INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE MIND AS THE LAST PRIVACY FRONTIER: WHY ENGLISH LAW MUST ACT BEFORE NEUROTECHNOLOGY RENDERS MENTAL AUTONOMY OBSOLETE

AUTHORED BY - NAISARGI YOGESH DESAI

ABSTRACT

The diffusion of consumer neurotechnology into the commercial sphere has proceeded with a conspicuous absence of legal scrutiny. With the advent of brain-computer interfaces, neural wearables and cognitive monitoring devices there now exists an unprecedented capacity to access the most intimate dimensions of human thoughts and mental life, however English law continues to offer no clear protection for what may be the innermost domain of human privacy. While Chile has constitutionally entrenched neurorights and US states such as Colorado and Montana have adopted standalone neural privacy legislations, the UK remains confined to only patchwork of safeguards embedded within its general existing data protection and privacy laws. This article argues that these prevailing legal frameworks are fundamentally ill-equipped to address the cognitive and mental integrity of individuals against neurotechnological intrusions. Unlike conventional biometric or health data, brain data constitutes a distinct category- it doesn't limit itself from merely capturing bodily functions but records the essence of thought, autonomy and mental integrity. Building on comparative jurisprudence and contemporary scholarship, this article contends that English common law and the Human Rights Act must work towards recognising mental privacy as a standalone fundamental right. Without explicit legal recognition of neurorights, individuals remain vulnerable to the systematic colonisation of their freedom of thought- a harm that extends far beyond conventional data protection concerns. The article investigates how English courts could shape this protection through expansion of existing rights while exploring potential reform avenues for its future. Ultimately, the dilemma is not whether English law will address neurorights, but whether it will engage with them proactively or retroactively, ensuring to establish a framework that is grounded in human dignity amid the rise of direct brain data exfiltration.

ISSN: 2582-6433

BACKGROUND

Neurotechnology encompasses any device capable of recording, interpreting or altering activity in the human brain and nervous system.[1] Only recently have such technologies largely remained confined within clinical and research laboratories. Yet the global neurotechnology market, valued at approximately USD 12.6 billion in 2024, is projected to reach USD 31.1 billion by 2033,[2] with dedicated consumer neurotechnology firms now accounting for 60% of the global landscape.[3] This explosive growth has been fuelled by miniaturisation, artificial intelligence integration and embedding of electroencephalography (EEG) sensors into everyday wearables such as headphones, earbuds, glasses, and wristbands.[4] Neuralink, founded by Elon Musk in 2016, implanted its first human participant with a brain-computer interface in January 2024.[5] By mid-2025, three individuals were using the N1 chip daily to control computers through thought alone.[6] Meta has developed neural interface wristbands that interpret electromyography (EMG) signals—electrical activity generated when the brain sends commands to muscles—to control augmented reality glasses without physical touch.[7] These wrist-worn devices, demonstrated with Meta's Orion AR glasses in September 2024, represent a non-invasive approach to brain-computer interaction that could reach mass consumer markets within years.[8]

The implications extend far beyond medical restoration. Consumer neurotechnology companies market devices promising cognitive enhancement, stress monitoring, focus optimisation and even thought-controlled gaming.[9] Yet unlike medical devices subject to rigorous ethical oversight and health privacy regulations, consumer neurotechnology operates in a regulatory vacuum. Neurotechnology risks becoming the "universal controller" for human-technology interaction—with profound consequences for privacy, autonomy, and self-determination if left unregulated.[10]

[1] Jan-Christoph Bublitz and Christoph Merkel, 'Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination' (2014) 8 Criminal Law and Philosophy 51, 53.
[2] 'Neurotechnology Market Size, Share, Trends Report 2025-33' (IMARC Group, 2024)
[3] 'Neurotech consumer market atlas – How the sector is making moves into the mainstream' (Centre for Emerging Technology and Security, 14 October 2025)
[4] Ibid.
[5] Andrea Lavazza, 'Neuralink's brain-computer interfaces: medical innovations and ethical concerns' (2025) 3 Frontiers in Human Dynamics 1.
[6] '9 Leading Brain-Computer Interface Companies and their current and prospective products' (Ross Dawson, 6 July 2025)
[7] 'Meta developed a "neural interface" for its next-gen Orion AR glasses' (TechCrunch, 24 September 2024)
[8] Ibid.
[9] 'Neurotech consumer market atlas' (n 3).
[10] Nita A Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St Martin's Press 2023) 8-10.

ISSN: 2582-6433

The Unique Nature of Neural Data: Beyond Biometric Classification

Brain data is largely regarded as different among traditional categories of personal information protected under existing frameworks. The UK General Data Protection Regulation (UK GDPR) classifies biometric data as "special category data" under Article 9, subject to heightened protection when processed "for the purpose of uniquely identifying a natural person."[11] Yet this provision, designed for fingerprints and facial recognition, inadequately addresses the revelatory nature of neural information.

Neural signals are involuntary; individuals cannot control what their brain activity reveals about their mental states, emotions, or cognitive processes.[12] As research demonstrates, brain recordings can identify individuals through unique neural signatures—much like fingerprints—but they also disclose far more sensitive information.[13] Advanced machine learning algorithms applied to EEG data can infer political beliefs, emotional states, unconscious biases, mental health conditions, and even predict future behaviour.[14] The European GDPR study commissioned by the European Parliament states that brain data should be treated as inherently sensitive, regardless of collection purpose, because its "potentiality for revealing personal data via processing or repurposing" is extraordinarily high.[15]

This presents a conceptual challenge for UK GDPR, which categorises data sensitivity based on collection purpose rather than intrinsic nature. Neural data collected for "wellness" or "productivity" monitoring in non-medical contexts may not qualify as health data under Article 9,[16] despite revealing precisely the same intimate mental information as medical brain scans. The UK Information Commissioner's Office (ICO) has suggested treating neurodata as health information under Article 9,[17] however this interpretation lacks binding authority and fails to address consumer neurotechnologies explicitly marketed for non-health purposes. The result gives rise to a critically risky void: corporate entities can harvest, analyse, and potentially monetise brain data without the stringent consent, purpose limitation and security requirements that govern medical information.

[11] UK General Data Protection Regulation, art 9(1).
[12] Colorado House Bill 24-1058, Legislative Declaration s 1(a) (2024).
[13] Sarah Rainey and others, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns related to neurotechnology?' (2020) 29 Journal of Law and the Biosciences 1, 8-12.
[14] Ibid 15-18.
[15] Ibid 24.
[16] Ibid 20-21.
[17] 'Neurodata Consent Frameworks: Managing EEG/Brain-Computer Interface Data Under GDPR and CCPA' (SecurePrivacy, 13 April 2025)

ISSN: 2582-6433

The Global Movement for Neurorights

Recognising these inadequacies, jurisdictions worldwide have begun establishing legal frameworks specifically addressing neural privacy. Chile represents the vanguard of this movement. In October 2021, Chile became the first nation to amend its Constitution to protect neurorights, inserting provisions safeguarding "mental integrity" and establishing that "scientific and technological development shall be carried out with respect for life and physical and mental integrity," with "special safeguards for cerebral activity as well as the information deriving from it."[18] This was followed by implementing legislation establishing five core neurorights: mental privacy, personal identity, free will, fair access to mental augmentation, and protection from algorithmic bias.[19]

In August 2023, Chile's Supreme Court applied these provisions in a landmark decision ordering US-based brain-computer interface company Emotiv to erase brain data collected from a Chilean senator without adequate consent.[20] The Court held that neural information constitutes an extension of personal identity deserving constitutional protection equivalent to bodily organs—it cannot be bought, sold, or manipulated without informed consent and robust safeguards.[21]

The United States has witnessed parallel developments at the state level. Colorado amended its Privacy Act in April 2024 to classify "neural data"—defined as "information generated by the measurement of the activity of an individual's central or peripheral nervous systems"—as sensitive data requiring explicit opt-in consent, data protection impact assessments, and respect for deletion requests.[22] The amendment, which took effect in August 2024, represents the first US privacy law explicitly addressing brain data.[23] Montana followed suit in May 2025, amending its Genetic Information Privacy Act to include neurotechnology data, with even more stringent protections including mandatory clear privacy notices, express consent requirements, consumer access and deletion rights, security safeguards, warrant requirements for government access, and restrictions on sharing with employers or insurers.[24] These provisions became

[18] Constitution of Chile, art 19(1) (amended 2021). See Sebastián Ruiz, 'Neurorights in the Constitution: from neurotechnology to ethics and law' (2024) 379 Philosophical Transactions of the Royal Society B 1.
[19] 'Mission' (Neurorights Foundation); Rafael Yuste and others, 'Four ethical priorities for neurotechnologies and AI' (2017) 551 Nature 159.
[20] María Inés Cornejo-Plaza, 'Chilean Supreme Court ruling on the protection of brain data, between neurorights and personal data' (2024) 15 Frontiers in Psychology 1.
[21] Ibid.
[22] Colorado Privacy Act (n 12).
[23] 'Colorado's Privacy Law Gets in on the Brain Wave Action' (Eye on Privacy, 5 August 2024)
[24] Montana Senate Bill 163 (2025).

ISSN: 2582-6433

effective on 1 October 2025.[25] California enacted similar protections through Senate Bill 1223 in 2024, classifying neural data as sensitive personal information.[26]

These jurisdictions share a common recognition: existing privacy and data protection frameworks, designed in pre-neurotechnology eras, cannot adequately safeguard the intimate sphere of human thought and mental autonomy. The question confronting English law is whether it will proactively develop comparable protections or reactively address harms only after neurotechnology has become deeply embedded in daily life.

English Law's Current Framework: Fragmented and Inadequate

English law approaches privacy through a patchwork of statutory and common law protections. The UK GDPR and Data Protection Act 2018 establish baseline requirements for personal data processing, including special protections for sensitive categories. The Human Rights Act 1998 (HRA) incorporates Article 8 of the European Convention on Human Rights (ECHR), guaranteeing the right to respect for private and family life.[27] Common law has incrementally developed breach of confidence and misuse of private information torts.[28] Yet none of these frameworks explicitly addresses neurotechnology or cognitive liberty.

The Limitations of UK GDPR

As discussed, UK GDPR's category-based approach to sensitive data proves inadequate for neural information. Article 9 protection applies only when biometric data is processed "for identification purposes."[29] Consumer neurotechnology companies collecting brain data for "wellness," "productivity," or "entertainment" can plausibly argue their processing falls outside this scope—despite the reality that such data inherently identifies individuals and reveals sensitive mental characteristics.[30]

Moreover, GDPR's consent mechanism assumes individuals can meaningfully understand and control what information they disclose. This assumption breaks down for neural data. As the Colorado legislative findings recognise, neural data collection is always involuntary in a

[25] 'Montana Sets New Standard for Brain Data Privacy with Neurotechnology Law' (Vensure, 13 July 2025)
[26] 'A MoFo Privacy Minute: Neural Data Added to Montana's Genetic Information Privacy Act' (Morrison Foerster, 14 August 2025)
[27] Human Rights Act 1998, sch 1
[28] *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457
[29] UK GDPR (n 11) art 9(1).
[30] Sarah Rainey and others (n 13) 20.

ISSN: 2582-6433

fundamental sense: "the person cannot be fully informed of and understand the content of the information they are sharing and how it might be used in the future."[31] The brain generates continuous electrical signals; users cannot selectively "consent" to revealing some neural patterns while withholding others. This renders traditional notice-and-consent frameworks insufficient for protecting cognitive privacy.

Article 8 ECHR and Mental Integrity

Article 8 ECHR provides more promising foundations for recognising mental privacy as a fundamental right. The European Court of Human Rights (ECtHR) has consistently held that "private life" under Article 8 encompasses both physical and psychological integrity.[32] In *Stoicescu v Romania*, the Court affirmed that Article 8 imposes positive obligations on states to protect individuals' physical and moral integrity, including "prevention of breaches of the physical and moral integrity of an individual by other persons when the authorities knew or ought to have known of those breaches."[33]

UK courts have interpreted Article 8 broadly, recognising that respect for private life "includes a person's physical and psychological integrity" and extends to protecting individuals' mental health and sense of self.[34] The question is whether this protection extends to safeguarding cognitive processes from neurotechnology interference—an issue no UK court has yet addressed. Legal scholar Sarah Ligthart argues that Article 8 already contains an implicit right to mental integrity protecting against adverse effects on psychological wellbeing,[35] but the threshold for triggering Article 8 protection requires showing "sufficiently adverse" effects on physical or psychological integrity.[36] This standard remains underdeveloped in the context of neurotechnology.

Crucially, Article 8's protection applies primarily to state interference. While the provision imposes some positive obligations on states to prevent private parties from violating privacy rights,[37] the extent of this duty in the commercial neurotechnology context remains uncertain.

[31] Colorado HB 24-1058 (n 12) s 1(b).
[32] *Stoicescu v Romania* App no 9718/03 (ECtHR, 26 July 2011).
[33] Ibid.
[34] 'Physical and Psychological Integrity of a Person: Distribution of the Field of Action Articles 3 and 8 of European Convention on Human Rights' (2018) 2(23) Slovo National School of Judges of Ukraine 1.
[35] Sjors Ligthart, 'The right to mental integrity in the age of neurotechnology' (2025) 12 Journal of Law and the Biosciences 1, 6-8.
[36] Ibid 8.
[37] *Stoicescu* (n 32) -

ISSN: 2582-6433

Corporate harvesting of neural data for profit may not automatically trigger Article 8 scrutiny absent state involvement or regulatory failure to prevent serious harm.

The Common Law Gap

English common law's protection of mental privacy is even more limited. The tort of misuse of private information, developed following *Campbell v MGN Ltd*,[38] requires claimants to demonstrate a "reasonable expectation of privacy" in the information disclosed. Courts balance this expectation against competing interests such as freedom of expression.[39] Applied to neural data, individuals could arguably claim a reasonable expectation that their brain activity—the most intimate information imaginable—should remain private. Yet no precedent exists, and neurotechnology companies could counter that users "consent" by purchasing and using brain-monitoring devices, thereby relinquishing privacy expectations.

Furthermore, common law remedies operate ex post facto, providing compensation after harm occurs. They cannot establish prospective protections preventing neurotechnology companies from collecting, analysing, and potentially weaponising neural data in the first instance. As Christoph Bublitz and Reinhard Merkel argue, "traditional legal categories such as lying and deception are insufficient to capture" manipulations occurring at the level of synapses and neurotransmitters.[40] New legal frameworks are required.

The Case for Recognising Mental Privacy as a Fundamental Right

The inadequacy of existing frameworks compels a fundamental question: should English law recognise mental privacy or cognitive liberty as an independent fundamental right? Several compelling justifications support an affirmative answer.

Cognitive Liberty as a Precondition for Other Rights

Cognitive liberty—the right of individuals to control their own mental processes, cognition, and consciousness—functions as a foundational right underlying other recognised freedoms.[41] Freedom of thought, protected by Article 9 ECHR and Article 18 of the Universal Declaration of Human Rights, presupposes that individuals possess sovereign control over their

[38] *Campbell* (n 28).
[39] Ibid.
[40] Jan-Christoph Bublitz and Christoph Merkel (n 1) 68.
[41] Jan-Christoph Bublitz, 'My Mind is Mine!? Cognitive Liberty as a Legal Concept' in Elisabeth Hildt and Andreas Francke (eds), *Cognitive Enhancement* (Springer 2013) 233, 238-242.

ISSN: 2582-6433

mental processes.[42] If external entities can access, monitor, or manipulate neural activity without consent, the very capacity for autonomous thought becomes compromised. As Bublitz argues, cognitive liberty is "not merely a political claim that one may favor or reject" but rather "an implicit assumption of any legal order based on individual self-determination and responsibility."[43]

This reasoning gains particular force in English law, which treats individuals as autonomous agents responsible for their actions. Criminal law presumes defendants possess *mens rea*—guilty minds reflecting free choice.[44] Contract law requires "meeting of the minds" for binding agreements.[45] If the law holds individuals accountable for mental states, it must logically grant them legal powers to protect those mental states from external interference. Cognitive liberty thus represents the right to the conditions necessary for autonomous action and moral responsibility.

Human Dignity and the Sanctity of the Mind

The mind constitutes the essence of personal identity and human dignity. As the preamble to the Universal Declaration of Human Rights recognises, "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."[46] Allowing commercial entities unfettered access to individuals' neural activity commodifies consciousness itself, reducing the human mind to a data extraction site.

Chile's constitutional framework reflects this principle by treating brain data as analogous to bodily organs: inalienable aspects of personhood that cannot be bought or sold.[47] This approach resonates with English law's prohibition on trading human organs under the Human Tissue Act 2004,[48] which recognises certain aspects of human embodiment as beyond commodification. If the law protects physical organs from market forces to preserve human dignity, it should extend at least equivalent protection to mental processes—arguably more central to personhood than kidneys or livers.

[42] Universal Declaration of Human Rights, art 18 (1948).
[43] Bublitz (n 41) 245.
[44] *R v Moloney* [1985] AC 905 (HL).
[45] *Kleinwort Benson Ltd v Lincoln City Council* [1999] 2 AC 349 (HL).
[46] Universal Declaration of Human Rights (n 42) preamble
[47] María Inés Cornejo-Plaza (n 20) 4.
[48] Human Tissue Act 2004, s 32.

ISSN: 2582-6433

The Asymmetry Problem: Corporate Power and Cognitive Vulnerability

Neurotechnology creates profound power asymmetries between individuals and corporate collectors of brain data. Unlike conventional data, which individuals might choose to share or withhold, neural signals are involuntary and continuous. Users cannot "opt out" of generating brain activity while using neurotechnology devices. Moreover, the complexity of neural data processing means individuals cannot meaningfully comprehend what information their brain activity reveals or how it might be used.[49]

This informational asymmetry enables exploitation. As Farahany documents, employers have begun deploying neurotechnology to monitor employees' attention, stress levels, and emotional states—creating pervasive workplace surveillance that employees cannot effectively resist without risking their livelihoods.[50] Without robust legal protections recognising mental privacy as a right, individuals face a Hobson's choice: either accept neural surveillance or forgo economic opportunities, social participation, and access to beneficial technologies.

The Preventative Imperative

Perhaps most importantly, waiting for harms to materialise before developing legal protections for mental privacy risks allowing irreversible damage to cognitive liberty. Once neurotechnology becomes deeply embedded in social and economic infrastructure—as smartphones are today—extracting meaningful consent or imposing limitations becomes exponentially harder. Network effects, market consolidation, and path dependency can lock populations into surveillance regimes that would be rejected if presented transparently at the outset.[51]

Chile's proactive constitutional reform reflects this preventative logic. As Dr Yuste testified to Chilean legislators, neurotechnology presents "fast-emerging frontiers without guardrails or guidance" requiring action before widespread deployment entrenches practices hostile to mental autonomy.[52] English law faces the same choice: act now to establish cognitive liberty as a fundamental right, or address harms reactively once the neurotechnology industry has established business models predicated on unfettered access to neural data.

[49] Colorado HB 24-1058 (n 12) s 1(b)
[50] Nita A Farahany (n 10) 45-68
[51] Ibid 189-210
[52] 'Rafael Yuste's Mission to Safeguard Neurorights in the Age of Neurotechnology' (Falling Walls, 19 August 2024)

ISSN: 2582-6433

Pathways Forward: Judicial Development and Legislative Reform

English law possesses multiple pathways for recognising and protecting mental privacy. Both judicial innovation and legislative action offer viable approaches.

Judicial Development Through Article 8 ECHR

UK courts could interpret Article 8's protection of "psychological integrity" to encompass cognitive liberty. The ECtHR has demonstrated willingness to adapt Convention rights to technological developments.[53] In *Amann v Switzerland*, the Court held that Article 8 protects communications regardless of technological medium.[54] Similar reasoning could extend psychological integrity protection to shield mental processes from neurotechnology interference.

A test case might involve an individual subjected to workplace neural monitoring without meaningful consent, suffering demonstrable psychological harm from the surveillance. Applying *Stoicescu*'s framework,[55] courts could find the state violated Article 8 positive obligations by failing to regulate neurotechnology, thereby permitting private entities to breach the claimant's mental integrity. Such a decision would not require creating new rights but merely recognising that existing Article 8 protections logically extend to cognitive autonomy.

Legislative Action: A Neurotechnology Act

More comprehensively, Parliament could enact dedicated neurotechnology legislation establishing clear protections for neural data and cognitive liberty. A UK Neurotechnology Act could incorporate core elements from Colorado and Montana's frameworks:

1. Classify neural data as a distinct category of sensitive information subject to heightened protection regardless of collection purpose.
2. Require explicit opt-in consent with clear explanations of what neural data will be collected, how it will be analysed, and with whom it will be shared.
3. Establish robust security requirements, including encryption and access controls protecting neural data from breaches.
4. Grant individuals rights to access, delete, and port their neural data, along with the right to revoke consent at any time.

[53] *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000).
[54] Ibid.
[55] *Stoicescu* (n 32).

ISSN: 2582-6433

5. Prohibit discriminatory uses, preventing employers, insurers, educational institutions, and government agencies from requiring neural monitoring as a condition of employment, coverage, admission, or services.
6. Require data protection impact assessments before deploying neurotechnology in high-risk contexts such as workplaces, schools, or law enforcement.
7. Create criminal penalties for egregious violations, such as using neurotechnology to manipulate decision-making without consent or selling neural data without authorisation.

Such legislation would provide the comprehensive, prospective protection that common law and GDPR cannot deliver. Crucially, it would affirm mental privacy as a societal value deserving explicit legal recognition rather than relegating it to fragmentary protections inferred from existing frameworks.

Integration with Emerging UK AI Regulation

The UK government has signalled intent to regulate artificial intelligence through a principles-based approach emphasising safety, transparency, fairness, accountability, and contestability.[56] Neurotechnology regulation should be integrated with this broader AI governance framework, given that neural data processing relies heavily on machine learning algorithms. The proposed AI Safety Institute could be tasked with developing technical standards for neurotechnology, ensuring algorithms used to interpret brain data are auditable, non-discriminatory, and subject to meaningful oversight.[57]

Moreover, the Copyright and Artificial Intelligence consultation (closed March 2025) raised questions about AI training data that implicate neural data.[58] If AI systems are trained on datasets including brain activity patterns, individuals should retain rights over this most intimate form of personal information. Neurotechnology legislation should clarify that neural data cannot be used for AI training without explicit, informed consent, with strong penalties for violations.

[56] 'A pro-innovation approach to AI regulation' (UK Government White Paper, March 2023).
[57] Ibid.
[58] 'Copyright and Artificial Intelligence' (UK Government Consultation, closed March 2025)

ISSN: 2582-6433

Conclusion

The mind represents the last privacy frontier. As neurotechnology transitions from medical research to consumer markets, English law confronts a fundamental choice: will it proactively recognise mental privacy as a fundamental right, or will it allow cognitive liberty to erode through regulatory inaction? The precedents set by Chile, Colorado, and Montana demonstrate that legal systems can respond to neurotechnology's challenges before irreversible harms occur. The frameworks exist in international human rights law, particularly Article 8 ECHR's protection of psychological integrity. The justifications are compelling, rooted in human dignity, autonomy, and the preconditions for democratic society.

Yet time is limited. The global neurotechnology market is projected to reach USD 52.86 billion by 2034,[59] with consumer devices already embedding neural sensors into everyday wearables. Meta's neural wristbands, Neuralink's brain implants, and countless startups are racing to make brain-computer interfaces ubiquitous. Without swift action, English law risks permitting the colonisation of consciousness—allowing commercial interests to harvest, analyse, and potentially manipulate the most intimate sphere of human existence.

The path forward requires both judicial courage and legislative will. Courts must interpret existing human rights protections generously, recognising that psychological integrity under Article 8 ECHR necessarily encompasses cognitive liberty. Parliament must enact comprehensive neurotechnology legislation establishing clear, enforceable protections for neural data and mental autonomy. The alternative—regulatory paralysis followed by reactive crisis management—would betray the fundamental principle that the law exists to protect human dignity and freedom.

The battle for our brains has already begun. English law must ensure that individuals, not corporations or states, ultimately win that battle. Mental privacy is not merely one right among many; it is the foundation upon which all other freedoms rest. To lose sovereignty over our own minds is to lose what makes us human. That is a cost no society premised on liberty and dignity can afford to pay.

[59] 'Neurotechnology Market Size to Surpass USD 52.86 Billion by 2034 Driven by Breakthroughs in Brain-Machine Interfaces' (BioSpace, 6 July 2025)