INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

NEUROTECHNOLOGY AND THE LAW: PRIVACY AND LIABILITY CHALLENGES OF BRAIN–COMPUTER INTERFACES IN THE DIGITAL AGE

AUTHOR - ATCHAYA A, GUEST LECTURER, GOVERNMENT LAW COLLEGE, TIRUCHIRAPPALLI

BEST CITATION - ATCHAYA A, NEUROTECHNOLOGY AND THE LAW: PRIVACY AND LIABILITY CHALLENGES OF BRAIN–COMPUTER INTERFACES IN THE DIGITAL AGE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 670-678, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI – https://doi.org/10.65393/RIWQ2280

ABSTRACT

The brain-computer interfaces (BCIs) are a revolutionary mixture of neuroscience, biomedical engineering, and digital technology that allows communication between the human brain and external devices. Paralysis, enabled new forms of communication is an examples of the therapeutic and assistive potential that have resulted from the BCI application. At the same time they bring up new critical legal issues. This article looks at the BCI technology's privacy, security, and liability issues together with its neuro-rights and existing legal frameworks. We investigate the concepts of traditional data protection, medical device regulation, intellectual property law, and tort liability as they relate to neural data and BCI systems, pinpoint the major shortcomings in existing legal protection, and recommend a regulatory framework that is comprehensive and unique that is specifically designed to manage the risks that are characteristic of neuro-modulation. India is given a special status where recent - went through the country's constitution - recognition of privacy and the Digital Personal Data Protection Act, 2023 are steps towards the future neuro-rights protection, though urgent statutory and regulatory reforms remain necessary.

Keywords: Brain–computer interfaces, neuro-rights, neural data, mental privacy, cybersecurity, liability, DPDPA, neurotechnology regulation

I. INTRODUCTION:

Neurotechnology has successfully integrated cutting-edge computing, bioelectronics, and AI, and has radically changed its application from mere theoretical use in clinics and commerce to practical ones, with brain-computer interfaces (BCIs) being the most significant of all[1130]. These elaborate systems, with the aid of non-invasive EEG headsets, semi-invasive sensors, or invasive microelectrode arrays, are capturing the brain signals of the users and then translating them into commands for external devices; Neuralink, for instance, is already working on human trails and their consumer products[1131]. In the field of therapy, BCIs are used not only to restore motor functions for the patients with spinal cord injuries, but also to allow the patients with ALS to communicate, and they are even being considered in the treatment of neuropsychiatric disorders[1132]. On the other hand, the range of consumer applications includes, but is not limited to, enhanced human-computer interaction, neuro-feedback gaming, education, and cognitive monitoring. Still, in the whole BCIs process, the most sensitive part of human consciousness thoughts, intentions, emotions,

[1130] Cybersecurity for Brain-Computer Interfaces: Protecting Neural Data, AKITRA (Feb. 26, 2025), https://akitra.com/cybersecurity-for-brain-computer-interfaces/.akitra

[1131] Han Yang, Regulating Neural Data Processing in the Age of BCIs, Neural Data Prot. Rev. (Mar. 27, 2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC11951885/.iapp

[1132] IP Protection for Neural Innovation: India's Patent Law, GLOBAL PAT. FILING (Feb. 18, 2025), https://www.globalpatentfiling.com/blog/Biomedical-Patent-of-Brain-Computer-Interface-Navigating-India-s-Ip-Protection-Framework.ijllr

and preferences that are undetectable by conventional surveillance is accessed, which raises concerns about privacy and security—besides data breaches, there is a whole range of these risks that include direct interference with will and mental states through hacking or malfunctioning. Neuro-rights are thus established as necessary safeguards against such abuses, thereby granting mental privacy and freedom[1133]. However, in India and most other places, these rights are still in their formative stages, and the protection afforded by medical device laws, data protection regulations, IP regimes, and tort doctrines which are all rather unsuitable for tech-driven contexts will have to continue[1134]. This article discusses the issues surrounding BCI privacy, cybersecurity, and liability and proposes legislative reforms as the solution.

II. UNDERSTANDING BRAIN–COMPUTER INTERFACES AND NEURAL DATA

A. Technology Architecture and Signal Processing:

BCIs work through a multi-stage process consisting of signal acquisition, preprocessing and feature extraction, decoding, and output. Non-invasive BCIs record brain activity by detecting electrical potentials across the scalp, which results in lower spatial resolution but offers a higher comfort level as well as fewer risks. Invasive BCIs use microelectrode arrays that can be placed directly on or inside the brain, thus achieving better quality signals and allowing more complicated decoding.

AI and deep learning are becoming an integral part of BCIs helping to decode extremely complex patterns in the brain. New developments in the field have enabled BCIs to recognize visual content of mental processing, silent speech, motor actions, mood states, and even tendencies towards particular behavior. Such inferences are made through statistical associations that are learned from the training data, and they are usually non-transparent to both consumers and authorities, this is commonly referred to as "algorithmic opacity."

B. The Unique Nature of Neural Data:

Neural data is a whole different story compared to standard personal data as it has the power to uncover very private feelings, wishes, and mental activities that people might not want to disclose or might not even be aware of, thus revealing the inner mental life without any filters in a manner that is neither through social media data nor through normal medical records. Brain-computer interface systems often take this data passively and continuously, allowing different uses to be made of the signals that were originally recorded for medical or limited purposes and later repurposed for deep analyses without the user being actively aware of it. Once the data is recorded, it can be preserved, reprocessed, and reinterpreted as the decoding techniques progress, thus the previous brain activity is always at risk of being subjected to new forms of analysis that the person whose data it is could never fully foresee or take back. Neural patterns, even if anonymized, still look distinct and stable enough for individuals to be distinctive when these datasets are merged with other information, and machine-learning models built on such data can make extensive inferences about features and states that are well beyond the original reason for collection[1135]. Being a collection of such features, they apply to the situation that warrants the treating of neural data as a unique instance with an exceptionally protected status rather than being classified as merely one more group of sensitive personal data that is subject to existing regulatory frameworks.

[1133] Shreya Agarwal, Neuro-Law: Ethical and Legal Challenges of Brain-Computer Interfaces, 15 INDIAN J. LEGAL RES. 45 (Dec. 27, 2024), https://www.ijllr.com/post/neuro-law-ethical-and-legal-challenges-of-brain-computer-interfaces.pmc.ncbi.nlm.nih

[1134] Mental Privacy and State Responsibility: Constitutional Dilemmas in the Codification of Neurorights, CONSTITUTIONAL DISCOURSE (Sept. 20, 2025), https://constitutionaldiscourse.com/mental-privacy-and-state-responsibility-constitutional-dilemmas-in-the-codification-of-neuro.digitalcommons.schulichlaw.dal

[1135] Id.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

III. CYBERSECURITY THREATS AND VULNERABILITIES IN BCIs

A. Threat Landscape:

BCI systems encounter complex cybersecurity threats that not only include traditional data breaches but also the direct manipulation of cognitive and motor functions, with vulnerabilities found in the entire chain from hardware through firmware, software, wireless transmission, cloud infrastructure, and even supply chain. Malicious firmware updates and weak wireless authentication in integrated processors can result in either malware injection or unauthorized access, while the problem of power limitations stops the use of strong encryption methods. Machine-learning decoders can be misled, for instance, by making inputs that lead the system to wrongly interpret the signal or by introducing biases in the training data through misleading samples, this type of attack is known as adversarial attack. Besides, there are also risks of neural data interception during wireless transmission to controllers or cloud servers that are not properly encrypted. Cloud processing increases the risk of database breaches and security gaps between different systems that lead to fragmented security, while a compromised supply chain from the manufacturing of components to the distribution of algorithms opens accidental entry points for systemic attacks[1136]. These intertwined vulnerabilities are the basis for the paradigm shift in security for BCI systems where their neural integrity is the core along with the traditional protection of data.

B. Attack Scenarios and Consequences:

BCI attack scenarios include covert surveillance as well as large-scale disruption, and their consequences affect deeply mental privacy, autonomy, and even physical safety. Through wiretapping or hacking of cloud storage, unauthorized access to the neural data may lead to remote "mind-reading" and exploitation of thoughts, memories, and likes for blackmail, discrimination, or targeted manipulation. In case of a neuro-stimulation system, bad actors could stimulate the users by sending them through unwanted sensations, emotions, or motor activities, whereas malware or ransomware could corrupt or even lock the users out of the BCI systems they use for communication or mobility, thus making the mind–machine link hostage. Even more subtle cognitive manipulation could be carried out by attackers if they alter the feedback or insert persuasive texts in BCI outputs, thus gradually changing the beliefs and decisions under the pretext of free choice[1137]. A major compromise in a BCI platform that has been widely deployed could have similar consequences for millions of concurrent users, which could not only lead to the incapacitation of key personnel, destabilization of social order but also facilitate hostile actors to collect sensitive mental information from entire populations[1138].

C. Current Inadequacies in Cybersecurity Standards:

There is still disagreement on the cybersecurity standards and best practices in the BCI field at the moment. The cybersecurity of regular medical devices tackles the usual threats like unauthorized changes to device settings or taking control of pumps or pacemakers from a distance but does not consider the unique neural interface aspect[1139]. Traditionally, companies that market consumer brain-computer interfaces (BCIs) have not considered neural data to be something that needs special protection, and as a result, privacy policies frequently allow brain data to be shared with external parties, along with

[1136] Colin Conrad and Carla Heggie, "Legal and Ethical Challenges Raised By Advances in Brain-Computer Interface Technology" (2024) 21:2 CJLT 201, Canadian Journal of Law and Technology, https://digitalcommons.schulichlaw.dal.ca/cjlt/vol21/iss2/1/

[1137] Study Offers Measures for Safeguarding Brain Implants, YALE NEWS (July 23, 2025), https://news.yale.edu/2025/07/23/study-offers-measures-safeguarding-brain-implants.news.yale

[1138] Livanis E, Voultsos P, Vadikolias K, et al. (April 14, 2024) Understanding the Ethical Issues of Brain-Computer Interfaces (BCIs): A Blessing or the Beginning of a Dystopian Future?, https://www.cureus.com/articles/232122-understanding-the-ethical-issues-of-brain-computer-interfaces-bcis-a-blessing-or-the-beginning-of-a-dystopian-future

[1139] Supra Note 1

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

vague restrictions on further sale or different uses.

IV. PRIVACY, MENTAL AUTONOMY, AND COGNITIVE LIBERTY

A. Mental Privacy as a Fundamental Right:

"Mental privacy" is a legal right that gives access to one's neural data and eventually helps to keep thoughts, intentions, and process of thinking known only to the person who wants to share them. It is different from the traditional privacy rights because it deals with the most private and deepest human experience the very being of one's mind. With the neuro-rights concept coming into being four basic protections are proposed:

1. ***Right to Mental Privacy:*** Control over neural data and not having thoughts accessed without permission.
2. ***Right to Cognitive Liberty (or free Will):*** Ability to make a choice whether to use neurotechnology or not and not to be forced or involuntarily made to change one's mind or capabilities.
3. ***Right to Mental Integrity:*** Guaranteed that consciousness will not be subjected to unauthorized interference or manipulation.
4. ***Right to Psychological Continuity:*** The identity of the person is maintained and self-represented over time consistently even though influenced by neurotechnology.[1140].

B. Cognitive Liberty and Manipulation Risks:

"Cognitive liberty" means that one has the right to think freely and also to determine if and in what way to make use of the cognitive-altering technologies. The brain-computer interface (BCI) is a case where the cognitive liberty to decide for oneself is at risk from many angles:

Coercive Enhancement and Surveillance: In workplaces or educational institutions, the use of BCIs may be forcibly or subtly adopted through the terms of productivity boost or safety monitoring[1141]. After the installation, BCIs give the possibility of continuous mind-reading of workers or students who may think that they are unable to refuse without losing the opportunity.

Algorithmic Bias and Opacity: The neural signal interpretation models based on machine-learning are typically "black boxes" even the developers and users cannot see and understand how they come up with the output. If the training data is biased against a certain group of people, they may have their signals misinterpreted. Users will not be able to comprehend easily why a BCI is producing certain commands and thus cannot correct or dispute wrong inferences.

Nudging and Persuasion: The BCI systems can be designed in a way that they will persuade you to choose a specific option by feeding you with the right kind of feedback at the right time, making the suggestion more persuasive, and so on. Unlike direct manipulation, subtle nudging goes on without your knowledge and feels like a choice to the person exerted upon.

Subliminal Stimulation: Neuro-stimulating BCIs can provide the stimulation that would lead to the changes in a person's mood, preference, or attitude towards the given decision. The users would not know that their mental state is being changed by technology[1142].

C. Data Protection Law and Its Limitations:

Neural data protection by the current regimes is still available but no proper measures are in place that could solve BCI-related issues.

GDPR of the European Union recognizes biometric data as a particular category of personal data which needs more protection and thus classifies it under Article 9. It is very likely that neural data will be included in this

[1140] Supra note 7

[1141] Francis X Shen, 'Mind, Body, and the Criminal Law' (2013) 36(2) Harvard Journal of Law and Public Policy 653 https://journals.law.harvard.edu/jlpp/wp-content/uploads/sites/90/2013/04/36_2_653_Shen.pdf

[1142] Supra Note 7

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

classification too. Unfortunately, though, the GDPR does not place explicit restrictions on the commodification of mental autonomy or on the use of such data for the purpose of predicting or influencing behavior. Furthermore, the consent-based model of the GDPR relies heavily on individuals' capacity to give informed consent to the processing; however, the process of granting consent to the collection of neural data happens to be very poorly informed most of the times, and additionally, consent cannot really be said to be fully voluntary if the process is encouraged or coerced through incentives[1143].

The Digital Personal Data Protection Act, 2023 (DPDPA) of India puts the individual as the focal point and provides for the individual's rights to transparency, data access, correction, and deletion. However, the DPDPA does not single out neural data as a category that needs to be protected or regulated in the same manner as other major categories of personal data. It defines "sensitive personal data" in a rather restrictive way and does not mention specifically brain signals or anything derived from the brain. This has led to a scenario where the brain data can be considered in light of the definition of "sensitive personal data" as being the same as biometric data but the legislation does not take into account the different risks associated with neural data such as access and manipulation [1144].

The Medical Device Regulations (in India, the Medical Device Rules, 2017) are focused on the safety, efficacy, and quality of medical devices but the regulation does not approach data protection and cybersecurity from a neuroscience perspective. The regulations were formulated when there was not so much neural data being handled and hence they are not equipped with the privacy and cognitive liberty dilemmas that BCIs present.

D. Recommended Enhancements to Privacy Protection:

In order to safeguard properly mental privacy and cognitive liberty, the legal reforms should be as follows:

1. ***Neural Data Should Be Assuredly Classified as Heightened-Risk Personal Data:*** Statutory frameworks should recognize neural data including brain signals, patterns derived from neural decoding, and inferences about mental states as being in a special category of sensitive data which merits enhanced protection beyond that of ordinary personal data.
2. ***Dynamic, Renewed Consent Should Be Mandated:*** The granting of static consent to BCI use should not be permissible. The law should stipulate that the BCI user's consent is to be periodically and explicitly renewed and that future inferences and uses of neural data that are foreseeable, will be listed out as part of the consent. It should not just be at the time of adoption that consent is required, but with every significant change in use case or inference capability thereafter.
3. ***Coercive Enhancement Should Be Prohibited:*** Legal frameworks should make it illegal to require the use of BCIs as a condition for employment, education, or access to essential services. Taking any steps that lead to BCI use becoming de facto compulsory should be regarded as a form of coercion.
4. ***Algorithmic Transparency Should Be Required:*** Organizations that apply BCI decoding algorithms should make public the ways in which mental state inferences are made, the algorithm's biases or limitations, and whether the algorithm has been tested on user groups that have similar characteristics to the user.

[1143] Securing Neuro-Privacy, VIDHI LEGAL POL'Y (Sept. 16, 2025), https://vidhilegalpolicy.in/blog/securing-neuro-privacy/.vidhilegalpolicy
[1144] Anurag Sourot and Deepali Kushwaha, "Critical Analysis Of The Digital Personal Data Protection Act, 2023", Indian Journal of Law and Legal Research, ISSN: 2582-8878 | Volume VII Issue II, PIF: 7.142

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

5. ***Cognitive Liberty Protections Should Be Established:*** The law should positively ban the use of subliminal stimulation, undisclosed persuasion, and manipulation through BCIs, while providing stronger penalties for such violations.

V. LIABILITY FRAMEWORKS AND BCI-RELATED HARMS

A. Nature of BCI-Related Harms:

The consequences of defective, insecure, or misused BCIs can be categorized in various ways:

Physical Injury: The failure of a BCI device or its decoding algorithm leads to an unexpected movement of the prosthetic limb, a faulty communication system, or a neuro-stimulation system delivering an excessive amount of current, which in turn, causes damage to the tissue.

Mental and Psychological Harm: Unauthorized access to neural data is a source of emotional distress, shame, or anxiety. The stimulation method causes unwanted emotional states (fear, pain, dysphoria). Cognitive interference impairs decision making.

Identity and Personality Alteration: The use of BCIs for repeated or long-term manipulation changes an individual's characteristics, values, or preferences in ways that threaten the psychological continuity and personal identity.

Economic and Social Harm: The invasion of privacy in the form of leaked neural data grants the access to, and ultimately, the treatment of an individual according to one's mental characteristics, thus facilitating discrimination (e.g. denial of employment, insurance, or credit), blackmail, or social exclusion.

Informational Injury: The unauthorized collection or reporting of neural data results in a dignitary harm a violation of cognitive autonomy even when there are no tangible physical, emotional, or economic effects.

B. Existing Liability Doctrines and Their Application:

Current liability theories are unable to effectively deal with BCI injuries due to the long causation chains and the nature of the injuries being non-physical. The Consumer Protection Act, 2019 which is an example of a product liability regime, holds the manufacturers responsible for the defective design or the manufacturing, but on the other hand, proving the direct causation is a big challenge when the insecure firmware allows for cyberattacks that result in subtle cognitive manipulation or delayed behavioral effects and thus, the traditional remedies are not enough to compensate for the great harm done to a person's dignity who is simply a victim of unauthorized access to neural control. Professional liability creates obligations for physicians and researchers with respect to informed consent, device setting up, and monitoring, but the division of responsibility among the non-medical parties such as tech manufacturers, software developers, and cloud providers makes the enforcement of such liability very difficult[1145]. General negligence requires proving a duty of care, for example, by installing state-of-the-art cybersecurity, breach through unencrypted communication, and a tangible injury resulting from exploited weaknesses, though a number of jurisdictions argue whether data access per se is sufficient to claim recoverable harm. Strict liability for abnormally dangerous activities provides possible advantages considering the close relationship between the brain and the injury's severity, but the courts are still not classifying BCIs in this way.

C. The Challenge of Causation and Proof:

One of the most significant hurdles to getting compensation for BCI-related damages is the issue of causation. For example, let's say a BCI user experiences emotional distress after unauthorized access to their neural data but cannot prove that the data was misused in any

[1145] Supra Note 4

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

way. Then, the question arises if harm has been done. Or consider a case where a user's character slowly transforms after a prolonged use of a persuasion-enabled BCI, can that transformation be the result of the BCI or just life experience and maturation? Courts are often so strict with their requirements that they ask for evidence of specific and identifiable injuries, however, the damages caused by the access or manipulation of neural data are often diffuse, cumulative, and difficult to link with certainty to the BCI. The comparative fault issue also gets very complicated: if a person sustains injury due to a device malfunction and, at the same time, there is a malicious third party attack, how will the compensation be divided? The traditional legal approach divides liability according to causal contribution, but in the case of cybersecurity, the line between manufacturer negligence and attacker's misconduct becomes very blurry.

D. Recommended Liability Reforms:

Legal frameworks should be developed to solve these problems as follows:

1. ***Recognition of Neural Data Access as a Compensable Injury:*** Law should treat unauthorized access to neural data as an injury to privacy and cognitive rights, which can be claimed even if there is no subsequent misuse or no economic/physical harm done.
2. ***Strict Liability or Enhanced Negligence Standards for BCI Cybersecurity:*** Due to the gravity of possible damages and the high level of technical knowledge of manufacturers, the legal system could impose strict liability for BCI cybersecurity breaches that lead to unauthorized access to neural data, or at the very least, a heightened negligence standard where BCI is considered negligent if it does not apply encryption, access controls, and other industry best practices.
3. ***Legal Protections for Good-Faith Disclosure:*** Law could set up safe harbors to limit liability for promptly disclosing and remedying security vulnerabilities and to keep full liability for negligent failure to discover or disclose known vulnerabilities.
4. ***Cybersecurity Insurance and Incident Response Plans Required:*** Regulatory requirements may be set up to ensure that BCI manufacturers and service providers have adequate cybersecurity insurance and have detailed incident response plans in place that cover the scenarios of neural data breach or cognitive manipulation, with users needing to be notified in specified timeframes.
5. ***Component Suppliers to be Held Jointly and Severally Liable:*** To avoid splitting of responsibility, the law could place joint and several liability on manufacturers, software developers.

VI. THE INDIAN LEGAL LANDSCAPE: CURRENT PROTECTIONS AND CRITICAL GAPS

The constitutional and statutory structure of India provides some support for the neuro-rights, but the existing privacy and regulatory systems still create considerable voids concerning neural data, security of the user's mind, and freedom of thought.

A. Constitutional privacy and Neuro-rights:

In K.S. Puttaswamy v. Union of India, the Supreme Court acknowledged privacy as a fundamental right, which also included informational privacy, through Article 21, and connected it with dignity and autonomy. The Court's insistence on privacy as a non-static concept implies that neural data privacy and cognitive freedom might eventually be inferred from Article 21 as neurotechnology becomes more advanced, albeit depending solely on judicial interpretation is still uncertain without clear amendments or new laws.

B. DPDPA 2023 and Neural Data:

The Digital Personal Data Protection Act, 2023 has a regulatory framework based on user

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

consent, designates sensitive personal information comprising biometrics among such data, gives rights to the data principals, and adds on the data fiduciaries with duties of disclosing, doing less data processing, and securing data under supervision of a Data Protection Board. For neural data, the main issues are: its uncertain position in the categories of sensitive data, excessive dependence on informed consent when neural inferences are unclear, lack of safeguards against cognitive manipulation, sanctions not adjusted according to the severity of neural invasions, and no cybersecurity standards for BCI.

C. Medical device and Patent Regimes:

Therapeutic Brain-Computer Interfaces (BCIs) are classified as Medical Devices according to the Medical Device Rules of 2017. Consequently, they are regulated based on risk, approvals and quality but not on neural privacy, cybersecurity or cognitive liberty. The patent law exclusions for algorithms and medical methods set forth in the Patents Act of 1970 create challenges for BCI patentability making it necessary to adopt trade secrets as the only option that leads to less transparency and therefore less regulatory and societal scrutiny of neurotechnologies[1146].

D. Emerging Discourse on Neuro-Rights in India:

The disagreements surrounding the cognitive freedom and the right to one's own thought processes are being progressively clarified by Indian scholarship, which advocates for their incorporation as aspects of dignity and privacy under Article 21. This is done through citing Puttaswamy and the wider controversies over AI-rights, thus coming to the conclusion that neuro-rights are a natural development of the already existing basic rights[1147].

VII. PROPOSED REGULATORY ARCHITECTURE FOR INDIA

A. Immediate Statutory Reforms:

Modification of DPDPA: The DPDPA should be modified:

1. To, in an unambiguous manner, identify neural data as a special category of sensitive personal data and thus, as a matter of course, subject to heightened protection;
2. To provide for obligatory, periodic consent renewal for the processing of neural data, with a clear specification of the intended uses and inferences;
3. To explicitly prevent the banning of employment, education, or access to basic services based on the refusal to use BCIs or the revelation of neural data;
4. To prescribe very high security measures for the protection of neural data;
5. To set fines that are specifically proportionate to the breaches of neural data.

Creation of a Neuro-Privacy Ombudsman: A legislative expert organization should be formed with the power to:

1. Look into grievances regarding access to neural data or manipulation of consciousness without authorization;
2. Perform inspections of BCI systems to check for adherence to cybersecurity and privacy standards;
3. Publish recommendations on the legal and illegal applications of neural data;
4. Keep the Parliament and regulators informed about the neurotechnology policy matters.

B. Medium-Term Regulatory Reforms:

Proposed Neurotechnology Regulation Act: This comprehensive neurotechnology-specific legislation should be enacted by India that would consist of the following features:

[1146] International Bioethics Committee of UNESCO. Ethical issues of neurotechnology-report adopted in December 2021. UNESCO, 2022, https://books.google.co.in/books?hl=en&lr=&id=9R2gEAAAQBAJ&oi=fnd&pg=PA9&ots=5WsouNtKSc&sig=25QNhZ_-3-s7ThHtzNaKSEsoarM&redir_esc=y#v=onepage&q&f=false

[1147] Supra Note 3

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

(a) Classification of BCI Systems: The classification system would classify BCI systems between high-risk devices that would be subjected to a regulatory regime that would be pre-market approval coupled with heightened scrutiny;

(b) Cybersecurity Requirements: Manufacturers would need to implement and keep up security standards that are in line with the best practices and include encryption, access controls, secure updates, and incident response protocols among others;

(c) Informed Consent Standards: The explicit and layman-friendly elucidation of the neural data collection, possible inferences, and future uses would be a requirement. Consent would be periodically reconfirmed and could be revoked;

(d) Transparency and Explainability: Transparency would be required for algorithms used in the decoding of neural signals; the manufacturers would be responsible for revealing training data composition, biases, and validation results;

(e) Prohibition on Cognitive Manipulation: There would be a statutory prohibition on subliminal stimulation, undisclosed persuasion, and cognitive manipulation through BCIs, and enhanced criminal penalties would be imposed;

(f) Special Protections for Vulnerable Populations: Children, persons with cognitive disabilities, and others in precarious situations would be granted increased protection, which would include stricter consent requirements and proxy safeguards;

(g) Liability Allocation: A clear distribution of duties would be among manufacturers, service providers, healthcare professionals, and users, with the possibility of joint and several liabilities where more than one party is at fault for the injury.

C. Long-Term Constitutional Recognition:

Long-term perspective, India should think of either i.e.,

(i) explicit constitutional acknowledgment of neuro-rights or,

(ii) Continuous judicial interpretation broadening Article 21 to cover cognitive liberty and neural privacy. Chile has set a precedent by granting constitutional recognition to the ***"right to mental integrity, free will, and thought"*** as a response to neurotechnology; India's similar approach cannot be ruled out.

The official recognition of neuro rights would bring the following advantages:

- Constitutional recognition is guaranteed to be enduring and immune to legislative changes;
- Elevating neuro-rights to that of fundamental rights which come with powerful judicial protection;
- Pronouncement that any type of interference with cognitive freedom is unheard of in the Constitution;
- Compliance with India's liberal democratic odds of giving and taking the rights of individual dignity and self-determination.

VIII. CONCLUSION

Brain–computer interfaces are revolutionary technologies that deliver major therapeutic advantages alongside creating enormous risks since they are positioned at the very source of human thinking. In this regard, cybersecurity threats are not limited to ordinary data breaches but can extend to the interference of thoughts and even the distortion of the mind. The current legal frameworks data protection law, medical device regulation, and tort liability can reduce some of the risks but at the same time they leave serious issues unaddressed, especially concerning mental privacy and cognitive manipulation. The idea of neuro-rights, which is the protection of mental privacy, cognitive liberty, mental integrity, and psychological continuity, presents a principled approach to fill the void created by these issues. The Indian Supreme Court's ruling that privacy is a fundamental right and the passing of the