From Privacy to Cognitive Liberty: Constitutional Protection against Neuro-Data Exploitation and Emerging Digital Technologies under India's Data Protection Framework

Mrs M Razia Begum[1], Dr. Md Adil [2]

[1]Assistant Professor in Law, Osmania University, Hyderabad.

[2]Associate professor, MSS Law College

DOI: 10.64823/ijter.2606004

***Abstract*:** With the advent of the digital age, there is a paradigmatic change in the exploitation and manipulation of information. Traditionally, the digital economy leveraged behaviorally induced externalities, including clicks, geolocations, shopping behaviors, and search records. But now, in the current context, the frontier of technological extraction extends much farther inward to invade the last bastion of personal freedom, namely, the individual mind itself. With the exponential rise in the field of neurotechnology, artificial intelligence (AI), and Brain-Computer Interfaces (BCIs), there has arisen a novel possibility of monitoring, recording, decoding, and even controlling human brain processes, thus raising existential, ethical, and juristic dilemmas, necessitating the development of jurisprudence for "cognitive liberty" and "mental privacy," not only globally but specifically within the Republic of India.

As global discourse intensifies, spurred by milestones such as Neuralink's continued human trials and the United Nations Educational, Scientific and Cultural Organization's (UNESCO) 2025 recommendations on the ethics of neurotechnology, jurisdictions worldwide are scrambling to erect statutory safeguards against neuro-data exploitation. Within India, the intersection of constitutional rights and digital data governance presents a complex tapestry of profound foundational protections juxtaposed against glaring statutory lacunae. While the Supreme Court of India has established formidable precedents safeguarding psychological integrity and the right against self-incrimination, the legislative architecture, most notably the Digital Personal Data Protection (DPDP) Act of 2023 and its subsequent 2025 Rules, remains dangerously unequipped to manage the unique threats posed by neuro-data extraction. This paper intends to shed light upon that discourse by providing a probable roadmap by the end.

Keywords: security, privacy , dignity, protection, technology

I. INTRODUCTION

The stakes in this regulatory battle cannot be overstated. A failure to regulate neural data exposes citizens to cognitive manipulation, unauthorized biometric profiling, and the erosion of free will. This report exhaustively

analyzes the scientific realities of neurotechnology, the constitutional anchors of mental privacy in India, the inadequacies of current data protection frameworks, the lessons from global comparative law, and the strategic imperatives required to safeguard cognitive liberty in the twenty-first century.

In order to effectively regulate neurotechnology, it is necessary to understand how it works, how it interacts within the wider context of digital technology, and its potential evolution. Neurotechnology refers to any technological tool, machine, or system that directly interacts with the human nervous system for the purpose of monitoring, recording, or manipulating neural activity. Neural data, sometimes also called brain data or neuro-data, refers to data derived from the measurement of nervous system activity.

II. Significance

Neural data capture is different across technological modalities, with different levels of fidelity, intrusiveness, and application. Commercial EEGs and NIRS measure localized scalp potentials and hemodynamic changes in relation to cortical neural activity, respectively. Both ear mounted and surface biometric sensors are currently being used to infer affective state, attention spans, and cognitive load without penetrating the skin. In contrast, invasive technologies like ultra-thin films, placed on the surface of the brain, and arrays of microelectrodes, which are implanted in the brain, are able to record high resolution, real-time brain activity from the tissue itself.

These neural signals are very much unlike the typical digital or behavioral data. They have the power to expose emotions, thoughts, intentions, prejudices, and attitudes that a person might presume to keep entirely to themselves and that he/she would not desire to be known. Combining these raw signals with the advanced capabilities of AI and machine learning enables the decoding of these signals into structured physiological and psychological profiles.

III. Scope Of The Study

This study examines the role of quantum technologies in transforming the defence sector, with a particular focus on India. It analyzes the strategic applications of quantum computing, communication, and sensing in military operations.

The scope includes an evaluation of India’s current capabilities, policy initiatives, and preparedness in adopting quantum technologies. It also explores global developments and comparative perspectives to assess India’s position in the international arena.

The study is limited to defence and strategic applications of quantum technologies and does not extend to their civilian or commercial uses.

IV. Aims And Objectives

Aims

To critically evaluate the vulnerabilities of India’s current digital data governance framework against the unique challenges posed by neurotechnology, and to propose a robust legal paradigm that guarantees "cognitive liberty" and "mental privacy".

Specific Objectives

- **Analyze the Technological Landscape:** To examine how neurotechnologies (EEGs, BCIs, and the Internet of Bodies) capture, decode, and potentially manipulate subconscious neural data.
- **Evaluate Constitutional Anchors:** To assess the depth of existing constitutional protections for psychological integrity under Article 21 (K.S. Puttaswamy) and the right against forced cognitive extraction under Article 20(3) (Selvi v. State of Karnataka).
- **Identify Statutory Lacunae:** To scrutinize the Digital Personal Data Protection (DPDP) Act of 2023 and its 2025 Rules, focusing on their failure to classify neural data as sensitive personal data and the risks of unchecked State exemptions.
- **Examine the Subconscious Economy:** To investigate the ethical and commercial implications of neuromarketing and the effectiveness of corporate self-regulation by 2026.
- **Formulate Regulatory Reform**: To propose specific statutory and constitutional recommendations, including algorithmic audits, strict data localization, and an explicit constitutional amendment for neuro-rights.

V. HYPOTHESIS

While India's constitutional jurisprudence implicitly safeguards mental privacy, the current statutory framework, specifically the DPDP Act, 2023, is fundamentally unequipped to regulate neuro-data. Without a dedicated, neuro-specific legal regime and an explicit constitutional amendment for cognitive liberty, citizens remain highly vulnerable to commercial exploitation and invasive State surveillance.

VI. RESEARCH METHODOLOGY

This study adopts a qualitative doctrinal research approach, focusing on the analysis of legal, strategic, and policy-oriented materials related to DPDP Act

Primary Sources:
Government reports, policy documents (such as national quantum missions), defence white papers, and official publications related to India's strategic and technological initiatives.

Secondary Sources:
Scholarly articles, research papers, books, think-tank reports, and expert analyses on quantum technologies and their defence applications.
The methodology aims to provide a critical and analytical understanding of the strategic, legal, and policy dimensions of cybersecurity, offering both descriptive insights and normative recommendations.

From Privacy to Cognitive Liberty: Constitutional Protection against Neuro-Data Exploitation and Emerging Digital Technologies under India's Data Protection Framework

The Transition from IoT to the Internet of Bodies (IoB)

The embedding of neurotechnology in the wider digital world has been a catalyst for the development of an "Internet of Bodies" (IoB) in which the human biological body is an ongoing, connected, and highly sensitive source of data. The IoB trajectory has three stages of increasing privacy threats.

The first generation includes peripheral smart wearables, like fitness trackers and smartwatches, that continuously stream a lot of peripheral biometric data to third-party servers. The second generation includes internalized, implanted medical devices including pacemakers or a digital ingestible pill that send medical information directly from inside the human body. The third generation is the new technological frontier and it directly integrates cutting-edge technology into the human biological system with Brain-Computer Interfaces. These systems are designed to be able to decipher brain waves and to be able to connect directly with cognitive functions. In this third generation, the sensor is not only measuring external actions, but it is measuring someone's inner life, and making the human mind a node in a commercial network.

Brain Fingerprinting and Bidirectional Capabilities.

A crucial aspect of this neurological transformation is the so-called "brain fingerprinting. The scientific evidence suggests that the human brain has unique traits that are influenced by a combination of genetic, non-genetic biological and environmental factors. This means that 3-D brain structure and the corresponding unique neural responses provide individual "biometric" signatures. Neural information is the most intimate of personal data that can be obtained because it carries information not only about predispositions towards disease but also about future behaviours and reveal deep personal characteristics of a subject without his or her conscious knowledge or control.

Moreover, neurotechnology is not a one-way street, while genomic sequencing is merely an observation-based science, neurotechnology has two faces. BCIs can be used to acquire brain data and to produce neurological inputs to change brain activity and behavior; these possibilities are extremely dangerous, not only in the context of commercial exploitation of the brain, but also when used by state actors or military for cognitive surveillance and cognitive enhancement of soldiers. With the ability to read and more importantly write into the neural circuitry, the cornerstone legal principles of intent, autonomy and culpability are undermined.

The Subconscious Economy: Neuromarketing in 2026

Neural data has commodified cognitively free repositories for profit, giving rise to what has been called the "subconscious economy"a market that commodifies cognitive freedom on an industrial scale. By 2026, the $155 billion global marketing industry will have turned to neuromarketing with unprecedented vigorleaving behind clicks, surveys, and focus groups, to uncover what the consumer's brain unconsciously discloses.

Since roughly 95% of our buying decisions are made unconsciously, and sincefours times longer Emotional Memory holds out thanfours times weaker Rational Memory, neuromarketing has proved an extraordinarily powerful commercial tool.

Constituting the modern day neuromarketing infrastructure, an elaborate technological matrix is in place which aims to transduce neural responses into predictive creative intelligence.

The quality of neural data that can be gathered using various modalities (fidelity, intrusiveness etc) also varies greatly. Non-invasive modalities (commercial EEG headsets, fNIRS for example) are capable of using the localized activity recorded at the scalp or brain surface to infer neural activity, while intrusives like different

body mounted and in-skin biometric sensors can be used to assess affect, focus, or workload. Invasive ways (esp. micropatterned arrays, ultra-thin cortical films) are able to provide high fidelity information in a highly spatially and temporally specific manner.
Unlike conventional digital or behavioral data, such neural data can expose mental states that individuals can justifiably assume to be truly privatelike subconscious emotional responses, unspoken intentions, implicit biases, or psychological predispositions. With sophisticated AI and machine learning algorithms, the raw biological information can be turned into structured biological, psychological profiles.

The Transition from IoT to the Internet of Bodies (IoB) The convergence of neurotechnology with the ubiquitous digital sphere has led to the development of the "Internet of Bodies" (IoB), a concept in which the human body makes up a ceaseless, interconnected stream of data of an extraordinarily private nature.

This journey can be defined by three successive generations of IoBs.The earliest generation is embodiedit's external and wearable, a device like a smartwatch or a wearable fitness monitor that feeds enormous amounts of biometric data to third-party servers.

The second generation, now a laboratory event, is embedded: medical implants, like digital ingestible pills and cardioverter-defibrillators that send information directly to the health-care network from within the body. The challenge now is to go further to move from the third generation sensors that reach inside the body and monitor us to those like Brain-Computer Interfaces that reach into the brain.

BCI's are designed "to measure brain waves and interface with brain activity." And this is where we are now. In the third, we're taking the human mind and turning it into an avatar or node on a commercial network.

Herein lies another fundamental consumer application of this neurological evolution, "brain fingerprinting". Researchers universally agree that each human brain's attributes are set by a person's specific blend of genetic, non-genetic biological, and ambient conditions.

So, every brain's structure and every cell's neural responses are an unparalleled biometric measure. As neural data is used to circumstantially determine one's health risks, project future actions, and reveal one's innermost self without that person's knowledge or consent, the "most private of private information" Further, Consider note that neurotechnology differs from genomic sequencing in that it has a two way street.

BCIs can receive and interpret data, as well as produce mental stimuli to change brain activity and behavior.1 This makes neurotechnology even more dangerous, enabling it to be exploited to influence consumer behavior against the individual's will, or to be used in military settings to spy on and then enhance soldier's minds. The progression to a writing and reading technology critically undermines the legal wheels of intent, agency, and culpability.

The commodification of neural data has quickly led to a "subconscious economy", a world where cognitive liberty is actively being sold to the highest bidder. For example, by 2026 the world market for marketing will have moved headlong into "neuromarketing, " abandoning clicks, surveys, and focus groups as too primitive to piece together half of the information stored in people's brains involuntarily.

Consider that around 95 percent of a buyer's decisions are made unconsciously, while emotional memory endures four times as long as rational memory; neuromarketing is a diabolically effective economic tool.

Today, neuromarketing architecture is built on a robust multi-leveled layer stack, which translates brain signals into predictive creative intelligence. Even proponents of neuromarketing admit that non-invasive ways of gathering data cannot "literally Read" thoughts, Still they do claim that such systems can accurately "decode" the neural and physiological responses that automatically occur in response to stimuli which are related to motivation, preference, and a person's values and identity.

For example, activity levels in the left prefrontal cortex have been found to be one of the most dependable neural markers of approach behavior and positive appraisal. It seems, perhaps disconcertingly, that neurophysiological responses to package art, story modulation and price points are like singularities that reliably inform marketers on what factors contribute most to valuation while at the same time eludes the consumer's rational god head.

The ethical line separating empathic marketing from coercive exploitation is dangerously close, when the use of AI-equipped neural data models can produce "real-time... emotional byproducts at scale.

"Absent legal barriers preventing corporatists from influencing individuals by how their subconscious mental health shapes their emotion, any agency consumer rationality cheats the door. To safeguard these risks, the industry in 2026 has adopted a self-regulatory code, the "Golden Rules of Neural Storytelling" requiring that no neural data should be gathered without consent, must only be kept in aggregate, and optimally used to serve, rather than manipulate the user.

Psychology's trust in this system will rely on its emotional veracity, its reciprocity, and the ability for the consumer to retain control over her biometrical streams. And, the industry increasingly adopts "conscious AI" produced systems like the conscious AI which ceases the ad when the program detects that the consumer is being far too cognitively or emotionally taxed. Yet history has demonstrated that corporate self-regulation is always less profitable than behavioral prediction, warning of the strength of the legal remedy necessary.

Though India does not have statutory law on neuro-rights, the theoretical and constitutional basis for protecting mental privacy is well-established within Indian jurisprudence. The Indian Supreme Court has steadily developed an understanding of fundamental rights that values the sanctity of the mental integrity of the individual.

Article 21 and K S Puttaswamy V Union of India

Article 21 of the Constitution of India brings for a fundamental right to life and personal liberty.
It serves as the Foundation for the right to self determination and personal autonomy. The furthest inthejurisprudential development of this right came from the nine-judge bench verdict of K. Puttaswamy(Rted) v. Union of India (2017). The judgment was unanimous in acknowledging the position that the right to privacy is a fundamental, inseparable component of the fundamental right to life and personal liberty. Importantly for the neurotechnology debate, Puttaswamy identified that privacy is not just physical in nature, but mental: it is psychological. The Court articulated the concepts of 'informational privacy' and 'informational self-determination' as intrinsic to human dignity, defending them in the human brain.

In so doing, the Court articulated that the concept of informational privacy safeguards the integrity of individual consciousness. The mind was a crucial component of a person's personal identity. In his plurality opinion, D.Y. Chandrachud J. observed that within our protected fundamental rights is the space of privacy including our right to mental integrity, decisional autonomy, and the sanctity of one's inner subjective life from unwarranted State/non-State intrusions, quoting Lily @ Rajesh v. State of Haryana, the Court held that a person has a right to legal remedies that too shall not nor subject his body or mind to any pain or anguish nor to any indignity. The Court linked the concept of autonomy to mental sovereignty once and for all, irrespective of whether such autonomy is encompassed within 'public order' or not. Article 19 is held to be fulfilled "only when a person shall be entitled to choose his own option uninfluenced by compulsion".

The implications of Puttaswamy for neuro-rights are far-reaching. If informational privacy is constitutionally implicit, then the involuntary extraction, commercial commodification, or non-consensual monitoring of neural data is a clear contravention of Article 21.

A bright line conditionality test of any intrusion into a right to privacy is set forth in the judgment: State or private interference must be authorized by law, necessary in a democratic society, proportionate (ie, the subjection of individual to public interests must be proportional to the benefits), and encumbered with procedural safeguards. right to cognitive liberty defined as the exercise of the self related to one's own thoughts and mental life free from external algorithms-making it a necessary extension of India's current privacy jurisprudence.

And, together with Article 19, which commands for the elevation of speech and expression to functional status, the right to form internal thoughts free from external corruptive algorithms (ie, the right to freedom of thought) can now be formally constitutionally immortalized.

Article 20(3) and Selvi v. State of Karnataka While Puttaswamy articulated the sweeping right to informational and mental privacy, the Supreme Court's 2010 decision in Selvi v. State of Karnataka, gives an extremely particularized safeguarding against the forcible collection of cognitive information.

The case considered whether it was constitutional to involuntarily administer early neuro-scientific methods of investigation, narcoanalysis, polygraph testing, and the Brain Electrical Activation Profile (BEAP) teston accused suspects and witnesses during investigation into a crime.2 The fundamental legal issue was whether the right against self-incrimination under Article 20(3) of the Indian Constitution (which protection was expressed in the negative no person accused of an offence shall be compelled to be a witness against himself) extended to the sale of such physiological responses as evidence.

The State argued that since the physiological responses are not verbal messages, it would be unreasonable to consider that any incriminating statement has originated from them.

But a three-judge bench presided by the then Chief Justice K. G. Balakrishnan unequivocally put an end to this argument. The Court made some newsworthy observation that directly set the limits for the contemporary neuro-rights debate: Expansion of Testimonial ActsUpon defining "testimonial acts" as the acts of another that reveal some knowledge, belief, or feeling, the Court then expanded the Court's definition to include

manifestations of bodily processes as means of testimonial acts. In so doing, the Court effectively equated brain electrical firing and autonomic physiological responses as testimonial acts.

Mental Privacy and Substantive Due Process: The Court explicitly references mental privacy and states that compelling a person to take part in such tests would violate the substantive due process line necessary to limit individual liberty. It is an unjustified intrusion into individual liberty and a clear violation of the right of privacy guaranteed by Article 21.

Total Ban on Forced Use of Techniques: The Court held that no person accused, suspect or witness could be made to undergo these procedures.

Testing in such cases had to be through totally voluntary and uninformed consent, with the person being aware of the nature and the effects of the test to be performed. Reliability and Human Dignity:The justification for the prohibition of forcing cognitive extraction in human subjects is to protect the reliability of evidence, voluntariness of confession and the fundamental dignity of the individual and boundaries of psyche. The use of machines that cause involuntary confessions violates the right to a fair trial.

The Selvi judgement continues as the bedrock for cognitive liberty in India. Overturning the practice of non-consensual probes into concealed awareness using primitive forms of neurotechnology (BEAP), Indian judiciary established the jurisprudential precedent to prohibit contemporary neural wide-net surveillance using AI.

While the constitutional guarantees of Puttaswamy and Selvi are But reassuring in language, the extent of India's statutory structure remains perilously underconstructed to regulate the intricacies of neuro-data. The Digital Personal Data Protection (DPDP) Act, 2023, and the DPDP Rules (followed in November 2025) represent India's first comprehensive regulation of the data processing lifecycle in digital personal data.

The Act is widely applicable across multiple fields and has extraterritorial jurisdiction, with any foreign company with Indian users subject to its regulations, and open to strict penalties up to IN 250 crore (roughly USD$ 30 million) if a committed breach. Still, a detailed examination reveals significant weaknesses of the law with cognitive freedom.

The most significant defect of the DPDP Act (except a few other) is that of not giving special treatment to neural data as a separate, special category of sensitive personal data. The prior regulation of the InternetChapter 5A of the Information Technology Act and the SPDI Rules, 2011 entitled "Sensitive Personal Data or Information" or (SPDI) to more substantial safeguarding by including sensitive data like neural and medical images.

By stark contrast, the DPDP Act 2023, by not providing a sub-category of sensitive data, imposes a level playing field on all kinds of information processing to have homogenized rules to govern all processing.

Statutory Deficits: Analyzing the DPDP Act 2023 and 2025 Rules

Despite the constitutional protections afforded by Puttaswamy and Selvi, India's statutory setup remains dangerously unprepared to address the subtleties of neuro-data processing. The DPDP Act, 2023 (also supported by its DPDP Rules, 2025 finalized in November 2025) is India's first comprehensive statute on digital personal data processing.

Its scope spans all sectors and has extraterritorial implications for global enterprises serving Indian citizens, with strict criminal penalties of up to INR 250 crore (about USD 30 million). On closer inspection of the statute itself Yet there are significant weaknesses in its approach towards cognitive liberty.

The lack of categorization of neural data as a separate, specialized category of sensitive personal data is the system's most significant defect. What in the pre-existing system was the more robust classification of 'Sensitive Personal Data or Information' (SPDI) or protectively under Section 43A of the Information Technology Act and 2011 Rules, could encompass biometric and medical data, among others is absent here - all personal data is treated as one. As a result, neuro-data, which is the most deeply personal immutable blueprint of humankind, is governed by exactly the same default mechanisms that govern everyday behavioral data, like e-mails or browsing patterns.

The IDPDP Act's failure leaves individuals vulnerable to "inferential misuse, " where tech firms harvest innocuous sounding raw neural waves and apply an AI-driven algorithm approach to identify the best mental/psychological profiles, subconscious emotional states, and the vulnerabilities of individuals with no statutory constraint. There are no separate countermeasures of the involuntary or passive data collection in the DPDP Act and consent alone cannot solve the basic issue of inability to opt out of brain waves.

Based on the notice and consent process, the DPDP Act grants consent for data processing. The implementation schedule applies a phased approach beginning 18 months after the Rules come into effect in November 2025. The DPB was set up in November 2025 for administrative authority. After the Consent Manager Setup comes into being by 13 November 2026, enterprises can also register as third-party intermediaries and consent managers so users are addressed for no less than 8 months.

All businesses within the coverage mark will then have until mid of May 2027. But, given a single static consent (often inferred through opaque labyrinths of ubiquitous Terms of Service and Terms and Conditions) cannot apply when involuntary, ongoing neural signals are collected, the legal community maintainsand the device industry agrees that users must be able discover, revoke and redefine consent.

In practice this will mean the meta-data (through firmware and companion smartphone apps) must include a live dashboard for 'open channels, ipso facto processing purposes, second and third-party recipients, and a 'limit and withdraw' option--a guideline in the silent provisions of the DPDP Act without explicit direct-to-consumer dynamic opt-in protocols, neurotech manufacturers will be able to install ongoing biological streams based on open-ended initial consent agreements.

Rule 13 of the DPDP Rules 2025 states specific requirements and obligations imposed on the Significant Data Fiduciaries (SDFs), which are key for consumption of new technology and high risks they entail. It mandates SDFs to perform a DPIAs once a year, subject to independent audit, and carry out due diligence to ensure technical measures including algorithmic software being used for processing fail to pose any risk of the Data Principal's rights; and undertake measures so that specific personal data (suggested by a committee of Central

Government) is not transferred outside the territory of India-this direction is a blueprint toward data localization.

If Rule 13 could be effective as monitoring in neurotechnology, it would be because consumer neurotech companies are still subjected to the volumetric or risk-based thresholds that would license their classification as SDFs. If such a neurotech startup processing brains, which are among the most sensitive of biometric data, would have a small group of users, would ever be categorized as non-SDF, then it would also not be subject to the most necessary DPIAs or algorithm audit.

For this reason, the most distinctive risks of biometric re-identification, cognitive manipulation, and neural data leakage, fall entirely outside regulatory control for a large proportion of the commercialization industry. State Exemptions and the Nature of Threat. So arguably the greatest threat of the DPDP system shows up at the State's wide exemptions to the Act.

It enables the government to escape from disclosure obligations with an entire range of clauses e.g. national security sovereignty law enforcement, public order.

When incorporated into the context of neurotechnology, these exceptions open the floodgates to devastating dual-use applications and the prospect of ubiquitous mental monitoring. In the absence of statutory carve-outs for mental privacy from government intrusion, it is conceivable that law enforcement or intelligence agencies could harness neurodata to ferret out intention, subconscious ethnic or racial biases and emotional states, So rendering the technology a tool for 'forcible extraction of thoughts'.

This presents a conflict-incapable of resolution with the applied constitutional safeguards as formed in Selvi and Puttaswamy, demanding the carve-out of an independent, neuro-specific statutory regime.

3. Algorithmic Audits and Prohibition of Cognitive Manipulation

There is a need for statutory red lines to ensure the prevention of the mutual weaponization of neuro-data through corporations.

Mandatory DPIAs: Regardless of their scale and classification as a Significant Data Fiduciary, any entity that processes neural data using AI technology needs to undertake mandatory and independent Data Protection Impact Assessments (DPIAs), with explicit focus being put on algorithmic biases, vulnerability to biometric manipulation, and the risk of emotional manipulation.

Subliminal Influence Prohibited: The use of brain-computer interface technology to stimulate the brain artificially in a manner that overrides consciousness, alters personality, and manipulates consumer behaviors should be regarded as a serious statutory crime.

Anti-Discrimination Measures: There must be an outright prohibition of sharing neural data with employers, educational institutions, and life and health insurance companies unless there is clear and un-coerced consent, thus ensuring the prevention of creation of a neuro-biological underclass.

4. Data sovereignty and state restraint

Brain data is very sensitive, and geographical and governmental barriers must be strong.

Strict Data Localization: Neural data must be subject to strict Data Localization or be inaccessible to foreign parties and subject to the whims of adversarial parties. It has to be under the control of India alone, not being able to be bypassed through international usage of servers.
The general exemption provision for the State in the DPDP Act should be significantly limited with regard to neural data. Data concerning citizens' cognition should not be allowed to be used routinely by law enforcement or intelligence services. The access should be made available only through an exceptional judicial warrant, which should be granted on the basis of the conditions of a strict probable cause, thus abiding by the absolute ban on forced cognitive extraction in Selvi v State of Karnataka.

5. Conclusion

Statutory provisions are required to give operational rules, but the best safeguard against the invasion of the human mind must be constitutional. While the speed at which technology is developing, there is a need for an express recognition in the law for the basis provided by the Supreme Court's interpretation of Article 21 in Puttaswamy. There is a need to include a constitutional amendment in the Indian Parliament that explicitly acknowledges neuro-rights, thereby giving rise to the right to cognitive liberty. This amendment should secure the mental privacy, psychological continuity and absolute freedom from non-consensual cognitive intervention as technology becomes increasingly integrated with human biology, the core dignity of the autonomous mind is to be preserved.
The fusion of the human mind and the cyber world is the highest level of technological development. With the advent of neurotechnology and AI, the subconscious layers of human identity are seamlessly uncovered, making traditional notions of data privacy appear outdated. India has the historical opportunity to pioneer the global south with a neuro-rights framework that explicitly safeguards the final sanctuary of human freedom, the unmonitored, autonomous mind, by incorporating international legal precedents with its rich constitutional jurisprudence.

VII. REFERENCES:

[1] . The Right to Privacy: History, Philosophy, and Law – NeGD ..., https://negd.gov.in/blog/the-right-to-privacy-history-philosophy-and-law/

[2] Digital Personal Data Protection Act, 2023 DPDPA SECTION 12 WITH INTERPRETATION, https://www.dpdpa.com/dpdpa2023/chapter-3/section12.htm
[3] Fraternity's Role in Indian Constitution | PDF | Justice | Crime & Violence - Scribd, https://www.scribd.com/document/739496314/FRATERNITY-SIDE-NOTES
[4] Preamble to the Indian Constitution: Meaning, Significance & More - NEXT IAS, https://www.nextias.com/blog/preamble-to-the-indian-constitution/
[5] Finding Method to Madness: The Indian Supreme Court's Dignity ..., https://repository.nls.ac.in/cgi/viewcontent.cgi?article=2029&context=nlsir
[6] Human Dignity in Indian Constitutional Adjudication (Chapter 1), https://www.cambridge.org/core/books/human-dignity-in-asia/human-dignity-in-indian-constitutional-adjudication/7BBB9960207BC44B913E61B155F87D84
[7] K.S. Puttaswamy v. Union of India [2017 SC] - Goa Police Constable PDF - EduRev, https://edurev.in/t/181628/k-s-puttaswamy-v-union-of-india-2017-sc-
[8] Constitutional Law Perspectives on Human Rights and Duties, https://ebooks.inflibnet.ac.in/hrdp01/chapter/constitutional-law-perspectives-on-human-rights-and-duties/
[9] Fundamental rights in India - Wikipedia, https://en.wikipedia.org/wiki/Fundamental_rights_in_India
[10] JUSTICE K.S. PUTTASWAMY (RETD.) & ANR. VS. UNION OF INDIA & ORS. - AWS, https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/justice-ks-puttaswamy-ors-vs-union-of-india-ors-5.pdf
[11] The POSH Act And Article 21: Dignity, Privacy, And Confidentiality In Workplace Harassment Proceedings - RJ Wave, https://www.rjwave.org/ijedr/papers/IJEDR2601086.pdf
[12] JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA - South Asian ..., https://translaw.clpr.org.in/case-law/justice-k-s-puttaswamy-anr-vs-union-of-india-ors-privacy/
[13] Puttaswamy v. Union of India - Wikipedia, https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India
[14] A Comprehensive Analysis of Data Privacy Evolution in India and Digital Personal Data Protection Act, 2023, https://research-communications.cmpcollege.ac.in/wp-content/uploads/2025/01/5-Raje-and-Dr.-Radheshyam-Prasad-REVISED-PAPER-A-Comprehensive-Analysis-of-Data-Privacy-Evolution-in-India-and-Digital-Personal-Data-Protection-Act-2023.pdf