NEURORIGHTS AND THE INDIAN CONSTITUTION: IS ARTICLE 21 ENOUGH TO PROTECT THE MIND?

by

Shivam Raj
&
Shashank Kumar

In April 2021, a monkey named Pager played a video game. No joystick. No controller. Just a Neuralink implant in his skull reading the electrical signals from his neurons and translating them into movement on a screen. Elon Musk posted the video. Scientists took note. Lawyers, largely, did not.[1]

Three years later, Neuralink put the same device into a human being.[2]

The legal profession's silence on this moment is not a minor oversight. It is a structural failure. Because the question that follows from that video is one that Indian law has no answer to: when a device reads your brain, who owns what it finds?

Neurotechnology is not a future problem dressed in science fiction. Consumer EEG headsets — sold today on e-commerce platforms under names like Emotiv and Muse, monitor brain activity for purposes ranging from sleep tracking to workplace productivity assessment. A 2024 audit of neurotechnology companies found that ninety-seven percent of them had contractually reserved the right to share user brain data with third parties. That figure is not an outlier it is the industry standard. That data is being shared with advertisers, insurers and, in some jurisdictions, employers drawn not from what a person says or does, but from the electrical activity of their neurons.[3]

The scope of the data-sharing practices identified in that audit goes beyond the headline figure. Sixty per cent of the companies surveyed provided no meaningful information to users about how

[1] 'Elon Musk's Neuralink Shows Video of Monkey Using Mind to Play Pong', *CNBC*, 9 April 2021 <https://www.cnbc.com/2021/04/08/elon-musk-neuralink-monkey-plays-video-game-with-mind.html> accessed 24 June 2026.

[2] Cristina Criddle, 'Elon Musk's Neuralink Implants Brain Chip in First Human', *Financial Times*, 30 January 2024 <https://www.ft.com/content/e28de6c5-d985-4c2d-81bb-0ecf6cad9e74> accessed 24 June 2026.

[3] Jared Genser, Stephen Damianos and Rafael Yuste, *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies* (Neurorights Foundation, April 2024) 4. The audit reviewed the privacy policies and user agreements of 30 consumer neurotechnology companies; 29 of the 30 reserved the right to access users' neural data with no meaningful limitations.

their neural data was specifically handled, fewer than half employed encryption, and the single company that imposed any meaningful restriction on data use was an outlier in the sector.[4] What the audit documents is not aggressive collection by individual bad actors but a structural absence of governance: an industry in which the default is unrestricted access to neural signals, and the consumer has no practical means of knowing what they have consented to.

This is already happening in India's neighbourhood. South Korean and Japanese technology firms have begun piloting EEG-based employee monitoring tools that track concentration levels and stress responses during working hours. The data generated is neural in origin it comes from attaching sensors to a worker's scalp, not from observing their behaviour. Several Indian IT companies have reportedly explored similar productivity monitoring tools in pilot programmes, though none have publicly confirmed deployment at scale. The point is not that mass neural surveillance is imminent. The point is that the technology is cheap enough, and the regulatory vacuum wide enough, that the question is when, not whether.

The commercial trajectory of consumer neurotechnology makes the question of regulatory timing especially consequential. The global neurotechnology market, valued at approximately USD 15.3 billion in 2024, is projected by multiple analysts to exceed USD 50 billion by 2034, with the Asia-Pacific region identified as the fastest-growing market over the forecast period.[5] India's own neuroscience sector, estimated at USD 1.88 billion in 2023, is projected to reach USD 3.1 billion by 2030.[6] Consumer-facing applications are the fastest-growing sub-segment of that market, and it is precisely those applications that collect neural data at scale with the fewest contractual constraints on its use.

There is no provision in any Indian statute that specifically governs this. The word "neural" does not appear in the Digital Personal Data Protection Act, 2023. "Brain-computer interface" appears nowhere in Indian law. A company selling an EEG headset in India today, whether for consumer

[4] Genser, Damianos and Yuste (n 3) 5; O Rose Broderick, 'Data Privacy Needed for Your Brain, Neurorights Foundation Says', *STAT News*, 17 April 2024 <https://www.statnews.com/2024/04/17/neural-data-privacy-emotiv-eeg-muse-headband-neurorights/> accessed 24 June 2026.

[5] Precedence Research, *Neurotechnology Market Size, Share and Trends 2025 to 2034* (Precedence Research, January 2025) <https://www.precedenceresearch.com/neurotechnology-market> accessed 24 June 2026.

[6] Grand View Research, *India Neuroscience Market Outlook 2024–2030* (Grand View Research, 2024) <https://www.grandviewresearch.com/horizon/outlook/neuroscience-market/india> accessed 24 June 2026.

wellness or workplace monitoring, operates in a complete regulatory vacuum so far as neural data is concerned.

A structural feature of the Digital Personal Data Protection Act 2023 deepens the regulatory gap. Unlike the earlier drafts of India's data protection legislation, and unlike the European Union's General Data Protection Regulation, which imposes heightened obligations on the processing of special categories of sensitive data, the 2023 Act makes no statutory distinction between data types on the basis of sensitivity.[7] Biometric data, health records and financial information are governed by the same general obligations as any other form of personal data. Neural data, with no equivalent in any prior Indian framework, therefore falls into an already under-specified category without even the modest attention that earlier drafts of the Bill had given to biometric sensitivity.

The obvious response and it will be made is that Article 21 covers this. The right to life and personal liberty, as interpreted by the Supreme Court across decades of expanding jurisprudence, has sheltered an extraordinary range of rights. The nine-judge bench in unanimously held privacy to be a fundamental right under Article 21, recognising within it the right to informational privacy, decisional autonomy and bodily integrity.[8]

That judgment is genuinely significant. But it was decided in 2017, a year before Neuralink held its first public demonstration. The Court's understanding of informational privacy was built around Aadhaar linkages, health records and financial data, the privacy concerns of a specific digital moment. Neural data is not a variation of those concerns. It is categorically different. It can reveal medical conditions a person has not yet been diagnosed with. It can even decode emotional states of a person who has not chosen to express. In at least some documented research contexts, it has captured intentions before the person has consciously acted on them.

There is also a dimension that Puttaswamy did not and could not have addressed: the evidentiary use of neural data in criminal proceedings. Several countries are already debating whether brain scans and neural activity recordings can be admitted as evidence of deception, criminal intent, or

[7] Shravishtha Ajaykumar, Amoha Basrur and Vaishnavi Sharma, *The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act* (Observer Research Foundation, March 2024) <https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023-recommendations-for-inclusion-in-the-digital-india-act> accessed 24 June 2026.

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

mental state. India's own courts have grappled with the admissibility of narco-analysis and brain mapping — the Supreme Court in Selvi v. State of Karnataka(2010) held that involuntary administration of such techniques is violation of Article 20(3)which gives protection against self-incrimination. But Selvi was concerned with State-administered tests. The harder question, not yet before any Indian court, is what happens when neural data has already been commercially harvested from a person before any criminal investigation begins, and law enforcement seeks access to it through a data request to a private company. The right against self-incrimination protects against compelled testimony. It was not designed for a world in which your brain's electrical activity has been logged, stored and made commercially available years before you became a suspect.[9]

The constitutional ground under Selvi was reaffirmed as recently as 2025. In Amlesh Kumar v State of Bihar, the Supreme Court restated that narco-analysis, polygraph and brain mapping tests cannot be directed by a court without the explicit, informed consent of the accused, confirming that the protections under Articles 20(3) and 21 laid down in Selvi continue to bind investigative and judicial procedure alike.[10] The harder problem, left unaddressed by both judgments, is the scenario that does not involve any State-administered test at all: where neural data has already been commercially harvested by a private company before the individual becomes a suspect, and law enforcement subsequently seeks access through a civil data request rather than any judicial process.

Puttaswamy's spirit is broad enough to reach these concerns. The problem is that a constitutional right, however expansively read, cannot by itself create a consent framework, classify neural data as a distinct sensitive category, impose data minimisation obligations, or drag a foreign neurotechnology company into an Indian court for violating a user's cognitive privacy. Fundamental rights tell the State what it cannot do. They do not, on their own, tell a private corporation operating under American terms of service what it must do. That gap between constitutional value and enforceable obligation is exactly where neural data currently sits.

Chile understood this earlier than most. In October 2021, it became the first country to write neurorights into its constitution, giving brain data the same protected status as a human organ, not transferable, not tradeable, not extractable without consent. The test came quickly. In 2023,

[9] *Selvi v State of Karnataka* (2010) 7 SCC 263.

[10] *Amlesh Kumar v State of Bihar* (2025) INSC 810, reaffirming *Selvi v State of Karnataka* (n 9).

Chile's Supreme Court ordered the American company Emotiv to delete brain-activity data collected from a Chilean user through a consumer headset. A foreign corporation was compelled by court order to destroy neural data it had gathered. That outcome was possible because Chile had a legal framework specific enough to support it. A court invoking a general right to privacy against a foreign company's terms-of-service agreement, without statutory backing, would have had considerably less ground to stand on.[11]

The factual background of the Chilean ruling illustrates precisely the kind of case that Indian courts may eventually face. Former Senator Guido Girardi Lavín had used an Emotiv Insight consumer EEG headset, a commercially available wireless device marketed for cognitive wellness, and the company's privacy policy purported to authorise its ongoing retention and commercial use of his neural data.[12] The Chilean Supreme Court ruled unanimously on 9 August 2023 that this retention violated his constitutional rights to physical and psychological integrity, and ordered not only deletion of the data but modification of Emotiv's privacy policy as a precondition for continued sales in Chile. The Court expressly set aside the company's argument that user consent to its terms of service constituted a sufficient legal answer.

Other countries are catching up. California, Colorado and Connecticut have each classified neural data as sensitive personal information under state data protection law. UNESCO adopted recommendations on the ethics of neurotechnology in November 2025. The European Union is already debating whether the AI Act's provisions on systems that infer emotional or mental states need to be extended.[13]

The pace of international governance is quickening. In February 2026, Canada's Office of the Privacy Commissioner updated its Interpretation Bulletin to classify neural data collected in commercial settings as sensitive personal information, making Canada the first country to achieve this protection at the national level without a constitutional amendment.[14] That development builds on the Organisation for Economic Co-operation and Development's 2019

[11] Chilean Constitutional Amendment, Article 19(1), October 2021; María Isabel Cornejo-Plaza, Roberto Cippitani and Vincenzo Pasquino, 'Chilean Supreme Court Ruling on the Protection of Brain Activity: Neurorights, Personal Data Protection, and Neurodata' (2024) 15 *Frontiers in Psychology* 1330439.

[12] Cornejo-Plaza, Cippitani and Pasquino (n 11); 'Hands Off My Brainwaves: Latin America in Race for Neurorights', *Context by Thomson Reuters Foundation*, 12 September 2023 <https://www.context.news/digital-rights/hands-off-my-brainwaves-latin-america-in-race-for-neurorights> accessed 24 June 2026.

[13] California Civil Code s 1798.140, as amended by SB 1223 (2025); UNESCO, *Recommendation on the Ethics of Neurotechnology*, adopted 12 November 2025, 43rd Session of the UNESCO General Conference.

[14] Neurorights Foundation, 'Canada: First Country to Protect Neural Data as Sensitive Information at the National Level' (February 2026) <https://www.neurorightsfoundation.org> accessed 24 June 2026.

Recommendation on Responsible Innovation in Neurotechnology, which established early international consensus around consent, transparency and risk management in consumer neurotechnology.[15] India participates in OECD processes as a key partner country, yet has articulated no corresponding domestic policy position on neural data governance.

India, in the meantime, passed the DPDP Act in 2023 — a statute built for the data economy as it existed before neurotechnology entered the consumer market. It is not a bad law. It is simply not designed for this problem. What the statute does not name, it does not protect with any meaningful specificity, and "personal data" in its conventional digital sense was never written to encompass neural signals.

The scholars Marcello Ienca and Roberto Andorno, writing in 2017, proposed four neurorights that have since become something of a foundational framework in the field. Mental privacy — the right to keep one's neural data from being accessed or shared without consent. Cognitive liberty — the right to refuse neurotechnology without consequence. Mental integrity — the right not to have one's brain activity externally manipulated. And psychological continuity — the right to a stable sense of personal identity that cannot be altered through neural intervention.[16]

The academic framework proposed by Ienca and Andorno has proven unusually generative in policy terms. Within eight years of its publication, versions of its four neurorights had informed constitutional amendments in Chile, legislative proposals in Mexico, Brazil and Colombia, and the normative framework adopted by UNESCO's 194 Member States in November 2025.[17] The UNESCO Recommendation draws explicitly on cognitive liberty, mental privacy and psychological continuity as foundational values that governments should protect through dedicated national regulation. That progression, from a journal article to an international instrument within a single decade, measures both the urgency with which the international community has approached this field and the speed at which an accurately diagnosed governance problem can move through institutional channels.

[15] OECD, *Recommendation on Responsible Innovation in Neurotechnology* (OECD Publishing, 2019).

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

[17] UNESCO, *Recommendation on the Ethics of Neurotechnology* (n 13); 'Ethics of Neurotechnology: UNESCO Adopts the First Global Standard in the Cutting-Edge Technology' (UNESCO, 8 November 2025) <https://www.unesco.org/en/articles/ethics-neurotechnology-unesco-adopts-first-global-standard-cutting-edge-technology> accessed 24 June 2026.

None of these are recognised anywhere in Indian law. One could argue that Puttaswamy's reading of Article 21 is elastic enough to eventually reach all four — the right to dignity, decisional autonomy and informational privacy are all there. But "elastic enough to eventually reach" is not a protection. It is a litigation strategy for people who can afford a decade of constitutional appeals. A person whose neural data was harvested by an EEG wellness app last Tuesday does not have that luxury.

The case for specific legislation is not complicated, though the design of it matters considerably. Neural data requires a framework that first classifies it as a distinct and sensitive category not merely a subset of biometric or health data, but a category that captures its unique characteristic: that it originates in the central nervous system and can, under the right conditions, reveal not just what a person has done but what they were thinking and feeling while doing it. From that classification, mandatory informed consent before collection follows naturally, as does a prohibition on secondary use without fresh consent and strict limits on retention periods.

The more difficult design question is jurisdiction. The companies collecting neural data from Indian users are overwhelmingly incorporated abroad. The DPDP Act's framework for cross-border data transfers gives the Government of India powers to notify countries for data transfer purposes, but enforcement against a foreign company that simply ignores an Indian order is a different matter. Chile's 2023 ruling against Emotiv worked partly because Emotiv had a presence in Chile that created legal exposure. A purely statutory approach requires thinking carefully about what levers actually function against companies with no Indian incorporation — and this is an argument for building neurorights obligations into procurement standards, app store regulations, and import requirements for neural devices, not just into a standalone data protection amendment.

None of this is beyond India's legislative capacity. The country produced a reasonably sophisticated data protection statute in 2023. The question is political will and professional urgency whether the legal community treats neurotechnology as something worth engaging with before the harm is already done.

India has a familiar pattern of legislating after harm has already accumulated. The data protection conversation began in earnest only after Aadhaar's vulnerabilities became impossible to ignore in litigation. The brain is a domain where that approach is particularly ill-suited. Neural data, once extracted and aggregated across millions of users, cannot be meaningfully recalled. The harm is

not reversible in the way that a data breach notification or a compensation payment might partially address. And unlike a password or a financial record, a person's neural profile their emotional responses, cognitive patterns, mental vulnerabilities is not something they can change after the fact.

Article 21 is the most expansive provision in the Indian Constitution, and the Supreme Court has used it to protect rights its framers almost certainly did not contemplate. That tradition of interpretive generosity is one of the genuine achievements of Indian constitutional law. But there is a difference between a right that exists in principle and a right that functions in practice that has institutions, mechanisms, and consequences behind it.

The mind is the one space that has historically been beyond reach. No surveillance camera, no informant, no search warrant has ever been able to go there. Neurotechnology is changing that, not dramatically and all at once, but gradually, commercially, through wellness apps and productivity tools and consent forms that nobody reads. The law needs to move before the architecture of neural data extraction becomes as entrenched as every other form of data extraction that regulators are now struggling to govern retroactively.

Chile built a framework. India has a constitutional tradition that is at least as serious about human dignity. The question is whether that tradition will produce a timely response or an eventual one.

References

1. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
2. *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
3. The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
4. Chilean Constitutional Amendment, Article 19(1), October 2021 (protecting mental integrity and brain activity).
5. California Civil Code § 1798.140, as amended by SB 1223 (2025) (classifying neural data as sensitive personal information).
6. Jared Genser, Stephen Damianos and Rafael Yuste, *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies* (Neurorights Foundation, April 2024).
7. OECD, *Recommendation on Responsible Innovation in Neurotechnology* (OECD Publishing, 2019).

8. UNESCO, *Recommendation on the Ethics of Neurotechnology* (UNESCO, November 2025).
9. Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 *Life Sciences, Society and Policy* 5. DOI: 10.1186/s40504-017-0050-1.
10. Elon Musk's Neuralink Shows Video of Monkey Using Mind to Play Pong', *CNBC*, 9 April 2021.
11. Chilean Supreme Court, *Emotiv ruling* (August 2023) — ordering deletion of neural data collected from Chilean user.