REGULATORY CHALLENGES FOR THE PROTECTION OF NEURODATA AND THE PROCESSING OF PERSONAL DATA THROUGH NEUROTECHNOLOGIES IN NON-MEDICAL FIELD

English translation - Only the Spanish version is deemed authentic

v. June 2026

INDEX

I. INTRODUCTION

Techniques for observing and manipulating human thought and behaviour, historically linked to disciplines such as social psychology, behavioural psychology, and social engineering, have been employed for various purposes, such as education, medicine, persuasion, propaganda, mind control, and, more recently, marketing. Over time, these practices have resorted to communication methods, coercive techniques, pharmacological interventions, and even invasive procedures such as psychosurgery.

However, recent years have witnessed significant advances in techniques that allow the direct recording of the static and dynamic characteristics of the human brain and nervous system using automated technologies. Likewise, these systems facilitate the digital processing of this information in order to infer data related to human thought, even making it possible to modify both the individual's thinking and behaviour through direct interaction on their neurological signals. In addition, these techniques are increasingly available for application in various fields and sectors that are beyond the ones carried out under the supervision of health professionals or within the context of medical treatments.

Without diminishing the importance of its use in the public health sector, regulated by specific sectoral legislation, it is imperative to analyse the particularity of its use beyond this context. Currently, there is a significant increase in the use of neurotechnologies in consumer products and services, whose application transcends medical, healthcare or public health purposes. The use of these technologies is extending to areas such as education, the work environment, entertainment or advertising, among others. It is also worth noting the increasing accessibility of these tools for non-specialist users. According to the report published by the Office of Science and Technology of the Congress of Deputies in Spain "*Advances in neuroscience: applications and ethical implications: Breakthroughs in neurotechnology*", at the end of 2023, 27% of companies in the sector were already focused on non-medical developments and up to 54% of scientific studies with non-invasive devices for recording activity focused on cognitive monitoring, communication, and control of external devices[1].

The increasing use of neurotechnology innovations in these fields requires an exhaustive analysis to guarantee the protection of the fundamental rights of the individual, as well as aspects related to consumer affairs, market sustainability, industrial property, civil liability, cybersecurity and the promotion of research and technological progress. In this regard, States must establish regulatory frameworks that encourage the responsible development of products and services based in neurotechnologies, aligned with human rights principles, and that guarantee the minimum impact on human beings, as well as access to effective remedies for people affected by them. According to the UNESCO report, "*Neurotecnologías y derechos humanos en América Latina y el Caribe: desafíos y propuestas de política pública*" [Neurotechnologies and Human Rights in Latin

[1] https://oficinac.es/sites/default/files/informes/OFICINAC_Neurociencia-aplicaciones-implicaciones-eticas__20231214_web.pdf

America and the Caribbean: Challenges and Public Policy Proposals], *"the greatest challenge of the technological society in which we live is to know how to identify in time the public policies that allow us to balance the advantages and risks of the new technological instruments that we have and that, above all, they preserve the dignity and freedom of people*[2]*"*.

This document aims to serve as a guide for the development of legal regulatory instruments, or other related ones (standards, certifications, technical norms, codes of conduct and others), both in the hands of personal data protection authorities (such as recommendations, guidelines, guides, resolutions or circulars) and by other bodies within the scope of their respective competences, especially when neurotechnologies are used in the framework of personal data processing.

In order to facilitate the development of appropriate legal developments, this document collects and analyses various challenges that, due to their nature and relevance, could be solved in a specific way in one or more regulatory instruments. The identification of these elements is intended to serve as a reference for both the legislator and the competent authorities, making it possible to address the challenges posed by the processing of neurodata in relation to the right to the protection of personal data and the impact of such processing on other fundamental rights and freedoms.

In addition, a number of actionable proposals and regulatory alternatives are included in the document, which offer various options for the evolution or improvement of existing legal frameworks, thus providing practical and flexible guidance that contributes to an adequate protection of fundamental rights in a harmonized manner in different jurisdictions. In this sense, "*regulatory innovation*" initiatives can be carried out, for aspects that require the adaptation of existing legislation or new standards because the current framework is insufficient, or it is susceptible to different interpretations, for those aspects where the current standards are applicable but their implementation in the context of neuroprocessing (neurodata processing) requires specific guidelines.

This analysis aims to support innovation in the field of neurotechnologies, since clear legal frameworks not only encourage responsible innovation by reducing uncertainty for organisations —thus facilitating investment in R&D—, but are also enriched by technological advances. Emerging technologies, such as neurotechnologies and Artificial Intelligence, challenge regulatory frameworks designed for earlier contexts, which necessitate their constant review and updating. This process encompasses not only legislative adaptation, but also the evolution of standards, certifications, technical norms and codes of conduct, which translate legal principles into practical requirements and good practices.

In this work is considered the work carried out in different forums, in particular in the Committee of Convention 108 of the Council of Europe, formally initiated in March 2024, on the protection of personal data in the context of neurosciences. The topics covered in this document include the intersection with other fundamental rights and regulatory

[2] https://unesdoc.unesco.org/ark:/48223/pf0000387079

frameworks, as well as additional aspects, leaving out the scope the field of health and public health research regulated by specific sectoral regulations.

II. DEFINITIONS

One of the main challenges in the field of neurotechnology lies in the absence of universally accepted definitions and the inclusion into regulatory instruments, such as *neurodata*, *neurotechnology*, *neuroprocessing (*as a process outside the medical field*)* and *neurorights*.

This conceptual deficiency leads to a lack of precision and clarity, which, in turn, leads to misunderstandings, unproductive debates, and ultimately an inadequate delineation of the related legal and ethical issues. The absence of a unified terminological framework makes it difficult to adopt effective and coherent regulations, which are essential to ensure the protection of fundamental rights in this emerging area[3].

A. DEFINITIONS OF NEURODATA

According to the Organisation for Economic Co-operation and Development (OECD) in its Recommendation on Responsible Innovation in Neurotechnology, neurodata is "*the information gathered from the brain and/or from the nervous system*",[4] including anatomical, physiological and functional data collected through neurotechnologies such as Electroencephalography (EEG), Functional Magnetic Resonance Imaging (fMRI), neural implants or brain-computer interfaces. The European Data Protection Supervisor (EDPS) and the Spanish Data Protection Agency (AEPD), in their TechDispatch on Neurodata[5], as well as the United Nations Educational, Scientific and Cultural Organisation (UNESCO) in different publications, adopt this definition from the OECD.

The OECD also defines brain data as "*data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states*". This same definition was used in the Resolution on the Principles Relating to the Processing of Personal Information in Neuroscience and Neurotechnology[6] by the Global Privacy Assembly (GPA) as a definition of neurodata.

For its part, in the report "*Foundations and principles for the regulation of neurotechnologies and the processing of neurodata from the right to privacy*" by the Special Rapporteur on the right to privacy, Ana Brian Nougrères, of the United Nations General Assembly[7], neurodata is defined as the information obtained from a person's central and peripheral nervous system through the use of neurotechnologies.

---

[3] George, A. S. (2024). Protecting Brain Privacy in the Age of Neurotechnology: Policy Responses and Remaining Challenges. *Partners Universal Innovative Research Publication*, *2*(5), 18-33

[4] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457#supportDocuments

[5] https://www.aepd.es/guias/neurodatos-aepd-edps.pdf

[6] https://globalprivacyassembly.com/wp-content/uploads/2024/11/Resolution-on-Neurotechnologies.pdf

[7] https://www.ohchr.org/en/documents/thematic-reports/ahrc5858-foundations-and-principles-regulation-neurotechnologies-and

From the above definitions, it can be concluded that neurodata refers to information obtained directly from the brain and nervous system, whose processing can be carried out using both digital and non-digital technologies.

In its technological dimension, neurodata is collected using specialized devices, such as brain-computer interfaces (BCIs), which pick up signals both invasively and non-invasively[8]. This information allows decoding patterns of brain activity related to cognitive functions, emotions or health states, thus being closely integrated with digital systems for interpretation and use.

On the other hand, non-digital collection and analysis of information from the brain and nervous system may involve manual or analogue techniques. These could include eye tracking, video oculography, typing dynamics, voice recognition and analysis, gait analysis, skin conductance, heart rate variability, observation of sleep movements, blood pressure measurement, facial emotion recognition systems, or microbiome[9] measurements. In any case, its relationship with digital technologies continues to be fundamental, since they are enabling tools for the storage, processing, and complex analysis of neurodata, allowing countless applications beyond medical and scientific fields, which require the integration of such information into sophisticated digital systems, increasingly including Artificial Intelligence (AI).

Sometimes the concepts of first, second, and third-order neurodata are used to consider different nuances present in the different definitions[10]. First-order data are directly recorded or measured, without intermediate processing. They are the raw data form and closest to the biological source. Second-order data are data derived or processed from first-order neurodata, using statistical analysis, machine learning, or other data science techniques. They represent an intermediate interpretation, for example, patterns of brain connectivity, biomarkers extracted from signals such as an index of mental fatigue, neuronal decoding (for example, reconstruction of images seen by the subject), etc. Finally, third-order data are inferred, predictive or contextual data, generated by manual and analogue methods or techniques mentioned above, after a digital processing, and enriched even with other sources of information (other biological measurements or records, medical records, social networks). For example, neuropsychological profiles or behavioural predictions.

It should be noted that, from the regulatory point of view, it is common that terms already defined and validated require revision, expansion or specification to adapt them to new scenarios, technological advances or social challenges. This does not imply that initial definitions are not useful, but rather that the context in which they are applied makes it necessary to specify the scope, to adapt them to innovations, and to harmonize with among different legal frameworks, to ensure legal certainty or to consider multidisciplinary approaches.

---

[8] Wolpaw, J. R. (2007, October). Brain-computer interfaces (BCIs) for communication and control. In *Proceedings of the 9th international ACM SIGACCESS conference on Computers and accessibility* (pp. 1-2)

[9] UNESCO (2025). Recommendation on the Ethics of Neurotechnology. https://www.unesco.org/en/legal-affairs/recommendation-ethics-neurotechnology

[10] ICO (2023). ICO tech futures: neurotechnology. https://ico.org.uk/media2/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf

Terms such as neural data, brain data or mental data can be found in different standards and regulations. They are aimed to take into account the different types of neurodata and information derived from the anatomy or physiology of the central and peripheral nervous system, records of mental and brain activity, including genetic data, neuroimaging and patterns of neural activity, data obtained by direct or indirect technologies (invasive or non-invasive), such as EEG, fMRI, or brain-machine interfaces. The term neurodata is usually considered more appropriate, since, by using the prefix "*neuro*" (related to the brain and nervous system) it is usually interpreted in a broader way, and not only in relation to the information generated by the activity of neurons, the brain or the mind (a concept difficult to comprise in a universal definition) exclusively. In addition, the term neurodata was used in the "*Declaración sobre Neurodatos de la Red Iberoamericana de Protección de Datos*" [Declaration on Neurodata of the Ibero-American Data Protection Network] approved in 2023[11].

Compromise proposal:

It is suggested to use the term neurodata in general, as opposed to other alternatives such as neural data, brain data or mental data.

The proposed definition for these neurodata, when a development with greater depth or specificity than that of the aforementioned proposals is needed, would be "*personal data obtained from a*[12] *specific technical processing (directly, indirectly or inferred), in relation to the anatomical, physiological, functional or behavioural characteristics of a natural person relating to brain activity and their nervous system*".

B. DEFINITIONS OF NEUROTECHNOLOGY

The Statement on Neurodata of the Ibero-American Data Protection Network defines neurotechnology as "*any development that allows monitoring or modifying the nervous system and brain functioning*."

The OECD defines neurotechnology as: *"devices and procedures used to access, capture, monitor, transmit, process, investigate, assess and/or manipulate the structure, activity and function of the neural systems of natural persons".* This same definition was used in the Resolution on the principles relating to the processing of personal information in neuroscience and neurotechnology by the GPA[13].

[11] https://www.redipd.org/documento/declaracion-neurodatos-ripd.pdf

[12] This term refers exclusively to the handling of information relating to identified or identifiable natural persons (*processing*) and does not include other meanings of "processing" such as medical, chemical, or industrial processes. In other words, processing is any operation or set of operations carried out on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of access, comparison or combination, restriction, erasure or destruction.

[13] https://globalprivacyassembly.com/wp-content/uploads/2024/11/Resolution-on-Neurotechnologies.pdf

A report by the UN Scientific Advisory Board[14] describes neurotechnology as: "*an umbrella term referring to any technology that records or modifies the neurons in the human nervous system. Neurotechnology performs at least one of three functions: neuroimaging (monitoring brain structure and function), neuromodulation (influencing brain functions), and direct brain-computer interfaces*".

UNESCO, in its document on the Ethics of Neurotechnology,[15] defines neurotechnology as: "*devices, systems and procedures – encompassing both hardware and software – that directly measure, access, monitor, analyse, predict or modulate the nervous system to understand, influence, restore or anticipate its structure, activity and function. Neurotechnology combines elements of neuroscience, engineering, material science and computing, among others*".

Similarly, in the report entitled "*Foundations and principles for the regulation of neurotechnologies and the processing of neurodata from the perspective of the right to privacy* " by the Special Rapporteur on the right to privacy, of the United Nations General Assembly, neurotechnology is defined as *"any technology that records, interprets, alters or interferes with brain activity using any optical, electronic, magnetic or nanotechnology technique that allows understanding of brain processes such as vision, sensations, perceptions, behaviour, ideas, memory, emotions, consciousness, imagination, decisions or the mind"*.

Invasive neurotechnologies are the techniques that record or alter brain activity from inside the brain, which involves intrusive medical procedures in the human body; and non-invasive neurotechnologies are techniques that record brain activity or alter brain activity from outside the skull.

Compromise proposal:

The proposed definition for neurotechnology is "*devices and procedures used to access, monitor, investigate, evaluate, manipulate, and/or emulate the anatomy, physiology, function, and behaviour of the brain and/or nervous system of people*."

C. OTHER DEFINITIONS

There are other definitions that could be important to establish within the framework of other regulatory areas, beyond it could be considered to be taking into account in the regulation of personal data.

A clear case, as already established in the 2024 declaration of the RIPD, is the discussion at the international level whether it is necessary to lay down new rights in

[14] https://www.un.org/scientific-advisory-board/sites/default/files/2026-04/1_neurotechnology_refined.pdf
[15] https://unesdoc.unesco.org/ark:/48223/pf0000394866

relation to neurodata and neurotechnologies, that is, neurorights[16], or whether the scope of existing rights should be reinterpreted in the light of technological advances in the field[17].

In particular, in doctrine, proposals have been developed to lay down five neurorights:

- Personal identity: It refers to limiting any neurotechnology that allows altering people's sense of "*self*" and preventing personal identity from being lost with connection to external digital networks.
- Cognitive freedom: It refers to preserving people's ability to make decisions freely and autonomously, that is, without any manipulation mediated by neurotechnologies.
- Mental privacy: It seeks to protect individuals from the use of data obtained during the measurement of their brain activity without their consent and expressly prohibits any commercial transaction with that data.
- Equitable access: It seeks to regulate the application of neurotechnologies to increase brain capacities, so that they are not only within the reach of a few and generate inequality in society.
- Protection against bias: It prevents people from being discriminated against by any factor, such as a mere thought, that can be arise using neurotechnologies.

In the aforementioned statement, it was established that those who offer products, services and applications based on neurodata must be aware of the obligation to comply with the rights and obligations in relation to the processing of neurodata in the terms laid down in the regulations on the protection of personal data, guaranteeing compliance by the data protection authorities supervision and subject to an executive enforcement procedures.

The term "*neurorights*" understood as the ethical, legal, social, or natural principles of freedom or self-determination related to a person's brain and mental domain; that is, the fundamental legal standards for the protection and preservation of the human brain and mind[18] could be defined as follows:

Compromise proposal:

The proposed definition for neurorights is "*a category of human rights and fundamental rights that seek to promote, guarantee, preserve and protect the dignity and freedom of persons in the context of neurotechnologies*".

[16] Yuste, R., Genser, J., & Herrmann, S. (2021). It's time for neuro-rights. *Horizons*, *18*, 154-164

[17] Andorno, R. (2025). Analysis of the existing European human rights framework concerning the human rights issues raised by neurotechnologies and their applications. Council of Europe. https://rm.coe.int/steering-committee-for-human-rights-in-the-fields-of-biomedicine-and-h/4880290460

[18] Ienca, M. (2021). On neurorights. *Frontiers in Human Neuroscience*, *15*, 701258

On the other hand, the deployment of products and services that involve the use of neurotechnologies, collection or processing of neurodata of different kinds, operations that involve stimulation or modulation may involve complex processes or processing that involve numerous techniques. The regulation of these processes and processing aimed at non-health-regulated or scientific research areas, as well as the systems used in them, may need to expand the set of definitions.

For example, some processing advertised as neuroaesthetics combine reading brain signals, enrichment with other sources (behavioural or other physiological data), inferences using AI, and neurostimulation using nervous system chemicals.

It should be noted that data processing is any operation or set of operations carried out on personal data, whether automated or manually. In the other hand, a neurotechnology system in this context is a part of the infrastructure (physical or digital) that makes the processing possible, among other systems. In other words, we are in a scenario of a set of tools, processes and people, including neurotechnologies, that allows processing personal data. Therefore, it is very important to identify which regulations apply to neuroprocessing and which regulations apply to neurotechnologies or the systems that contain them.

Compromise proposal:

The proposed definition for neuroprocessing is "*processing of personal data whose purpose is to evaluate, access, infer, exploit, manipulate or modify the anatomy, physiology, function or behaviour of the brain or nervous system, and therefore of a natural person, both directly and indirectly*".

III. CONSIDERATION AS PERSONAL DATA

Personal data is any information about an identified or identifiable natural person, either directly or indirectly. For example, the data "*blood type X*" by itself does not constitute personal data, but when it is associated with an identifier such as a name or any information that allows the identification of a person (or singling out within a group), it becomes considered personal data.

Therefore, the status of neurodata in terms of its nature as personal data depends not only on its intrinsic content, but also on its context and the potential to link it to an identifiable person in accordance with current personal data protection regulations. Any neurodata, of any kind, about an identified or identifiable natural person is personal data.

In the event that an isolated neurodata is analysed independently, it is essential to evaluate whether this data could function as an identifier or if it can act as a pseudo-identifier when used in combination with other data that allow the individual's singularization. The answer is that the information of the nervous system and the brain

is unique and personal[19], a hallmark as unmistakable as the fingerprint. All this, without prejudice to the fact that, as in any other type of identifier, anonymization, obfuscation, aggregation techniques, etc., could be used.

Compromise proposal:

Neurodata can be concluded to be personal data to the extent that it is linked to an identified or identifiable person directly or indirectly and, unless proven otherwise in a specific context, could act as identifiers or pseudo-identifiers.

IV. SPECIAL PROTECTION FOR NEURODATA

Most regulations relating to the protection of personal data do not explicitly refer to neurodata. Consequently, these could be excluded from the enhanced or special protection regime that applies to certain categories of data contemplated in them, since they cannot always be considered, in all contexts of use, as biometric data for identification or authentication, and/or health data, which do usually benefit from such extended protection.

The starting point might be to consider neurodata as a particular special category of personal data distinct from other special categories of personal data, bearing in mind the relation that certain neurodata could have with other categories of data (such as biometric or health).

Neurodata are obtained through specific technical processing, related to the physical, physiological, function or behavioural characteristics of a natural person. This is defined as biometric information from a technical point of view (ISO/IEC 24745 *Biometric information protection*). However, there is no evidence that in all cases neurodata allows or confirms the unique identification of such a person, therefore, in some jurisdictions (e.g. the GDPR in its art. 4.14), it would not fall within the definition of biometric data. If so, and in such framework, could be considered a special category of personal data.

It is important to note that the aforementioned report by the United Nations Special Rapporteur on the right to privacy defines sensitive personal data as information relating to a data subject that affects their privacy or whose improper use may lead to discrimination, such as data that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of trade unions and social or human rights organisations, or that promote the interests of any political party or guarantee the rights and guarantees of opposition political parties, as well as data relating to health or sex life, biometric data and neurodata.

[19] Hon. Supreme Court of Chile, Rol 105065/2023 entitled GIRARDI/EMOTIV. INC: https://www.doe.cl/alerta/11082023/20230811001

The report further states that neurodata has been consolidated as a special category of personal data that requires ethical, professional and diligent processing to guarantee the protection of people and safeguard their human dignity. This data, generated by the brain and nervous system, has unique characteristics that set it apart from any other personal information. In addition, neurodata not only makes it possible to identify a person but also offers an unprecedented depth in understanding their individuality. Neurodata is characterized by having a unique and exceptional sensitivity, has a direct and deep correlation with cognitive and affective states, and reflects the personal experiences and emotions of human beings.

Neurodata may reveal other special categories, such as health information, but this is not unique to neurodata. Health information may be disclosed based on genetic data, biometrics, or even by the combination of personal data not *per se* considered sensitive. On the other hand, health data could reveal information about sexual orientation, for example.

From the above, both the United Nations and the GPA and the RIPD itself[20], have pointed out that, given the sensitive nature of neurodata, high-level protections should be applied to its processing, like other special categories of personal data. This type of conclusion is also reflected in the OAS Declaration of Inter-American Principles on Neurosciences, Neurotechnologies, and Human Rights[21].

Compromise proposal

Neurodata should be regarded as a special category of personal data due to its highly sensitive nature, whose processing can have a high impact on the rights and freedoms of natural persons. In this sense, their processing must be subject to a regime of special protection equivalent to that applied to health, genetic, religious or philosophical beliefs and convictions, ethnic origin or others.

If neurodata is considered as a new special category of personal data, it would be necessary to study the specific cases in which its processing could be carried out, as long as the same provisions indicated in the personal data protection regulations are complied with for sensitive personal data that are currently recognized, such as the protection of vital interests, public interest, or consent. In the latter case, the challenge of ensuring that consent is truly specific, free and informed, as will be discussed later in this document, would have to be faced.

[20] RIPD (2024) Declaration of the Ibero-American Data Protection Network on neurotechnologies and neurodata within the framework of personal data protection regulations.

[21] https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf

V. ABSOLUTE BANS

The rapid development of AI and neurotechnologies increases the risk of sophisticated subliminal manipulation and their ability to effectively influence human behaviour subconsciously. The combination of AI with brain-machine interfaces means that advanced techniques such as dream hacking and brain surveillance are seen as possible in the not-too-distant future. For this reason, it could be considered to include absolute prohibitions of certain types of neuroprocessing in the legislation on the matter (data protection or otherwise). There is a clear parallel in how absolute prohibitions have been established for certain genetic techniques with the aim of protecting human dignity, avoiding serious risks to society, and preventing perverse or dangerous uses such as genetic engineering for eugenic purposes, the creation of biological weapons or human [22]cloning. These prohibitions seek to prevent arbitrary modifications of the human genome, especially in the germ line, since they would affect not only the individual but their descendants and humanity as a whole, and could undermine fundamental principles such as equality and genetic identity. In addition, such prohibitions respond to the need to avoid the instrumentalization of human beings and to preserve human rights.

Consideration should be given to introducing specific, "*technical*" or functional exceptions in relation to the rights of individuals in a broader framework of data protection, for which, taking as a reference the Report of the Special Rapporteur on the right to privacy, entitled "*Elements for the development of a model law on neurotechnologies and the processing of neurodata from the perspective of the right to privacy* "[23], it is envisaged that all manipulation of the brain or neural information should be prohibited, except when it is carried out for the following purposes:

- Health protection.
- Diagnosis, treatment, rehabilitation or palliation of diseases, within the framework of the fundamental right to health.
- Scientific research in the fields of biology, psychology and medicine, aimed at alleviating suffering or improving health, provided that it is carried out in accordance with the applicable ethical and legal standards.

In addition, it contemplates that an exclusively therapeutic application of the increase in cognitive abilities must be carried out, since neurotechnologies must be used for medical purposes such as health promotion, prevention, diagnosis, treatment, rehabilitation and palliative care of diseases. That is why it is crucial to prevent cognitively enhanced individuals from being created, with artificially enhanced brains, as opposed to non-enhanced individuals, with their natural brains. Therefore, great caution should be exercised in the use of neurotechnologies to increase or improve human cognitive abilities or alter human nature beyond therapeutic or health application or for other uses not related to medicine.

---

[22] Annas, G. J., Andrews, L. B., & Isasi, R. M. (2002). Protecting the endangered human: toward an international treaty prohibiting cloning and inheritable alterations. *American journal of law & medicine*, *28*(2-3), 151-178

[23] https://docs.un.org/en/A/80/283

Bans could be interpreted as a limitation on innovation, but also as a guarantee for a sustainable and acceptable development of technological advances. Limitations or even prohibitions have been established on the marketing of radioactive material in educational products[24] or more recently for domestic or commercial use or for "biohacking" of genetic material editing kits using CRISPR technologies and that allowed the uncontrolled editing of one's own genome, manipulation of embryos by non-medical professionals[25] or the risk of uncontrolled creation of new viruses.

Therefore, it must be considered that a fundamental aspect is to guarantee that the integrity and neurocognitive privacy of each person are not violated or manipulated in a way that puts their well-being at risk. Likewise, any attempt to alter freedom of thought and conscience, or to generate dependence on a third party, must be prohibited. In other words, it is unacceptable to allow brain manipulation that turns human beings into mere puppets under the control of others.

With this idea of avoiding non-therapeutic uses that alter the human brain for different purposes, prohibitions could be established, regardless of the special category classification that neurodata could receive:

- By type of information inferred: unconscious thought, conscious thought, beliefs, emotions, etc.
- By type of neurotechnology used: neurostimulation or neuromodulation in non-clinical cases or research, Brain to Brain interfaces, resurrection technologies, etc.
- For explicit or implicit purposes: neuroweapons, manipulation of behaviour or thought without consent, mass surveillance of brain activity.
- Prohibitions could be pointed out with different criteria:
    - By purpose or use case: invasive neurosurveillance in the workplace or education; neurotechnological doping in sport; obtaining evidence in judicial proceedings.
    - By domain: education, entertainment, non-criminal justice, administrative procedures, etc.
    - By category of stakeholders: prohibition of the use of commercial neurotechnology in children and adolescents until its safety is scientifically demonstrated.
    - It could be a combination of the above: For example, in advertising and marketing, the use of neurodata for behavioural advertising without express consent should be prohibited, following the California (California Consumer Privacy Act, CCPA[26]) model.

Compromise proposal

It is necessary, in each jurisdiction, to lay down absolute prohibitions of certain types of neuroprocessing that are not sufficiently covered by the current regulations,

[24] https://thebulletin.org/virtual-tour/worlds-most-dangerous-toy-radioactive-atomic-energy-lab-kit-with-uranium-1950/
[25] https://www.thehastingscenter.org/crispr-china-parents-give-consent/
[26] https://oag.ca.gov/privacy/ccpa

regardless of the consideration that neurodata could have the protection of personal data regulation. For example, it could be considered to prohibit:

- Subliminal, manipulative, deceptive neuroprocessing or those that aim to alter the behaviour of people or groups for purposes other than medical purposes (the aforementioned health protection).
- Neuroprocessing that aims to exploit the vulnerabilities of individuals or groups.
- Neuroprocessing to profile, evaluate, categorise or qualify people or groups for purposes other than doctors.
- Neuroprocessing aimed at evaluating, evidencing or predicting a possible crime.
- Neuroprocessing to infer emotions in the workplace or education.
- Neuroprocessing in children and adolescents, as well as in people belonging to other groups considered vulnerable (for example, with mental or psychosocial disabilities), for purposes other than medical ones.

VI. LIMITATIONS ON THE LEGAL BASES FOR PROCESSING

Currently, processing activities using neurodata, or implemented using neurotechnologies, do not have a singular categorisation, nor there are any distinctions made in relation to the applicability of any of the possible legal bases or, where appropriate, the exceptions applicable to the processing of such data when it is not based on consent.

The case of consent, due to its specificity, is contemplated in the following section. On the other hand, specific limitations could be contemplated to the legal bases, or for the exceptions, that enable the processing of neurodata, given its sensitive characteristics and the high impact on the individual through the approach of different strategies.

Compromise proposal

It is proposed to consider:

- Restrict the applicability of "*legitimate interest*" only to public, biomedical, or clinically supervised research purposes, excluding its use for commercial, digital services, advertising, or personalization purposes.
- Restrict the applicability of "*performance of a contract*" exclusively to strictly necessary processing in health services or clinical neurotechnology, and not to other services (wellness, entertainment, work, productivity or neuromarketing, etc.). This would prevent platforms, services or *apps* from incorporating neurodata processing as an ordinary contractual condition, so that, for example, services cannot be accessed if neuroprocessing is not carried out.
- Restrict the applicability of "*consent*" (see next section).
- Limit the compatibility of purposes for the further use of neurodata. It could be conditioned to a relevant, justified public interest subject to independent review.
- Limit the use of the public interest, except for strictly necessary processing in the field of public health.

VII. CONDITIONS FOR VALID CONSENT

Although it is not exclusive to neurodata processing, it should be borne in mind that consent as a lawful basis for the processing of high-risk personal data presents significant challenges, especially when there is an imbalance of power and information asymmetry between the data subject and the data controller. This is established in the working document "*Emerging Neurotechnologies and data protection*"[27] prepared by the so-called Berlin Group (International Working Group on Data Protection in Technology). In these cases, consent can hardly be considered free because the data subject may be unaware of the processing that will be carried out on their data, feel pressured or fear negative consequences for refusing. This is common in relationships where there is dependence or inequality, such as in employment, education, health or relation with public authorities, common domains of application for neurotechnologies. It is also important to bear in mind the difficulty for an average citizen to understand how neurotechnologies work and what the real impact on their rights and freedoms may be (information asymmetry).

As mentioned above, limiting this legal basis for the processing of personal data could be considered, since it is very difficult to obtain valid consent[28] (free, informed, express,

[27] https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20250515-WP-Neurotechnologies.pdf?__blob=publicationFile&v=2

[28] This term refers to the freely given, specific, informed and unambiguous expression of will by which the data subject, by means of a statement or a clear affirmative action (such as ticking a box or signing a document), agrees to the processing of his or her personal data for one or more specific purposes. It does not cover other types of consents, such as those required in medical, legal or contractual contexts unrelated to the protection of personal data.

specific and unequivocal, and always with a lawful and specific purpose) in most use cases.

Consent raises problems of validity, not only because it could be not freely given, but also because of the difficulty of making it specific and informed, given the uncertainties generated by neurotechnologies, specifically with regard to their ability to infer emotions, memories, thoughts, etc., or to "*write*" in the brain (neurostimulation and neuromodulation). Consent should not constitute a lawful basis where the controller cannot determine in advance, with reasonable precision, what inferences will be drawn from the processing of neurodata.

In addition, the question arises as to the validity of whether consent can be truly free after a neurostimulation or neuromodulation operation that has modified the subject's personality or appetite for risk. The ability of neurotechnologies to influence the subject's behaviour should be taken into account when assessing consent as a possible lawful basis.

Compromise proposal

Consent may not be a lawful basis for any neuroprocessing that:

1) produces neurostimulation or neuromodulation (i.e., with writing operations in the brain using neurotechnology)

2) has the capacity to alter or manipulate the conduct or behaviour of the data subject.

Such consent would never be valid given the ability of neuroprocessing to influence the decisions of the data subject.

VIII. TRANSPARENCY

The Convention 108+ Committee in its report " *the privacy and data protection implication of the use of neurotechnology and neural data from the perspective of Convention 108+*"[29] contemplates guidelines on the use of neurotechnology and neurodata, through the inclusion of four key elements: the application of fundamental human rights, the prevention of misuse and unethical applications, non-discrimination and non-neurodiscrimination, and the protection of people in vulnerable situations. And it specifically points out that transparency is necessary at multiple levels of neurodata processing.

At the procedural level, organisations performing neuroprocessing must provide clear, specific, and accessible information about their practices, detailing how data is

[29] Bertoni, E., Ienca, M. (2024). Expert Report on the Implications of the Use of Neurotechnology and Neural Data on Privacy and Data Protection from the Perspective of Convention 108+. Council of Europe. https://www.coe.int/en/web/data-protection/-/the-privacy-and-data-protection-implication-of-the-use-of-neurotechnology-and-neural-data-from-the-perspective-of-convention-108

collected, stored, used, and shared, as well as the purposes of collection and potential risks. At the algorithmic level, transparency involves explaining how algorithms process neurodata, including the methodologies and assumptions that underpin it. To do this, organisations must disclose and communicate how neurodata is analysed and interpreted, ensuring that users understand the logic and potential biases of algorithms. There must also be clarity about the decision-making processes influenced by such algorithms and the criteria used to generate results or recommendations. This level of transparency helps build trust and allows for external audits to ensure fairness, accuracy, and accountability.

Transparency also includes that stakeholders must be informed about the techniques used for data collection, and whether these are invasive or non-invasive. This information should be provided in a way that each person can understand, considering their ability to assimilate it.

Traditional transparency mechanisms, although required, may be insufficient for the complexity and level of sensitivity involved in neurodata processing, given the difficulty for data subjects to clearly understand how their neurodata will be used and the technologies that have been implemented for this purpose, as well as the possible consequences derived from the processing of their data.

Compromise proposal

Include specific transparency requirements for neuroprocessing:

- The obligation to inform always clearly what data are collected from the neurological or mental perspective (type of neurodata, invasive vs. non-invasive, additional biosignals) and what mental or behavioural states are inferred, with what scientific basis and reliability. When providing traditional information in accordance with transparency obligations, its important to bear in mind to inform who can access directly collected data, processed characteristics and inferences. Also, to inform about the use of neurodata to train AI models beyond the service provided to the data subject.
- The obligation to report separately on the aspects (including risks) relating to reading operations and those relating to writing operations, and the possible consequences of such processing.
- The obligation to report on specific aspects such as the reversibility or irreversibility of processing in which there is neurostimulation or neuromodulation.
- The obligation to incorporate mechanisms of continuous or "active transparency" regarding with neurotechnologies, with updates and reminders beyond a static privacy policy.

All this considering that in future scenarios it would be possible situations where neurodata collection takes place remotely (quantum sensors[30]).

IX. TRANSPARENCY IN THE VALUE CHAIN

In order for to provide effective, truthful and complete information to the natural person subject to neurodata processing, with neurotechnologies or neuroprocessing, it is necessary that exist an information flow along the value chain (from development to deploying in processing activities) for the services that supports these neuroprocessing operations, such for the systems that allow the processing of neurodata of any kind.

Value chain transparency refers to the ability to know, track, and communicate in a clear and accessible way all relevant information about how a product or system is designed, produced, distributed, and commercialized. In other words, it implies that both companies, supervisory authorities, and consumers can know all aspects of design, implementation, adaptation, distribution, monitoring and maintenance of products and services.

Transparency in the value chain is of key importance in many aspects, such as in consumer affairs, and in particular in data protection, since when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or that process personal data to fulfil their function, it may be appropriate to be able to know if the suppliers of the products, services and applications have applied the principles to respect the right to data protection, and in this case neurorights, when developing and designing these products, services and applications. In addition, they ensure that controllers and processors can comply with their data protection obligations.

Compromise proposal

Transparency in the value chain means that neurotechnological systems that allow the implementation of neuroprocessing or process neurodata of any kind, are developed and used in a way that allows adequate traceability and explainability, and that, at the same time, makes people aware of when neurodata is being collected or when stimulation or modulation is being carried out. In addition, to duly inform to the controllers about the capacities and limitations of these systems and to inform the people subject to such processing about their rights.

[30] Faccio, D. (2024). The future of quantum technologies for brain imaging. *PLoS Biology*, *22*(10), e3002824

X. EXPLAINABILITY IN NEUROPROCESSING USING ARTIFICIAL INTELLIGENCE

In relation to the previous section, the challenge of explaining the operations, or inferences of neurodata of different orders, carried out by AI systems in the framework of a neuroprocessing must be specifically addressed. In this case, the AI models should offer suitable results for the intended purpose, but also it is necessary to be able to understand how and why the inferences are generated by those AI models.

In this context, when requested by the data subject, explanations must be provided in clear and understandable language regarding the use of AI in the neuroprocessing. Such an explanation must not only accurately describe the process carried out by the system to reach a conclusion (as well as its capabilities and limitations), but must also be understandable, truthful, complete and specific for the data subject's case. All the necessary information and explanations should be provided so that people understand how the results that affect them were reached and so that they can have tools to defend their human rights or request a review of a conclusion.

In addition, human intervention must be available, that is, there must be designated personnel available to answer the data subject's concerns related to the conclusions or results, to exercise of rights, and personnel in charge of promoting the evaluation and review of the final conclusions and results.

Explainability in neuroprocessing must encompass three different layers:

- Raw signals (EEG, fMRI, intracranial recordings), which are often noisy and unintuitive to non-experts, so even "transparent" signal processing is not self-explanatory.
- AI models that decode neurodata and convert it into inferences of emotions, intentions, or cognitive states. As in other applications of AI, they are usually treated as "black boxes", with the classic problems of explainability that this entails (opacity, complexity, spurious correlations).
- The results obtained are not, in many cases, facts, but inferences about mental states (such as thoughts, emotions or intentions). These inferences lack a verifiable "fundamental truth" and, in many cases, do not have a solid or universally accepted scientific basis. Unlike direct measurements (such as a blood test or X-ray), there are no objective labels or reference standards that allow their accuracy to be unequivocally validated. This makes their verification and explanation a complex challenge, as they depend on subjective interpretations, algorithmic models or assumptions that can vary depending on the context, the technology used or even the biases of those who analyse them.

Explanation tools can provide incomplete or biased narratives that do not accurately reflect how the model actually works, which is especially problematic when people rely on these explanations to make important decisions about the use of neurotechnology. A false sense of objectivity and legitimacy should be avoided, masking uncertainty, experimental status and possible neurodiscrimination.

Compromise proposal

It is necessary include specific explainability requirements for AI used in neuroprocessing by role/responsibility:

- Always record which model, dataset, and parameters produced an inference or conclusion in a particular neuroprocessing, allowing for ex post reconstruction and review.
- Generate different explanations for each of the processing phases or operations: (a) data acquisition and preprocessing, (b) feature extraction and AI model, (c) inference/results logic and its use. Each phase or operation must have its own explanatory artifact (technical and stakeholder-oriented).
- All results of neuroprocessing using AI should be associated with calibrated intervals of uncertainty or confidence, and those uncertainties should be expressed in a way that is understandable to both professional audiences (auditors, deployers) and data subjects (e.g., "low reliability, experimental characteristic").
- Prohibit categorical statements (e.g., "you are anxious," "you have lied") unless they are supported by solid and rigorous scientific evidence; otherwise, should be used expressions with the meaning of probabilistic or tentative information along with clear warnings.
- Provide explanations of "why" the results have been produced, in accessible and visual language. Accompany these explanations with "what if" scenarios that show how changing conditions (task difficulty, session duration, device setting) would alter outputs, making it clear when the results obtained are context-dependent and not static.
- Include a mandatory "limitations" section in the user interface that emphasizes experimental status, the possibility of false positives/negatives, specific biases, or non-suitability for certain high-risk uses or specific cases.
- Implement reporting mechanisms when new types of inference are introduced (e.g., the model now infers "stress" in addition to "attention").

XI. DECEASED PERSONS' RIGHTS

Rights related to data protection (such as restriction of processing, access, rectification, deletion or opposition) are extinguished upon the death of the data subject. Many regulations do not explicitly address the consideration that the neurodata of deceased people should have, not only in relation to data protection, but, for example, in relation to image rights.

This means that the deceased person can no longer exercise them directly. Normally, after death, certain people relative to the deceased person (such as heirs or direct relatives) could exercise some rights over their data, providing that there is a legitimate interest and it had not been expressly prohibited by the deceased person in life. However,

if the data is of special or sensitive categories, access or processing by third parties is more restricted. In addition, if the deceased person stated clear instructions (e.g. in a specific will or document) about the fate of their data, these would prevail.

The use of neurodata from deceased people may be of great interest for medical research. However, it allows, among others, the creation of avatars or digital twins of deceased people[31], something that already exists as a service using other types of data and, taking advantage of AI techniques, it could reach much more complexity. The commercialisation of deceased "digital people" generated from neurodata, such as celebrities or family members, could have positive aspects, but also pathological aspects. For example, allowing abusers to prolong their practices beyond the death of the victim or having at their disposal a "personality" that was not accessible in life to vent traumas or frustrations. This information could also be used on a different scale to develop more refined techniques for manipulating people or masses, generating *bots* or *trolls* refined on the Internet for disinformation, being used as a social engineering technique against acquaintances of the deceased, etc.

Compromise proposal

The creation of avatars or digital twins based on neurodata without the express wish of the deceased person must be explicitly prohibited, as well as the commercialisation of their neurodata after their death. If such consent has been granted, the processing of neurodata must be limited to the specific purposes for which it was granted. The data subject must designate who exercises their rights and who carries out the corresponding follow-up after their death.

XII. LIMITATIONS ON AUTOMATED DECISION-MAKING

Including neuroprocessing in automated decision-making introduces critical peculiarities due to the potential inaccuracies of their results and the extreme sensitivity and intimacy of these data, which may reflect unique mental states, emotions, or brain patterns. Decision-making based on brain profiling can significantly affect people's privacy, autonomy and dignity, generating new risks of discrimination, which can be called "neurodiscrimination" and which, by going beyond "traditional" discrimination, are even more difficult to detect.

Brain profiling can reveal biological or psychic information that is far more intrusive than other personal data, requiring a much higher level of transparency and control in automated decisions. The lack of human intervention can amplify negative impacts, since inferences or decisions derived from neurodata could be erroneous, biased or directly discriminatory.

[31] Shengli, W. (2021). Is human digital twin possible? *Computer Methods and Programs in Biomedicine Update*, *1*, 100014

Possible impacts could include discrimination based on neural states, biases in the allocation of resources or services, undue restrictions of rights, etc. Current legislation already regulates automated decisions and the associated rights (such as the right not to be subject to automated-only decisions and the right to receive an explanation), but it does not specifically address the complexity and uniqueness of neurodata in this context. Regulation must be strengthened to prevent the misuse and discriminatory use of neurodata in algorithmic systems. Any use could be directly prohibited, clear and rigorous limits could be established, including the obligation of specialized and responsible human supervision, bias audits and clear explanations to those affected, etc.

Compromise proposal

In each jurisdiction, it is necessary to identify how to explicitly prohibit automated decision-making based on neuroprocessing when these produce legal effects on the data subject or significantly affect him or her in a similar way. An exception could be considered if such decision-making is authorised by the national or supranational law that applies to the controller and that it also provides for appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject.

XIII. RISK ASSESSMENT

As neurodata processing is not currently explicitly distinguished from that of other categories of data, there are no specific obligations or guidelines regarding its level of risk.

As stated in the RIPD declaration[32] , *" Los neurodatos pueden considerarse datos que entrañen un alto riesgo de afectación del derecho a la protección de datos personales de los titulares de conformidad con el apartado 41.1 de los Estándares, puesto que son datos que corresponden a la esfera más íntima de la persona y tiene el potencial de afectar no solo nuestra privacidad, sino también a los Derechos Humanos ligados a ella, como son la libertad de pensamiento, la libertad de expresión, la integridad corporal, la personalidad, la dignidad de las personas, la no discriminación y la equidad y la justicia. Además, los avances técnicos y científicos no se encuentran libres de errores, tendencias, sesgos, interpretaciones políticas y religiosas o prejuicios, por lo que pueden llevar a situaciones de neurodiscriminación. Incluso, como se ha señalado anteriormente, pueden utilizarse para tratamientos que modifiquen nuestro comportamiento"* [Neurodata can be considered data that entails a high risk of affecting the right to protection of personal data of the owners in accordance with section 41.1 of the Standards, since they are data that correspond to the most intimate sphere of the person and have the potential to affect not only our privacy, but also our privacy, but also to the human rights linked to it, such

[32] RIPD (2024) Declaration of the Ibero-American Data Protection Network on neurotechnologies and neurodata within the framework of personal data protection regulations.

as freedom of thought, freedom of expression, bodily integrity, personality, dignity of persons, non-discrimination and equity and justice. In addition, technical and scientific advances are not free of errors, trends, biases, political and religious interpretations or prejudices, which can lead to situations of neurodiscrimination. They can even, as noted above, be used for processing that modify our behaviour].

Therefore, consideration should be given to assess the inclusion of all types of processing that includes neurotechnologies and neurodata processing, as aspects that make the processing directly "high-risk" processing and, consequently, to apply the appropriate guarantees, after an objective assessment[33], that such processing really complies with the intended purpose, that they comply with a sufficient degree of effectiveness and suitability, in addition to the fact that the advantages that can be obtained from such processing for the individual and society outweigh the possible negative impacts on fundamental rights in general, and on neurorights in particular.

For example, in a proportionality analysis, it would be necessary to analyse the degree of impact that may be caused on the individual by the type of neurodata processed or whether neurostimulation or neuromodulation operations are included. Continuing with this example, it would be necessary to determine whether it is necessary to differentiate between signals that can be considered purely functional (like the ones that allow to move a prosthesis, for example), such as "low risk" or without inferential value, which could automatically be excluded from the enhanced protection regime, unless there is a combination with other data.

Any assessment of the impact on fundamental rights would have to be based on scientific evidence of current technology, and plausible technological development in the medium term, applying in turn the precautionary principle if such evidence is not yet available.

A work that remains pending and that could be of great help would be to develop and identify specific threats (by obtaining and publishing evidence, the definition of threat models, etc.) in these neuroprocessing operations to make it easier to identify everything that could have impacts on the rights and freedoms of data subjects in the different use cases. With these threat maps, then, to develop data protection techniques use cases, or others, that allow effective risk management. At the same time, to identify categories of neuroprocessing operation that by default should offer guarantees of the highest degree in order to be deployed as products or services.

Another strategy is to introduce a mental privacy impact assessment framework into standard practice[34]. Like data protection impact assessments used in other domains, this framework would help assess the potential risks and benefits of neurotechnology applications. This approach seeks to anticipate risks and guarantee the protection of fundamental rights, while at the same time allowing the benefits of these emerging technologies to be assessed. This form of impact assessment would encompass both

[33] Bertoni, E., Ienca, M. (2024). Expert Report on the Implications of the Use of Neurotechnology and Neural Data on Privacy and Data Protection from the Perspective of Convention 108+. Council of Europe. https://www.coe.int/en/web/data-protection/-/the-privacy-and-data-protection-implication-of-the-use-of-neurotechnology-and-neural-data-from-the-perspective-of-convention-108

[34] Ienca, M., & Malgieri, G. (2022). Mental data protection and the GDPR. *Journal of Law and the Biosciences*, *9*(1)

neural and non-neural cognitive biometric data, for which it could involve an audit of the technological components of the processing (e.g. when it is carried out using AI) and a thorough assessment, as well as a possible reconsideration of the algorithm, to determine whether some risks can be mitigated by design[35].

Compromise proposal

Develop regulations for the consideration of high risk of neuroprocessing, neurodata processing, or systems that allow the processing of neurodata of any order or inference of neurodata.

Develop requirements for objective assessment of the suitability, necessity and proportionality of such processing and systems, as well as minimum organisational, legal or technical guarantees that should be implemented.

Include in the lists of processing operations that involve a higher risk and that, therefore, have an obligation to deploy additional guarantees.

XIV. DATA PROTECTION MEASURES BY DESIGN AND BY DEFAULT SPECIFIC TO THE NATURE OF THE NEURODATA

In relation to the previous section, the current regulation does not require the incorporation of specific protection measures, when it is possible that the traditional ones are not effective and do not allow compliance with the principles of data protection by design and by default. In accordance with the "*Declaración Interamericana de Principios sobre Neurociencias, Neurotecnologías y Derechos Humanos*" [Inter-American Declaration of Principles on Neurosciences, Neurotechnologies and Human Rights][36] , where its Principles are very clear regarding the connection between neurotechnologies, the need to respect current human rights and the current principles of personal data protection, the protection of Human Rights is contemplated in the design of neurotechnologies. To this end, a human rights-based approach must be promoted in the development of neurotechnologies, seeking to guarantee comprehensive protection and respect for human rights in the design of these technologies, in their research methods, as well as in their implementation, commercialisation, evaluation and use.

In this context, it must be considered that the development and use of neurotechnologies must be guided by an ethical and human rights-based approach from their conception. This means that, before initiating any research or design, an assessment must be carried out that identifies potential risks to fundamental rights and freedoms, describes how neural data will be processed, and establishes preventive measures and controls to ensure its protection.

[35] https://rm.coe.int/expert-report-neuroscience/1680b12eaa

[36] https://www.oas.org/es/sla/ddi/docs/publicaciones_digital_Neurociencias_Neurotecnologias_Derechos_Humanos_2025_ESP.pdf

It is also stressed that these measures must be maintained throughout the life cycle of neurodata, applying technological, organisational and procedural strategies that avoid breaches or improper use. Ethics, conceived "by design and by default", must permeate every stage of the process: from research and experimentation to the commercialisation and application of neurotechnologies. Therefore, any study or protocol must conform to the rules and guidelines of research ethics, ensuring that respect for human dignity is the central axis of these practices[37].

The deployment of processing with such a high potential impact requires the use of equally advanced data protection techniques: federated learning, Secure Multi-Party Computation (SMPC), confidential computing, secure processing environments, homomorphic encryption and other PET (*Privacy-Enhancing Technologies*) techniques are just one example of them. Traditional approaches of anonymization and pseudo-anonymization can be compromised by the nature of neurodata and advances in data processing, such as AI. Therefore, the need to develop specific protection strategies must be considered, in addition to extending those of transparency (as mentioned in this document previously) beyond compliance with minimums, data traceability and access management mechanisms, as well as, where appropriate, consent management tools.

Finally, in relation to the use of AI in neuroprocessing and according to the Specific Guidelines for Compliance with the Principles and Rights that Govern the Protection of Personal Data in the Artificial Intelligence Projects of the RIPD[38], from the design of AI in the program, system, platform or any other technology that involves the processing of personal data, the controller must apply measures that enable effective compliance with the obligations arising from the applicable regulations on personal data. In addition, when AI is being developed, consideration should be given to achieving objectives in a less intrusive manner for data subjects, in terms of ethics, adherence to principles and assessing the relationship between usability and privacy.

Compromise proposal

As far as possible, neuroprocessing should be carried out in devices or environments controlled by and in the possession of the data subject, favouring their autonomy and control over their data. Otherwise, the data controller must implement specific data protection measures that include techniques in accordance with the impact of the processing. Similarly, whenever possible, a good practice is to offer a non-neurological approach that allows the same purpose to be achieved.

At the same time, the current technological environment has shown the fragility of security measures when it comes to protecting personal data, particularly when the target of the attacks is of high value (and therefore of high motivation and return on

[37] https://docs.un.org/es/A/HRC/58/58
[38] https://www.redipd.org/documento/guia-orientaciones-especificas-proteccion-datos-ia-es.pdf

investment for adversaries). But it is also necessary to consider the attractiveness of this information to be processed in an authorised manner for other purposes, as has already happened in relation to genetic data, by personnel with authorization from the organisation itself or by state security and information actors.

The creation of large repositories of neurodata, over a long period of time, the accuracy of the personal information contained, the explicit linking of such data to natural persons, will increase the impact of any breach. Therefore, regulators should determine to implement specific data protection measures to minimize the set of data processed.

Compromise proposal

All neuroprocessing must determine, evaluate and justify with evidence, at least, the need to retain neurodata, the precision and granularity of the neurodata collected or inferred, the extension over time of the neuroprocessing, the concentration in large repositories of neurodata and the linking of such data with identifiable natural persons.

XV. SPECIFIC OBLIGATIONS FOR DATA CONTROLLERS

Given the special sensitivity of neurodata and the impact of the processing, it should be considered that, in these cases, the people responsible for the neuroprocessing would be obliged to implement specific data protection and security measures, designed to minimise the risks that may affect fundamental rights, especially neurorights. These measures must be adequate, proportionate and adapted to the sensitive nature of the neurodata, to prevent possible vulnerabilities arising from its processing.

In addition, in a framework of accountability in relation to its obligations, it is essential to adopt and be able to demonstrate that are implemented measures useful, timely, relevant, and effective. These must guarantee regulatory compliance, avoiding unauthorised access, authorised misuse, manipulation or destruction of neurodata. In addition, such measures must be subject to periodic evaluations to ensure their continuous improvement and adaptation to emerging risks.

Neurotechnologies and the systems that include them are not isolated entities, they are integrated into networks, services, products and digital platforms. Without a global governance framework, problems of fragmentation, inequality and security can arise. For this reason, governance mechanisms are needed that align with data protection principles and requirements, but also with other global Internet and digital governance initiatives[39]. Only in this way will it be possible to guarantee an adequate level of coherence (the same "rules" for all), responsible innovation and respect for human

[39] Radu, R. (2025). Cognitive frontiers: neurotechnology and global internet governance. *Frontiers in Digital Health*, 7, 1690489

rights, and a *"trustworthy, transparent, and accountable ecosystem"* such as the one that is intended to be promoted in different forums and declarations such as the León Declaration on European Neurotechnology[40].

Public and private actors responsible for neuroprocessing must comply with proactive disclosure obligations, as a means of minimising the risk for the data subject and for society, informing in a clear and detailed manner about the existence of the processing operations, their purposes, the technologies used, the risks identified and the results of the impact assessments. In the case of publicly funded projects, these obligations are reinforced, requiring greater transparency and accountability to ensure the ethical and responsible use of resources. Transparency in the processing of neurodata is not limited to the publication of information. Decision-makers should foster public understanding and debate, allowing society to assess the benefits and risks associated with the use of neurotechnologies. To this end, the information must be accessible, understandable and timely, and the project documentation must be available in accordance with the applicable transparency and access to information regulations. This approach ensures that citizens can participate in an informed way in the deliberation on the impact of these technologies.

In addition, specific contracts for processors-sub-processors must be established that include specific clauses regarding the transparency of the value chain.

Compromise proposal

Neuroprocessing controllers should:

- Adopt appropriate and specific data protection and security measures to minimise the risks that such processing may pose to fundamental rights, particularly neurorights.
- Adopt and implement useful, timely, relevant, effective, and demonstrable measures for regulatory compliance, especially measures that prevent improper or unauthorised access, circulation, supply, and use of neurodata, as well as its manipulation or destruction, which must be subject to review, evaluation, and permanent improvements.
- Be subject to proactive disclosure obligations about the existence of the processing operations, their purposes, technologies used, risks identified and results of impact assessments. For publicly funded projects, these accountability obligations should be strengthened.
- Facilitate public understanding and debate and allow evaluation and deliberation on the use of neurotechnologies, their benefits and risks, making the information accessible, understandable and timely, and that the documentation of projects incorporating neurotechnologies is available in accordance with the applicable legislation on transparency and access to information.

[40] https://digital.gob.es/content/dam/portal-mtdfp/DigitalizacionIA/declaracion_de_Leon.pdf

- In the contracting and subcontracting of neuroprocessing, specific clauses on the processing of neurodata must be required, in which the organisational, technical and legal measures established from the design are explained in detail, which in turn must have a degree of specificity according to the impact of these processing operations. Subcontracting must require prior, express and written authorisation from the data controller.

XVI. PERSONAL DATA BREACHES

A neurodata breach can have an impact of the highest degree on people's rights and freedoms. The knowledge of what is happening in the digital world in relation to processing of such impact should be immediate, both for the agencies that are in charge of citizen security, as well as for all the actors that protect fundamental rights.

As noted above, the RIPD has already established the high-risk nature of these processing operations. Therefore, any data breach should be known, at least, to the data protection, cybersecurity and citizen security authorities to determine appropriate measures. The intrusion that the dissemination, loss or lack of integrity of neurodata could entail for privacy could have an unknown impact on the data subjects and should be reported immediately.

Compromise proposal

Any data breach should be immediately notified to the data protection, cybersecurity and public safety authorities, as well as immediately communicated to the data subjects.

XVII. POTENTIAL CHALLENGES IN OTHER REGULATORY AREAS

Within the competences that make up the Ibero-American Data Protection Network, this document has been developed paying special attention to the aspects that could be established in our respective legal areas in relation to this processing of personal data. However, throughout the text, aspects have already been pointed out that it would be either necessary, or opportune for regulatory clarity, not to include in the data protection regulation but in other regulatory developments in relation to different competences. Data protection regulations, or those that intersect with this field, have a limited sphere of action that does not cover, among others, processes or impacts on people, the market or society not directly related to the processing of personal data.

A. CONSTITUTIONAL AMENDMENTS

Chile was the first country in the world to incorporate the protection of neurorights in its Constitution[41]. The amendment to Article 19, paragraph 1 of the Chilean Constitution, through Law No. 21,383, establishes:

"*El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella"* [Scientific and technological development shall be at the service of people and shall be carried out with respect for life and physical and mental integrity. The law shall regulate the requirements, conditions and restrictions for its use in persons, and shall especially safeguard brain activity, as well as the information coming from it].

It is worth considering that the opportunity to laid down neurorights, both in their definition and in their development, if it is considered necessary, at the level of the fundamental norm, which allows their development in other regulatory areas.

B. PRODUCT REGULATIONS

When developing, designing, selecting and using systems, applications, services and products that are based on the processing of personal data or that process personal data to fulfil their function, the producers of the services and applications should be encouraged to take into account the right to data protection when developing and designing these products, and to ensure, with due regard to the state of the art, that controllers and processors are in a position to comply with their data protection obligations (as set out in recital 78 of the GDPR).

Therefore, it may be appropriate to have regulations that go beyond data protection and make it possible to guarantee and be able to demonstrate that products and services comply with minimum quality standards that protect the set of rights and freedoms that may be affected by the processing of neurodata. This is achieved through the implementation of specific market surveillance regulations for systems based on neurotechnologies, it is necessary to develop various essential aspects that guarantee their effectiveness and safety.

- Establish a clear coordination framework (governance) between competent authorities, defining roles, responsibilities and mechanisms for continuous supervision[42].
- Formulate policies and guidelines that ensure compliance with technical, ethical and data protection requirements, aligned with current national and international regulatory frameworks.

---

[41] Lee, A. (2026). Neurorights as Constitutional Rights: Enforcement Gaps in Chile and Lessons for Comparative Neurodata Governance. *Neurotechnology, Society & Governance*, *1*(1), 21-39

[42] OECD (2025). Neurotechnology Toolkit. https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf

- Develop management processes that should include detailed procedures for the assessment and control of the specific risks associated with neurotechnology-based systems, ranging from pre-approval to post-marketing monitoring.
- Define the conformity assessment mechanism must include rigorous protocols that verify that products comply with safety, efficacy and quality regulations, certification mechanisms, including clinical tests when necessary.
- Implement a system of notifications throughout the value chain, to supervisory bodies and to users, which must be robust and transparent, ensuring that manufacturers, distributors and authorities report in a timely manner any incident, defect or risk detected to allow a rapid and adequate response for the benefit of consumer protection and the safeguarding of fundamental rights.

Closely related to market surveillance regulations is the development in the standardization of neurotechnologies, since it is essential that products comply with clear and rigorous standards, homogeneous in all markets, which allow the practical application of the requirements for the protection of fundamental rights, and ensure their proper functioning and the minimization of physical or psychological risks.

C. CONSUMER REGULATIONS

For the neuroprocessing and neurotechnologies market, basic consumer regulations must focus on guaranteeing safety, efficacy and protection of users' rights. This type of regulation will be linked to market surveillance regulations.

The following consumer rights must be considered:

- Right to security (protection from dangerous, deceptive or addictive goods and services).
- Right to be informed (accurate information on price, quality, quantity and conditions).
- Right to choose (access to goods and services at competitive prices).
- Right to be heard and to seek redress (access to complaints and dispute bodies).
- Rights to repair or replacement of the product

Liability for defective, unsafe or deficient products and services must also be regulated:

- Rules on when a product is considered "defective," misleading, and/or addictive and who is responsible (manufacturer, importer, retailer).
- Remedies for consumers: repair, replacement, refund, damage, or compensation.

Unfair practices and contractual conditions must be addressed:

- Prohibitions of unfair or deceptive trade practices (misleading advertising, deception, omission of key information).

- Control of unfair contractual clauses, especially in standard contracts (e.g. clauses that seriously harm consumers).

Information obligations and other marketing practices must also be regulated:

- Provide clear, accurate, and non-misleading information about goods, services, and digital content. Mandatory requirements for clear and understandable information for the consumer should be established, detailing permitted uses, possible side effects and relevant warnings.
- Develop specific standards for advertising, e-commerce, distance selling, and sometimes environmental or "Made in."

And provide complaint management and redress mechanisms:

- Establishment of consumer councils, ombudsmen, or courts/commissions to hear complaints.
- Procedures for individual and sometimes collective redress, including mediation or alternative dispute resolution.

D. LIABILITY REGULATIONS

The rules of liability that determine how damage can be compensated – caused by human activities or by goods or systems for which people are held legally responsible – have proven to be particularly complex in their application in the context of emerging digital technologies, and could not be less so in the case of the use of neurotechnologies and neuroprocessing.

Such rules could provide a variety of avenues for victims to claim compensation. In particular, they could offer that the victim could bring a liability action for damages arising from products or services based on a person's conduct (fault liability). This type of action in different regulations requires the accreditation of the existence of damage, the concurrence of fault or negligence on the part of the responsible party, as well as the causal relationship between said conduct and the damage caused.

Likewise, it could be considered whether the victim could claim compensation for the damage regardless of the existence of fault (strict liability). In this case, liability would be attributed based on the risk, without the need to prove the existence of fault.

Therefore, a regulatory framework that would provide legal coverage for liability claims could consider several factors, including:

- To delimit the object and scope of application of the proposal in relation to the above.
- Align product liability terminology with existing consumer and product safety frameworks and industry standards.
- Respond to the reality of products in the digital age through a technology-neutral approach, including software and development documentation within the

product concept, and specifying in which cases a related service should be considered as a component of a product.

- Possibly, expand the concept of damage (patrimonial or extra patrimonial) to include the loss or corruption of neurodata.
- To lay down the rules governing the liability of economic operators for damage caused by defective products, as well as the conditions under which natural persons are entitled to compensation.
- Establish the criteria for determining whether a product is defective, that is, whether it offers the safety that the general public can legitimately expect.
- Given the global economy, the possible requirement that there is always an economic operator established in the territory against which the action for compensation can be directed.
- Determine the cases in which operators who modify a product can be held liable.
- Determine who bears the burden of proof. If it falls on the injured person or if mechanisms are introduced to relax this burden in order to achieve a balance between the interests of the industry and consumers.
- Assumptions in economic operators could be exempt from liability.
- Aspects such as joint and several liability and the case of third-party intervention.
- Cases in which the victim's own conduct could lead to a reduction in compensation.
- Cases, or impossibility, in which liability cannot be excluded or limited by contract or other legal provisions.
- Consider setting maximum or minimum limits to the amount of compensation.
- The deadlines for the exercise of actions.
- Transparency measures on judicial decisions in this area.

E. INTELLECTUAL PROPERTY REGULATIONS

Other ways of protecting neurorights are emerging. The example of the recent experience in Denmark stands out, where in 2025 the government, with broad parliamentary support, presented a draft reform of copyright legislation to address the phenomenon of *deepfakes* and hyper-realistic digital imitations generated by AI.[43]

The bill introduces new provisions into the Danish Copyright Act, in particular the new 65a and 73a, with the aim of strengthening protection against non-consensual digital reproductions of a person's appearance, voice or distinctive features. The logic of the system is to use the tools of copyright and related rights to prevent the creation and dissemination of digital imitations that simulate a real person. Thus, the affected person could demand the removal of the content, the cessation of its use and, where appropriate, the corresponding compensation for damages. The model also provides for

[43] https://technical-regulation-information-system.ec.europa.eu/en/notification/27420/text/D/EN

enhanced protection for performers and maintains traditional exceptions, such as parody or satire.

In this context, the protection of one's own image and biometric data that underlies this approach could also be projected on the processing of the so-called neurodata, configuring itself as an additional way of protection against new forms of capture and use of highly sensitive information linked to brain activity. This development could be important for contemplating the regulation of the neurodata of deceased people.

F. PUBLIC SECTOR TRANSPARENCY REGULATIONS

The public administrations responsible for neuroprocessing are obliged to comply with the principles of proactive disclosure in the deployment of applications based on neurotechnologies and in the processing of neurodata. These commitments must be explicitly regulated in the transparency regulations of public administrations, ensuring that citizens have clear and detailed access to information on the use, purposes and risks associated with these technologies.

In the case of public projects, or projects carried out by third parties that are financed with public funding, the requirements of transparency and accountability take on a reinforced character. This approach not only seeks to ensure the publicity of information, but also to guarantee strict control over the use of resources, ensuring their ethical and responsible destination. In this way, the legitimacy of institutions is strengthened and public management that prioritizes integrity, citizen participation and the common good is promoted.

G. CYBERSECURITY

Despite the advantages introduced by brain-computer interfaces (BCIs), they present specific security challenges. The literature has documented the possibility of attacks directed against such interfaces, compromising the integrity and availability of data and services, as well as access to sensitive information, which affects confidentiality[44]. Cybersecurity applied to neurodata and neurotechnological systems must be addressed in a comprehensive manner, transcending the mere protection of confidentiality. It is essential to ensure not only that information remains inaccessible to unauthorised actors, but also that other essential dimensions, such as the availability and, especially, the integrity of the data, are preserved. The latter acquires critical relevance when neurodata is used in stimulation or neuromodulation processes, where any unauthorised alteration could have serious and irreversible consequences on people's health and well-being.

In short, the most worrying risk lies in the security of users, since attackers could take control of neurostimulation devices to induce or prevent neural overstimulation, carrying out denial-of-service attacks on the device. In this context, the concept of neural

[44] Landau, O., Puzis, R., & Nissim, N. (2020). Mind your mind: EEG-based brain-computer interfaces and their security in cyber space. *ACM Computing Surveys (CSUR)*, *53*(1), 1-38

cyberattacks has been defined[45], which take advantage of vulnerabilities in next generation neurostimulation systems to alter spontaneous neuronal activity through stimulation or inhibition processes. It would be possible to find ourselves in a scenario that would affect national security, either through attacks aimed at persons of interest, or within the framework of an economy of scale, with millions of users using the same systems.

Different types of specific attacks are documented in the literature. For example, the so-called Neuronal Flood (FLO), Neuronal Scanning (SCA), which focus on overstimulating the neurons that the attack selectively activates differently, Neuronal Jamming (JAM) as a cyberattack capable of inducing neuronal inhibition maliciously. These attacks use recreations of the cerebral cortex, or part of it, to execute specific actions against the subjects and induce states or actions[46].[47]

This scenario underscores the need to implement new robust security protocols and limitations in connectivity and interoperability, capable of preventing, detecting and neutralizing threats that may compromise not only privacy, but also the physical and mental integrity of individuals and their effects on society, the latter when an economy of scale makes a massive use of these devices for non-clinical uses a reality. The possibility that cyber threats, such as computer viruses, transcend the digital realm to directly affect the physical and biological world of human beings could impact the most intimate part of human identity and cognition, generating risks of a magnitude that has so far been difficult to imagine.

XVIII. FINAL THOUGHTS

This document addresses the need to analyse data processing based on neurotechnologies that beyond the field of public health and regulated health research, which are not subject to specific sectoral regulations. In this context, it is essential to recognize that the particularities of the medical field cannot be directly extrapolated to other sectors of application, such as commercial, educational or labour. Therefore, it is recommended to carry out a detailed study of the specifics of both groups of processing operations – both inside and outside the medical field – even though they share common grounds.

Likewise, the development of a systematic analysis of specific threats associated with these neuroprocessing operations in relation to the protection of personal data, to provide guarantees for scientific development and healthcare treatment, is identified as a pending and priority line of work.

---

[45] Schroder, T., Sirbu, R., Park, S., Morley, J., Street, S., & Floridi, L. (2025). Cyber risks to next-gen brain-computer interfaces: analysis and recommendations. *Neuroethics*, *18*(2), 34

[46] López Madejska, V. M., López Bernal, S., Martínez Pérez, G., & Huertas Celdrán, A. (2024). Impact of neural cyberattacks on a realistic neuronal topology from the primary visual cortex of mice. *Wireless Networks*, *30*(9), 7391-7405

[47] Bernal, S. L., Celdrán, A. H., & Pérez, G. M. (2022). Neuronal Jamming cyberattack over invasive BCIs affecting the resolution of tasks requiring visual capabilities. *computers & security*, *112*, 102534

There is a great deal of work ahead to develop, in relation to neuroprocessing, the collection and publication of empirical evidence, and the development of threat models that allow the identification of potential risks to the rights and freedoms of data subjects in the different use cases. With these threat maps, it would be possible to design use cases for data protection techniques – such as Privacy-Enhancing Technologies (PETs) – and other measures that facilitate effective risk management. In addition, it is proposed to categorise neuroprocessing according to their level of risk, establishing maximum guarantees by default for those that, due to their nature or potential impact, require a greater degree of protection before their deployment as products or services.

Scientific evidence is necessary to have criteria to evaluate the suitability, necessity and proportionality of processing. Research is needed on the quality of neurodata (directly collected and inferences) and on the short- and long-term effects of the use of neurotechnologies, especially in vulnerable populations such as children and adolescents, etc.

An area of special relevance, still to be explored in depth, is the integration of neurotechnologies with Artificial Intelligence. AI, by enhancing the capacity for analysis and inference of neurodata, can facilitate its massive and systematic use, which opens a range of possibilities for innovation and the improvement of the quality of human life. However, this technological advance also entails a significant increase in the risks associated with the protection of personal data and the safeguarding of fundamental rights, such as mental privacy, autonomy and non-discrimination.

This scenario requires a regulatory and ethical approach that balances taking advantage of the opportunities offered by AI in the neurotechnological field with the implementation of robust guarantees to prevent misuse, algorithmic biases or violations of fundamental rights.