Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Mind, Machine, And Mens Rea Criminal Liability for Actions Mediated by Brain-Computer Interfaces in India

Nagesh Komati

Aurora Higher Education and Research Academy
Deemed to be University
School of Law (LL.M)

Abstract

Brain-computer interfaces (BCIs) translate measured neural activity into commands for computers, communication systems and external devices. Their therapeutic and assistive potential is substantial, but their use complicates a foundational premise of criminal law: that prohibited conduct can be attributed to an accused person who acted voluntarily with the mental element required by the offence. A BCI-mediated event may involve a conscious command, an ambiguous or involuntary neural signal, signal-processing error, algorithmic misclassification, device malfunction or malicious third-party interference. The physical execution of a command therefore does not, without more, establish the user's intention or control.

This article examines the problem through the Indian legal framework, with particular attention to the Bharatiya Nyaya Sanhita 2023 (BNS), the Bharatiya Sakshya Adhiniyam 2023 (BSA), the Constitution of India and the Information Technology Act 2000. It argues that the BNS definition of ‘voluntarily’ in section 2(33) is an under-examined statutory point of entry: it focuses on causing an effect by means intended, or known or reasonably believed likely, to cause it. That definition must be applied to the actual technological chain and cannot be converted into a presumption that a recorded neural signal is a conscious intention. The article also distinguishes the general exception of accident from unsoundness of mind, analyses the constitutional limits on compelled neural interrogation, and explains why admissibility of device records is distinct from the scientific validity of an inference about mens rea.

The article's original contribution is a proposed Neuro-Technological Attribution Test (NTAT), a structured inquiry into (i) the prohibited effect and statutory mental element, (ii) the user's intentional or knowing engagement with the relevant means, (iii) the reliability and operation of the BCI chain, (iv) control and practical capacity to intervene, (v) causation and intervening acts, and (vi) the allocation of responsibility among users and other actors. It further proposes minimum neuro-forensic safeguards for Indian criminal proceedings. The central claim is that criminal liability must rest on legally attributable culpability, not merely on the association between a person's neural data and a machine's output.

Keywords: Brain-computer interface; mens rea; actus reus; voluntariness; Bharatiya Nyaya Sanhita; neural data; neuro-rights; electronic evidence; criminal attribution; cybercrime.

1. Introduction

Criminal law ordinarily proceeds on the premise that a person may be held responsible for conduct that the law prohibits, provided the relevant external elements and the mental element prescribed for the offence are proved. Brain-computer interface technology unsettles the factual simplicity of that premise. A BCI does not merely record brain activity. It acquires neural signals, filters and classifies them, converts the resulting interpretation into a command and transmits that command to a connected device. The device may then move a robotic limb, operate a cursor, communicate a message or control another system. The resulting physical event is therefore mediated by a chain of human, computational and mechanical processes.

The legal difficulty is not that a machine has become a person or that criminal law must recognise a new form of legal subject. The difficulty is attribution. If a BCI-controlled robotic arm injures a bystander, the prosecution must establish who did what, through which means, with what state of mind and with what causal contribution. A person who intentionally directs a machine to injure another cannot avoid liability merely because the machine supplies the final movement. Conversely, a user should not be treated as the author of every machine output merely because the device was connected to that user's neural signals.

The issue has been identified in international scholarship as a possible ‘responsibility gap’ at the intersection of mind and machine. Bublitz, Wolkenstein, Jox and Friedrich examine the legal liabilities of BCI users and the difficulty of assigning responsibility where a user's agency and the machine's operation interact. Their analysis provides an important starting point, but it does not resolve how Indian statutory language, constitutional protections and evidentiary rules should address the problem. This article develops that India-specific inquiry.[1]

The argument is deliberately narrower than a general account of neuro-rights. It focuses on criminal responsibility for conduct mediated by a BCI, including physical acts performed by connected devices and digital acts executed through a neural interface. It does not assume that present-day BCIs can read unrestricted thoughts, reveal a person's complete mental state or reliably decode complex intentions. The legal analysis must be proportionate to the actual capabilities and limitations of the system in question.
A further distinction is necessary between a BCI that merely records neural activity and a BCI that translates activity into operational commands. A record of brain activity may be relevant to a medical or scientific inquiry; an operational interface creates a potential causal pathway from neural activity to external conduct. The latter is the central concern of this article.

2. Research Problem, Questions and Method

2.1 Research problem

The Indian criminal law framework does not contain a bespoke offence or defence for BCI-mediated conduct. The absence of a BCI-specific provision does not mean that ordinary offences cannot apply. Rather, existing rules must be applied to a new factual configuration in which the relationship between

1 Christoph Bublitz, Andreas Wolkenstein, Ralf J Jox and Orsolya Friedrich, ‘Legal Liabilities of BCI-Users: Responsibility Gaps at the Intersection of Mind and Machine?’ (2019) 65 International Journal of Law and Psychiatry 101399 <https://doi.org/10.1016/j.ijlp.2018.10.002> accessed 4 November 2026.

intention, command, machine execution and consequence may be uncertain. The risk is twofold: over-attribution, where a user is prosecuted on the basis of device association alone; and under-attribution, where deliberate misuse or culpable design is obscured by the involvement of technology.

2.2 Research questions

1. How should the BNS concept of voluntarily causing an effect apply where a neural signal is processed by software before a machine acts?
2. Can a neural recording, by itself, prove intention or knowledge for a particular offence?
3. When may BNS sections 18, 19, 22, 23, 24 and 32 be relevant, and what are their limits?
4. How should criminal responsibility be allocated among the user, manufacturer, developer, maintainer and external attacker?
5. What constitutional limits govern compulsory acquisition or interpretation of neural data in criminal investigation?
6. How should the BSA regulate the admissibility, authenticity and probative value of BCI logs and neural recordings?
7. What minimum legal and forensic safeguards should India adopt?

2.3 Methodology and scope

The article adopts a doctrinal and analytical methodology. It examines the text and structure of the BNS and BSA, constitutional provisions, Supreme Court decisions and relevant legislation governing digital systems. It also engages with established interdisciplinary literature on BCI operation, neurotechnology ethics and BCI-related responsibility. Hypothetical fact patterns are used to test the legal propositions. No empirical claim is made about the error rate of any particular commercial or clinical device. Such questions require device-specific evidence and, where appropriate, expert testimony.

The article uses ‘neural signal’, ‘decoded command’ and ‘machine output’ as separate terms. ‘Neural signal’ refers to recorded physiological data; ‘decoded command’ refers to the output of the signal-processing and classification chain; ‘machine output’ refers to the action actually performed by the connected device. The distinction is central to the proposed attribution test.

3. Literature Review and The Article's Original Contribution

The literature relevant to this subject falls into three overlapping strands. The first concerns the technical and clinical development of BCIs. Wolpaw and colleagues describe BCI systems as communication and control pathways that do not depend on the brain's normal output pathways of peripheral nerves and muscles. Their account helps explain why a BCI can translate measured neural activity into external commands, but technical capability does not itself answer the legal question of intention.[2]

The second strand concerns the ethical and human-rights implications of neurotechnology. Ienca and Andorno identify cognitive liberty, mental privacy, mental integrity and psychological continuity as rights that may become increasingly important as technologies access and process brain information. Yuste and colleagues similarly identify privacy and consent, agency and identity, augmentation and bias as ethical

2 Jonathan R Wolpaw and others, ‘Brain-Computer Interfaces for Communication and Control’ (2002) 113 Clinical Neurophysiology 767.

priorities for neurotechnology and artificial intelligence. These contributions illuminate the constitutional stakes, but their primary focus is broader than the elements of criminal liability.[34]

The third strand addresses legal responsibility arising from BCI use. Bublitz and co-authors directly consider the potential responsibility gaps that may arise when brain signals are translated into machine action. Their work is the closest antecedent to the present inquiry. It demonstrates that conventional assumptions about agency and control may be strained when a device mediates the relationship between intention and action.

The present article does not claim that the subject has never been discussed internationally. Its originality lies in the integration of four Indian-law questions that are not resolved by the general literature: first, the significance of the BNS definition of 'voluntarily' in section 2(33); second, the correct separation of accident, necessity, unsoundness of mind and compulsion; third, the interaction between BSA electronic-record provisions and expert evidence; and fourth, the constitutional distinction between compelled testimonial neural examination and the use of operational device data. The proposed NTAT translates these strands into a structured legal method that can be used by investigators, prosecutors, defence counsel and courts.

The article also rejects two overbroad positions. It does not propose that every BCI-related accident should be treated as automatism or unsoundness of mind. Nor does it propose that neural data should be inadmissible as a class. The correct position is conditional: the data may be relevant and, where statutory requirements are met, admissible; but its meaning, reliability and connection to the accused's mental state must be separately established.

4. Technical Architecture and The Problem of Attribution

4.1 The BCI processing chain

A simplified BCI system involves signal acquisition, pre-processing, feature extraction, classification or decoding, command generation and device execution. The precise architecture varies with the device, the intended task, the user, the training process and the clinical or commercial setting. A system may use non-invasive sensors, implanted electrodes or another interface. It may operate in a closed loop, in which feedback from the device affects subsequent user activity, or in a more limited open-loop arrangement.
Each stage creates a distinct evidentiary question. A sensor may capture noisy data; software may filter or transform that data; a classifier may assign a command label; the operating system may transmit the command; and the connected device may execute it. A later forensic report that simply states 'the user's brain signal caused the movement' may conceal the intermediate inferences that require proof.

4.2 The four attribution scenarios

For legal analysis, BCI events should initially be classified into four scenarios:

3 Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life Sciences, Society and Policy 5 <https://doi.org/10.1186/s40504-017-0050-1> accessed 4 November 2026.

4 Rafael Yuste and others, 'Four Ethical Priorities for Neurotechnologies and AI' (2017) 551 Nature 159 <https://doi.org/10.1038/551159a> accessed 4 November 2026.

- Intentional command: the user knowingly generates or selects a command and the system executes it in the intended manner.
- Unintended signal or misclassification: the system treats involuntary, ambiguous or noisy activity as a command, or decodes the signal incorrectly.
- Technical malfunction: the system generates or executes an output because of a hardware, software, calibration, integration or maintenance failure.
- External interference: a third party compromises, alters or remotely controls the interface or connected device.

These categories are not mutually exclusive. A user may intentionally initiate a sequence, after which a malfunction changes the result. A third party may compromise a device that is otherwise functioning normally. A developer's defective design may interact with an operator's failure to update or maintain the system. The purpose of classification is not to predetermine liability but to identify the factual issues that must be investigated.

4.3 Why neural data are not mind-reading

A neural recording is a measurement produced by a particular sensor and processing arrangement. It is not a transparent transcript of a person's thoughts. The same broad neural pattern may be affected by context, task, movement, fatigue, signal quality, training and the decoding model. A system trained to recognise a limited set of commands cannot automatically be treated as capable of identifying a complex criminal intention. The evidentiary claim must therefore be no broader than the validated function of the system.
The distinction between a signal and an intention is particularly important where the prosecution relies on a classifier's output. The classifier may provide evidence that the system assigned a particular command label. It does not, without further proof, establish that the user consciously selected that command, understood its consequence or possessed the mens rea required by the charged offence.

5. Actus Reus, Mens Rea and The BNS Concept of Voluntariness

5.1 The ordinary structure of criminal responsibility

The prosecution must prove the ingredients of the offence charged. Depending on the statutory provision, those ingredients may include conduct, consequence, circumstance, causation and a specified mental state. Indian criminal law generally treats mens rea as an important component of criminal liability unless the statute, expressly or by necessary implication, excludes it. Nathulal v State of Madhya Pradesh is commonly cited for the presumption that mens rea is ordinarily required. State of Maharashtra v Mayer Hans George illustrates that the statutory scheme and legislative purpose may displace that presumption in a particular regulatory offence. Neither decision permits a court to invent a mental element that the statute does not require or to disregard one that it does.[56]

In BCI cases, the relevant mental element must be identified offence by offence. Intention, knowledge, dishonesty, fraudulence, rashness and negligence are not interchangeable. A prosecution for an intentional

5 Nathulal v State of Madhya Pradesh AIR 1966 SC 43.

6 State of Maharashtra v Mayer Hans George AIR 1965 SC 722.

offence cannot be established merely by proving that a device produced a harmful output. A negligence-based offence requires proof of the relevant duty, breach, foreseeability and causal connection according to the applicable legal standard.

5.2 Section 2(33) BNS: voluntarily causing an effect

A central statutory feature is the BNS definition of 'voluntarily'. Section 2(33) provides, in substance, that a person causes an effect voluntarily when the person causes it by means by which the person intended to cause it, or by means which, at the time of employing them, the person knew or had reason to believe were likely to cause it. The definition is directed to the causal effect and the means employed. It is not a general scientific definition of conscious intention, and it should not be treated as one.[7][8][9]

The provision is significant because a BCI user may employ a technological means to produce an effect without physically moving the relevant limb. If the user knowingly selects a command that is designed to make a robotic arm strike another person, the fact that software and motors perform the final movement does not defeat voluntary causation. The user has employed the interface as a means to cause the intended effect.

The harder case is one in which the user generates a signal for a benign purpose but the decoder misclassifies it, or the device executes an unintended output. The court must ask whether the user employed the means that caused the effect and whether, at the time of employing those means, the user intended the effect or knew or had reason to believe that the means were likely to cause it. A user's mere use of a BCI is not equivalent to knowledge that every possible output is likely. The relevant inquiry is contextual and must be informed by the system's design, warnings, training, known limitations, configuration and the user's actual understanding.

The words 'had reason to believe' should not be converted into strict liability. They require an objective assessment grounded in the facts known or reasonably available to the particular user in the circumstances. A trained operator who bypasses a warning that a device may execute an unsafe movement may stand differently from a patient using a prescribed assistive interface in accordance with instructions. The user's capacity, experience, access to information and practical ability to prevent the result may all be relevant.
Section 2(33) therefore offers an important bridge between conventional criminal law and BCI-mediated conduct. It does not solve every problem. It does, however, direct attention away from the simplistic question 'whose brain was connected?' and towards the legally relevant question 'who employed which means, with what intention or knowledge, to cause which effect?'

5.3 Act, omission and distributed execution

Section 3(4) BNS extends references to acts, unless the context indicates otherwise, to illegal omissions. Sections 3(5) and 3(6) address common intention and joint participation with criminal knowledge or intention; section 3(7) recognises that an effect may be caused partly by an act and partly by an omission.

7 Bharatiya Nyaya Sanhita 2023, s 2(33).

8 BNS 2023, s 2(33).

9 BNS 2023, s 2(33); BNS 2023, s 18.

These provisions may matter where a user, operator or technician has a legally relevant duty to disable, maintain or secure a system and fails to do so. They do not create a free-standing duty to prevent every machine malfunction. The source and scope of the alleged duty must be identified.[10][11][12][13]

The same provisions may be relevant to coordinated misuse. If several people knowingly participate in a plan to use a BCI-connected device to commit an offence, the ordinary rules of common intention, abetment or conspiracy may apply, provided their statutory ingredients are proved. The machine is a means through which the criminal act is carried out; it is not a substitute for proof of the participants' individual states of mind.

5.4 Automatism and the Indian statutory framework

Common-law jurisdictions have developed doctrines concerning automatism, including distinctions between insane and non-insane automatism. Decisions such as R v Quick, Hill v Baxter and Bratty v Attorney-General for Northern Ireland illustrate judicial attempts to distinguish involuntary conduct from conduct for which the accused may be held responsible. These cases may be useful by analogy, but they are not binding interpretations of the BNS. Indian courts should begin with the text of the BNS, the constitutional framework and Indian precedent.[14]

A BCI malfunction should not automatically be characterised as automatism in the medical or legal sense. The term may describe a factual claim that the accused's bodily or machine-mediated conduct was not consciously controlled, but the legal consequences must be determined under Indian law. The issue may go to the prosecution's proof of the act or mental element, to the general exception of accident, or to another applicable defence. It should not be forced into section 22 merely because the conduct was unusual or technologically mediated.

6. General Exceptions and Their Limits

6.1 Section 18: accident in doing a lawful act

Section 18 BNS protects an act done by accident or misfortune, without criminal intention or knowledge, while doing a lawful act in a lawful manner, by lawful means and with proper care and caution. A BCI-controlled device that unexpectedly moves and causes injury may raise this exception. The statutory conditions are cumulative in substance: the activity must be lawful; the manner and means must be lawful; the actor must have exercised proper care and caution; and the relevant criminal intention or knowledge must be absent.[15]

10 Bharatiya Nyaya Sanhita 2023, s 3(4)–(7).

11 BNS 2023, s 3(5)–(7), ss 45 and 61.

12 BNS 2023, ss 3(5)–(6), 45 and 61.

13 BNS 2023, ss 3(5)–(7), 45 and 61.

14 R v Quick [1973] QB 910; Hill v Baxter [1958] 1 QB 277; Bratty v Attorney-General for Northern Ireland [1963] AC 386.

15 BNS 2023, ss 18–19.

The user cannot establish the exception merely by asserting that the device malfunctioned. The court should examine whether the system was properly configured, whether required updates or maintenance were ignored, whether the user had been warned about a foreseeable hazard, whether an emergency stop was available and whether the user acted in accordance with training. Conversely, a malfunction that could not reasonably have been detected or prevented despite proper precautions may support the exception.
The exception must also be distinguished from a case in which the user deliberately initiates a dangerous command but claims that the ultimate injury was unintended. Section 2(33) may treat an effect as voluntary where the means employed were intended or known or reasonably believed likely to cause it. The court must therefore identify the relevant effect and the means, rather than relying on the user's description of the event.

6.2 Section 19: necessity

Section 19 BNS concerns an act likely to cause harm but done without criminal intention and in good faith to prevent or avoid other harm. It may be relevant where a BCI-controlled device is used in an emergency and a harmful consequence occurs while a greater harm is being prevented. The statutory illustration and conditions must guide the analysis. Necessity is not a general licence to disregard safety protocols, and a user cannot invoke it simply because a machine action was convenient or beneficial.[16]

6.3 Section 22: unsoundness of mind

Section 22 BNS is concerned with a person who, at the time of doing the act, by reason of unsoundness of mind, is incapable of knowing the nature of the act or that the act is wrong or contrary to law. The provision is not a general defence for involuntary neural signals, software errors or device malfunction. A person may be mentally sound while a device misclassifies a signal. Conversely, a person may have a legally relevant mental incapacity independently of the interface.

Dahyabhai Chhaganbhai Thakkar v State of Gujarat explains the relationship between the prosecution's continuing burden to prove the offence and the accused's burden to establish the general exception. The accused's burden in relation to the exception is on the civil standard; evidence may also raise a reasonable doubt about the prosecution's proof of mens rea even where the exception is not conclusively established. Hari Singh Gond v State of Madhya Pradesh reiterates the distinction between medical and legal insanity. These principles are relevant where the accused's mental capacity is genuinely in issue, but they must not be confused with a purely technical failure.[17]

6.4 Sections 23 and 24: intoxication

Sections 23 and 24 BNS address intoxication, including intoxication administered without the person's knowledge or against the person's will and offences requiring particular intention or knowledge. They are not directly applicable merely because a BCI system alters, stimulates or records neural activity. A medical device or neural stimulation is not, without more, ‘intoxication’ within these provisions. If medication or

16 BNS 2023, s 19.

17 BNS 2023, s 22; Dahyabhai Chhaganbhai Thakkar v State of Gujarat AIR 1964 SC 1563.

another intoxicating substance is independently involved, the statutory requirements must be examined on the evidence.[18]

6.5 Section 32: compulsion by threats

Section 32 BNS concerns compulsion by threats that reasonably cause apprehension of instant death, subject to statutory exclusions and provisos. Remote interference with a BCI may involve coercion, but not every cyber intrusion amounts to compulsion by threats within section 32. If a third party takes control of a device without the user's consent, the primary issue may be whether the resulting act is attributable to the user at all. If the user is forced to act under a qualifying threat, section 32 may be considered, but its strict statutory conditions must be satisfied.[19]

6.6 The danger of doctrinal overreach

A recurring analytical error would be to treat every involuntary machine output as a case of unsoundness of mind, or every malfunction as an accident defence. The better sequence is to ask first whether the prosecution has proved the act and mental element. If it has, the court then considers whether a statutory general exception applies. This preserves the distinction between failure of proof and an affirmative defence.

7. Causation and The Allocation Of Responsibility

7.1 The user

A user may be criminally responsible where the prosecution proves that the user intentionally or knowingly employed the BCI system as a means of causing the prohibited effect, or otherwise satisfies the mental element of the charged offence. The device's autonomy does not by itself sever attribution. A person who deliberately sends a command through a machine is not less responsible because the machine performs the physical movement.

The difficult case is an output that departs from the command the user intended or could reasonably foresee. The court should consider whether the departure was so material and independent that it changes the causal attribution, whether the user knew of the risk and whether the user had a practical opportunity to intervene. The analysis should be offence-specific; a negligence offence may apply on facts that do not establish an intentional offence.

7.2 Manufacturer, developer and maintainer

A manufacturer, software developer or maintainer should not be criminally liable merely because a defect is later discovered. Criminal liability requires proof of the elements of an applicable offence, including the relevant mental state where required. Civil product liability, regulatory non-compliance and criminal negligence are distinct forms of responsibility.

Where death is caused by a rash or negligent act, section 106 BNS may be relevant if its ingredients are established. The prosecution would need to identify the responsible person, the relevant act or omission,

18 BNS 2023, ss 23–24; Basdev v State of PEPSU AIR 1956 SC 488.

19 BNS 2023, s 32.

the applicable standard of care, the causal link and the degree of negligence required by the offence. Jacob Mathew v State of Punjab, although arising in the medical negligence context, cautions against converting every error or civil negligence into criminal negligence. Its reasoning may be used carefully by analogy, not as a direct rule for every software or product case.[202122]

A developer who intentionally inserts code to cause unauthorised harm, or knowingly participates in a plan to cause an offence, may be liable under the ordinary provisions of the BNS and, where applicable, the Information Technology Act. A negligent coding error, without the necessary statutory elements, should not be labelled a crime simply because the consequence is serious.

7.3 Third-party interference and cybercrime

An external attacker may compromise the BCI, the user's account, a cloud service or the connected machine. Sections 43 and 66 of the Information Technology Act may be relevant where unauthorised access or other conduct within section 43 is carried out dishonestly or fraudulently. Section 66F should be considered only where its specific statutory requirements for cyberterrorism are satisfied; ordinary hacking or malicious access should not be casually characterised as cyberterrorism.[2324]

Where the attacker causes physical injury through the compromised system, the investigation should consider both the cyber intrusion and the resulting offence against the person or property. The fact that the victim's or user's device generated the final command does not resolve who controlled the system or who caused the result.

7.4 Multiple actors and individualised culpability

A BCI incident may involve a user, developer, manufacturer, maintainer, clinician, service provider and attacker. The presence of multiple actors does not mean that responsibility must be assigned to only one. Nor does it justify collective guilt. Sections 3(5) and 3(6), section 45 on abetment and section 61 on criminal conspiracy may apply where the facts establish the relevant participation, common intention, assistance or agreement. Each accused person's conduct and mental state must be evaluated individually.

8. Constitutional Dimensions: Privacy, Autonomy and Self-Incrimination

8.1 Article 21 and mental privacy

The Supreme Court's nine-judge decision in Justice K S Puttaswamy (Retd) v Union of India recognises privacy as a fundamental right grounded in liberty, dignity and autonomy. Neural information may be especially intimate because it can disclose or support inferences about a person's cognitive processes,

20 BNS 2023, s 106(1).

21 Jacob Mathew v State of Punjab (2005) 6 SCC 1.

22 BNS 2023, s 106; see also Jacob Mathew (n 28) on the need to distinguish civil negligence from criminal negligence in the medical context. The analogy is limited and does not mechanically determine software or product liability.

23 Information Technology Act 2000, ss 43 and 66.

24 IT Act 2000, ss 43, 66 and, where the statutory ingredients are independently satisfied, s 66F.

health, preferences or responses. The degree of sensitivity depends on the device and the data actually collected; it should not be assumed that every BCI can reveal every thought.[25][26]

Any State acquisition or use of neural data must have a lawful basis and satisfy constitutional requirements applicable to restrictions on privacy, including legality, legitimate aim, necessity and proportionality. The State's legitimate interest in investigating serious crime does not eliminate the need for safeguards governing collection, retention, access, interpretation and disclosure. The same concerns arise where a private BCI provider holds data that investigators seek to obtain through lawful process.

8.2 Article 20(3) and compelled neural examination

Article 20(3) protects an accused against being compelled to be a witness against himself. In Selvi v State of Karnataka, the Supreme Court held that involuntary administration of narcoanalysis, polygraph examination and Brain Electrical Activation Profile tests violated Articles 20(3) and 21. The Court's reasoning is important to neurotechnology because it addresses the constitutional limits of compelling a person to undergo scientific procedures designed to elicit information from the mind.[27][28][29]

A distinction must be drawn between a compelled investigative test and operational data generated during ordinary, voluntary use of a BCI. A device log showing that a command was transmitted may be physical or electronic evidence; it is not automatically testimonial communication. But if the State compels an accused to undergo a neural procedure or to disclose the contents of mental processes in a manner that amounts to testimonial compulsion, Selvi becomes directly relevant. The constitutional question depends on the nature of the procedure, the information sought, the compulsion involved and the use proposed.

State of Bombay v Kathi Kalu Oghad and Selvi require careful attention to the distinction between physical evidence and testimonial compulsion. It would be inaccurate to claim that Article 20(3) automatically excludes every neural recording or every item of BCI-generated data. It would be equally inaccurate to treat neural interrogation as an ordinary device search without considering the mental and testimonial dimensions.

8.3 Due process and equality

A fair criminal process requires that an accused be able to understand and challenge the technical case advanced against them. If the prosecution relies on a proprietary classifier, undisclosed training data or a device report that cannot be independently tested, the defence may be deprived of a meaningful opportunity to challenge the inference. Article 21's fair-trial dimension and Article 14's guarantee against arbitrary State action support transparent and reviewable evidentiary procedures.

25 Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

26 Constitution of India 1950, arts 14, 20(3) and 21; Puttaswamy (n 9).

27 Constitution of India 1950, arts 20(3) and 21.

28 Selvi v State of Karnataka (2010) 7 SCC 263.

29 State of Bombay v Kathi Kalu Oghad AIR 1961 SC 1808.

8.4 Data protection

The Digital Personal Data Protection Act 2023 may apply where neural information is digital personal data relating to an identifiable individual, subject to its definitions, commencement and applicable exemptions. Section 17(1)(c) provides an exemption for specified processing necessary for prevention, detection, investigation or prosecution of an offence or contravention. The existence of an exemption does not answer every constitutional question, and the Act should not be presented as a complete neuro-rights code. A more tailored framework may be needed for neural data, particularly in commercial and clinical settings.[30]

9. Neural Evidence Under the Bharatiya Sakshya Adhiniyam, 2023

9.1 Admissibility is not probative force

The BSA recognises electronic and digital records and regulates the proof of their contents. Sections 61 and 62 address the legal status and proof of electronic or digital records; section 63 sets out the admissibility framework for computer outputs and includes a statutory certificate in the Schedule. BCI logs, device histories, signal files, software outputs and network records may fall within the broad field of electronic or digital records, depending on their form and the manner in which they are produced.[3132]

The central evidentiary distinction is between admissibility and weight. A record may satisfy the statutory conditions for admission but still be weak evidence of the proposition for which it is tendered. A system log may prove that the device recorded a signal or issued a command. It does not necessarily prove that the accused consciously intended the command, understood its meaning or foresaw the resulting injury.

9.2 Section 39: expert opinion

Section 39 BSA makes relevant the opinion of persons specially skilled in science, art or another field when the court must form an opinion on such a matter. BCI litigation may require expertise in neuroscience, biomedical engineering, signal processing, machine learning, cybersecurity, software engineering and digital forensics. No single expert should be assumed competent to answer every question in that chain.[3334]

The expert should identify the system examined, the relevant software and firmware versions, the signal acquisition method, the preprocessing steps, the decoding model, the command mapping, the device output and the limitations of the analysis. The expert should distinguish observation from inference and disclose any uncertainty, error rates or validation limitations that are relevant and available. An expert should not express a legal conclusion that the accused possessed mens rea; that is a matter for the court.

30 Digital Personal Data Protection Act 2023, ss 2 and 17(1)(c).

31 BSA 2023, ss 61–63 and the Schedule to the Adhiniyam.

32 BSA 2023, s 63(4) and the Schedule; BSA 2023, ss 61–62.

33 Bharatiya Sakshya Adhiniyam 2023, s 39.

34 BSA 2023, s 39; Selvi (n 8).

9.3 Section 63 and the statutory certificate

The Schedule to section 63 requires specified information about the electronic record source and device, including identifying details and a hash value, and provides for certification by the party and the expert in the prescribed form. Investigators should preserve the original source where possible, make forensic copies, calculate and record hash values, document the extraction method and maintain a chain of custody. Where data are generated across a distributed system, the certificate and accompanying documentation should accurately identify the relevant devices, servers, cloud sources and custodians.

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal and Anvar PV v PK Basheer interpreted section 65B of the former Indian Evidence Act. Those decisions remain important for understanding the predecessor regime and the general concerns surrounding electronic evidence. However, BSA section 63 now governs records to which the BSA applies. The earlier decisions should be used with attention to the statutory text and Schedule of the BSA, rather than assuming that every detail of the former section 65B regime is identical.[35]

9.4 Burden of proof and special knowledge

Section 108 BSA places on the accused the burden of proving circumstances bringing the case within a general exception, while the court presumes the absence of such circumstances. That allocation does not transfer the prosecution's primary burden to prove the offence. Dahyabhai explains that the prosecution must prove the requisite mens rea beyond reasonable doubt; the accused's burden in establishing an exception is on the civil standard, and the evidence may independently create reasonable doubt about an ingredient of the offence.[3637]

Section 109 BSA concerns facts especially within a person's knowledge. It must be applied consistently with Shambhu Nath Mehra v State of Ajmer, which cautions that the special-knowledge rule does not relieve the prosecution of its general burden. In BCI cases, the accused may have particular knowledge of how they used the device, but manufacturers, service providers and investigators may control important logs, source code, configuration records and maintenance information. The court should not assume that technical facts are exclusively within the user's knowledge.[3839]

9.5 A neuro-forensic protocol

8. Preserve the device, source files, logs, firmware, software versions, configuration settings and relevant network records without altering the original data.
9. Record the acquisition method, date and time, time-zone settings, clock synchronisation, operator identity and chain of custody.

35 Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1; Anvar PV v PK Basheer (2014) 10 SCC 473.

36 BSA 2023, ss 108–109; Dahyabhai (n 14).

37 BSA 2023, s 108; Dahyabhai (n 14).

38 Shambhu Nath Mehra v State of Ajmer AIR 1956 SC 404.

39 BSA 2023, s 109; Shambhu Nath Mehra (n 23).

10. Generate and document cryptographic hash values for forensic images and relevant extracted files; retain the hash report.
11. Obtain the BSA section 63 certificate and Schedule documentation where required, identifying each relevant source accurately.
12. Separate raw neural data from filtered data, decoded labels, generated commands and physical device outputs.
13. Disclose material system documentation, validation information and known limitations sufficient to permit meaningful challenge, subject to lawful and proportionate protection of genuine trade secrets.
14. Test plausible alternative explanations, including signal artefact, calibration error, software update, malfunction, unauthorised access and remote interference.
15. Use independent, appropriately qualified experts and require them to state the limits of what the data can establish.

This protocol does not create a new statutory admissibility test. It is a proposed best-practice framework designed to improve reliability, fairness and transparency within the existing BSA structure.

10. The Proposed Neuro-Technological Attribution Test (NTAT)

This article proposes a six-stage Neuro-Technological Attribution Test (NTAT) for courts and investigators. The NTAT is an analytical framework, not a statement of existing binding law. It is intended to organise the questions that must be answered under existing statutory and constitutional rules.

Stage 1: Define the offence and the prohibited effect

The court should identify the precise offence, its conduct element, consequence or circumstance, and the mental element prescribed by the statute. The analysis must not begin with a general impression that a BCI was involved. It must begin with the legal ingredients of the charge.

Stage 2: Identify the means employed and the user's relationship to them

The court should identify what the user actually did: activated the device, selected a command, trained the decoder, accepted an automated suggestion, maintained a mode of operation or did nothing despite a legal duty to act. Section 2(33) BNS requires attention to the means employed and the user's intention, knowledge or reason to believe at the time those means were employed.

Stage 3: Reconstruct the technical chain

The court should distinguish the raw signal, processed signal, decoded command, transmitted instruction and machine output. Each link should be supported by reliable records and appropriately qualified evidence. A conclusion that skips intermediate steps should be treated with caution.

Stage 4: Assess control, capacity to intervene and foreseeability

The court should examine whether the user had practical control over the relevant operation, whether an emergency stop or cancellation facility existed, whether the user was trained, whether the system gave warnings, and whether the risk was reasonably foreseeable to that user. The analysis must be sensitive to disability and the intended assistive function of the device. A person who relies on a BCI because of severe motor impairment should not be judged by assumptions based on a fully able-bodied operator.

Stage 5: Determine causation and intervening events

The court should examine whether the user's conduct remained a legally relevant cause of the prohibited effect, whether a malfunction or external intervention materially changed the chain, and whether any alleged omission was legally blameworthy. The mere presence of multiple causal contributors does not automatically exonerate the user, but an independent and unforeseeable intervention may affect attribution.

Stage 6: Allocate liability individually and test constitutional and evidentiary safeguards

The court should determine the responsibility of each participant separately and ensure that neural evidence was obtained and presented consistently with the Constitution and BSA. The conclusion should state what the evidence proves, what it does not prove and why the applicable mental element or exception is, or is not, established.

10.1 NTAT decision matrix

Scenario	Core question	Likely legal focus
Deliberate harmful command	Did the user intend or knowingly employ the means to cause the effect?	BNS s 2(33); offence-specific mens rea; causation
Signal misclassification	Was the output genuinely selected or reasonably foreseeable?	Technical reliability; act attribution; s 18 where conditions fit
Unforeseeable malfunction	Did the user exercise proper care and caution?	BNS s 18; negligence only if independently established
Emergency intervention	Was harm caused in good faith to prevent greater harm?	BNS s 19
Mental incapacity	Was the statutory incapacity present at the time?	BNS s 22; Dahyabhai
Remote compromise	Who controlled the system and caused the output?	IT Act ss 43/66; BNS offences; causation
Defective design or maintenance	What duty, breach, foreseeability and mental state are proved?	Applicable BNS offence; s 106 where death by rash/negligent act is established

10.2 Why the test is preferable to device ownership or signal association

A rule based on device ownership would be over-inclusive: it could attribute a machine's output to a person who had no control over the device at the relevant time. A rule based solely on the presence of a neural signal would confuse physiological measurement with intention. A rule that always treats malfunction as an intervening cause would be under-inclusive: users may deliberately exploit known system behaviour or ignore foreseeable risks. The NTAT avoids these errors by requiring a staged inquiry into legal elements, technical facts and individual culpability.

11. Hypothetical Applications

11.1 Intentional injury through a robotic limb

A user deliberately selects a BCI command that directs a robotic limb to strike a named person. The device accurately executes the command. The fact that the limb, rather than the user's biological arm, makes contact does not defeat attribution. The prosecution must still prove the ingredients of the particular hurt or homicide offence, including the relevant mental element and causation. Section 2(33) supports the conclusion that a person may voluntarily cause an effect through technological means.

11.2 Accidental injury during assistive use

A person with significant motor impairment uses a prescribed BCI to control a wheelchair. A sensor fault and decoder error cause the wheelchair to move unexpectedly and injure a pedestrian. The prosecution must not infer intention from the fact that the user's neural data were present in the system. It should investigate device condition, calibration, user training, warning information and the possibility of third-party or software interference. Section 18 may be relevant if its requirements, including proper care and caution, are established.

11.3 Known risk and conscious disregard

A trained operator receives repeated warnings that a BCI-controlled industrial arm may misclassify a particular signal and cause a dangerous movement. The operator disables a safety interlock and continues using the system. If injury follows, the case is materially different from an unforeseeable malfunction. The evidence may support knowledge or a negligence-based charge, depending on the offence and the operator's role. The prosecution must prove the applicable statutory elements rather than rely on the seriousness of the result.

11.4 Remote cyber manipulation

An attacker obtains unauthorised access to a BCI-connected device and sends commands that cause injury. The user did not authorise the commands and had no practical control over the compromised system. The investigation should preserve access logs, authentication records, firmware, network traffic and command histories. The attacker may face liability under the IT Act and relevant BNS provisions if the ingredients are proved. The user should not be treated as the principal actor merely because the device was registered to them.

11.5 Compelled or coerced operation

A person is threatened with instant death unless they operate a BCI device to perform an unlawful act. Section 32 may be relevant only if its precise conditions and exclusions are met. If instead the attacker bypasses the interface and directly controls the device, the more fundamental question is whether the user's conduct can be attributed at all. The distinction between coercion and remote control must be preserved.[40]

40 BNS 2023, s 32.

12. Legislative and Institutional Recommendations

12.1 Do not create a broad new offence prematurely

The present doctrinal gap does not necessarily require a new standalone BCI offence. Many harmful acts can already be addressed by existing offences where their ingredients are established. A premature offence could duplicate existing provisions, criminalise mere technical failure or create uncertainty about the relationship between the user and the device. The immediate need is for clear attribution principles, forensic standards and proportionate regulation.

12.2 Adopt a national neuro-forensic protocol

The Ministry of Home Affairs, Ministry of Electronics and Information Technology, forensic science institutions and relevant medical and technical bodies should develop a protocol for preserving and examining neural-interface evidence. The protocol should specify minimum requirements for acquisition, chain of custody, system documentation, validation, expert independence, disclosure and testing of alternative explanations.

12.3 Establish device safety and incident-reporting duties

High-risk BCI systems should be subject to proportionate safety and cybersecurity requirements. Depending on the device and its regulatory classification, these may include pre-deployment testing, change management, vulnerability reporting, audit logs, emergency shutdown mechanisms, user warnings and post-incident preservation. The obligations should be allocated to the actors who can realistically perform them.

12.4 Protect neural data through purpose limitation and access controls

Neural data should be subject to strict purpose limitation, access control, security, retention and disclosure safeguards. A regulatory framework should distinguish data necessary for clinical care from data collected for advertising, profiling, employment, law enforcement or criminal investigation. The legal regime should recognise that a single data set may reveal sensitive health information and may also be used to infer aspects of cognition.

12.5 Build multidisciplinary capacity

Judicial academies, police training institutions, prosecution services and forensic laboratories should develop modules on BCI architecture, neural data, machine-learning classifiers, device logs and constitutional safeguards. Courts should be encouraged to seek properly scoped expert evidence rather than rely on broad claims that a device can ‘read intention’.

12.6 Preserve defence access and adversarial testing

Where the State relies on proprietary BCI software, it should provide sufficient disclosure to enable the accused to challenge the relevant inference. Legitimate trade secrets may be protected through confidentiality orders or controlled inspection, but secrecy should not render the prosecution's decisive technical evidence effectively unchallengeable. The precise disclosure order must balance fair-trial rights with genuine confidentiality interests.

13. Conclusion

Brain-computer interfaces do not displace the foundations of criminal law. They make the factual inquiry into those foundations more complex. The central issue is whether a prohibited effect can be attributed to a person who employed a neural interface and whether the mental element required by the offence is proved. The BNS definition of voluntarily causing an effect in section 2(33) is a particularly important statutory starting point because it directs attention to the means employed and the user's intention, knowledge or reason to believe at the relevant time.

The BNS general exceptions must be applied with doctrinal discipline. Section 18 may address a genuine accident where the statutory conditions are met; section 19 may address necessity; section 22 concerns legal incapacity by reason of unsoundness of mind and is not a general malfunction defence; sections 23 and 24 concern intoxication; and section 32 addresses narrowly defined compulsion by threats. None should be stretched to cover every instance of technologically mediated conduct.

Constitutional safeguards are equally important. Puttaswamy grounds privacy in liberty, dignity and autonomy, while Selvi establishes limits on involuntary scientific techniques that intrude into the mind and implicate self-incrimination. The BSA permits electronic and digital records to be proved subject to statutory conditions, but admissibility does not establish that a neural signal proves conscious intention. Expert evidence must explain the complete technical chain and its limitations.

The proposed Neuro-Technological Attribution Test offers a structured method for identifying the offence, examining the means employed, reconstructing the technical chain, assessing control and foreseeability, determining causation and allocating responsibility individually. It seeks to prevent both unjust attribution to BCI users and artificial immunity for intentional misuse, culpable design or malicious interference.
The governing principle should be clear: a machine's output may be evidence of human conduct, but it is not a substitute for proof of human culpability. Criminal liability in the age of neurotechnology must remain anchored in legality, individual responsibility, reliable evidence and constitutional liberty.

Bibliography

A. Legislation

- Constitution of India 1950.
- Bharatiya Nyaya Sanhita 2023 (Act 45 of 2023).
- Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023).
- Information Technology Act 2000 (Act 21 of 2000).
- Digital Personal Data Protection Act 2023 (Act 22 of 2023).

B. Cases

- Anvar PV v PK Basheer (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
- Basdev v State of PEPSU AIR 1956 SC 488.
- Bratty v Attorney-General for Northern Ireland [1963] AC 386.
- Dahyabhai Chhaganbhai Thakkar v State of Gujarat AIR 1964 SC 1563.
- Hari Singh Gond v State of Madhya Pradesh (2008) 16 SCC 109.

- Hill v Baxter [1958] 1 QB 277.
- Jacob Mathew v State of Punjab (2005) 6 SCC 1.
- Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
- Nathulal v State of Madhya Pradesh AIR 1966 SC 43.
- R v Quick [1973] QB 910.
- Selvi v State of Karnataka (2010) 7 SCC 263.
- Shambhu Nath Mehra v State of Ajmer AIR 1956 SC 404.
- State of Bombay v Kathi Kalu Oghad AIR 1961 SC 1808.
- State of Maharashtra v Mayer Hans George AIR 1965 SC 722.

C. Secondary literature

- Bublitz C, Wolkenstein A, Jox RJ and Friedrich O, 'Legal Liabilities of BCI-Users: Responsibility Gaps at the Intersection of Mind and Machine?' (2019) 65 International Journal of Law and Psychiatry 101399.
- Ienca M and Andorno R, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life Sciences, Society and Policy 5.
- Wolpaw JR and others, 'Brain-Computer Interfaces for Communication and Control' (2002) 113 Clinical Neurophysiology 767.
- Yuste R and others, 'Four Ethical Priorities for Neurotechnologies and AI' (2017) 551 Nature 159.

D. Official and institutional materials

- University Grants Commission, Public Notice, F No 1-1/2018(CARE/JOURNAL) (16 July 2025).
- Consortium for Academic and Research Ethics, UGC-CARE website (accessed 4 November 2026).
- India Code, Government of India, official text of the Bharatiya Nyaya Sanhita 2023 and Bharatiya Sakshya Adhiniyam 2023.