

Neural Data as Critical National Infrastructure: The Case for a Reclassification

Kritika

Introduction

The Digital Personal Data Protection (DPDP) Act, 2023 is an important milestone in India's data governance framework. At the same time, there is an unspoken, no so subtle, absence within the policy, with no mention of neural data, the Electroencephalographic (EEG) signals, outputs of Brain-Computer Interfaces (BCIs), and cognitive biometrics produced by defence neuroscientific laboratories, military medical institutions, and a burgeoning consumer neurotechnology market. This is no coincidence. Neural data is not financial, it is neither health nor communications, it is neural. It captures mental states, emotional reactions, decision making behaviours and crucial data from the thinking processes of defence and intelligence officers, who are real strategic assets. Presently, there are seven sectors that are included in the Critical Information Infrastructure (CII) of India under Section 70 of the Information Technology Act, 2000. These are different from the neural data repository. The article proposes three reasons neutral why the inclusion should be done as soon as the international governance frameworks are developed. First, it is essential for securing India's interests, second, it offers an opportunity to set norms, and third, it is a pressing need.

The Neural Data Landscape in India

Under the cluster of Life Sciences domain, the Defence Research and Development Organisation (DRDO) runs active neuroscience research programmes, focussing on cognitive workload studies of pilots and soldiers, brain-machine interface research, and monitoring of neural fatigue for high-altitude deployments.¹ Neural data is gathered from Indian defence hospitals during psychiatric evaluations and combat stress evaluations and during the rehabilitation of wounded soldiers. In the civilian sector, India's consumer neurotechnology sector is growing, with consumer products like EEG meditation devices, cognitive training software, and neurofeedback devices now being widely available. None of these are covered under neural data streams that are currently included by the general and weak security requirements contained in the DPDP Act, 2023.² The Act does not define what constitutes sensitive personal data that warrant enhanced security and fails to impose any sector-specific security requirements that are comparable to those imposed by the CII designation.

India's Critical Information Infrastructure Framework: The Structural Gap

Section 70 of the Information Technology Act provides for the Central Government to declare any computer resource to be a CII if its incapacitation or destruction would have a crippling effect on national security, national economy, public health, or public safety. Neural data repositories, such as those of the DRDO's Institute of Nuclear Medicine and Allied Sciences, Armed Forces Medical College, or licensed neurotechnology companies in India, do not belong to any of the sectors recognised

by the National Critical Information Infrastructure Protection Centre (NCIIPC).³ It is a serious concern. If some adversary could extract neural data from a defence institution's neuroscience lab today, India does not have a no notification law to govern this breach. There is neither minimum security standard, nor is there a protocol for responding to any breach in the lab. The consent and notice approach in the DPDP Act is completely insufficient to deal with strategic assets.

Global Precedents: A Governance Architecture Forming Without India

The international community has proceeded towards urgent action. The first state to provide comprehensive privacy protections specifically to neural data was Chile⁴, and followed by Colorado⁵ and Minnesota⁶, and by the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) Recommendation on the Ethics of Neurotechnology⁷ in Nov 2025, explicitly introducing cognitive liberty, mental privacy, and psychological continuity as core rights requiring protection. In a democratic legal system, neural data is being considered a new, highly-sensitive class. Even in the midst of the developing neuroscience research base and in the context of its democratic claims, India has failed to come up with something similar. This governance gap can be put in the context of time as shown in Figure 1.

The European Union's (EU) dimension is of special interest. Neural data is regarded as a 'Special Category' data by the EU's General Data Protection Regulation (GDPR) and has strict consent and processing requirements for biometric or health data.⁸ The EU's Artificial Intelligence (AI) Act (2024) also classifies AI systems that draw inferences about mental states as high-risk systems which are required to comply with conformity assessments. The NeuroRights Foundation has discovered that 96.7 per cent of consumer neurotechnology companies could allow third parties to access the data from their brains, and the majority of policies were ambiguous about the sale or brokerage of brain data.⁹ The finding is directly applicable to the consumer neurotechnology market in India, which does not have an equivalent requirement to audit transfers of data. Chile has taken it a step further and has obtained a precedent-setting judicial decision that mandates the removal of brain data of a former senator. India's absence from this norm-setting moment is more than just a regulatory oversight, it is a strategic vulnerability that can be targeted by adversaries, commercial actors, and others.

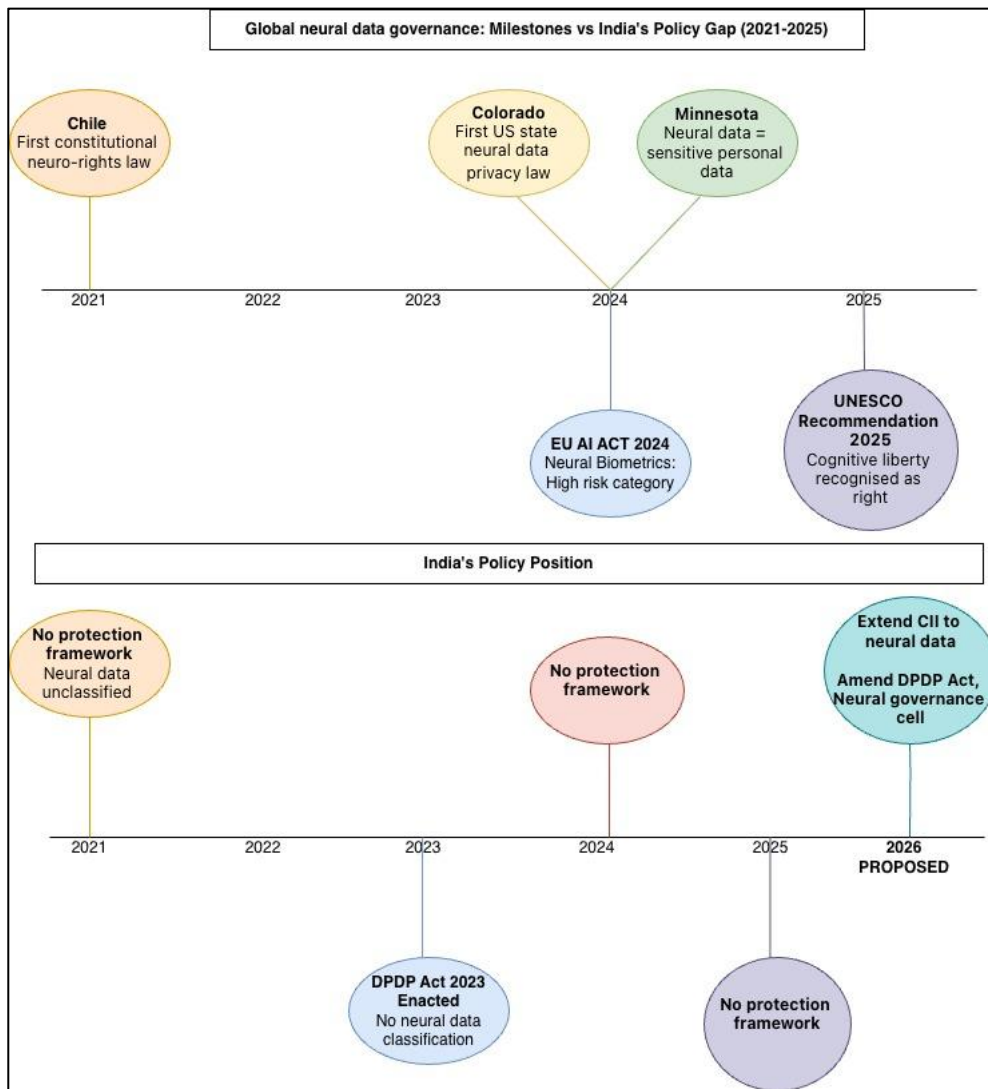


Figure 1: Global Neural Data Governance Milestones vs India's Legislative Gap (2021–2025)

Source: Compiled by Author

The Strategic Case for Reclassification

This is part of a bigger issue and moves beyond the realm of a privacy debate with the defence dimension. Neural data attributes of military leaders relate to decision-making tendencies, stress thresholds, and blind spots. The leakage of such information would provide a new dimension to psychological or cognitive warfare to adversaries, allowing them to conduct targeted influence operations, strategic response prediction, and precision disinformation targeting individual decision-makers. While the DRDO research in India is valuable, it is not as protected as classified data would be under CII designation, as is the case in the Chinese military doctrine.¹⁰ Furthermore, the adversaries do not have to directly investigate into the DRDO systems. Consumer neurotechnology devices such as wearable EEG headsets, smart helmets, cognitive performance monitoring devices used by defence personnel during personal time in the current regulatory framework are completely unregulated and, hence, become an easy target of exploitation.

A Legislative Pathway

There are solutions available for to action mechanism. First, the NCIIPC should add the designation of CII to neural data repositories that are stored in the defence establishments as well as to the licensed companies that have developed neurotechnology solutions, starting with the 'Healthcare' or 'Strategic Enterprises' sub-sector of the CII. Second, there should be a clear distinction between types of personal data within the definition of second-class legislation under the DPDP Act, categorising neural data as a unique sub-genre of sensitive personal data, imposing encryption regulations, access logging and notification procedures that are necessary for it. Third, the DRDO needs to form a Neural Data Governance Cell to align India's interests in deliberations under the United Nations Group of Governmental Experts on Information Security and Open-ended Working Group with the country's research security practices at home. The three-step pathway is possible with existing institutional arrangements without the need for new pieces of legislation to be passed in parliament to start it.

Conclusion

The opportunity window to establish neural data governance is stark. However, Chile, the European Union, Colorado, Minnesota, and the UNESCO have already set a trend, which is going to become a binding international benchmark in the next. India has a choice: to be involved in their design by showcasing its own seriousness and undergoing CII reclassification, or play by the rules created by others without wide concern for India's strategic environment. Neural data is not a future worry anymore; it is being generated in present at Indian defence laboratories and civilian markets. India is known for its democracy, scientific capability, and diplomatic stature and has the capability to take the leadership on this question. The strategic intent will be tested by observing whether it acts in advance of the setting of the architectural framework set by others.

References

¹ DRDO, "Pioneering Military Psychology Research For India's Armed Forces", *Technology Focus*, Vol 23, Issue 02, Mar-Apr 2025, accessed 02 Jun 2026, https://drdo.gov.in/drdo/sites/default/files/publication-document/TF_MarApr2025.pdf

² Ministry of Electronics and Information Technology, Government of India, 'The Digital Personal Data Protection Act, 2023', *Gazette of India*, 11 Aug 2023, accessed 02 Jun 2026, <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

³ National Critical Information Infrastructure Protection Centre, "Guidelines for Protection of Critical Information Infrastructure", *NCIIPC*, 2021, accessed 02 Jun 2026, https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

⁴ República de Chile, "Ley No. 21.383: Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas", *Biblioteca del Congreso Nacional*, Oct 2021, accessed 02 Jun 2026, <https://www.bcn.cl/leychile/navegar?idNorma=1166983>

⁵ Colorado General Assembly, "HB 24-1058: Concerning Protecting the Privacy of Individuals' Biological Data", signed 17 Apr 2024, accessed 02 Jun 2026, <https://leg.colorado.gov/bills/hb24-1058>

⁶ Minnesota Legislature, "HF 4757: Consumer Data Privacy Act", 2024 Session, accessed 02 Jun 2026, <https://www.revisor.mn.gov/bills/bill.php?b=House&f=HF4757&ssn=0&y=2024>

⁷ “Recommendation on the Ethics of Neurotechnology”, *UNESCO*, 11 Nov 2025, accessed 02 Jun 2026, <https://www.unesco.org/en/legal-affairs/recommendation-ethics-neurotechnology>

⁸ “TechDispatch #1/2024-Neurodata”, *European Data Protection Supervisor*, 2024, accessed 02 Jun 2026, https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en

⁹ Jared Genser, Stephen Damianos, and Rafael Yuste, “Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies”, *NeuroRights Foundation*, Apr 2024, accessed 02 Jun 2026, https://perseus-strategies.com/wp-content/uploads/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf

¹⁰ Larry M Wortzel, “Chinese Expectations for Biotechnology and Cognitive Enhancement in Future Warfare”, *Modern War Institute at West Point*, 2022, accessed 02 Jun 2026, https://mwi.westpoint.edu/wp-content/uploads/2022/10/2022-10-05-MWI_Chinese_Biotechnology_Wortzel.pdf

Ms Kritika is an experienced interdisciplinary researcher specialising in the bridging of human, technical, and organisational perspectives of digital risk. Her work spans over the disciplines of cybersecurity, neuro-cybersecurity, human centric psychology and cyber diplomacy.

Article uploaded on 06-07-2026

Disclaimer: The views expressed are those of the author and do not necessarily represent the views of the organisation that he/she belongs to or of the USI of India.