

Workplace Neurosurveillance: Is the Employee's Mental Privacy Protected Under International Law?

Marta Sosa Navarro*

ABSTRACT: This paper analyses the implications for international human rights and labour law resulting from the use of neurotechnology in the workplace. It distinguishes between brain-reading devices, which collect and process neural data and may affect privacy and freedom of thought, and brain-altering technologies, which may affect mental integrity. By mapping the international, regional, and ILO frameworks, this paper highlights protection gaps created by fragmented regulation of this disruptive technology. It argues that the precautionary principle, soft-law instruments, and anticipatory regulation are essential to address these challenges. Ultimately, it contends that safeguarding dignity in the digital workplace requires a principled and proactive governance model to prevent cognitive surveillance and exploitation.

KEYWORDS: neurotechnology; workplace surveillance; mental privacy; freedom of thought; international labour law

SUMMARY: 1. Introduction – 2. International human rights system of protection against workplace surveillance – 2.1. Privacy as a precondition: special focus on Convention 108+ of the Council of Europe and Article 17 ICCPR – 2.2. The right to freedom of thought in the workplace under international human rights law – 3. The International Labour Organization and emerging challenges of workplace surveillance – 3.1. ILO safeguards of mental privacy – 3.2. ILO safeguards of mental integrity – 4. An overview of the human-centered but fragmented European normative framework protecting the worker's mental privacy and mental integrity – 4.1. The role of Article 88 GDPR in workplace personal data processing – 4.2. The EU Medical Device Regulation 2017/745 – 4.3. The AI Act and the regulation of emotion-inference technologies in the workplace – 5. Conclusive remarks.

1. Introduction

In a 2022 report commissioned by the British Law Society on the implications of neurotechnology for law and the legal profession, Australian criminal law scholar Allan McCay drew attention to the risks of workplace neurotechnologies by introducing the provocative idea of a “billable unit of attention”.¹ In this report, McCay cautioned that the collection and processing of neural data through attention-monitoring neurotechnologies could allow law firms to adopt forms of neurosurveillance disguised as billing innovations, charging clients for the “measurable attention”

* Assistant Professor in International Law, University of Milano-Bicocca. Mail: martamaria.sosanavarro@unimib.it. This article was subject to a blind peer review process.

¹ A. MCCAY, *Neurotechnology, law and the legal profession*, in *Horizon Report for The Law Society on Neurotechnology*, 2022, 26.

devoted to their case rather than for hours worked. Although still a hypothetical scenario, current market and investment trends in consumer neurotechnologies, coupled with the post-COVID expansion of workplace surveillance, suggest the emergence of a trend likely to penetrate everyday life, often unnoticed behind the smokescreen created by the contemporary normalization of self-tracking practices, which require individuals to disclose highly personal information, including health and biometric data, to private corporations.² These dynamic underscores the urgency of assessing whether, in a context of increasingly invasive technology-driven workplace monitoring, the international human rights system is adequately equipped to safeguard workers' rights and dignity.

Neurotechnology refers currently to devices, systems, and procedures — encompassing both hardware and software — that directly measure, access, monitor, analyze, predict or modulate the nervous system to understand, influence, restore, or anticipate its structure, activity and function.³ If we consider that this AI-powered technology, already embedded in consumer wearables such as earbuds or headbands,⁴ can measure neural activity,⁵ infer cognitive, emotional, and neurological states, connect the brain to digital systems via brain-computer interfaces (BCIs),⁶ and alter brain functioning,⁷ its transformative impact beyond the individual, extending to society as a whole is not hard to imagine.⁸

As neurotechnologies continue to advance and move beyond clinical contexts, where they have significantly improved the lives of patients with neurological conditions such as Parkinson's disease, epilepsy, locked-in syndrome, and treatment-resistant depression⁹ into direct-to-consumer markets, international debate has intensified regarding the human rights risks associated with their non-medical applications. In particular, scholars have highlighted privacy threats arising from the collection and use of neural data,¹⁰ including risks to freedom of thought¹¹ and freedom of expression,¹² while stressing the

² D. LUPTON, *The Quantified Self*, Cambridge, 2016, 2-3.

³ UNESCO, *Final Draft Recommendation on the Ethics of Neurotechnology* (hereinafter *UNESCO Recommendation*), Paris, 2025, 4.

⁴ L. BERNAEZ, V. MAHIEU, *Neurotech consumer market atlas. How the sector is making moves into the mainstream*, in *Center for Future Generations*, 2025. Available at: <https://cfg.eu/neurotech-market-atlas/#subchapter-6>.

⁵ Through electroencephalography (EGG) (Electroencephalogram), in *Mayo Clinic*, or functional magnetic resonance (fMRI). fMRI is a non-invasive method for studying the functional anatomy of the human brain. International Bioethics Committee (IBC) of UNESCO, *Report of the International Bioethics Committee of UNESCO (IBC) on the Ethical Issues of Neurotechnology* (hereinafter *IBC Report*), Paris, 2021, 8.

⁶ M. SOSA NAVARRO, A. LAVAZZA, M. BALCONI, M. IENCA, F. MINERVA, F. PIZZETTI, M. REICHLIN, F. SAMORÈ, V.A. SIRONI, S. SONGHORIAN, *Neuralink's brain-computer interfaces: medical innovations and ethical challenges*, in *Frontiers in Human Dynamics*, 7, 2025.

⁷ Both through transcranial direct stimulation (TDCs) or transcranial magnetic stimulation (TMS). Transcranial direct current stimulation (tDCS) or Transcranial electrical stimulation (tES) involve devices delivering continuous currents supposedly to enhance concentration or relaxation. *IBC Report*, cit. Transcranial magnetic is a non-invasive tool for the electrical stimulation of neural tissue, including cerebral cortex, spinal roots, and cranial and peripheral nerves. M. KOBAYASHI, *Transcranial magnetic stimulation in neurology*, in *The Lancet Neurology*, 2(3), 145-156.

⁸ C. BUBLITZ, S. LIGTHART, *The new regulation of non-medical neurotechnologies in the European Union: overview and reflection*, in *Journal of Law and the Biosciences*, 11(2), 2024, 14

⁹ M. SOSA NAVARRO, S. DURA-BERNAL, *Human Rights Systems of Protection From Neurotechnologies That Alter Brain Activity*, in *Drexel Law Review*, 15, 2023, 908-913.

¹⁰ P. KELLMAYER, *Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices*, in *Neuroethics*, 14, 2021, 87-90.

serious threats that neurotechnologies capable of altering neural activity may present to mental integrity and personal identity.¹³ Echoing these concerns, the UN Human Rights Council has recently adopted a report from the Human Rights Advisory Committee which underscored neurotechnology's unique character and socially disruptive potential noting that such technologies generally "(a) enable the exposition of cognitive processes; (b) enable the direct alteration of a person's mental processes and thoughts; (c) bypass the individual's conscious control or awareness; (d) enable non-consensual external access to thoughts, emotions and mental states; (e) are nurtured by "neurodata", which are needed for their own functioning, calibration and optimization; and (f) collect, analyse and process large personal datasets of a highly sensitive nature".¹⁴ The heightened awareness expressed by this UN report, coupled with a global neurotechnology market projected to hit \$24.2 billion by 2027,¹⁵ has triggered the adoption of numerous policy reports and recommendations at regional and international levels,¹⁶ alongside a patchwork of domestic legislative initiatives.¹⁷

Against this background, the deployment of neurotechnologies to augment workplace productivity by measuring and enhancing workers' concentration levels and cognitive performance poses

¹¹ C. BUBLITZ, *Freedom of Thought in the Age of Neuroscience*, in *Archiv für Rechts und Sozialphilosophie*, 100(1), 2014.

¹² S. LIGTHART, *Freedom of thought in Europe: do advances in "brain-reading" technology call for revision?*, in *Journal of Law and the Biosciences*, 7(1), 2020.

¹³ S. LIGTHART, M. IENCA, G. MEYNEN *et al.*, *Minding Rights: Mapping Ethical and Legal Foundations of Neurorights*, in *Cambridge Quarterly of Healthcare Ethics*, 32(4), 2023.

¹⁴ UNGA, Human Rights Council, *Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights*, A/HRC/57/61, 8 August 2024, 2-3. This report follows from a HRC resolution from 2022 that specifically requests the Advisory Committee to examine the risks and challenges arising from neurotechnologies. UN, Human Rights Council, *Res. 51/3. Neurotechnology and human rights*, Doc. No. A/HRC/RES/51/2, 13 October 2022.

¹⁵ M. SQUICCIARINI, L. XU, *Unveiling the Neurotechnology Landscape: Scientific Advancements, Innovations and Major Trends*, UNESCO, Paris, 2023, 9. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000386137>. Last visited 25/07/2025.

¹⁶ See, among others, OECD, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, OECD/LEGAL/0457, 11 December 2019; UNESCO *Recommendation*, cit.; 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 Advisory Committee, UN Human Rights Council/UN General Assembly, 8 August 2024. For a full analysis of soft law instruments that have emerged in the last decade see chapter 6 of M. SOSA NAVARRO, *The role of soft law in the regulation and governance of human rights challenges posed by neurotechnologies*, Torino, 2025, 140 ff.

¹⁷ In this sense, while Chile was the first country to amend its Constitution to protect psychological integrity and brain activity. Others have followed in Latin America with discussions underway in both Mexico and Brazil. D. BORBÓN, *Challenges of the inconsistent neurorights framework in Latin America*, in *Nat Neurosci*, 28, 2025, 1363-1364. Such a trend can also be identified in the Global North. Notably, France — through its Bioethics Law of 2 August 2021 — added Article L.1151-4 to the Public Health Code, prohibiting "any acts, procedures, techniques, methods or equipment that modify brain activity and pose a serious or suspected serious risk to human health". In light of that enactment, Article 16-14 of the French Civil Code was revised to provide that "brain-imaging techniques may only be used for medical or scientific research purposes, or in the context of a judicial expert appraisal, expressly excluding, in that context, functional brain imaging (fMRI)". In the US, States like Colorado (General Assembly 2024), California (SB 1223, 2024) or Montana (Senate Bill 2025) have adopted binding regulation to protect the privacy of neural data in response to the rapid development and market proliferation of neurotechnology. See M. SOSA NAVARRO, *Los neuroderechos en el norte global* in *Temas Selectos de Neuroética*, Ed. Aranzadi, Pamplona (forthcoming).

unprecedented challenges for the international human-rights framework.¹⁸ Assessing their current and potential use in employment settings therefore demands not only a review of overarching human-rights instruments but also a close examination of sector-specific regimes, including international data-protection treaties and relevant documents adopted within the International Labour Organisation (ILO). This article undertakes a transversal analysis of international law's capacity to safeguard against infringements of human and labour rights arising from market-driven cognitive and emotional monitoring and enhancement.¹⁹

The paper is structured in three substantive parts. Section 2 examines how the rights to privacy and freedom of thought provide safeguards against workplace neurotechnologies, with particular focus on neural data protection and the interpretive developments of this notion within international law. Section 3 turns to the right to mental integrity, addressing the distinctive challenges posed by brain-altering neurotechnologies and the potential role of international labour standards. Section 4 explores the European regulatory framework, analysing the GDPR, the Medical Devices Regulation, and the AI Act to assess how regional instruments confront the risks of neuromonitoring and neuromodulation in employment contexts.

2. International human rights systems of protection against workplace surveillance

The recent proliferation of the so-called “bossware”, which comprehends productivity monitoring systems such as software that tracks workers’ keystrokes, breaks, and screen activity, marks the onset of new era of workplace surveillance with serious human-rights implications.²⁰ In this same context, wearable neurotechnologies have moved beyond niche safety workplace applications (such as monitoring fatigue levels in lorry drivers)²¹ into everyday use, particularly within the consumer wellness market. Miniaturized EEG sensors embedded in headbands or earbuds, powered by machine-learning-based AI systems, are now marketed for purposes such as enhancing concentration, reducing stress, and monitoring attention levels.²² These devices do not only monitor our cognitive and emotional states but can also, via closed-loop feedback, alter them. If used without stringent safeguards in environments characterised by power imbalances and a quest for higher productivity, such as the workplace, these

¹⁸ S. ALEGRE, *Rethinking freedom of thought for the 21st Century*, in *European Human Rights Law*, 3, 2017, 232; J.M. MUÑOZ, J.A. MARINARO, *Neurorights as reconceptualized human rights*, in *Frontiers in Political Science*, 2023, 2.

¹⁹ J.M. PEAKE, G. KERR, J.P. SULLIVAN, *Critical Review of Consumer Wearables, Mobile Applications, and Equipment for Providing Biofeedback, Monitoring Stress, and Sleep in Physically Active Populations*, in *Frontiers in Physiology*, 9, 2018, 743.

²⁰ A. ALOISI, V. DE STEFANO, *Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon*, in *International Labour Review*, 161, 2022, 289. Such a concern is illustrated in Ken Loach’s recent film “Sorry we missed you” and has led to the so-called Amazonian Era, a name inspired by the technology company Amazon, that often spearheads illegitimate collection of worker’s personal information. A. GILBERT, A. THOMAS, *The Amazonian era. How algorithmic systems are eroding good work*, 2021. See also S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019.

²¹ N. FARAHANY, *The Battle for your Brain*, New York, 2023, 41; J. LAROCCO, M. DONG LE, D.G. PAENG, *A Systemic Review of Available Low-Cost EEG Headsets Used for Drowsiness Detection*, in *Frontiers in Neuroinformatics*, 14, 2020.

²² L. BÉRNAEZ TIMÓN, V. MAHIEU, *Neurotech consumer market atlas. How the sector is making moves into the mainstream*, in *Centre for future generations*, 2025, 18-20.

technologies may pose serious threats to employees' dignity by undermining privacy, freedom of thought, and mental integrity, while also affecting their sense of identity and personal agency.²³ Building on Istace's distinction between neurotechnologies that merely collect neural data and those that actively reshape neural activity, this section proceeds in two complementary strands. First, it assesses whether existing safeguards for privacy at an international level can protect employees against the novel risks posed by neurotech-driven workplace monitoring.²⁴ Second, it explores whether the right to freedom of thought can serve as a brake on market-driven workplace surveillance.

2.1. Privacy as a precondition: special focus on Convention 108+ of the Council of Europe and Article 17 ICCPR

The International Law Commission (ILC) reminds us that privacy and personal data protection is all but a new concern to the international community.²⁵ It is thus unsurprising that, as Della Morte observes, this field benefits from a highly developed system of international and regional protections.²⁶ International human-rights law long recognized privacy as an essential facet of the broader right to private life, enshrined in Article 12 of the UDHR, Article 17 of the ICCPR, Article 8 of the ECHR and Article 11 of the ACHR. Notably, in its General Comment 16 on Article 17 ICCPR, the UN Human Rights Committee affirmed that protections against "arbitrary or unlawful interference" with privacy extend not only to State action but also to conduct by non-State actors, including private entities.²⁷ This broadened interpretation is especially pertinent in light of escalating workplace surveillance, now potentially encompassing neurotechnologies and "bossware" capable of collecting and processing employees' neural data and making inferences on their cognitive and emotional states from it.²⁸ Such developments have prompted scholars like Malgieri and Ienca to argue that the unique sensitivity of neural data demands safeguards tailored to the specific risks of cognitive surveillance, manipulation, and discrimination.²⁹

²³ P. KELLMEYER, *Big Brain Data*, cit., 1

²⁴ T. ISTACE, *Human rights law: an incomplete but flexible framework to protect the human mind against neurotechnological intrusions*, in *Law, Innovation and Technology*, 16(1), 2024, 18.

²⁵ It has actually been a concern "since the late 60s". International Law Commission, *Report of the International Law Commission on the work of its Fifty-eighth session, 7 May-8 June and 9 July-10 August 2006*, UN GAOR, 61st sess, Supp No 10, UN Doc A/61/10. D. *Protection of Personal Data in Transborder Flow of information*, 493.

²⁶G. DELLA MORTE, *Big Data e Protezione Internazionale dei Diritti Umani*, Naples, 2018, 271-273. For a comprehensive analysis of these protective frameworks — which is further enriched by extensive ECtHR and CJEU case law and a suite of soft-law principles summarized by the ILC in eleven overarching tenets — see Chapter I of Part II in the authoritative volume cited above.

²⁷ UN Human Rights Committee, *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, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), para. 1

²⁸ Neurotechnology based tools sold as "EEG tech to aid workplace wellness" are already available in the market. See for instance, Emotiv or SmartCaps, an EEG-based technology currently used as safety equipment for fatigue monitoring.

²⁹ G. MALGIERI, M. IENCA, *Mental data protection and the GDPR*, in *Journal of Law and the Biosciences*, 9(1), 2022, 2, 8 and 10. In the same line, other scholars had advocated for a human rights impact assessment for AI, a proposal that was ultimately introduced in the AI Act for high-risk systems. A. MANTELETO, *Human Rights Impact Assessment and AI in Beyond Data*, in *Information Technology and Law Series*, 36, 2022.



Against this backdrop, Convention 108+, the modernized successor to the 1981 Council of Europe Data Protection Convention, offers a particularly promising framework. As the first binding international treaty devoted to personal data protection, its amended form, scheduled to enter into force sometime in 2026,³⁰ interestingly extends its scope to data processed for national security and defence,³¹ an innovation of direct relevance to dual-use or converging technologies such as the one under consideration.³² The choice is especially noteworthy given that legislative initiatives regulating AI do not necessarily extend to military applications, as illustrated by the EU AI Act, an omission that some commentators have described as one of its “most glaring oversights”.³³

Under Convention 108+, the collection and processing of personal data must satisfy seven core principles: transparency; purpose specificity; necessity and proportionality; data minimization and accuracy; secure processing; and respect for data-subject rights of access, rectification, objection and erasure. However, these obligations apply only to data that remain ‘personal’ in the sense of enabling identification or re-identification. Followingly, neural information that has been fully anonymized currently falls outside this regime and would require bespoke protective measures.³⁴ It is, however, important to note that although the Convention establishes a qualified category of personal data, emotions and thoughts not linked to health status, sexuality, or political and religious beliefs are not explicitly included in this category and are thus not granted specific protection.³⁵ This oversight has not gone unnoticed within the international scholarly community. At the 46th Plenary Meeting of the Council of Europe, held on 5 June 2024, international legal scholar Edoardo Bertoni and bioethicist Marcello Ienca presented a paper which, after reviewing the biological, legal, and ethical foundations of the risks to mental privacy posed by the proliferation of non-medical neurotechnologies, urged Member States to adopt a risk-based classification system. Central to their proposal was the introduction of a “*Mental*

³⁰ At the time of writing only 33 out of the 38 required States for the Convention to enter into force have ratified Convention 108+. See updated chart of signatures and ratifications here: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=223> (Last accessed 26/01/2026).

³¹ Previously, Article 3(2)(a) permitted exemptions for data collection and processing carried out in the national security and intelligence domain. By contrast, the GDPR expressly excludes any processing for national security or intelligence purposes and the proposed AI Act likewise omits coverage of these activities. See R. JANSEN, M. REIJNEVELD, *Convention 108+, the GDPR, and Data Processing in the National Security Domain*, in *EUR. DATA PROT. L. REV.*, 8, 2022, 423.

³² A comprehensive examination of the challenges that converging technologies such as neurotechnologies pose to trade regulation, both at the international and regional levels, lies beyond the scope of this paper. For an in-depth discussion see Chapter 5 (Dual use neurotechnology in the era of technological convergence) of M. SOSA NAVARRO, *The role of soft law in the regulation and governance of human rights challenges posed by neurotechnologies*, cit. See also J.M. RICKLI, M. IENCA, *The Security and Military Implications of Neurotechnology and Artificial Intelligence*, in O. FRIEDRICH, A. WOLKENSTEIN, C. BUBLITZ, R.J. JOX, E. RACINE, (eds), *Clinical Neurotechnology meets Artificial Intelligence. Advances in Neuroethics*, Cham, 2021.

³³ O. POLLICINO, F. PAOLUCCI, *Regulating AI Autonomy: A Constitutional Framework for the Digital Era*, in M. DURANTE, U. PAGALLO (eds.), *Handbook on Law and Digital Technologies*, de Gruyter, forthcoming, Bocconi Legal Studies Research Paper No. 5098433, Milan, 2024, 16.

³⁴ For a full-fledged distinction between anonymous and pseudoanonymous data, pursuant to the innovative framework introduced by the GDPR see G. DELLA MORTE, *Big Data e Protezione Internazionale*, cit., 156-157.

³⁵ *Ivi*, 26. This may fail to grant protection to data collected about these internal processes when they are not related to the cited categories, that is, when they broadly identify thoughts and feelings.

Data Protection Impact Assessment”, modelled on the AI Act’s fundamental-rights impact assessment.³⁶ Such an approach would constitute a first step towards aligning international data-protection law with the UN Guiding Principles on Business and Human Rights, embedding substantive human-rights due diligence into the core of neurotechnology governance.

To date, both Convention 108 and its modernised version, Convention 108+, have prompted domestic legislative reforms across Europe to bring national laws into closer alignment with their principles. Certain safeguards and standards contained in these instruments, specifically the requirements of proportionality and necessity, have informed the reasoning of two landmark judgments of the European Court of Human Rights.³⁷ Nonetheless, the Conventions have not shaped the Court’s privacy jurisprudence to the same extent as the Oviedo Convention on Human Rights and Biomedicine has. This instrument, also adopted under the Council of Europe, has significantly influenced the ECtHR’s case-law with regards to the ethical challenges arising from advances in genetics, particularly genome sequencing and editing technologies.³⁸ Within the specific context of employment, prior to the modernization of Convention 108, the Council of Europe had already addressed the protection of personal data in the workplace through its Recommendation of 18 January 1989, subsequently updated by Recommendation CM/Rec (2015)5 of 1 April 2015. Notably, this instrument stresses the desirability of extending to the employment sector the principles enshrined in Convention 108 and its Additional Protocol concerning supervisory authorities and transborder data flows. At the same time, it explicitly underscores that the processing of personal data must respect human dignity and privacy so as to ‘allow for the free development of the employee’s personality as well as for possibilities of individual and social relationships in the workplace’ (para. 3). While explicitly prohibiting the use of information systems and technologies whose direct and principal purpose is to monitor employees’ activity and behaviour (para. 15), the Recommendation nevertheless acknowledges that certain monitoring-adjacent technologies may be introduced for legitimate organisational objectives. In such cases, their deployment must be preceded by consultation with employees’ representatives and comply with the additional safeguards set out in Principle 21, reflecting an awareness of the potentially significant indirect effects of workplace monitoring on workers’ rights.³⁹

³⁶ *Ivi*, 30.

³⁷ ECtHR, *Centrum för Rättvisa v. Sweden*, Application no. 35252/08, Judgment (Grand Chamber), 25 May 2021, Strasbourg; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Judgment (Grand Chamber), 25 May 2021, Strasbourg.

³⁸ F. SEATZU, *The Experience of the European Court of Human Rights with the European Convention on Human Rights and Biomedicine in Utrecht Journal of International and European Law*, 31(81), 2015. For a specific analysis of the Oviedo Convention’s influence on the Strasbourg Court’s interpretation of the right to family life and the content of the right to informed consent see 10-11. G. CATALDI, *La Convenzione sui Diritti Umani e la Biomedicina*, in L. PINESCHI (ed.), *Tutela Internazionale dei Diritti Umani*, Giuffrè, Milano, 2006, 589. For a comprehensive examination of this instrument see also R. SAPIENZA, *La Convenzione europea sui diritti dell’uomo e la biomedicina*, in *Rivista di Diritto Internazionale*, 1998, 457-470.

³⁹ For a detailed analysis of the content of this Recommendation see A. SARTORI, *Il controllo tecnologico dei lavoratori, La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Milan, 2020, 8-9. The additional safeguards set out in Principle 21, and whose respect should be ensured by the employers include: a. informing employees before the introduction of information systems and technologies enabling the monitoring of their activities. (...); b. taking appropriate internal measures relating to the processing of that data and notify employees in advance; c. consult employees’ representatives in accordance with domestic law or practice, before

It can be inferred from the above that despite the significant efforts undertaken by the Council of Europe, the limited protection of thoughts and emotions, combined with the Convention's regional scope, highlight important shortcomings in the only binding international instrument on personal data protection currently in force. This gap reinforces the role of Article 17 of the ICCPR as the principal normative anchor at the global level and underscores the urgent need for a coherent and consensual interpretation of the right to privacy that can encompass the emerging dimension of mental privacy. Such an effort was undertaken in part by the UN Special Rapporteur on the Right to Privacy, Ana Brian Nougères, who between 2022 and 2025 issued a series of reports, two of which are of particular relevance for the purposes of this paper.⁴⁰

The first report,⁴¹ adopted in 2022, articulates the normative foundations of privacy and personal data protection, identifying ten guiding principles⁴² as the core components of what the Special Rapporteur characterizes as a global regulatory architecture. According to Nougères, these principles serve a dual function: they both guide the interpretation of the existing normative framework and facilitate its consistent application across diverse contexts. The Rapporteur goes a step further when asserting that these principles are not to be treated as mere recommendations, but as essential benchmarks for the lawful and ethical processing of personal data.⁴³ The principle of purpose specification requires that data be collected solely for explicit and legitimate purposes, with repurposing prohibited if incompatible with the original aim. The principle of transparency demands that the objectives of processing, along with the identity and contact details of controllers or their representatives, be disclosed at all times.⁴⁴ Consent, widely recognized at the international level as a legal ground for processing and closely tied to the principle of legality, must be freely given, specific, informed, unambiguous, and revocable.⁴⁵ Under the principles of data minimization and proportionality, only data strictly necessary for the stated purpose may be processed, and such processing must be proportionate to the aim pursued. Proportionality,

any monitoring system can be introduced or in circumstances where such monitoring may change. (...); d. consult, in accordance with domestic law, the national supervisory authority on the processing of personal data.

⁴⁰ It is worth noting that, although neither of these two documents made explicit reference to workers, the right to privacy had already been invoked at the UN level in General Assembly Resolution 45/95 of 14 December 1990, which adopted the *Guidelines for the Regulation of Computerized Personal Data*, and more recently in Resolution 68/167 of 18 December 2013 on the right to privacy in the digital age. Although this marked the first step in placing privacy on the UN digital agenda, led by the General Assembly, significant developments have followed. These include a series of reports by the Office of the High Commissioner for Human Rights (OHCHR, 2014, 2018, 2022) addressing surveillance, big data, AI, and digital identity, as well as the establishment in 2015 of a dedicated Special Rapporteur on the right to privacy, whose successive mandates have produced extensive thematic reports covering, inter alia, state and corporate surveillance, algorithmic management, and most recently neurotechnologies, several of which will be next examined.

⁴¹ A.B. NOUGÈRES, *Principles Underpinning Privacy and the Protection of Personal Data, Report to the UN Human Rights Council*, UN Doc A/77/196 (20 July 2022).

⁴² These principles are legality, lawfulness and legitimacy, consent, transparency, purpose specification, fairness, proportionality, data minimization, data quality, accountability, and security.

⁴³ A.B. NOUGÈRES, *Principles Underpinning Privacy and the Protection of Personal Data, Report to the UN Human Rights Council*, UN Doc A/77/196 (20 July 2022), cit., 3.

⁴⁴ A.B. NOUGÈRES, *Principles Underpinning Privacy and the Protection of Personal Data, Report to the UN Human Rights Council*, UN Doc A/77/196 (20 July 2022), cit., 11.

⁴⁵ A.B. NOUGÈRES, *Principles Underpinning Privacy and the Protection of Personal Data, Report to the UN Human Rights Council*, UN Doc A/77/196 (20 July 2022), cit., 8.

moreover, requires the controller to use the processing operation that is least invasive in terms of privacy.⁴⁶

Yet, the recognition of these principles has not removed the qualified nature of the right to privacy under international and regional human rights law. In practice, privacy is generally conceived as a right subject to limitations, provided that restrictions are lawful, necessary, and proportionate.⁴⁷ This has particular relevance in safety-critical sectors (e.g., transport, aviation, healthcare), where interferences with employee privacy may be justified to prevent serious harm,⁴⁸ such as through sleep reporting, alertness monitoring, or real-time drowsiness detection for drivers.⁴⁹

Despite not enjoying the protections granted to absolute rights, the Special Rapporteur has underscored that neural data present distinctive challenges that go beyond traditional privacy considerations. In her most recent report, published in January 2025, Nougères examines the foundations and principles for regulating neurotechnologies and the processing of neural data through the lens of the right to privacy.⁵⁰ She highlights that the heightened sensitivity of neural data derives not only from its capacity to identify individuals but also from its ability to reveal cognitive and affective states and to reflect personal experiences and emotions.⁵¹ In light of these features, the Special Rapporteur proposes the creation of a Model Law that serves as a tool to harmonize domestic regulations by establishing minimum standards for the safe and ethical use of neurotechnologies.⁵² Such Model Law, should not only integrate the general principles governing privacy and data protection in general but should also include a set of neuro-specific requirements.⁵³ In addition to demanding that any processing be necessary and narrowly tailored, the 2025 report calls for: (i) a human-rights and human-dignity-based approach across the design, development, deployment, commercialization and use of neurotechnologies; (ii) recognition of neurodata as highly sensitive given its capacity to reveal cognitive and affective states; (iii) application of the precautionary principle and safety-by-design; and (iv) rights-protective governance instruments (including stricter transparency, oversight and effective remedies). Taken together, these standards establish a heightened threshold for the regulation of neurotechnology-based monitoring in the workplace. A human-dignity based approach would thus call for the revision of the role attributed to employees' consent to provide access to his/her neural data in the workplace. As some authors have noted, the inherently imbalanced nature of the employment relationship renders employee consent an insufficient safeguard, thereby necessitating additional

⁴⁶ A.B. NOUGÈRES, *Principles Underpinning Privacy and the Protection of Personal Data, Report to the UN Human Rights Council*, UN Doc A/77/196 (20 July 2022), cit., 15.

⁴⁷ ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Application no. 62332/00, Judgment (Chamber), 6 June 2006, para 88.

⁴⁸ N. FARAHANY, *The Battle for your Brain*, cit., 41.

⁴⁹ P.M. RAMOS, C.B. MAIOR, M.C., MOURA, I. D. LINS, *Automatic drowsiness detection for safety-critical operations using ensemble models and EEG signals*, in *Process Saf. Environ. Prot.*, 164, 2022, 566-581.

⁵⁰ 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).

⁵¹ *Ivi*, 6.

⁵² *Ivi*, 7.

⁵³ *Ivi*, 9-10.

protective measures.⁵⁴ Failure to comply with these requirements risks not only infringing privacy but also eroding workers' autonomy and dignity.

In the absence of a specific regulatory framework governing the workplace use of EEG-enabled earbuds, headbands, or smart glasses, the growing deployment of digital monitoring tools that collect, process, and interpret neural data exposes workers' right to mental privacy to significant risks. By enabling employers to monitor attention, emotional states, and cognitive patterns, these technologies leave mental privacy particularly vulnerable. This vulnerability creates a concrete risk of discrimination, as neurotechnologies may enable employers to make hiring, promotion, or incentive decisions based on performance-related, emotional, or health-related information inferred from neural data.

Ultimately, while Article 17 of the ICCPR provides a foundational safeguard against arbitrary or unlawful interferences with privacy, including by non-State actors, the unique characteristics of neural data call for an updated interpretation of its scope to address the specific and evolving risks of neurotechnology-based surveillance, particularly in the workplace. As emphasised by the UN Special Rapporteur on the right to privacy in her report on neural data, these risks highlight the need to reconceptualise the protection of mental privacy. Although the Special Rapporteur's reports are formally non-binding, they extend beyond interpretive guidance: they provide evidence of an emerging global practice that may contribute to the formation of customary standards in data protection and privacy by both interpreting the existing framework and harmonising its application across diverse regulatory contexts. As such, Article 17 ICCPR calls for further normative development and interpretive expansion, particularly through the Human Rights Committee's jurisprudence, and most notably its General Comments, to provide a framework capable of regulating the emerging "digital mind" paradigm in workplace settings and ensuring that workers' mental privacy is not violated under the guise of productivity or safety.

2.2. The right to freedom of thought in the workplace under international human rights law

While the preceding section framed respect for privacy as a precondition for safeguarding workers' rights in environments increasingly permeated by monitoring practices, this section turns to the right to freedom of thought. The extent to which this right may provide protection against violations stemming from the use of neurotechnological monitoring tools for efficiency, performance or well-being purposes is examined.

The right to freedom of thought (RFoT) enjoys longstanding protection under core international and regional human rights instruments (Article 18 of the UDHR and the ICCPR, Article 9 of the ECHR, and Article 13 of the ACHR). Traditionally, this right has been interpreted as safeguarding the external manifestations of thought, such as speech or conduct, rather than the internal cognitive processes themselves. However, the proliferation of neurotechnologies capable of accessing, inferring, or even altering mental states has prompted renewed scholarly and institutional efforts to reconceptualize the RFoT in light of these developments.⁵⁵

⁵⁴ H. ABRAHA, *A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace*, in *International Data Privacy Law*, 12 (4), 2022, 294.

⁵⁵ C. BUBLITZ, *Freedom of Thought in the Age of Neuroscience*, cit.; S. MCCARTHY-JONES, *The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century*, in *Front. Artif. Intell.*, 25(1), 2019; S. ALEGRE, *Rethinking*

Two main approaches have emerged. The first calls for an explicit expansion of the RFoT to include protection of the internal dimension of thought, what some refer to as cognitive liberty.⁵⁶ The second proposes adding a relative component to this traditionally absolute right in order to strengthen it and stimulate its application in practice.⁵⁷ From this perspective, the development of narrowly tailored implied limitations to certain aspects of the right, such as the freedom against impermissible alteration of thought, may be legally grounded in the understanding that inner thoughts are not entirely beyond the reach of state power, whether from a factual, epistemic, or normative standpoint.⁵⁸ This reconceptualization acquires particular relevance in the context of neurotechnologies and carries significant implications for their use in workplace settings, where access to inner thoughts may extend to both public and private employers.

As the UN Special Rapporteur on Freedom of Religion or Belief, Ahmed Shaheed, outlined in his 2021 report, the RFoT should be understood as multidimensional. These dimensions include: (1) the right not to disclose one's thoughts; (2) freedom from punishment based solely on one's thoughts; (3) protection from impermissible interference or alteration of thought; and (4) the creation of an enabling environment for free thinking.⁵⁹ Each of these dimensions is potentially jeopardized by the introduction of cognitive-monitoring tools in professional settings.⁶⁰ For instance, when employers deploy technologies capable of decoding levels of attention, emotional states, or mental fatigue, they may indirectly compel disclosure of internal mental states, violating the first dimension. Even in the absence of explicit coercion, the existence of such surveillance tools may foster a chilling effect where workers self-censor their thoughts or emotions in anticipation of scrutiny (second dimension).⁶¹

In line with the aforementioned discussion, experts from international organizations and academia advocate for using the precautionary principle to guide the regulation of neurotechnologies.⁶² This principle, long recognized in international environmental and health law as having crystallized into customary law,⁶³ is particularly suited to contexts where scientific uncertainty intersects with high-stakes risks for individual rights and societal well-being.⁶⁴ It allows regulators to take protective action in the face of credible threats, even in the absence of conclusive scientific proof.

freedom of thought for the 21st Century, cit.; S. LIGTHART C. BUBLITZ, T. DOUGLAS, L. FORSBERG, G. MEYNEN, *Rethinking the Right to Freedom of Thought: A Multidisciplinary Analysis*, in *Hum. Rts. L. Rev.* 1, 3, 2022.

⁵⁶ M. IENCA, *On neurorights*, in *Frontiers in Human Neuroscience*, 15, 2021; N. FARAHANY, *The Battle for your Brain*, New York, 2023.

⁵⁷ S. LIGTHART, *Reconsidering the absolute nature of the right to freedom of thought*, in *Human Rights Law Review*, 25 (3), 2025, 26.

⁵⁸ *Ivi*, 5-6.

⁵⁹ A. SHAHEED (Special Rapporteur on Freedom of Religion or Belief), *Interim Report on the Freedom of Thought*, 14, U.N. Doc. A/76/380, Oct. 5, 2021, para. 25.

⁶⁰ A. MCCAY, *Neurotechnology, law and the legal profession*, cit., 5.

⁶¹ K. BALL, *Electronic Monitoring and Surveillance in the Workplace. Literature review and policy recommendations*, Publications Office of the European Union, 2021, 34-40 for the individual level of analysis of the effect of the impact of surveillance/monitoring systems in the workplace. See also 71 and 78.

⁶² See OECD, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, cit., 6-9.

⁶³ C. RAGNI, *Scienza, Diritto e Giustizia Internazionale*, Naples, 2020, 103 ff.

⁶⁴ N. DE SADELEER, *Environmental principles. From political slogans to legal rules*, Oxford, 2002, Chapter 3. *The precautionary principle*, in particular, 174 ff.

From another perspective, the use of such technologies undermines the enabling environment essential for the autonomous development of thought. Drawing from Shaheed’s framing, the freedom to think does not merely require the absence of interference, it requires the certainty that one’s mental processes remain fully private during the critical “rumination phase” of thought formation (fourth dimension).⁶⁵ This concern is magnified in employment settings marked by power asymmetries,⁶⁶ where the unregulated use of neurotechnologies may undermine workers’ effective ability to exercise their rights, particularly if neural data is used for productivity metrics or behavioral profiling. While national constitutional protections may offer pathways for enforcement and remedy in case of violation, international law remains underdeveloped in this area. The current absence of clear regulatory boundaries means that the normative dimensions of RFoT, especially in the workplace, remain inadequately protected.

Ultimately, this section has argued that protecting workers’ mental privacy and freedom of thought in the age of neurotechnology demands both innovative legal reasoning and the dynamic reinterpretation of existing rights frameworks. In particular, it underscores the pressing need for robust safeguards against practices that compel, incentivize, or normalize the disclosure of internal mental states for commercial or productivity-related purposes. Crucially, the positive obligations arising from so-called “negative” rights, consistently recognized in human rights jurisprudence,⁶⁷ must be fully acknowledged in this context. These obligations require not only refraining from unlawful interference,⁶⁸ but also adopting proactive measures, such as enacting regulatory frameworks, to prevent non-state actors from infringing upon individuals’ rights.⁶⁹ Some of these concerns, particularly those relating to surveillance and working conditions, will be examined in the following section, which considers the protections afforded to workers under International Labour Organization (ILO) conventions against human rights violations arising from surveillance practices.

3. The International Labour Organization and emerging challenges of workplace surveillance

3.1. ILO safeguards of mental privacy

The International Labour Organization (ILO) is among the oldest existing international organisations, tracing its origins to 1919 when it was established as part of the Treaty of Versailles to “reflect the belief

⁶⁵ N. FARAHANY, *The Costs of Changing Our Minds*, in *Emory L.J.*, 69, 2019, 98.

⁶⁶ The European Court of Human Rights has emphasized that the validity of consent hinges on the existence of a “real choice”. It has held that even when individuals disclose personal data voluntarily or with consent, such disclosure does not strip them of the protections under Article 8 ECHR if no real choice exists – such as when an employer requires the disclosure of a job-seeker’s criminal record as a condition of employment. ECtHR, *M.M v. United Kingdom*, Application no. 24029/07, Judgment of 13 November 2012, para. 189.

⁶⁷ V. STOYANOVA, *The Disjunctive Structure of Positive Rights under the European Convention on Human Rights*, in *Nordic Journal of International Law*, 87(3), 2018, 345. See specifically footnote 1.

⁶⁸ S. LIGTHART, *Freedom of thought in Europe: do advances in ‘brain-reading’ technology call for revision?*, cit., 18 and 15-16 noting the range of case-law interpreting Article 9 of the ECHR, that only recent cases “provide a bit more clarification”, and that, in general, “case-law and decisions do not extensively elaborate on the meaning and scope of the notion of thought as protected by Article 9 ECHR”.

⁶⁹ S. ALEGRE, *Rethinking freedom of thought for the 21st Century*, cit., 222.

that universal and lasting peace can be accomplished only if it is based on social justice".⁷⁰ International labour law is primarily composed of ILO Conventions and Recommendations, which differ in legal character: while Conventions create binding obligations for States that ratify them, Recommendations are non-binding and provide guidance for national policy, legislation, and practice. Both instruments are adopted at the International Labour Conference and must subsequently be submitted by all 187 Member States to the competent domestic authority for consideration. Ratification of a Convention entails concrete effects at the national level, as enterprises become directly subject to laws, regulations, judicial decisions, and collective agreements implementing international labour standards.

To date, the only instrument specifically addressing the protection of workers' privacy within the ILO framework is the *Code of Practice on the Protection of Workers' Personal Data*, adopted at a meeting of experts on privacy held from 1-7 October 1996.⁷¹ Unlike Conventions or Recommendations adopted under Article 19 of the ILO Constitution, Codes of Practice are non-binding technical standards developed through expert meetings convened by the ILO Governing Body. Drafted within the Organisation's tripartite structure, they involve representatives of governments, employers and workers. Once adopted, they are published by the ILO as practical guidance intended to assist in the implementation of existing standards. Their status is therefore that of soft law: they do not constitute formal sources of international labour law, nor are they subject to supervision by the ILO's Committee of Experts on the Application of Conventions and Recommendations (CEACR). Nevertheless, CEACR reports occasionally cite Codes of Practice as interpretive aids, and in practice such instruments often serve as important reference points for the development of legislation, collective agreements, workplace regulations, and company practices,⁷² illustrating the post-law function of soft law in guiding normative interpretation and development.⁷³

Despite being almost 3 decades old, the ILO's *Code of Practice on the Protection of Workers' Personal Data* introduces interesting guidance with regard to technology-based monitoring of workers. While not prohibited, it requires that workers be informed in advance of the reasons, methods, timing, and scope of any monitoring, and that employers minimise intrusions into privacy. Secret monitoring is allowed only where authorised by national law or justified by reasonable suspicion of criminal activity or other serious misconduct, while continuous monitoring is restricted to circumstances necessary for health, safety, or property protection (para 6.14). The *Code of Practice* also addresses invasive testing practices (paras. 6.10-6.12), prohibiting the use of polygraphs or similar 'truth-verification' technologies, strictly limiting genetic screening to instances expressly authorised by law, and requiring that personality tests remain consistent with privacy protections while preserving the worker's right to object. These provisions, although formulated in the mid-1990s, resonate strongly with contemporary debates on neurotechnology in the workplace. Brain-reading devices, much like polygraphs or personality profiling, seek to access otherwise inaccessible aspects of a person's inner life (emotions, mental states, or

⁷⁰ G. CASALE, *Fundamentals of International Labor Law*, 4th Ed., Milan, 2024, 23.

⁷¹ On this topic, S. GIUBBONI, *Potere datoriale di controllo e diritto alla privacy del lavoratore. Una sinossi delle fonti europee e internazionali*, in *Riv. giur. lav. prev. soc.*, 1, 2012, 81.

⁷² F. HENDRICKX, *Employment privacy* in R. BLANPAIN (ed.), *Comparative Labour Law and Industrial Relations in Industrialized Market Economies*, The Netherlands, 2014, 476.

⁷³ For an in-depth study of the triple function of soft law theory in international law see E. TRAMONTANA, *Il soft law e la resilienza internazionale*, in *Ars interpretandi*, 2, 2017.

predispositions) and therefore raise comparable, if not heightened, risks for privacy, dignity, and freedom of thought.

In this sense, the *Code of Practice* can be seen as an early attempt to grapple with the very concerns that neurotechnologies now amplify in workplace settings, suggesting that its framework could be updated and expanded to explicitly encompass the unique risks posed by contemporary brain-monitoring and cognitive surveillance tools.

3.2. ILO safeguards of mental integrity

The preceding sections have examined the protection of neural data and freedom of thought, showing that these aspects can be effectively anchored within the existing international human rights framework. However, when it comes to neurotechnologies capable of altering brain activity, a significant normative gap emerges. While medical applications of neurotechnology benefit from heightened legal and ethical scrutiny, the increasing use of wearable brain-altering devices for productivity enhancement purposes remains largely unregulated at a global level.⁷⁴ This asymmetry raises serious concerns regarding worker's safety, discrimination, mental health, and the preservation of mental integrity.

Given its primary focus on privacy and freedom of thought, this paper does not seek to offer a comprehensive analysis of the risks to mental integrity arising from the spread of wearable neurostimulation devices, nor does it provide an exhaustive account of the legal safeguards afforded to workers under international law in this area. It does, however, aim to clarify the practical distinctions between brain-reading and brain-altering neurotechnologies, examined here from conceptual, practical, and normative perspectives.

In their foundational articulation of neuro-rights, *Ienca and Andorno* define mental integrity as the right to be protected against unauthorized alterations of neural computation, particularly where such changes result in harm.⁷⁵ According to their framework, three conditions must be met for an action to constitute a threat to mental integrity: (i) direct access to and manipulation of neural signals, (ii) lack of informed consent from the individual, and (iii) resulting harm to mental or physical well-being, including, for instance the side-effects of neuromodulation, an increasing risk due to the growing number of wearable neurostimulators on the market.⁷⁶ Importantly, the requirement of an action (to alter, manipulate, erase) excludes neurotechnologies used solely for monitoring or inference, sufficiently covered by the right to privacy and the right to freedom of thought examined in the previous sections of this article.

Establishing the fulfilment of the second condition — the absence of informed consent — is particularly problematic in workplace settings, where structural power imbalances between employer and employee call into question the voluntariness of any purported consent. This dynamic heightens the risk of coercive or exploitative uses of consumer neurostimulation devices aimed at enhancing worker

⁷⁴ In section 4.2., we will see this is not the case at the EU level, which has recently amended the Medical Devices Directive to include non-invasive non-medical brain stimulation devices within in the highest risk category of medical devices.

⁷⁵ M. IENCA, R. ANDORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sci Soc Policy*, 13(5), 2017, 18.

⁷⁶ A. WEXLER, P.B. REINER, *Oversight of Direct-to-Consumer Neurotechnologies*, in *Science*, 2019, 234.

performance. While minor physical effects like skin irritation may be addressed under general product safety regimes,⁷⁷ the more significant concern lies in their potential to modulate cognitive states without genuine, informed, and voluntary consent. This challenge becomes even more pressing given the growing accessibility of non-invasive neurostimulators, which now appear in forms as discreet as earbuds or headbands and are marketed as everyday productivity tools.⁷⁸

The internationally recognized right to bodily integrity might provide some protection in this context. While some authors suggests that any interference with bodily or mental autonomy should be assessed by the severity of its impact,⁷⁹ others argue that any unconsented modification of neural functioning, even via external stimulation, constitutes a violation of bodily integrity.⁸⁰ Building on this reasoning, *Istace* emphasizes that non-invasive devices like transcranial direct stimulation (TDCs) or neurostimulation earbuds must still fall within the scope of the right to bodily and mental integrity. This author challenges the adequacy of traditional legal distinctions based on physical. This perspective acquires particular relevance in light of increasing empirical evidence of the measurable effects of these technologies on attention, memory, and mood.⁸¹

Against this background, unregulated neuromodulation in the workplace, particularly when deployed in contexts of implicit coercion, raises concerns not only for the right to privacy, but for the core rights to bodily and mental integrity and personal dignity.⁸² Although the right to bodily integrity may play a central role in safeguarding mental autonomy against such interventions, its application within the employment context demands a more tailored analysis. The unique vulnerabilities of the workplace, including structural power imbalances already referred to and the pressure to enhance performance, call for a perspective that transcends the general international human rights framework.

A possible avenue to explore could be the normative acquis of the International Labour Organization (ILO). Existing instruments already contain principles that provide specific guardrails against exploitative or harmful workplace practices that could be extended to cover neurotechnologies Convention No. 155 (1981) on Occupational Safety and Health and Recommendation No. 164 impose duties on employers to protect workers' physical and mental well-being; Convention No. 187 (2006) encourages continuous national improvement in occupational safety regimes; Convention No. 190 (2019) addresses psychological harm and harassment, including that enabled by technology; and Convention No. 111 (1958) prohibits discrimination in employment, which is relevant to algorithmic or neuro-based evaluations of performance.

⁷⁷ A. WEXLER, *A Pragmatic Analysis of the Regulation of Consumer Transcranial Direct Current Stimulation (TDCS) Devices in the United States*, in *J.L. & BIOSCIENCES*, 2, 2015, 683. This is mostly the case in the US, In the EU, as section 4.2. will illustrate physical effects of non-medical applications of neurostimulation devices fall under the Medical Device Regulation.

⁷⁸ N. FARAHANY, *The Battle for your Brain*, cit., chap. 3.

⁷⁹ V. TESINK, T. DOUGLAS, L. FORSBERG *et al.*, *Neurointerventions in Criminal Justice: On the Scope of the Moral Right to Bodily Integrity*, in *Neuroethics*, 16, 2023, 26

⁸⁰ J. RYBERG, *Neurointerventions, Crime, and Punishment: Ethical Considerations* Oxford, 2019, 52.

⁸¹ T. ISTACE, *Human rights law: an incomplete but flexible framework to protect the human mind*, cit., 18

⁸² R. BLUHM, M. CORTRIGHT, ED ACHTYES, LY CABRERA, *They Are Invasive in Different Ways: Stakeholders' Perceptions of the Invasiveness of Psychiatric Electroceutical Interventions*, in *AJOB Neuroscience*, 14 (1), 2023.

In conclusion, the analysis underscores that while privacy and freedom of thought provide an important starting point for regulating workplace neurotechnologies, the advent of devices capable of altering neural activity exposes a profound normative lacuna in international law. The risks of coercion, discrimination, and compromised mental autonomy associated with consumer neurostimulation tools evidence that workers' mental integrity cannot be adequately safeguarded by existing privacy-oriented frameworks alone. Although the right to bodily integrity offers a potential avenue for protection, its application in the employment context remains insufficiently theorised and operationalised. The ILO *acquis*, with its established emphasis on health, safety, dignity, and non-discrimination in the workplace, could serve as a promising foundation for extending protection to this emerging frontier.

4. An overview of the human-centered but fragmented European normative framework protecting the worker's mental privacy and mental integrity

Following the preceding discussion on the capacity of international human rights law to safeguard workers' rights to privacy and freedom of thought in the light of emerging workplace surveillance trends, it is now useful to consider how the European regional framework addresses these concerns. This perspective provides a more concrete view of how such rights, enshrined in the European Convention on Human Rights, can be enforced through binding legal instruments. Within this context, particular attention will be given to the General Data Protection Regulation (GDPR), and especially Article 88, which permits Member States to introduce specific rules on data processing in the employment context, provided these rules incorporate suitable and specific safeguards for human dignity and fundamental rights.

In addition, reference will be made to the EU Medical Devices Regulation (MDR), which contains provisions for the marketing of neurostimulation devices, including those intended for non-medical purposes, such as cognitive enhancement or performance modulation, that may be used in the workplace. These safeguards provide a legal foundation for regulating potentially harmful neurotechnological interventions in professional environments.

More recently, the EU Artificial Intelligence Act has expanded this framework. Of particular significance is Article 5, which prohibits the use of AI systems designed to infer emotional states in employment and education. This prohibition acknowledges the heightened risks of affective computing and emotion-recognition tools in contexts shaped by structural power imbalances and reduced individual autonomy. Collectively, these instruments provide a set of protections that, although uneven and still evolving, signal a growing regional commitment to regulating neurotechnologies in ways that align with fundamental rights and take account of workplace-specific vulnerabilities.

4.1. The role of Article 88 GDPR in workplace personal data processing

A number of GDPR provisions touch upon data processing in the workplace.⁸³ Central to this discussion, however, is Article 88(1), the so-called "opening clause", which empowers Member States to adopt specific rules for handling workers' data. This focus reflects the need to examine the scope of national discretion in an era where neurotechnologies allow unprecedented monitoring of emotions and

⁸³ See for instance, Article 24 GDPR on the duties of data controllers.



cognitive capacities, thereby raising concerns for dignity, autonomy, and mental privacy. The analysis proceeds from a human rights perspective, considering both the GDPR's text, the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

During the negotiations of the GDPR, efforts by the European Commission and the Directorate-General for Employment to establish a uniform regulatory framework for workplace data processing were ultimately resisted by Member States.⁸⁴ Article 88(1) was introduced as a compromise, granting flexibility to legislate in this sensitive field, often privileging consent as a legal ground for the processing of personal data in the employment context. Germany and Finland have enacted dedicated legislation under the clause, Spain and Greece have embedded workplace rules in broader data protection laws, while other jurisdictions, such as Croatia, France, and Luxembourg, have regulated specific issues, including biometrics and surveillance.⁸⁵

Yet this discretion under this provision is not unlimited. Article 88(2) stipulates that national measures must include "suitable and specific safeguards" for dignity, legitimate interests, and fundamental rights. A 2022 preliminary ruling by the CJEU confirmed that national autonomy is conditional upon these safeguards.⁸⁶ The Court's reasoning in *Omega*, upholding a German prohibition on a laserdrome game on the basis of dignity, demonstrates that although conceptions of dignity may vary, they cannot undermine the core of EU law.⁸⁷ This logic mirrors Article 88 itself: diversity of national regulation is permissible only insofar as it grants full protection of dignity and fundamental rights.

The ECtHR's jurisprudence on Article 8 ECHR adds further guidance.⁸⁸ In *Barbulescu v. Romania*, the Court laid down criteria for evaluating workplace surveillance: prior notice, the scope and intrusiveness of monitoring, the existence of legitimate grounds, the possibility of less invasive alternatives, the impact on the employee, the presence of safeguards, and access to remedies.⁸⁹ These principles were extended to video surveillance in *Lopez Ribalda v. Spain*.⁹⁰ In *Surikov v. Ukraine*, a violation was found where an employer retained and shared mental health data beyond what was necessary for assessing promotion. The Court underlined that even where employers pursue legitimate interests, the collection of sensitive data must remain proportionate, lawful, and necessary in a democratic society.⁹¹

The question of consent has also been central in the Strasbourg Court's jurisprudence. In *Antović and Mirković v. Montenegro*, tacit consent to workplace video monitoring did not eliminate the intrusive character of surveillance,⁹² while in *M.S. v. Sweden*, the Court stressed that prior consent is not determinative in assessing whether private life has been interfered with.⁹³ National practice is far from

⁸⁴ H. ABRAHA, *A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace*, cit., 280.

⁸⁵ *Ivi*, 281.

⁸⁶ CJEU, Case C-34/21, *Bundesrepublik Deutschland v. JW*, Judgment, 30 June 2022, para 21.

⁸⁷ CJEU, Case C-36/02, *Omega Spielhallen – und Automatenaufstellungs – GmbH v. Oberbürgermeisterin der Bundesstadt Bonn*, Judgment, 14 October 2004, paras. 32-39.

⁸⁸ For a detailed analysis of the ECtHR's case-law on technological surveillance see A. SARTORI, *Il controllo tecnologico dei laboratori*, cit., 14 ff.

⁸⁹ ECtHR, *Bărbulescu v. Romania* [GC], Application no. 61496/08, Judgment, 5 September 2017, para. 121

⁹⁰ CtHR, *López Ribalda and Others v. Spain* [GC], Applications nos. 1874/13 and 8567/13, Judgment, 17 October 2019, para. 116.

⁹¹ ECtHR, *Surikov v. Ukraine*, Application no. 42788/06, Judgment, 26 January 2017, para. 94.

⁹² ECtHR, *Antović and Mirković v. Montenegro*, Application no. 70838/13, Judgment, 28 November 2017, para. 44.

⁹³ ECtHR, *M. S. v. Sweden*, Application no. 20837/92, Judgment, 27 August 1997, paras 31, 35.

uniform: for instance, while in Portugal, consent cannot justify processing where employers derive a benefit⁹⁴ in Italy, reliance on consent for sensitive employee data is discouraged through soft law guidance.⁹⁵ Such divergences expose the lack of harmonisation across the EU and question the reliability of consent as a safeguard in relationships defined by power imbalance.

4.2. The EU Medical Device Regulation 2017/745

While a detailed examination of brain-altering neurostimulation devices lies beyond the scope of this paper, it has been highlighted that the use of commercially available neurotechnologies, marketed to enhance concentration, induce relaxation, or improve cognitive performance, raises serious concerns for the protection of mental integrity.⁹⁶ By directly modulating neural activity, such devices move beyond observation or inference, entering the domain of active alteration of mental states. Yet, existing regulatory regimes for neurostimulation devices, especially those available to consumers, remain largely focused on health and safety, paying limited attention to the broader implications of unconsented interference with neural functioning.⁹⁷

The EU Medical Devices Regulation (MDR) 2017/745 already provides a legal framework to address some of these concerns. Binding across all Member States, the MDR includes provisions for so-called “non-medical purpose” devices, listed in Annex XVI, which are functionally analogous to medical devices but are marketed for general use, such as cognitive enhancement, improving stress levels or for wellness purposes. Neurostimulation devices are included in this category and are 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”.⁹⁸

The MDR requires manufacturers and other economic operators to comply with general safety and performance requirements set out in Annex I, including pre-market conformity assessments laid down in Annexes IX to XI. It is important to note that in December 2022, the European Commission issued *Common Specifications*⁹⁹ that further clarify obligations for manufacturers of non-medical, non-invasive neurostimulation devices, placed in class III, the highest risk category. Among these is the obligation to establish a comprehensive risk-management process to identify, minimise, or eliminate risks associated with neurostimulation technologies. These regulatory requirements, which have received critiques from

⁹⁴ Art 28(3) of Portuguese Law n° 58/2019 of August 8.

⁹⁵ Art 1.4.1.d of Italian Order 146/2019.

⁹⁶ For an in-depth consideration of the risks arising from brain-altering neurotechnologies see M. SOSA NAVARRO, S. DURA-BERNAL, *Human Rights Systems of Protection From Neurotechnologies*, cit.

⁹⁷ A. WEXLER, *A Pragmatic Analysis of the Regulation of Consumer Transcranial Direct Current Stimulation (TDCS) Devices in the United States*, cit., 672.

⁹⁸ 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, para. 173.

⁹⁹ 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 [2022] OJ L 311/57; Commission Implementing Regulation (EU) 2022/2347 of 1 December 2022 laying down rules for the application of Regulation (EU) 2017/745 of the European Parliament and of the Council as regards reclassification of groups of certain active products without an intended medical purpose [2022] OJ L 311/72.

the neuroscience research community,¹⁰⁰ gain heightened importance in occupational settings, where workers may be subjected to subtle or explicit pressure to adopt neurostimulation tools aimed at enhancing productivity or attention. However, their effective implementation may be hindered by the conceptual ambiguity found in the wording of the risks that manufacturers are required to identify and mitigate, such as “atypical or other idiosyncratic effects” (art. 3.3.h, Annex VII) and “neural and neurotoxicity risks” (art. 3.3. b, Annex VII), thereby limiting the overall effectiveness of the regulatory framework.

4.3. The AI Act and the regulation of emotion-inference technologies in the workplace

In May 2024, the European Union adopted the AI Act,¹⁰¹ the first comprehensive and binding framework on artificial intelligence worldwide. Designed to act as a regulatory benchmark, the Act establishes a stratified risk-based system and entrusts oversight to the newly established AI Office and AI Board, which are tasked with issuing further interpretative guidance. As is often the case with ambitious legislation, several notions remain undefined, leaving space for legal uncertainty that will ultimately require judicial clarification.

For employment contexts, Article 5(1)(f) is of particular importance. It prohibits the marketing, deployment, or use of AI systems designed to infer human emotions in the workplace and in educational settings. Under Article 3(39), an emotion-recognition system is defined as “an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data”. Recital 44 further elaborates that the term “emotion” covers a broad range of internal states, including happiness, sadness, anger, disgust, surprise, shame, contempt, satisfaction, and amusement. The prohibition is justified on the grounds of the structural imbalance of power in these environments and the resulting risks of discrimination and other harms. An exception exists for systems used strictly for medical or safety purposes, a carve-out that requires careful interpretation to avoid creating regulatory loopholes.

The Commission’s interpretative guidelines confirm that the prohibition applies to a wide array of practices in employment, including the use of brain-reading neurotechnologies such as EEG or neuroimaging to “monitor emotions or boredom of employees” or to implement “well-being applications for making workers happier”.¹⁰² The guidelines further recall, in line with Recital 18, that physical states such as pain and fatigue do not fall within the notion of “emotion”. Thus, while AI systems designed to detect driver fatigue and issue alerts are explicitly excluded, the broader exclusion of fatigue and pain is not confined to safety contexts. As a result, even in workplaces where fatigue is not a safety-critical factor, data of this kind would fall outside the scope of the prohibition set out in

¹⁰⁰ C. BUBLITZ, S. LIGTHART, *The new regulation of non-medical neurotechnologies in the European Union*, cit., 11-12.

¹⁰¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 445/1.

¹⁰² European Commission, *Guidelines on Prohibited AI Practices under the AI Act*, European Commission, 25 April 2025, p.71.

Article 5 and could therefore qualify as information that employers may collect and use in their decision-making processes, giving rise to discrimination risks based on neural-data inferences.¹⁰³

The guidelines also clarify the breadth of the “workplace” concept, which should be understood as covering “any specific physical or virtual space where natural persons engage in tasks and responsibilities” assigned by an employer or organisation. This extends to employees, contractors, volunteers, and the self-employed. Significantly, Article 5(1)(f) also applies during recruitment processes, given both the imbalance of power and the intrusive nature of emotion recognition at the hiring stage.¹⁰⁴

Moreover, Article 6(2) and Annex III classify several workplace-related AI systems (such as those used for recruitment, promotion, dismissal, or performance monitoring) as “high-risk”, subject to stringent compliance requirements including risk management, human oversight, record-keeping, and public registration. Non-compliance can result in fines of up to €35 million or 7% of global annual turnover. Although the AI Act does not expressly regulate neurotechnologies, scholars such as Bublitz and Molnár-Gábor argue that its scope is wide enough to include technologies capable of inferring emotions or intentions from brain activity.¹⁰⁵ Recital 57 strengthens this reading by establishing a conceptual link to the GDPR (and therefore to the protection of personal data, including neural data) and underscoring the need for consistency in fundamental rights protections.

From the perspective of mental privacy and freedom of thought, two elements of the AI Act will be particularly decisive for workplace applications. First, the categorical exclusion of fatigue monitoring from the definition of emotion under Article 5(1)(f) risks leaving significant aspects of workers’ neural data (which, as this paper has discussed, is critical for shielding against exploitative, productivity-driven neurosurveillance) outside the scope of protection. Second, the medical and safety exception to the prohibition on emotion recognition may invite expansive interpretations by employers, thereby weakening the ban’s protective function. Together, these interpretive challenges will play a central role in determining whether the AI Act can provide meaningful safeguards for workers’ mental privacy in practice.

5. Conclusive remarks

This paper has argued that the proliferation of neurotechnologies in the workplace raises a complex set of challenges for international law. A conceptual distinction between brain-reading devices, which collect and process neural data and engage primarily the rights to privacy and freedom of thought, and brain-altering devices, which directly modulate neural activity and thus implicate mental integrity, helps to illuminate distinct risk profiles. Yet the boundary is porous: intensive neuromonitoring can foster self-censorship and erode autonomy, while brain-altering techniques may suppress thought formation itself.

¹⁰³ *Ivi*, 79 and 84.

¹⁰⁴ *Ivi*, 81.

¹⁰⁵ C. BUBLITZ *et al.*, *Implications of the Novel EU AI Act for Neurotechnologies*, in *Neuron* 112, 18, 2024, 3014-3015.

In both cases, the foundational value of human dignity emerges as the decisive normative anchor, transcending debates over which single rights provides the most appropriate legal fit.¹⁰⁶

Against this normative backdrop, the analysis has mapped an evolving but fragmented regulatory landscape. At the international level, Article 17 ICCPR, as elaborated by the Special Rapporteur on privacy, provides a principled framework for personal data processing that can be applied to neural data. In Europe, three instruments are of particular relevance: the GDPR, whose Article 88 delegates workplace-specific rules to Member States, producing uneven reliance on consent in an inherently imbalanced relationship; the MDR, which regulates non-medical neurostimulation devices but excludes brain-reading technologies, leaving them subject only to horizontal product-safety law; and the AI Act, which prohibits emotion-recognition systems in employment settings yet carves out medical and safety exceptions and excludes fatigue and pain from its scope. Considered together, these frameworks create overlapping protections but also inconsistencies and loopholes, exposing workers to protection gaps while at the same time generating regulatory uncertainty for innovation.

The precautionary principle, which has crystallised into customary international law, offers a valuable compass for navigating such uncertainty. Applied to neurotechnologies, it legitimises precautionary action in the face of scientific indeterminacy and underscores the need for a normative definition of ‘thought’.

Soft law also plays a critical role in bridging regulatory gaps. The ILO’s Code of Practice on Workers’ Personal Data and the Council of Europe’s Recommendation CM/Rec (2015)5, though formally non-binding, have shaped national laws, workplace policies and collective agreements with regard to this matter. Their practical influence illustrates why scholars regard soft law as an appropriate modality in contentious and fragmented fields such as workers’ privacy, avoiding the paralysis of treaty negotiations.¹⁰⁷ Some even argue that sustained reliance on these instruments may contribute to the gradual crystallisation of customary norms.¹⁰⁸

The European Union’s approach further demonstrates the potential benefits of anticipatory regulation. By adopting the AI Act pre-emptively, the EU has sought to avoid the regulatory failures that allowed ungoverned digital platforms to entrench socially harmful practices. Although not free of interpretive ambiguities, this anticipatory model provides a useful template for addressing the disruptive potential of workplace neurotechnologies before harmful practices become entrenched.

In conclusion, the governance of workplace neurotechnologies requires an approach that is principled, precautionary, and anticipatory. International law must integrate the rights to privacy, freedom of thought, bodily and mental integrity, and non-discrimination into a coherent framework responsive to both neurosurveillance and neuromodulation. This entails interpretive development of existing instruments, reliance on soft-law guidance, and recourse to the precautionary principle to address uncertainty. Above all, regulation must ensure that technological innovation does not come at the

¹⁰⁶ F. D’AGOSTINO, *Bioetica e dignità dell’essere umano*, in C.M. MAZZONI (ed.), *Un quadro europeo per la bioetica*, Firenze, 1998, 153; G. PECES BARBA, *Dignidad humana*, in J.J. TAMAYO (ed.), *10 palabras clave sobre derechos humanos*, Navarra, 2005, 55.

¹⁰⁷ S. SIMITIS, *Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees’ Personal Data*, in *ELJ*, 1999, 50-51.

¹⁰⁸ A. SITZIA, *Lavoro e privacy: adempimenti obbligatori e procedure*, 2nd edition, Milan, 2012, 128-129.

expense of human dignity, and that the workplace remains a space for human flourishing rather than one of mental surveillance and cognitive exploitation.

Finally, legal frameworks must address not only the rights of individual workers but also the wider societal consequences of normalising continuous neuromonitoring, including its effects on deliberation, dissent, and creativity. Embedding multistakeholder and anticipatory governance upstream is essential to align regulatory standards with social values before technological dependence takes root.

