

Mapping a right to mental privacy within European and international human rights law^()*

Marta SOSA NAVARRO*, Felicitas HOLZER**

Sommario: 1. Introduction 2. Conceptual mapping of mental privacy 2.1. The normative foundations of mental privacy within the privacy debate 2.1. Privacy understood as informational control 2.3. “Mental states” and inferences to mental states 2.4. “Mental data” 3. Mapping the relevant binding instruments 3.1. The right to mental privacy and current international data protection frameworks applying to novel challenges posed by neurotechnology 3.3. Regional systems of human rights protection and the right to mental privacy 3.4. The EU legal framework protecting mental privacy 4. Conclusion

1. Introduction

The concept of “mental privacy” has recently gained significant prominence as a means of protecting individuals’ thoughts, emotions, mental states, and neural activity from unauthorised collection, analysis, or manipulation. At its core, mental privacy aims to protect one’s mental sphere, that is, beliefs, memories, emotions, and intentions, claiming that the “mental” deserves distinct and robust safeguards. Alongside freedom of thought and mental integrity, the protection of mental privacy has emerged as one of the central challenges of the digital age, particularly in the context of rapidly expanding the application of artificial intelligence and consumer neurotechnologies. Scholars such as Ienca, Andorno¹ and Lavazza² have therefore advocated the recognition of mental privacy designed to safeguard personal autonomy and identity against these emerging threats.

Recent advances in decoding brain activity have amplified these concerns. Most notably, the once-speculative notion of “mind reading” is moving closer to reality, as scientific advances increasingly make the direct interpretation of mental states plausible.³ Additionally, the capacity to infer emotions, intentions, or cognitive patterns from brain data, behavioural indicators, or biometric signals has led to renewed debate about who should have access to the intimate realm of human thought.⁴ Critical discussions now centre on the potential misuse of neurotechnological and algorithmic tools for digital

(*) This work was supported by a grant in the ERA- NET NEURON funding program (JTC2023 – ELSA) to the Universidad Carlos III de Madrid and to the University of Zurich in the project “PRIVETDIS – Mental privacy, neurotechnology and disability: ethical, legal and social aspects”.

* Assistant Professor in International Law and Member of the TeCSEDU Interdepartmental Laboratory (Emerging technologies, society, ethics, and human rights) at University of Milano-Bicocca.

** Senior postdoctoral researcher in Philosophy and Bioethics at the Institute of Biomedical Ethics and History of Medicine, University of Zurich.

¹ M. Ienca, R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences, Society and Policy*, 3/2017, p. 5.

² A. Lavazza, *Freedom of thought and mental integrity: The moral requirements for any neural prosthesis* in *Frontiers in Neuroscience*, 12/2018, p. 82.

³ C. Rathkopf, J. Heinrichs, B. Heinrichs, *Can we read minds by imaging brains?*, in *Philosophical Psychology*, 36/2023, p. 2.

⁴ M. Ienca, *On neurorights* in *Frontiers in Human Neuroscience*, 2021, p.15; P. Kellmeyer, *Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices*, in *Neuroethics*, 14/2021, p. 1.

surveillance, data profiling, and behavioural prediction, raising ethical and legal questions about the limits of personal freedom and the right to mental self-determination.⁵

This paper examines how a right to mental privacy can be anchored within existing legal frameworks, with particular focus on international and European human rights instruments. To do so, the discussion begins with a conceptual groundwork that situates mental privacy within the broader field of privacy theory and human rights protection. Section 2 offers a conceptual mapping of mental privacy as developed in the academic literature, reframing it as control over one's information and the inferences drawn about one's mental states. This section also explores the normative foundations of mental and informational privacy, the special status of mental data, and the epistemic challenges of inferring mental states. Section 3 then maps international and regional law systems of human rights protection to assess how these mechanisms collectively contribute to safeguarding a working concept of mental privacy. Ultimately, relevant case law and European regulatory instruments that can be interpreted to be applicable to mental privacy—including the EU's General Data Protection Regulation (GDPR), the Product Safety Regulation, the Artificial Intelligence Act, the European Medical Devices Regulation—will be examined.

2. Conceptual mapping of mental privacy

Although discussed in academic literature since the late 20th century, the concept of mental privacy has recently gained prominence in the wake of rapid technological developments.⁶ Early debates arose within broader discussions of privacy in the context of surveillance technologies and cognitive freedom.⁷ These discussions, however, often overlooked the qualitative distinction between general privacy and the more specific notion of “mental privacy”, that is, protection against intrusions into the mental sphere, such as access to data enabling inferences about an individual's mental states, emotions, memories, or predispositions. This distinction matters normatively because the mental sphere occupies a uniquely intimate domain: it is the space in which identity, values, and autonomous decision-making are formed, and its exposure carries risks of manipulation and coercion that general privacy frameworks were not designed to address.⁸ In recent years, the focus on mental privacy as a distinct issue has intensified, particularly in calls for recognition of a specific right protecting individuals from non-consensual intrusions, including what some scholars have referred to as “brain reading”.⁹

A central concern in the debate about a legal right to mental privacy is that existing privacy frameworks may not adequately address the invasive capabilities of emerging neurotechnologies. Normative arguments have therefore entered legal discourse, raising the question of whether current privacy protections can be extended to meet the specific challenges posed by mental privacy. Yet the necessity and normative basis of a separate legal right remain contested. Scholars such as Bublit and Lighthart caution against normative inflation, questioning whether mental privacy warrants distinct legal recognition or whether existing rights—and in particular freedom of thought or general privacy protections under international law—already offer sufficient safeguards.¹⁰

⁵ P. Magee, M. Ienca, N. Farahany, *Beyond Neural Data: Cognitive Biometrics and Mental Privacy*, in *Neuron*, 112/2024, p. 18.

⁶ M. Ienca, *On neurorights*, cit.

⁷ A. Westin, *Privacy and Freedom*, New York, 1967; D. Solove, *Conceptualizing privacy*, in *California Law Review*, 90/2002, p. 1087.

⁸ M. Ienca, R. Andorno, *Towards new human rights*, cit.

⁹ R. G. Boire, *On cognitive liberty*, in *Journal of Cognitive Liberties*, 2/2001, pp. 7–22; S. Lighthart, *Mental privacy as part of the human right to freedom of thought?*, in C. Bublit and M. Blitz (eds.), *The law and ethics of freedom of thought: Cognitive liberty and privacy*, 2nd edn, London, 2025.

¹⁰ C. Bublit, *Neurotechnologies and Human Rights: Restating and reaffirming the multi-layered protection of the person*, in *The International Journal of Human Rights*, 28/2024, p. 5; S. Lighthart et al., *Minding rights: Mapping ethical and legal foundations of “neurorights”*, in *Cambridge Quarterly of Healthcare Ethics*, 32/2023, p. 4.

Since the purpose of this paper is to explore how mental privacy might be anchored in European and international legal instruments, we temporarily set aside the question of whether a new right is required. Instead, the focus in this section is to explore a conceptual frame that can serve as the foundation for subsequent discussions on the potential legal recognition and protection of mental privacy. We will sustain that in the current literature, mental privacy is most frequently understood as control over information about one's mental states and the inferences that can be drawn from that information. To support this understanding, we examine the following interrelated dimensions: (2.1) the normative foundations of mental privacy and the claim that it extends beyond traditional notions of privacy; (2.2) the relevance of privacy understood as "informational control"; (2.3) the nature of mental states and the conditions under which inferences about them can be made; and (2.4) the conceptual elaborations on "mental data".

2.1. The normative foundations of mental privacy within the privacy debate

At the core of current debates on mental privacy lies the question of how neurotechnological intrusions affect the cognitive dimension of personhood related to the sphere of conscious and unconscious mental activity through which individuals think, imagine, and engage with the world. As in classical privacy theory, mental privacy is regarded as a precondition for autonomy, not only by safeguarding the capacity for free choice but also by protecting the internal space of deliberation, imagination, and moral reasoning from external interference.¹¹ Advocates of recognising mental privacy as a distinct concept from privacy argue that without protection of this inner domain, where thought can unfold free from observation or manipulation, the formation of beliefs, values, and intentions risks becoming reactive or coerced. In this sense, mental privacy constitutes a foundational condition for personal autonomy. As Stenlund and Slotte note, the inner domain is essential to both independence and authenticity.¹² Wajnerman Paz similarly contends that mental privacy forms the psychological basis of broader privacy rights, as it underpins the development of personal identity.¹³ The ability to choose what mental content, such as thoughts or emotions, to share and with whom is central to trust, intimacy, and mutual recognition in social relations. Autonomy is thus not merely an internal quality but a relational one, exercised through controlled self-disclosure and identity.¹⁴ When technological or institutional mechanisms impose forced transparency, individuals risk being reduced to data sources rather than autonomous participants in reciprocal relationships. Such conditions also expose them to surveillance and discrimination based on inferences about their mental states or mental content, thereby undermining autonomy.¹⁵

Lighthart adds that neurotechnologies capable of decoding or modulating mental states render the boundaries of the self increasingly "porous".¹⁶ When external actors can intrude in or stimulate internal processes, the mental sphere ceases to be fully shielded; the external world begins to infiltrate the inner domain without passing through the usual filters of agency, language, or consent. In this sense, neurotechnology threatens to erode the boundaries of what has traditionally been understood as the "most private realm" of "the private", that is, the *forum internum*. With the emergence of a "forum externum" capable of accessing or interpreting mental content, the classical distinction between internal and external dimensions of privacy becomes increasingly blurred.

¹¹A. Lavazza, *Freedom of thought and mental integrity*, cit; A. Wajnerman Paz, *Is your neural data part of your mind? Exploring the conceptual basis of mental privacy*, in *Minds and Machines*, 32/2022, p. 2; A. Wajnerman Paz, *Is mental privacy a component of personal identity?*, in *Frontiers in Human Neuroscience*, 15/2021.

¹²A. Stenlund and P. Slotte, *Forum internum revisited: Considering the absolute core of freedom of belief and opinion in terms of negative liberty, authenticity, and capability*, in *Human Rights Review*, 19/2018, p. 4.

¹³A. Wajnerman Paz, *Is your neural data part of your mind?*, cit.

¹⁴C. Taylor, *Sources of the self: The making of the modern identity*, Cambridge, 1989; R. Yuste, T. De La Quadra-Salcedo *Neuro-rights and new charts of digital rights: a dialogue beyond the limits of the law*, in *Ind. J. Global Legal Studies*, 30/2023, p. 15.

¹⁵N. Farahany, *The battle for your brain: defending the right to think freely in the age of neurotechnology*, New York, 2023.

¹⁶S. Lighthart, *Mental privacy as part of the human*, cit.

What makes neurotechnology distinct in this respect —as compared to other forms of surveillance or data collection— is its capacity to bypass the mediating layers through which individuals normally manage self-disclosure. As Ienca and Andorno argue, existing privacy frameworks were designed to regulate access to information that individuals have already chosen to externalise through language, behaviour, or expression; neurotechnology, by contrast, “targets the very substrate from which mental life emerges”, potentially accessing subconscious processes that the individual has never chosen to disclose and may not even be aware of.¹⁷ Farahany similarly argues that the capacity to decode neural activity represents a shift “from reading the traces left by the mind to reading the mind itself”, raising concerns that cannot be addressed by informational privacy frameworks alone.¹⁸ This point is reinforced by Magee, Ienca and Farahany, who note that as multimodal data ecosystems increasingly combine neural signals with behavioural and biometric data, the boundary between inference and direct mental access becomes progressively harder to maintain.¹⁹

However, this position has not remained without its critics. Lippert-Rasmussen argues that the absence of brain privacy does not necessarily undermine intimacy or authenticity, and Susser and Cabrera caution that behavioural and social data already enable highly intrusive inferences about mental states —often with greater accuracy than current neurotechnological tools.²⁰ Rathkopf, Heinrichs and Heinrichs add that what counts as “reading” a mental state remains deeply contested, and that neural correlates of mental states should not be conflated with the states themselves.²¹ These critiques suggest that the distinctiveness of neurotechnology as a privacy threat is better understood as a matter of degree rather than kind, which is precisely why an adequate framework for mental privacy must be grounded in the nature of the information revealed rather than in the technological pathway through which it is accessed.

2.2. Privacy understood as informational control

As Section 2.1 develops, from both normative-ethical and legal perspectives, privacy has long been understood as a condition for autonomy. In particular, control over personal information, exercised through cognitive processes of selection, disclosure, and concealment, is widely regarded as central to meaningful privacy. The ability to think freely, filter information, and decide what to share is a prerequisite for exercising autonomy and preserving the inner sphere of the self.²²

Control-based approaches understand privacy not merely as the absence of external interference, but as the individual’s capacity to govern access to their personal domain. A situation is private when a person can determine who may gain access, under what conditions, and for what purposes. This form of control extends across multiple dimensions: over personal information, over physical and mental access to oneself, and over decisions that shape one’s life and relationships, enabling self-expression and the development of social bonds.²³ In this view, privacy is intimately linked to autonomy: as Benn observes, the ability to manage access to oneself or one’s information is a manifestation of freedom and moral agency, reflecting respect for the individual as a self-determining being.²⁴

¹⁷ M. Ienca, R. Andorno, *Towards new human rights*, cit.

¹⁸ N. Farahany, *The battle for your brain*, cit.

¹⁹ P. Magee, M. Ienca, N. Farahany, *Beyond Neural Data*, cit., p. 3054.

²⁰ K. Lippert-Rasmussen, *Brain Privacy, Intimacy, and Authenticity: Why a Complete Lack of the Former Might Undermine Neither of the Latter!*, in *Res Publica*, 23/2017, p. 261; D. Susser, L.Y. Cabrera, *Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy?*, in *AJOB Neuroscience*, 15/2023, p. 1.

²¹ C. Rathkopf, J. Heinrichs, B. Heinrichs, *Can we read minds*, cit.

²² W.A. Parent, *Privacy, Morality, and the Law*, in *Philosophy & Public Affairs*, 12/1983, p. 4; C. Inness, *Privacy, Intimacy, and Isolation*, New York, 1992; T. M. Scanlon, *Thomson on Privacy*, in *Philosophy and Public Affairs*, 4/1975, p. 4.

²³ J. DeCew and S. Wagner, *Constitutional Privacy, Judicial Interpretation, and Bowers v. Hardwick*, in *Social Theory and Practice*, 15/1989, p. 3; B. Roessler and D. Mokrosinska, *Privacy and Social Interaction*, in *Philosophy & Social Criticism*, 39/ 2023, p. 8.

²⁴ S. I. Benn, *Privacy, Freedom, and Respect for Persons*, Oxford, 1984.

Control-based models of privacy highlight the individual's right to delineate the boundaries of disclosure.²⁵ Privacy is thus a normative interest grounded in the agency of the individual as an epistemic subject: someone capable of managing when and how information about them is exposed to others. Infringements on this agency, particularly through technological means that are opaque, non-consensual, or systematically applied, may raise serious concerns —though whether such interference amounts to a rights violation will depend on a proportionality assessment, including whether it pursues a legitimate aim and is necessary.²⁶

Standard approaches to “mental privacy” more particularly, especially those concerned with protecting an individual's inner sphere from intrusion, are consistent with this control-based perspective. Mental privacy embodies the cognitive and emotional autonomy necessary to maintain coherent self-concepts and authentic relationships. Scholars such as Floridi and Lavazza argue that mental privacy requires the ability to preserve an inner domain of unobserved mental activity, where reflection, judgment, and self-authorship can occur without external interference.²⁷

Moreover, protection must extend to both the content of thought (the ‘what’) and the cognitive process itself (the ‘how’). Even the mere awareness of neuro-surveillance can distort cognition, leading to self-censorship, behavioural adaptation, and diminished critical deliberation. By ensuring meaningful control over both the content and process of thought —acknowledging that much cognitive activity is unconscious and not directly accessible to the individual—mental privacy safeguards the individual's autonomy as an epistemic subject, preserving a domain in which the mind remains insulated from non-consensual observation.²⁸

2.3. “Mental states” and inferences to mental states

A central pillar of mental privacy is the question to what extent mental states can be accessed or inferred. The prospect of “direct access” to the mind has led some to describe mental privacy as the “last frontier” of privacy protection.²⁹ Advances in so-called “brain decoding”, particularly through machine learning applied to neural patterns, have intensified this debate. Progress in speech neuroprosthetics and language decoding holds clear medical promise but simultaneously revives long-standing anxieties about “mind reading.” But as Rathkopf, Heinrichs, and Heinrichs observe, conceptual ambiguity persists as to what counts as mental access, and under what conditions, remains insufficiently defined.³⁰

Debates about “directness” in mental access often centre on whether data are derived from neural activity rather than observable behaviour. Yet, as Brown notes and as we will explain in the following section, this distinction may be overstated.³¹ Advanced algorithms already infer mental states from digital footprints, facial expressions, or behavioural data, and in some cases may reach or exceed the inferential capacity of current neurotechnologies when multiple data streams are combined – with a degree of precision that warrants serious attention.³²

At the same time, scholars, such as Lippert-Rasmussen, Susser, and Cabrera caution against overstating current neurotechnological capabilities to “intrude” the sphere of the mental. Existing methods do not permit genuine “mind reading,” and the extent to which cognitive processes can be

²⁵ A. F. Westin, *Privacy and Freedom*, New York, 1967.

²⁶ I. M. Young, *Justice and the Politics of Difference*, Princeton, 1990. W.A Parent, *Privacy, Morality*, cit., C. Inness, *Privacy, Intimacy*, cit., T. M. Scanlon, *Thomson on Privacy*, cit. See also the further discussions in part 3 about the operationalization of mental privacy in law and in particular the EU's trend towards concentrating efforts on preventing psychological damage.

²⁷ A. Lavazza, *Freedom of thought and mental integrity*, cit.; L., Floridi, *The fight for digital sovereignty: What it is, and why it matters, especially for the EU*, in *Philosophy & technology*, 33/2023, p. 3.

²⁸ *Ibid.*

²⁹ M. Ienca, R. Andorno, *Towards new human rights*, cit.; A. Lavazza, *Freedom of thought and mental integrity*, cit.

³⁰ C. Rathkopf, J. Heinrichs, B. Heinrichs, *Can we read minds*, cit.

³¹ M. Brown, *Neurorights, Mental Privacy, and Mind Reading*, in *Neuroethics*, 17/2024, p. 2.

³² *Ibid.*, P. Magee, M. Ienca, N. Farahany, *Beyond Neural Data*, cit.

decoded remains uncertain.³³ This is the case because brain data is always interpreted and can never be directly “read”. Moreover, inferences about mental states depend on complex interpretative models shaped by social contexts.³⁴

However, against this stands the position that such uncertainty does not diminish the urgency of ethical and legal reflection. Given the accelerating pace of innovation and the lag of regulatory responses, proactive analysis is both prudent and necessary. Brown’s “modality-agnostic” model of mental privacy captures this point by shifting the focus from the technological pathway of access to the nature and potential impact of the information obtained.³⁵ Since privacy threats increasingly arise from multimodal digital ecosystems rather than from neurotechnology alone, a technology-neutral framework is needed —one that addresses the epistemic and normative implications of accessing information about mental states, regardless of source or medium.³⁶

Ultimately, this brings the discussion back to the nature of the “mental” itself. Philosophically driven debates about the relationship between mental and physical processes, and about the internal or external content of mental states, eventually shape how one assesses the risks posed by neurotechnologies. Mental privacy, therefore, cannot be treated as a fixed or uniform value; it depends on how the mind and the “mental” are conceptualised.³⁷

Despite these theoretical complexities, a phenomenological distinction remains crucial: being ‘mentally read’ without awareness or consent generates a unique form of epistemic vulnerability, independent of the mere possibility of directly inferring mental states. As Lavazza and Wajnerman Paz argue, even the anticipation of mental exposure can have a chilling effect, prompting individuals to censor thoughts or alter cognitive habits to avoid detection.³⁸ Such anticipatory self-censorship undermines spontaneity, imagination, and deliberation, which are core components of freedom of thought. This epistemic vulnerability is at the heart of mental privacy.

2.4. “Mental data”

Another conceptual clarification is essential to advance the mapping of legal instruments protecting “mental privacy”. Building on the definition developed in Section 2, mental privacy can be most likely understood as a concept concerning control over information about an individual’s mental states when drawing on the literature. This framing raises a critical question: what types of data genuinely provide insight into mental states? Often, the issue is not the origin of the data but its semantic and normative proximity to mental content, that is, the (gradual) extent to which it reflects an individual’s “inner life”.

As some scholars have argued, the unique sensitivity of mental privacy derives from the nature of mental data, which serves as a quasi-identifier of mental states.³⁹ Mental data not only mirrors the inner workings of the mind but is also intrinsically linked to the individual’s personality and lived experiences. This deep entanglement highlights that mental states, including raw sensory experiences, beliefs, intentions, and desires, cannot easily be separated from their source.⁴⁰ The intimate and uniquely personal nature of such information underscores the necessity for specific protections, a

³³ K. Lippert-Rasmussen, *Brain Privacy, Intimacy, and Authenticity*, cit.; D. Susser, L.Y. Cabrera, *Brain Data in Context*, cit.

³⁴ J. Pickersgill, *How Personality Became Treatable: The Mutual Constitution of Clinical Knowledge and Mental Health Law*, in *Social Studies of Science*, 43/2013, p.1.

³⁵ M. Brown, *Neurorights, Mental Privacy*, cit., p.2.

³⁶ *Ibid.*

³⁷ F. Holzer, S. Pedziwiatr, P. Kellmeyer, O. Friedrich, *On the normative status of mental privacy rights*, manuscript under review, journal *Minds & Machines*.

³⁸ A. Lavazza, *Freedom of thought and mental integrity*, cit., A. Wajnerman Paz, *Is your neural data part*, cit.

³⁹ M. Ienca, R. Andorno, *Towards new human rights*, cit., A. Wajnerman Paz, *Is your neural data part*, cit.

M. Ienca, R. Andorno, *Towards new human rights*, cit.; H. Feigl, *The “Mental” and the “Physical”*, in *Minnesota Studies in the Philosophy of Science*, 2/1958, p. 370 ff.

point reinforced by Ienca and Andorno, who emphasize that the particular methods employed to obtain mental data further justify tailored legal safeguards.⁴¹

Mental data has previously been defined as brain data or proxy data indicative of neurological, cognitive, and/or affective processes.⁴² While early debates focused on the sensitivity of neurodata, discussions have since expanded to question whether a meaningful distinction between “mental” and “non-mental data” can be drawn. Some scholars contend that any data enabling inferences about mental states warrants special protection.

Regarding the first point of view, some scholars have argued that neurodata (as opposed to “mental data”) is fundamentally distinct from other types of information for two principal reasons. First, neurodata captures not only conscious thoughts but also subconscious processes, which constitute the majority of brain activity. This ‘diagnostic depth’ allows neurodata to reveal latent emotions, subconscious dispositions, moral intuitions, and intentions, often before they are accessible to the individual themselves.⁴³ As Yuste and Quadra-Salcedo note, advances in neurotechnology may soon render subconscious neural activity, such as neuronal firing patterns, interpretable, raising concerns about potential misuse and the heightened vulnerability of individuals.⁴⁴

Second, neurodata is according to some scholars distinguished by its epistemic immediacy. It can be collected directly, bypassing mediating mechanisms such as language or behaviour, and thus circumventing intentional disclosure or informed consent. This direct access constitutes a conceptual shift: while thought was previously inaccessible and therefore naturally protected, emerging neurotechnologies enable probabilistic decoding and inferential reconstruction of mental content, challenging traditional notions of privacy.⁴⁵

However, regarding the latter position, recent scholarship, including the work of Ienca and Malgieri, further emphasizes that technological transformations have expanded the sources from which inferences about mental states can be drawn. Behavioural, physiological, and social data, in addition to neural interfaces, can reveal aspects of mental life, demonstrating that mental data extends beyond purely neural sources. Importantly, also not all neural data qualifies as mental data; only those data that allow meaningful inferences about mental states do. Consequently, mental data can comprise both behavioural and neural data. Yet, only a subset of behavioural or neural data qualifies as mental data, that is, all data that is distinguished by its capacity to reveal the inner mental life of individuals.⁴⁶ In the following sections of part 3, we will refer to “mental data” as any data capable of enabling inferences about an individual’s mental states (see Section 2.D). This working definition is intentionally broader than the earlier formulation of mental data as “brain data or proxy data indicative of neurological, cognitive, and/or affective processes”: whereas that definition focuses on the nature of the data source, ours focuses on the functional capacity of data to reveal mental states, regardless of its origin. We adopt this modality-agnostic framing to capture the full range of data types—neural, behavioural, physiological—that may engage mental privacy concerns under applicable legal frameworks.

3. Mapping the relevant binding instruments

As discussed in Section 2 from a philosophical standpoint, the conceptualization of the right to mental privacy necessarily derives from a thorough reinterpretation of the right to privacy as informational control, while also intersecting with other fundamental rights frequently invoked in

⁴¹ M. Ienca, R. Andorno, *Towards new human rights*, cit.

⁴² *Ibid*; M. Ienca, *On neurorights*, cit.

⁴³ A. Wajnerman Paz, *Is your neural data part*, cit.

⁴⁴ R. Yuste, T. De La Quadra-Salcedo, *Neuro-rights and new charts of digital rights*, cit.

⁴⁵ P. Magee, M. Ienca, N. Farahany, *Beyond Neural Data*, cit., p.18; M. Ienca, *On neurorights*, cit.

⁴⁶ M. Ienca and G. Malgieri, *Mental Data Protection and the GDPR*, in *Journal of Law and the Bioscience*, 9/2022, p. 1.

this context, such as freedom of thought and the rights to physical and mental integrity. For the purpose of this paper, the focus will be placed on the former.

3.1. *The right to mental privacy and current international data protection frameworks applying to novel challenges posed by neurotechnology*

From an international human rights law perspective, the right to privacy is conceived as an integral part of the right to private life, as recognized in most international and regional human rights instruments. This protection is enshrined in Article 17 of the ICCPR, which states:

1. "No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honor and reputation."

2. "Everyone has the right to the protection of the law against such interference or attacks."

While the language of this article aligns with similar provisions in other human rights frameworks,⁴⁷ the UN's Human Rights Council General Comment (GC) No. 16 on Article 17 provides a critical clarification with respect to its content and scope. By stressing that 'this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons⁴⁸', the GC extends the subject scope of application to interferences by non-State actors, including corporations.

Further guidance on how to delineate this right can be found in the Special Rapporteur on the right to privacy's reports. In its 2014 document, the qualified nature of this right is highlighted and the conditions under which it may be restricted are specified. According to the Rapporteur, for an interference with the right to privacy not to be considered arbitrary or unlawful, it must be 'proportional to the end sought and be necessary in the circumstances of any given case⁴⁹'. This requires using the method 'which is the least intrusive option available', and 'which has some chance of achieving the proposed goal⁵⁰'.

However, the key issue lies in determining how Article 17 of the ICCPR should be interpreted by States seeking to adopt legislative frameworks capable of extending enhanced protection to mental data. In particular, it is necessary to assess whether the collection, storage, and processing of such data, given their capacity to reveal highly sensitive information relating to cognitive and mental states, justify a special legal treatment and heightened safeguards in light of the significant risks they pose to individual rights and fundamental freedoms, including mental privacy. Firstly, it is essential to determine whether this category of data can be classified as highly sensitive therefore benefitting from heightened legal protection akin to health-related or genetic data. This question becomes particularly salient when considering that the UNGA has endorsed a set of guiding principles put forward by the Special Rapporteur on the right to privacy in relation to health-related data with the scope of providing an international baseline for minimum data protection standards in this context.⁵¹ Under this framework, health-related data is broadly defined as: "all personal data concerning the physical or mental health of an individual, including the provision of health-care services, that reveal information about the individual's past, current, and future health."

A strict interpretation of this definition might exclude mental data unless it is explicitly linked to health conditions or medical interventions. However, an extensive interpretation would encompass mental data within the category of health-related data. This is particularly justifiable given that mental data potentially reveals, infers, or can be used to manipulate mental states, cognitive functions,

⁴⁷ Art 12 UDHR, Art. 17 of the ICCPR, Art. 8 ECHR, Art. 11. ACHR.

⁴⁸ UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para. 1.

⁴⁹ OHCHR, Report of the Special Rapporteur on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, June 30, 2014, p. 7 at para 21.

⁵⁰ *Ibid.*, para 23.

⁵¹ UNGA, *Right to privacy, Recommendation on the protection and use of health-related data*, A/74/277, 5 August 2019, Annex, chapter 1, 1.2.

emotions, and even decision-making processes, as outlined in section 2.1. This seems to be the position shared by UNESCO. In its Recommendation on the Ethics of Neurotechnology, adopted in November 2025 following final negotiations in Paris in May 2025 attended by over 190 UNESCO Member States, UNESCO deems the protection of neural data, and of non-neural data enabling inferences about cognitive states, essential to safeguarding mental privacy,⁵² and calls for “clear safeguards against the misuse or unauthorised access of neural data and non-neural data allowing cognitive states inferences, including prior, free and informed consent, data minimization and purpose limitation, autonomy over data including to access, correct, erase and suspend processing of data, and data security and protection, particularly in contexts where such data might be aggregated with other sources, taking into account that it is becoming increasingly difficult to anonymize data.”⁵³ This is consistent with the theoretical arguments underpinning the special sensitivity of mental data discussed in section 2.4. Some scholars argue that neural data differs fundamentally from other forms of data because it captures not only conscious thoughts but also subconscious neural processes that shape identity and behaviour, exposing individuals to new forms of hidden vulnerability. Moreover, its direct, language-free collection grants unprecedented epistemic access to mental content, challenging traditional notions of intentional disclosure and informed consent. Against this background, in his 2022 report, the Special Rapporteur on the right to privacy stressed the urgent need to classify the different categories of sensitive personal data. Such an objective is considered essential if national laws are to be amended in order to grant this mental data, as a particular type of personal data a special treatment and higher protection in the light of the greater risks that their collection and processing pose to rights and fundamental freedoms.⁵⁴

At present, it remains premature to offer a definitive answer to the question of whether international law has developed overarching principles of data processing that can effectively safeguard the right to privacy. Such a finding would be essential to identify a consensus on the interpretation of article 17 when applied to mental privacy. However, important progress has been made in this direction, notably through the work of the Special Rapporteur on the right to privacy, who, between 2022 and 2025, issued three pivotal reports that significantly advance our understanding of the content and scope of this right. The first report provides an in-depth exploration of the normative foundations of privacy and personal data protection, thereby delineating the contours of the right to privacy in the digital era.⁵⁵ The second report undertakes a comparative assessment of the legal frameworks currently in place across five continents.⁵⁶

In her first report, the Special Rapporteur, Ana Brian Nougères, undertakes a systematic comparative analysis of ten guiding principles that, she argues, constitute the backbone of a global regulatory architecture for privacy and personal data protection. Far from mere soft-law aspirations, they operate as essential benchmarks for lawful and ethical processing: legality; lawfulness and legitimacy; consent; transparency; purpose specification; fairness; proportionality; data minimisation; data quality; accountability; and security.⁵⁷ The analysis, is complemented by a second report from 2024 which carries out a comparative study of existing legal frameworks across five continents, draws on seven cornerstone instruments (the GDPR; the modernised Convention 108; UNGA Res. 45/95; the Ibero-American

⁵² UNESCO, *Recommendation on the Ethics of Neurotechnology*, adopted by the General Conference at its 43rd session, Samarkand, Uzbekistan, 11 November 2025., para 48: “Neurotechnology and other technologies that collect non-neural data allowing cognitive states inferences raise issues pertaining to privacy due to their increasing ability to collect direct and indirect data about the nervous system that is uniquely sensitive”.

⁵³ *Ibid.*, para 50.

⁵⁴ UNGA, *Right to privacy*, A/77/196, 20 July 2022, at para 6.

⁵⁵ *Ibid.*

⁵⁶ UN Human Rights Council, *Legal safeguards for personal data protection and privacy in the digital age*, A/HRC/RES/55/46, 18 January 2024.

⁵⁷ UN General Assembly, *Right to privacy*, A/77/196, 20 July 2022, at para 149.

Standards; the OECD Guidelines; the APEC Privacy Framework; and the OAS Updated Principles) and suggests a meaningful degree of convergence around these principles.⁵⁸

The role of these reports as interpretative tools in the scope of mental data protection gained additional prominence following Nougères' 2025 report, which examines neurotechnologies and neural data through the lens of the right to privacy⁵⁹. Neural data, while not protected by absolute rights, pose risks that exceed conventional privacy harms due to two main reasons: their capacity to reveal cognitive states, emotions and lived experience and their potential collection without conscious interaction (passive collection).

The report proposes a model law to harmonise domestic regimes via minimum standards that go beyond generic data-protection rules, embedding neuro-specific safeguards: a human-rights and dignity-based approach across the full lifecycle; recognition of neural data as uniquely sensitive; precaution and safety-by-design; and governance measures ensuring transparency, oversight, effective remedies, and strict security and retention limits. These conditions set a heightened threshold for lawful processing of neural data which includes narrowly defined purposes, a ban on incompatible repurposing, and a demonstrable necessity and proportionality burden on controllers, failure of which risks not only privacy violations but also the erosion of autonomy and human dignity. Only a few months later, in July 2025, the Special Rapporteur adopted a second report complementing the first one and laying the foundations for the development of a model law on neurotechnologies from the perspective of the right to privacy⁶⁰. Following the introduction and a background section which summarized the main findings contained in the previous report, including the principles that should guide the use of neurotechnologies and the processing of neural data⁶¹, the report is divided in four main sections: section III, which examines the most recent business practices in the area of neurotechnologies; section IV which looks into the advances in neurotechnologies and their impacts on society; section V, which delves into the pillars of a regulatory framework for neurotechnologies and a last section (VI) containing recommendations.

When examining existing business practices, the Special Rapporteur refers to a study carried out by the Neurorights Foundation, which analysed the privacy policies and user agreements of thirty companies producing publicly available consumer neurotechnologies, concluding that the privacy of users' neural data is not adequately protected⁶². Such concerns have also been raised in recent years by academics,⁶³ research centres⁶⁴ and civil society. For instance, after conducting a similar study on nearly 160 neurotechnology consumer companies, of which 56 focus on wellness applications, the Centre for future generations has concluded that consumers are rarely clearly informed about how their (neural) data are collected, stored, shared, or used.⁶⁵

⁵⁸ A.B. Nougères, 'Legal Safeguards for Personal Data Protection and Privacy in the Digital Age', Report to the UN Human Rights Council, UN Doc A/HRC/55/46 (18 January 2024).

⁵⁹ A.B. Nougères, "Foundations and Principles for the regulation of neurotechnologies and the processing of neurodata from the perspective of the right to privacy", Report to the UN Human Rights Council, UN Doc A/HRC758/58 (15 January 2025).

⁶⁰ A.B. Nougères, "Elements for the development of a model law on neurotechnologies and the processing of neurodata from the perspective of the right to privacy", Report to the UN Human Rights Council, UN Doc A/80/83 (31 July 2025).

⁶¹ *Ibid.*, p. 5-7. The original wording in the report refers to neurodata, but neural data has been maintained for the purpose of consistency.

⁶² *Ibid.*, p. 8: "In the study, they conclude, inter alia, that: (i) consumers do not have adequate information about data practices, privacy or their rights as users; (ii) there is enormous ambiguity regarding whether companies consider neural data a form of personal data; (iii) data collection and storage practices are ambiguous; (iv) almost all the companies can share data with third parties; (v) the extent to which companies can or cannot sell data is unclear; (vi) user rights, such as withdrawing consent to data processing and requesting data deletion, are not uniformly extended; and (vii) the data safety and security provisions of consumer neurotechnology companies are generally ill - equipped to safeguard neural data."

⁶³ R. Field, *The Data We Leave Behind: Limits of Legal Protections for Neurotechnology and Genomic Data*, in *Drexel Law Review*, 15(4)/2023, p. 812.

⁶⁴ A. Mochan and others, *Emerging applications of neurotechnology and their implications for EU governance*, European Commission Joint Research Centre (Luxembourg, Publications Office of the European Union, 2025).

⁶⁵ Centre for Future Generations, [Promise and Peril in Wellness Neurotech](#), 29 March 2026.

Among the ideas embedded in the model law, several are particularly relevant from the perspective of mental privacy. First, the Rapporteur emphasizes that international harmonization efforts must inform any regulation concerning neurotechnology, given that these technologies have global impacts and transcend national borders. This necessarily requires engagement with the work carried out by various international and regional organizations on data protection privacy standards applicable to neural data, including the Organization of American States, COE, UNESCO and OECD. Second, closely linked to the first one, the model Law affirms that States have a duty to respect, protect and safeguard human rights in all actions relating to the design, development, implementation, marketing, assessment and use of neurotechnologies. Third, it advocates for ethics and human rights protection “by design and by default”, applicable from the very moment neural data are collected⁶⁶. Fourth, the Rapporteur explicitly invokes the precautionary principle under international law as a safeguard to prevent “serious or irreversible risks that may jeopardize human dignity, personal integrity, mental privacy and other fundamental rights.”⁶⁷

Most importantly, the model law develops a particularly robust approach to mental privacy. According to the Rapporteur, neural data should be classified as highly sensitive personal data subject to enhanced protection, including effective safeguards ensuring confidentiality, integrity and availability, as well as protocols guaranteeing compliance with privacy rights and informed consent.⁶⁸ The text further stresses the need for stricter security measures governing the processing of neural data in order to prevent unauthorized access, manipulation, alteration, disclosure or destruction. In this regard, it also refers to proposals contained in the UNESCO Recommendation on the Ethics of Neurotechnology, aimed at ensuring privacy protection while simultaneously enabling secure cross-border data sharing for research purposes. The Rapporteur additionally affirms that the prior, free, informed, express, specific and unequivocal consent of the data subject constitutes a prerequisite for any processing of neural data.⁶⁹

Finally, the report introduces an interesting idea by regarding neural data as a common heritage of humanity, which should not be subject to financial gain, trade or enrichment by third parties.⁷⁰ This position, which is consistent with an enhanced protection of mental privacy, challenges the commodification of mental data and, it may even be argued, implicitly invites States to adopt a clear normative stance against the use of mental data in specific contexts. This may include but not be limited to the processing of mental data in the workplace for productivity purposes⁷¹ and mental-data-based profiling in contexts involving manipulation, behavioural influence and cognitive warfare.⁷²

At the UN level, the HRC has likewise expressed concern regarding these challenges, including by specifically addressing the implications of neurotechnologies for mental privacy. In its Resolution 58/6 of the 2nd April 2025, it noted that the rapid development of neurotechnology presented challenges to physical and mental integrity and the safeguarding of human rights and requested its Advisory Committee to draft a set of recommended guidelines for applying the existing human rights framework to the conception, design, development, testing, use and deployment of neurotechnologies.⁷³ This invitation stems from the publication, less than a year earlier, by the same Advisory Committee of the report *Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights*, presented to the Human Rights Council at its fifty-

⁶⁶ A.B. Nougères, “Elements for the development of a model law”, cit., p. 12-13.

⁶⁷ Id., p. 13.

⁶⁸ Id., p. 13.

⁶⁹ Id., p. 14.

⁷⁰ Id., p. 15.

⁷¹ M. Sosa Navarro, *The rise of the neuroslave*, in *European Data Protection Law Review* (EDPL), 10(1)/2024.

⁷² C.E. Lewis, H.C.J. Kwik, *Neurotechnology and Cognitive Warfare*, in *Opinio Juris*, 5 February 2026.

⁷³ UN Human Rights Council, *Neurotechnology and human rights*, UN Doc A/HRC/RES/58/6 (2 April 2025).

seventh session. In this report, neurodata is not only recognized as “highly sensitive information”⁷⁴ but its protection is closely connected to freedom of thought, thus requiring enhanced safeguards. The Advisory Committee also joins the Special Rapporteur in calling for context-specific standards and reinforced consent requirements.⁷⁵

Taken together, these developments suggest the gradual emergence of an international normative framework that, while still fragmented and largely soft-law-based, increasingly recognises the exceptional sensitivity of neural and mental data and the need for enhanced safeguards grounded in privacy, human dignity, autonomy, and mental integrity.

3.2. *The Council of Europe’s Convention 108+ and the protection of neural data*

Although Convention 108+ is a regional instrument of the Council of Europe rather than a universal treaty, its inclusion in this mapping of international data protection frameworks is warranted by its status as the only existing binding multilateral instrument specifically devoted to data protection, whose principles have demonstrably influenced legislative developments across continents and informed the comparative convergence identified by the Special Rapporteur in her 2024 report.

Originally adopted in 1981, Convention 108 was the first binding international treaty on data protection. Its modernized successor, Convention 108+⁷⁶, expected to enter into force imminently, broadens these principles to cover national security and defense contexts and offers updated interpretive guidance on big data, AI, health data, and biometrics. Scholars have urged that mental data, whether statistical inferences about cognitive traits (Mental Privacy in the Broad Sense) or decoded semantic content of thoughts (Mental Privacy in the Narrow Sense), fall squarely under Convention 108+’s protections. They argue that mental data present unique privacy risks: from unauthorized profiling and discrimination (e.g., inferring susceptibility to mental illness or criminal propensity) to state or corporate manipulation of thoughts.⁷⁷

Convention 108+’s risk-based approach, coupled with its enhanced data subject rights, offers a promising avenue to regulate neurotechnologies outside purely medical contexts. The instrument’s principles, transparent processing, purpose specificity, necessity and proportionality, data minimization, security safeguards, and robust subject-rights, could be explicitly applied to mental data⁷⁸. Yet, as with the GDPR’s Article 9, current definitions of sensitive data omit emotions and non-health-related cognitive states, suggesting that mental data requires a new, qualified category. Moreover, Convention 108+’s extension to security and defense data is particularly apt for dual-use neurotechnology capable of surveillance or military enhancement. A formal interpretation or amendment to cover mental data would provide Member States with clear obligations to carry out Mental Data Protection Impact Assessments, mirroring the AI Act’s fundamental-rights impact assessments, and to implement proportionate safeguards against misuse.

⁷⁴ UN Human Rights Council Advisory Committee, *Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights. Report of the Human Rights Advisory Committee*, UN Doc. A/HRC/57/61, 8 August 2024, p. 3

⁷⁵ *Ibid.*, p. 5 and p. 7.

⁷⁶ Adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018). See the Council of Europe, [Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#), Strasbourg, 10.X.20180.

⁷⁷ E. Bertoni, M. Ienca, *The privacy and data protection implication of the use of neurotechnology and neural data from the perspective of Convention 108*, T-PD (2024)1, Paper presented before the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, p. 12.

⁷⁸ *Ibid.*, p. 25.

3.3. Regional systems of human rights protection and the right to mental privacy

3.3.1. The Inter-American framework of human rights protection

While domestic case law on mental data privacy violations remains anecdotal and confined to a single jurisdiction⁷⁹, the jurisprudence of regional human-rights courts on privacy offers valuable guidance on applying proportionality and necessity tests to intrusive technologies. Both the Inter-American and European human-rights systems offer complementary precedents for delimiting when and how States may legitimately interfere with mental privacy. Under the American Convention on Human Rights, Article 11 guarantees the inviolability of “private life, family, home, or correspondence”, a right the Inter-American Court of Human Rights (IACtHR) has read expansively, linking privacy to human dignity and autonomy in cases such as *Escher v. Brazil*⁸⁰. Article 12’s absolute protection of the *forum internum*, which represents the core element of mental privacy as developed in this article, has been further confirmed both in the IACtHR’s case-law⁸¹ and Advisory Opinions.⁸² Within the soft law instruments, the Organization of American States (OAS) 2021 Updated Principles on Privacy and Personal Data Protection should be recalled as they recognise sensitive data (notably health, biometric and genetic) and anchor their processing in the principles of proportionality, consent, and purpose limitation.⁸³ For the reasons outlined in the previous sections, mental data may likewise be regarded as fulfilling the criteria for qualification as sensitive data.

The American continent has been at the forefront of the development of soft and hard law⁸⁴ initiatives addressing neurotechnologies’ potential in this scope⁸⁵. In 2023, the Inter-American Juridical Committee of the Organization of American States promulgated the *Declaration of Principles on Neuroscience, Neurotechnologies and Human Rights*⁸⁶. Comprising ten overarching principles, the Declaration synthesizes and advances the existing consensus on the ethical and legal challenges posed by neurotechnologies, without privileging either medical or consumer applications. Each principle is supplemented by a “Concepts and Comments” section, which elaborates its normative foundation, ethical rationale, and practical scope. A joint reading of Principles 3 and 4 makes clear that the

⁷⁹ In *Girardi v. Emotiv*, the Chilean Supreme Court held that the use of “Insight,” a wireless EEG device, infringed the user’s right to privacy because the company failed to demonstrate that the user had given express consent for their neural data to be used in scientific research. Corte de Apelaciones de la República de Chile. Sentencia Recurso de Protección GIRARDI/EMOTIV INC de 24 de mayo de 2023. Base Jurisprudencial del Poder judicial de la República de Chile, 24 Mayo 2023 (https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2Fadjlz-YUdmbGx1UWNKWmV6ZjZ3dz09).

⁸⁰ Inter-American Court of Human Rights, *Escher et al. v Brazil* (Merits, Reparations and Costs) Judgment of 6 July 2009, Series C No 199, at para 195.

⁸¹ Inter-American Court of Human Rights, *Atala Riffo and Daughters v Chile* (Merits, Reparations and Costs) Judgment of 24 February 2012, Series C No 239, at para 85.

⁸² Inter-American Court of Human Rights, *Advisory Opinion OC-1/82 on Freedom of Expression and Information* (13 November 1982) Series A No 1, at para 21.

⁸³ Inter-American Juridical Committee, *Updated Principles on Privacy and Protection of Personal Data, with Notes* (Resolution CJI/Res. 266 (XCVIII-21), April, 2021 (<https://www.oas.org/en/sla/dil/docs/CJI-638-21-EN.pdf>)).

⁸⁴ D. Borbón, *Challenges of the inconsistent neurorights framework in Latin America*, in *Nat Neurosci* 28/2025, pp. 1363–1364. Among the countries that have addressed the issue, Peru is the only one to have adopted binding legislation recognising neural data as sensitive data, while Argentina, Brazil, and Uruguay have merely introduced legislative proposals, respectively to regulate the use of neurotechnologies, amend data protection rules to safeguard mental privacy and equitable access, and classify neural data as sensitive, none of which have yet been approved.

⁸⁵ The present Declaration follows up from two prior initiatives from the General Assembly of the OEA: the *Updated Principles on Privacy and Personal Data Protection*, prepared by the Inter-American Juridical Committee, through resolution AG/RES. 2974 (LI-O/21), in November 2021; and that the Inter-American Juridical Committee adopted the *Declaration on Neuroscience, Neurotechnologies, and Human Rights: New Legal Challenges for the Americas* (CJI/DEC. 01 (XCIX-O/21), in August 2021.

⁸⁶ OAS, Inter-American Juridical Committee, *Inter-American Declaration of Principles regarding Neuroscience, Neurotechnologies and Human Rights*, Doc. No. CJI/RES. 281 (CII-O/23) corr.1, 9 March 2023.

Committee regards mental data as sensitive personal information, meaning any access to brain-derived data must be predicated on express, informed consent.⁸⁷

3.3.2. The European framework of human rights protection: the European Court of Human Rights

At a European level, the Council of Europe offers one of the most important human rights protection frameworks: the European Convention on Human Rights (ECHR). Its Article 8 provides considerable protection to personal data collection and storage. The ECtHR has progressively developed a rich body of case law under this provision, extending the notion of “private life” well beyond its original scope to encompass the collection, retention, and use of personal data. This expansive reading of Article 8 is directly relevant to mental data: if biometric or biological information, by qualifying as sensitive personal data, already triggers the Convention's protections, there are strong grounds to argue that mental data, which is uniquely intimate and capable of revealing mental states, emotions, and intentions, falls squarely within the scope of private life that the ECHR is designed to protect. Consistently, some scholars support the view that data related to the human brain and mind qualify as personal data if they allow the data subject to be identified.⁸⁸

A particularly instructive line of ECtHR case law concerns the retention of biological and genetic data by state authorities. In *S. and Marper v. the United Kingdom* (2008), the Grand Chamber affirmed that the taking and retention of cellular samples and DNA profiles are sufficiently intrusive to constitute an interference with the right to respect for private life under Article 8 of the ECHR. The Court emphasized that the mere retention of sensitive personal data by public authorities, independently of subsequent use, was sufficient to trigger Article 8 protection. Importantly, the judgment recognized that the protection afforded by Article 8 increases where the data processed concern unique biological characteristics capable of revealing intimate aspects of identity⁸⁹. This reasoning is highly significant for mental (and neural) data governance, since EEG signals and other neurophysiological information may similarly disclose highly sensitive information relating to emotions, intentions, attention patterns, or mental health conditions. In this regard, according to some authors, the ECtHR's flexible and evolutive interpretation enables existing privacy guarantees to adapt to emerging technological risks, including those posed by neurotechnologies.⁹⁰

According to the ECtHR, any legal basis for interference must be sufficiently clear to enable citizens to understand the conditions and circumstances under which authorities are authorized to implement data collection or secret surveillance measures⁹¹. Furthermore, the scope and manner in which discretion is exercised must be explicitly defined to ensure the minimum level of protection required by the rule of law in a democratic society⁹². Key considerations include the technology's legitimate purpose, its data-collection methods, and the acceptable margin of error.⁹³ These requirements take on particular urgency in the context of mental data. The more intimate the data being processed, the

⁸⁷ OAS, Inter-American Juridical Committee, *Inter-American Declaration of Principles regarding Neuroscience, Neurotechnologies and Human Rights*, Doc. No.CJI/RES. 281 (CII-O/23) corr.1, 9 March 2023, Principle 3 and 4 at 8-9.

⁸⁸ F. Zuiderveen Borgesius, *Singling out People without Knowing Their Names: Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, in *Computer Law & Security Review*, 32/2016, p. 256; S. Rainey et al., *Is the European Data Protection Regulation Sufficient to Deal with Emerging Data Concerns Relating to Neurotechnology?*, in *Journal of Law and the Biosciences*, 1/2020, pp. 9-10. For an exhaustive analysis of the protection of neural data in the context of the processing of personal data in the European Union see J. Bastidas Cid, *Neurotecnología: Interfaz Cerebrocomputador y Protección de Datos Cerebrales o Neurodatos en el contexto del Tratamiento de Datos Personales en la Unión Europea*, in *Revista Iberoamericana de Derecho Informático*, 11/2021, pp. 101-176.

⁸⁹ ECtHR, *S. and Marper v. the United Kingdom*, Grand Chamber, Appl. Nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para. 72.

⁹⁰ T. Istace, *Human Rights Law: An Incomplete but Flexible Framework to Protect Against Neurotechnological Threats?*, in *The International Journal of Human Rights*, 2024, pp. 339-340.

⁹¹ ECtHR, *Shimovolos v. Russia* (Application no. 30194/09), Judgment of 21 June 2011, para 68.

⁹² ECtHR, *Piechowicz v. Poland* (Application no. 20071/07), Judgment of 17 April 2012, para 212.

⁹³ ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, para 112 and 125.

stricter the legal framework must be, a logic that the EU Fundamental Rights Agency has confirmed in the analogous context of facial recognition, noting that the more intrusive a technology is, the more exacting the necessity and proportionality test must become.⁹⁴ Mental data, which can reveal thought, intention, and emotion, is by any measure more intrusive still, which suggests that the doctrinal threshold developed through this case law would be especially demanding when applied to neurotechnological surveillance.

It follows from the above that regional human-rights jurisprudence has made a significant, though still indirect, contribution to the emerging protection of mental privacy, offering interpretative guidance on when and how States may legitimately interfere with the mental domain. Both the Inter-American and European systems provide complementary precedents. Together, these regional approaches outline the jurisprudential contours of mental privacy protection, while also revealing its conceptual and legal limits including the lack of a coherent and consistent definition of mental data, the difficulty of identifying the violation of mental privacy, and the challenge of balancing this right against competing rights and legitimate public interests, all of which remain at the core of the broader conclusions developed in this paper.

3.4. The EU legal framework protecting mental privacy

While mental data are not limited to neural data, as argued throughout this article, one of the regulatory pathways currently emerging within the EU normative framework consists in advocating for the enhanced protection of a specific category of data that may fall within the broader notion of mental data, namely neural data. A comprehensive understanding of the applicable legal protections to mental privacy at an EU level calls for an analysis of EU secondary law.

In this sense, the first and most immediate normative framework to consider is the General Data Protection Regulation (GDPR).⁹⁵ The inclusion of neural data within the special category of personal data regulated by article 9 GDPR has been identified by some authors as a priority, as it would automatically grant it the same heightened level of protection that this provision currently affords to genetic data.⁹⁶

As the debate has evolved, inspired by normative theoretical constructions such as Brown's modality-agnostic model of mental privacy examined in the previous section, legal scholars have emphasized that it is not the mere nature of neural data that qualifies it as sensitive and thereby eligible for heightened protection, but rather the type of information it reveals. In this sense, neural data that discloses a mental pathology would clearly fall within the definition of health data under Article 9(1) of the GDPR⁹⁷ while neural data revealing levels of fatigue would not immediately qualify under this category. In line with this paper's position on the broader conception of mental data as comprehensive of but not limited to neural data, there are compelling reasons to assert that the purpose for which mental data is collected is also relevant in determining whether it should be classified as sensitive. For instance, Malgieri and Ienca argue that while emotions are not inherently considered sensitive data under the GDPR, they may qualify as such when collected through emotion detection

⁹⁴ EU FRA, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (2019), FRA Focus, at 22.

⁹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) (Text with EEA relevance). *Official Journal of the European Union*, L 119, 1-88.

⁹⁶ M. Ienca et al., *Towards a Governance Framework for Brain Data*, in *Neuroethics*, 2022, p. 8; J. C. Bublitz, *Novel Neurorights: From Nonsense to Substance*, in *Neuroethics* 15/2022, p. 7.

⁹⁷ Full list of sensitive data categories in Article 9(1): data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

systems that rely on biometric tools, such as facial recognition. This may give rise to new conflicts of interpretation since, according to the GDPR, biometric data can only be processed when it serves the specific purpose of uniquely identifying the data subject.⁹⁸

In fact, the cited authors suggest that for this amendment to be effective, rather than focusing strictly on predefined categories, the priority should be evaluating mental data protection on the basis of the nature of the processing and the associated risks.⁹⁹ The legal gap identified by scholars such as Rainey¹⁰⁰ does not, as Ienca and Malgieri argue, arise from the GDPR's failure to recognize neural data as a distinct category of sensitive data, but rather from its silence on whether indirect inferences, those not explicitly or contextually linked to the sensitive categories listed in Article 9(1), should nonetheless receive heightened protection when they concern the mental domain, including aspects such as emotions, mood, or levels of concentration.¹⁰¹

Another interesting theoretical idea has recently entered the academic debate, with Elizabeth Steindl has alternatively proposed amending the GDPR not by introducing neural data as an additional special category of personal data, but by recognising "mind data" as a new sui generis special category defined as "personal data resulting from automated processing for the purpose of identifying or inferring emotions, thought, intentions or psychological states of a natural person."¹⁰² The rationale underlying this umbrella notion is that it shifts the focus away from creating a new category tied to data processed through a specific technology, such as neural data collected via neurotechnology and instead centres protection on the sensitive information itself, irrespective of the Mind Datafying Technology (MDT) employed to collect, process, or infer such information, including biometric systems and neurotechnologies. Steindl coins the term "Mind Datafying Technologies" (MDTs) in her book to refer broadly to technologies capable of generating, extracting, or inferring information relating to individuals' mental states.¹⁰³

The processing of the special category of personal data falling within Article 9 GDPR is, in principle, prohibited, except under specific and limited circumstances. If such reasoning were extended to the international level, through inclusion in binding conventions or declarations currently under negotiation, the effect would be twofold: on the one hand, it would ensure adequate protection and governance of highly sensitive personal data, while, on the other, safeguarding its processing for legitimate scientific and biomedical purposes.¹⁰⁴ Should the GDPR be reformed to explicitly include neural data within the special categories of personal data under Article 9, such data would benefit from the enhanced protections attached to particularly sensitive forms of information. This outcome, which a growing number of scholars have advocated for in the context of the Digital Omnibus discussions,¹⁰⁵ may represent a less ambitious but more realistic first step than pursuing the full-fledged legal recognition of mind data as an autonomous protected category, particularly in light of the significant definitional and conceptual complexities that continue to surround this notion.¹⁰⁶

From a *de iure condendo* perspective, a full picture of the legal framework protecting mental privacy under EU law requires looking into the Medical Devices Regulation (MDR) 2017/745.¹⁰⁷ The

⁹⁸ M. Ienca and G. Malgieri, *Mental Data Protection and the GDPR*, in *Journal of Law and the Biosciences*, 9(1)/2022, p. 10

⁹⁹ *Ibid.*

¹⁰⁰ S. Rainey, K. McGillivray, S. Akintoye et al., *Is the European Data Protection Regulation Sufficient to Deal with Emerging Data Concerns Relating to Neurotechnology?*, in *Journal of Law and the Biosciences*, 7/2020, p. 1.

¹⁰¹ M. Ienca and G. Malgieri, *Mental Data Protection*, cit., p. 11.

¹⁰² E. Steindl, *A datafied mind: untangling EU regulation of emotion technology and neurotechnology*, Cambridge, 2025, p. 36.

¹⁰³ The author highlights emotion technology and neurotechnology as two technologies that stand out for their ability to translate mental faculties, states and processes into data: *Id.*, p. 1.

¹⁰⁴ *Ibid.*

¹⁰⁵ European Expert Group on Human Rights and Emerging Technologies, [Open Letter: a plea to make neural data a special category under the GDPR](#).

¹⁰⁶ E. Steindl, *A datafied mind: untangling*, cit., p. 36-37.

¹⁰⁷ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009, and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1.

MDR focuses on the safety, performance and effectiveness of medical devices. It represents an example of a modern trend in this context which consists in emphasizing health and safety risks associated with the use of these products while overlooking less evident implications resulting from the use of these technologies such as inferences made from the collection and processing of mental data, unconsented interference, and potential impacts on neural activity.¹⁰⁸ Now, the Regulation covers devices listed in Annex XVI, which includes products without an intended medical purpose but which may pose safety risks similar to those of medical devices. Among these, neurostimulation devices are expressly regulated, defined as ‘equipment intended for brain stimulation that apply electrical currents or magnetic or electromagnetic fields that penetrate the cranium to modify neuronal activity in the brain’. The requirements that these devices should respect are fleshed out in Chapter II of the MDR, which establishes the obligations for economic operators, including strict compliance with the general safety and performance requirements detailed in Annex I. In fact, the Common Specifications adopted by the European Commission in December 2022 require manufacturers of these devices to implement a comprehensive risk management process aimed at analyzing, eliminating, or reducing as far as possible the risks associated with hazards or harms specifically related to neurostimulation devices.¹⁰⁹

It is important to note that the scope of the MDR is limited to devices that actively stimulate the brain. Although the GDPR fully applies to the MDR,¹¹⁰ neurotechnologies that solely collect or process mental data, fall outside the scope of this regulatory framework and are therefore not subject to its specific safety and performance requirements. This regulatory gap has been contested by some academics.¹¹¹ Bublitz and Litgthart argue that the inapplicability of the MDR to the collection of neural data, and thus to mental privacy stems from the fact that having one's thoughts, opinions or emotions revealed through brain-reading neurotechnologies does not seem to be covered by the notion of risk enshrined in the MDR.¹¹² This assumption, according to the authors, could be challenged in a way that opens the door to the inclusion of brain-reading technologies within the scope of the MDR on the basis of the risks associated with access to neural information, currently only partially addressed by the GDPR and the AI Act.¹¹³ Support for this position may be found in the literature calling for an expansion of the MDR's conception of risk beyond the “vulnerability of the human body”¹¹⁴ to include mental impacts, either directly or through comprehensive risk impact assessments to be carried out by companies operating in the consumer neurotechnology sector.

Whether heightened protection of neural data, and, by extension, of *mental privacy*, will emerge through an expansion of the MDR to encompass all neurotechnologies, or rather through the consumer and product-safety frameworks recently adopted at EU level, remains an open question. With the entry into force of the General Product Safety Regulation (EU) 2023/988 (GPSR) in December 2024,¹¹⁵ replacing the former Directive, product safety assessment criteria have been modernized to better address risks associated with digital products, and can be deemed applicable to brain-reading neurotechnologies. Article 6(1)(g) explicitly recognises the relevance of cybersecurity, which may be

¹⁰⁸ A. Wexler, *A Pragmatic Analysis of the Regulation of Consumer Transcranial Direct Current Stimulation (TDCS) Devices in the United States*, in *Journal of Law and the Biosciences*, 2/2015, p. 677.

¹⁰⁹ Commission Implementing Regulation (EU) 2022/2346 of 1 December 2022 laying down common specifications for the groups of products without an intended medical purpose listed in Annex XVI to Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices, OJL 311, 2.12.2022, para. 60.

¹¹⁰ Art 1(13) and Recital 5 of the MDR.

¹¹¹ J. C. Bublitz, J. Chandler, F. Molnár-Gábor et al., *A Moratorium on Implantable Non-Medical Neurotech Until Effects on the Mind are Properly Understood*, in *Neuroethics*, 18/2025, p. 6.

¹¹² C. Bublitz, S. Litgthart, *The new regulation of non-medical neurotechnologies in the European Union: overview and reflection* in *Journal of Law and the Biosciences*, 11/2024, p. 15.

¹¹³ For a more detailed analysis of how the AI Act addresses risks linked to the AI- powered manipulation, the exploitation of vulnerabilities or the inference of emotions (all of which require necessarily the prior collection of data) see below.

¹¹⁴ C. Bublitz, S. Litgthart, *The new regulation of non-medical neurotechnologies*, cit., p. 14.

¹¹⁵ Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, OJ L 135, 23.5.2023, pp. 1–51. It applies from 13 December 2024.

applicable to the risk of unconsented access or processing of neural data through consumer neurotechnology. Moreover, letter (h) of Article 6(1) requires that, when assessing whether a product is safe, due account be taken of the nature of the product as well as of its evolving, learning, and predictive functionalities, features that may directly affect the effective enjoyment of the right to mental privacy. A cross-analysis of these instruments reveals a clear regulatory trend: instead of defining or safeguarding mental privacy as such, the legislator has required manufacturers and providers to identify and mitigate psychological risks arising from the use of neurotechnologies. This approach, visible in the Product Liability Directive (2024) and the Product Safety Regulation (2023), reflects a conceptual gap in the EU's understanding of mental privacy, namely, uncertainty about what constitutes its violation and how it can be measured.

The revised Product Liability Directive, applicable from December 2026, exemplifies this approach by extending liability beyond physical devices to digital services integrated into a product, a crucial inclusion for connected or AI-driven neurotechnologies. Under Article 6, “damage” explicitly covers *death, personal injury, and medically certified psychological harm*, thereby recognising mental health impacts as compensable harms.

Taken together, these provisions show that EU law currently manages psychological harm rather than risks that may result from the violation of mental privacy. Yet, this paper argues that the consequences of violating mental privacy are not limited to psychological harm: mental privacy is intimately linked to identity, agency and personality development, and its infringement constitutes the precondition for violations of other fundamental rights, including freedom of thought and mental integrity.

Whether the future will bring an expansion of the MDR to all neurotechnologies, thereby recognising breaches of neural data as risks that manufacturers must mitigate, remains to be seen. Alternatively, mental data protection could remain within the scope of the GDPR, provided that its provisions are updated and more precisely interpreted. In the meantime, academic proposals to strengthen the existing risk-assessment frameworks, including calls for Mental Data Protection Impact Assessment (MDPIA) or the adoption of a mandatory Mental Impact Assessment for non-medical applications of implantable neurotechnologies,¹¹⁶ deserve close attention and further development as potential tools to operationalise mental privacy within EU law.¹¹⁷

Lastly, a brief reference should be made to the mental privacy implications of the lack of precision in the wording of the recently adopted AI Act.¹¹⁸ While Article 5(1)f of the AI Act prohibits the placing on the market, putting into service, or use of AI systems aimed at inferring emotions in the workplace and educational settings, the drafting of this provision leaves room for potential protection gaps.¹¹⁹ Specifically, Recital 44 introduces an exception for AI systems marketed for medical or safety reasons, including those intended for therapeutic use. This carve-out, while understandable in clinical contexts, may be too broadly framed, potentially allowing employers or educational institutions to justify the deployment of AI-based mental data inferences under the guise of ensuring ‘safety’ or ‘well-

¹¹⁶J. C. Bublitz, J. Chandler, F. Molnár-Gábor et al., *A Moratorium on Implantable*, cit.

¹¹⁷M. Ienca and G. Malgieri, *Mental Data Protection*, cit.

¹¹⁸ European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. *Official Journal of the European Union*, L, 1689, 1-163.

¹¹⁹ Prohibited AI practices in letters b) and d) might also be worth examining here for their implications for people with disabilities: “(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm; (d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity”.

being'. For example, systems designed to monitor mental states to prevent accidents, assess fatigue, or manage stress could arguably fall within this exception, despite their intrusive nature and the imbalance of power that characterizes workplace and educational relationships. Some authors have expressed criticism of the distinction between mental states and emotions from the perspective of its consistency with this philosophy of the mind.¹²⁰ Furthermore, under its current form, this prohibition risks becoming porous, potentially permitting forms of emotional surveillance that the regulation explicitly seeks to prevent. A more precise delineation of what constitutes a legitimate safety reason would be necessary to prevent the circumvention of the intended protections and to ensure that the right to mental privacy is effectively safeguarded. From this perspective, some scholars have pointed out that, while the AI Act explicitly addresses the risks posed by AI-based neurotechnologies used to infer emotions or intentions in educational and workplace settings, the regulation of manipulative techniques involving neurotechnologies remains contingent upon the fulfilment of a series of rather vague criteria. This regulatory uncertainty may present a significant challenge that would require further clarification by the newly established EU AI Office, particularly if such applications become widespread. Under these circumstances, it will be crucial to closely track and evaluate how the GDPR, MDR, product safety regulation and the AI Act intersect in the regulation of neurotechnologies in the years to come.¹²¹

4. Conclusion

The aim of this paper has been to examine whether “mental privacy” can be mapped onto existing legal frameworks, particularly those of international and European human rights law. To enable such an analysis, Section 2 first established a conceptual grounding of mental privacy, while Section 3 mapped relevant case law and regulatory instruments addressing its protection.

At the conceptual level, we argued that the current literature commonly defines mental privacy as control over information concerning one’s mental states and the inferences that may be drawn from it. This understanding is supported by the normative foundations of mental privacy, namely, the protection of personhood and autonomy that depend on a safeguarded inner sphere of thought, imagination, and moral reasoning. Recent scholarship warns that technologies capable of accessing or manipulating mental states risk collapsing the boundary between inner and outer privacy, and thus threaten individual autonomy underpinning identity and personhood. We further contended that the concept of “informational control” in this context rests on these normative foundations and extends beyond traditional conceptions of privacy.

Debates on mental privacy also focus on the extent to which mental states can be accessed or inferred, as advances in brain decoding and multimodal data analysis blur the line between neural and behavioural inference. Although current technologies may not genuinely “read minds”, the mere possibility or anticipation of such mental intrusion creates epistemic vulnerability and self-censorship.

In operationalizing mental privacy within legal frameworks, a key conceptual challenge still needs further investigation: when exactly do information and data reveal an individual’s mental state? The critical issue is not the origin of the data but its semantic and normative proximity to an individual’s inner mental life. Scholars continue to debate whether only *neural data* —which can expose subconscious processes and bypass intentional disclosure— or also *behavioural and physiological data* should be considered “mental data.” A growing consensus suggests that any data enabling meaningful inferences about mental states merits distinct legal protection.

This broader approach appears increasingly relevant in light of the growing number of national initiatives specifically aimed at protecting neural data. Laws addressing neural data protection have

¹²⁰ J. C. Bublitz, F. Molnár-Gábor and M. R. Soekadar, *Implications of the Novel EU AI Act for Neurotechnologies*, in *Neuron*, 112/2024, p. 3014.

¹²¹ *Ibid*, p. 3015.

already been adopted in jurisdictions such as Colorado, California, Montana and Connecticut in the United States, as well as in Chile and Canada, while legislative proposals are currently pending in countries including Brazil, Mexico and Argentina. However, if effective safeguards are to be granted to rights such as mental privacy, these protections should not remain limited to neural data narrowly understood, but should extend to the broader category of mental data. In our conceptual framework, mental data refers to any data capable of enabling inferences about an individual's mental states.

At an international level, the ICCPR, the work of Special Rapporteurs, and evolving scholarly positions have significantly shaped the foundational understanding of mental privacy, in a broad sense, within international human rights law. The ICCPR, through Article 17, establishes the right to privacy as a key protection, extending it to interference not only by State authorities but also by private entities, as clarified by General Comment No. 16. The Special Rapporteur on the right to privacy has further developed this concept, emphasizing the conditions under which privacy interferences can be justified, most notably the principles of proportionality, necessity, and minimal intrusion. Importantly, in recent reports, the Special Rapporteur has identified a set of globally shared privacy principles that should guide the processing of personal data, including mental data. There is growing recognition, supported by UNESCO and several legal scholars, that the inferences drawn from mental data pose serious risks to privacy and mental integrity, warranting heightened protection comparable to that granted to health-related and genetic data.

At a regional level, the Inter-American and European human rights systems have complemented and advanced this protection by focusing on the nuanced assessment of mental data's sensitivity and the need for its robust regulation. The Inter-American system, through the jurisprudence of the IACtHR and the OAS Declaration of Principles on Neuroscience, Neurotechnologies and Human Rights (2023), has played a leading role in framing neural data as sensitive personal information, requiring express and informed consent for any access or processing. By linking privacy to dignity and autonomy, and by articulating proportionality and consent as core principles, the Inter-American approach provides a progressive soft-law foundation for States to develop coherent national frameworks for neurotechnological governance. In contrast, the European regional system, through the case law of the ECtHR, has contributed primarily by refining proportionality and necessity tests applicable to intrusive data processing, emphasizing legality, foreseeability, and safeguards against abuse. While these principles indirectly protect mental privacy, the absence of a clear legal definition and the lack of consistent recognition of neural data as a distinct sensitive category limit their effectiveness.

Within the European Union, the protection of mental privacy arises from the interplay between the GDPR and the Medical Devices Regulation (MDR), though both instruments reveal significant conceptual and normative gaps. While Article 9 GDPR grants heightened protection to "special categories" of personal data, its application to neural data remains uncertain, depending on whether such data directly relate to health or mental conditions. Scholars increasingly argue that sensitivity should be determined not solely by the data's nature but by the type of inferences it allows and the risks it generates. The MDR, meanwhile, narrowly regulates neurostimulation devices and fails to address neurotechnologies that solely collect or process brain data, leaving non-medical applications outside its scope. It remains uncertain whether heightened protection of neural data —and, by extension, of mental privacy— will arise through an expansion of the Medical Devices Regulation (MDR) to encompass all neurotechnologies. Currently, the analysis of this instrument reveals a significant regulatory gap, as its safety-oriented framework covers only neurostimulation devices, while leaving neurotechnologies that merely collect or process mental data outside its scope.

Beyond these core instruments, the Product Safety Regulation (2023) introduces indirect protection by recognising psychological harm as compensable damage and by requiring risk assessments for vulnerable consumers. However, these measures address only tangible manifestations of harm, not violations of mental privacy itself. Similarly, the AI Act seeks to limit emotional surveillance but contains broadly worded exceptions for medical and safety uses, risking under-protection in practice. The gaps that emerge from this analysis of EU secondary law will require either an expansion of the MDR to

encompass all neurotechnologies or targeted reforms of the GDPR, possibly supported by new governance tools such as a Mental Data Protection Impact Assessment (MDPIA) or a Mental Impact Assessment (MIA), to operationalise the right to mental privacy within EU law.

The central question addressed in this paper has been whether mental privacy, as reconstructed through the conceptual mapping developed above, is protected under international and European human rights law. A first conclusion emerging from this analysis is that, while the normative architecture capable of affording such protection already exists through evolving interpretative pathways at both the international and European levels, greater conceptual clarity remains necessary regarding the precise scope of mental privacy and the circumstances under which the collection and processing of mental data may amount to its violation. At the same time, the developments examined throughout this paper suggest the gradual emergence of a normative framework which, although still fragmented and largely grounded in soft law, increasingly recognizes the exceptional sensitivity of neural and mental data and the corresponding need for enhanced safeguards rooted in privacy, human dignity, autonomy, and mental integrity. Advancing such protection will ultimately depend on the adoption of an effective anticipatory approach, both through the development of binding regulation and through the interpretative evolution of existing human rights instruments, capable of integrating philosophical reflection with evolving scientific understanding.

Abstract

The concept of “mental privacy” has gained increasing attention as a means of protecting individuals’ thoughts, emotions, and neural data from unauthorized access, analysis, or manipulation. As advances in artificial intelligence and neurotechnology make the decoding of mental states increasingly plausible, concerns over the misuse of such data for surveillance, profiling, and behavioural prediction have intensified. In this paper, we first situate mental privacy within broader privacy theory and the conceptual discussion on the foundations of mental privacy before examining the international and regional instruments applicable together with their normative limitations and interpretative challenges. Building on this framework, the paper maps the principal international and European legal instruments relevant to the protection of mental privacy, including the ICCPR, GDPR, MDR, Product Safety Regulation, AI Act, and Council of Europe’s Convention 108+. It argues that while the normative architecture for its protection exists, it remains fragmented and conceptually underdeveloped.

Key words: mental privacy, neurotechnology, neural data, soft law, international and regional human rights frameworks, GDPR

*

Il concetto di “privacy mentale” ha suscitato un interesse crescente come strumento per proteggere i pensieri, le emozioni e i dati neurali degli individui da accessi, analisi o manipolazioni non autorizzati. Man mano che i progressi nell’intelligenza artificiale e nella neurotecnologia rendono sempre più plausibile la decodifica degli stati mentali, si sono intensificate le preoccupazioni relative all’uso improprio di tali dati a fini di sorveglianza, profilazione e previsione comportamentale. In questo articolo, collochiamo innanzitutto la privacy mentale all’interno della più ampia teoria della privacy e della discussione concettuale sui fondamenti della privacy mentale, prima di esaminare gli strumenti internazionali e regionali applicabili insieme ai loro limiti normativi e alle sfide interpretative. Partendo da questo quadro, l’articolo mappa i principali strumenti giuridici internazionali ed europei rilevanti per la protezione della privacy mentale, tra cui l’ICCPR, il GDPR, l’MDR, il Regolamento sulla sicurezza dei prodotti, l’AI Act e la Convenzione 108+ del Consiglio d’Europa. Si sostiene che, sebbene esista un’architettura normativa per la sua protezione, essa rimane frammentata e concettualmente sottosviluppata.

Parole chiavi: privacy mentale, neurotecnologia, dati neurali, soft law, cornici internazionali e regionali dei diritti umani, GDPR