft law, including

[25] Ley N° 21.383, Modifica la Carta Fundamental, para Establecer el Desarrollo Científico y Tecnológico al Servicio de las Personas (Oct. 25, 2021) (Chile).
[26] *Girardi v. Emotiv Inc.*, Corte Suprema, Rol No. 105065-2023 (Aug. 9, 2023) (Chile).
[27] Colorado House Bill 24-1058 (2024), amending the Colorado Privacy Act.
[28] California Senate Bill 1223 (2024), amending the California Consumer Privacy Act of 2018.
[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 9.
[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art. 5(1)(f).

rights relating to neurotechnologies in its Charter of Digital Rights,[31] and the United Kingdom's data protection regulator has published a detailed analysis of the privacy risks of neurotechnology.[32]

7.4 International Standards

At the international level, the OECD adopted in 2019 the first intergovernmental standard on neurotechnology, calling for the safeguarding of personal brain data and the promotion of responsible innovation.[33] In November 2025, UNESCO's General Conference adopted the Recommendation on the Ethics of Neurotechnology, the first global normative framework in the field, which addresses the full life cycle of neurotechnology and highlights risks in education, employment and consumer markets.[34] India, as a Member State of UNESCO, is among the countries to which the Recommendation is addressed. The Recommendation is not binding, but it provides an authoritative reference point for national legislation and strengthens the case for India to act.

8. Towards Neural Privacy in India: Recommendations

First, the DPDP Act should be amended to recognise a category of specially protected personal data that expressly includes neural data, along with health, genetic and biometric data. The definition of neural data should cover information generated by measuring the activity of the central or peripheral nervous system and inferences drawn from it. Pending amendment, the Central Government should use its power to designate Significant Data Fiduciaries, which already takes account of the sensitivity of data, to bring neurotechnology companies within the Act's enhanced obligations, including data protection impact assessments and independent audits.

Second, consent for neural data should be separate, specific and renewable. It should be obtained independently of general terms of service, distinguish between core functionality, research and commercial use, and lapse unless renewed after a defined period. Secondary uses, including the training of algorithms and sale to third parties, should require fresh consent, and the inference of health conditions should be prohibited unless the user has specifically requested it.

Third, the employment-related legitimate use should not extend to neural data. Brain monitoring in the workplace should be permitted only where strictly necessary for safety, on the basis of a prior impact assessment and consultation with workers, and never for

[31] Gobierno de España, *Carta de Derechos Digitales* (July 2021) (Spain).
[32] Information Commissioner's Office, *ICO Tech Futures: Neurotechnology* (ICO, Wilmslow, June 2023).
[33] OECD, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, OECD/LEGAL/0457 (Dec. 11, 2019).
[34] UNESCO, *Recommendation on the Ethics of Neurotechnology* (adopted by the General Conference at its 43rd Session, Samarkand, Nov. 2025).

evaluating productivity, engagement or emotional state. A similar rule should apply in schools and colleges, building on the protections for children already in the Act.

Fourth, the boundary between medical and wellness devices should be narrowed. Products that collect neural data should be subject to minimum data security and transparency standards regardless of whether they claim a medical purpose, and the Central Drugs Standard Control Organisation and the Data Protection Board should develop coordinated guidance.

Fifth, any use of neurotechnology by State agencies, whether for security, policing or welfare, should be governed by statute, subject to judicial authorisation where it affects individual rights and bound by the principles laid down in *Selvi*. The exemption power under the DPDP Act should not be used to place such activities beyond independent oversight.

Sixth, the Data Protection Board should be equipped to deal with neurotechnology. This means access to technical experts, the power to commission independent audits of anonymisation and deletion claims, and clear guidance that the rights of correction and erasure extend to inferences and derived profiles, not only to raw recordings.

Finally, India should draw on the UNESCO Recommendation to develop a national strategy on neurotechnology that supports medical innovation while protecting mental privacy. Indian researchers and companies can lead in this field, and clear rules will help rather than hinder them by building public trust.

9. Conclusion

The mind has always been the last refuge of privacy, protected less by law than by the limits of technology. Those limits are receding. Neurotechnology offers real benefits, from restoring communication to people with paralysis to improving the diagnosis of neurological disease, and nothing in this paper suggests that India should stand in its way. But the same technology can be used to monitor, profile and influence people in ways that strike at the core of human dignity.

Indian constitutional law is well equipped to meet this challenge. *Selvi* recognised that the State may not compel access to the workings of the mind, *Puttaswamy* established privacy as a fundamental right and *Common Cause* affirmed the autonomy of individuals over their own bodies. The weakness lies in the statutory framework. By abandoning the category of sensitive personal data, the DPDP Act has left neural data without any special protection at the very moment when it is beginning to be collected at scale. The countries that have acted, from Chile to Colorado, show that the remedy need not be complicated: recognise neural data as special, require meaningful consent, restrict its use in coercive settings and hold those who process it to higher standards.

The title of this paper suggests that thinking is not data yet. That is still largely true. Whether it remains true will depend on choices that lawmakers make now, while the technology is still young. India has the constitutional principles it needs. It should give them statutory form before the question is decided by the market instead.