www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 15(5), Dec 2024, 17-35. ISSN: 2007-1558.
https://doi.org/10.61467/2007.1558.2024.v15i5.555

Brain Data Security and Neurosecurity: Technological advances, Ethical dilemmas, and Philosophical perspectives

Jorge A. Ruiz-Vanoye [1], Ocotlán Díaz-Parra [1], Francisco Marroquín-Gutiérrez[1], Juan M. Xicoténcatl-Pérez[1], Ricardo A. Barrera-Cámara [2], Alejandro Fuentes-Penna[3], Eric Simancas-Acevedo[1], Jazmín Rodríguez-Flores [1], Josue R. Martínez-Mireles [1]

[1] Universidad Politécnica de Pachuca, México.
[2] Universidad Autónoma del Carmen, México.
[3] El Colegio de Morelos, México.
Email: jorge@ruizvanoye.com

E-mails

Abstract. The rapid development in neurotechnology has significantly advanced our ability to understand and manipulate brain functions. However, these advancements have raised critical concerns regarding the security and privacy of brain data. This paper aims to explore the multifaceted issues surrounding the protection of brain data, focusing on neurosecurity. We begin by reviewing the current technological landscape, focusing on methods used to secure brain data, including encryption, authentication protocols, and anonymisation techniques. Drawing parallels with established computer security practices, we highlight both the strengths and limitations of these approaches when applied to neural data. Next, we delve into the ethical dilemmas posed by brain data security. Issues such as mental privacy and informed consent are analysed. The implications of unauthorised access to brain data and the misuse of such data in various contexts, including criminal justice, employment, and military applications, are discussed in detail. Furthermore, we examine the philosophical perspectives on brain data security, particularly concerning personal identity, autonomy, and freedom of thought. We explore how the manipulation and protection of brain data intersect with longstanding debates in ethics and philosophy, proposing frameworks for addressing these challenges. By combining a technological review with an ethical and philosophical analysis, this paper aims to provide a comprehensive understanding of neurosecurity and brain data security. We conclude with recommendations for future research and policy development to ensure the ethical and responsible use of brain data, emphasising the need for robust governance frameworks that protect individual rights while fostering technological innovation.
Keywords: Brain Data Security, NeuroSecurity.

Article Info
Received May 10, 2024.
Accepted Nov 20, 2024.

1 Introduction

The brain is divided into several functional areas that play different roles in information processing. These include the cerebral cortex, which is responsible for most cognitive and sensory functions; the brainstem, which controls vital functions such as breathing and blood circulation; and the cerebellum, which helps coordinate muscle movements.

The central nervous system (CNS) includes fundamental structures such as the spinal cord, hindbrain, midbrain, and forebrain, each with specific functions critical to the functioning of the human body. The spinal cord, which extends from the medulla oblongata to the lumbar region of the spinal column, acts as a signal transmission pathway between the brain and the body, coordinating simple reflexes (Kandel, Schwartz, & Jessell, 2000). The hindbrain, composed of the cerebellum, pons, and medulla oblongata, controls essential autonomic functions such as breathing and balance (Bear, Connors, & Paradiso, 2007).

The midbrain, located between the diencephalon and hindbrain, regulates motor functions, temperature, vision, hearing, and eye movements (Nolte, 2002). Finally, the forebrain, the largest and most advanced part of the brain, which includes the telencephalon and diencephalon, is responsible for complex functions such as thought, memory, emotion, and endocrine regulation, with the telencephalon encompassing the cerebral cortex, which is crucial for cognitive and sensory processing (Martin, 2003). These structures (Figure 1) work together to ensure the coordination and efficient functioning of the human body.

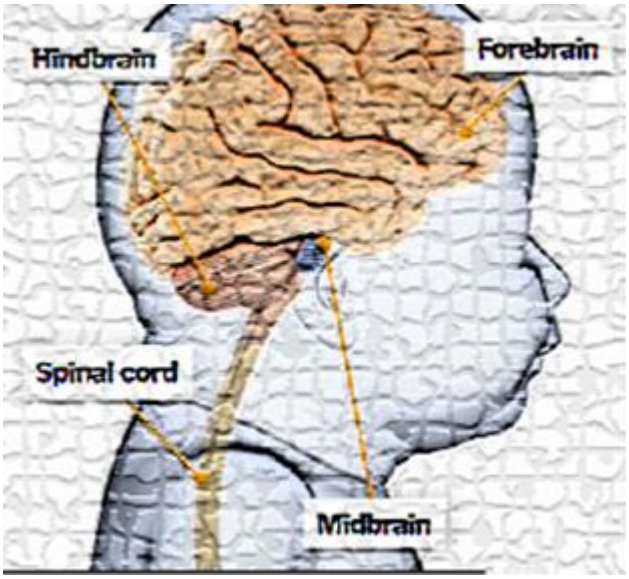

Fig. 1. Image of the brain with the entire central nervous system.

The brain is a complex and highly specialised organ containing billions of interconnected neurons that transmit electrical signals to each other through connections called synapses. Electrical signals are produced in response to external or internal stimuli, such as sensory perception, emotion, and thought.

Brain data refers to the information that is stored and processed in the brain. Data processing in the brain is carried out by a series of protocols and electrical signals that occur in neurons. Nerve cells, or neurons, are composed of a cell body, known as the soma, and several extensions called dendrites and axons. Dendrites receive electrical signals from other neurons, while axons transmit these signals to other neurons in more remote areas of the brain. This neural activity is produced by a series of highly complex biochemical and electrical processes that are not yet fully understood.

In short, brain data is the information that is stored and processed in the brain through a series of components such as neurons and synapses, along with protocols and electrical signals that allow them to communicate with each other.
In neurons, information travels as electrical impulses through long extensions called axons. The axons are coated with an insulating substance (myelin) that functions like a plastic sheath around an electrical wire and allows for the correct and rapid transmission of electrical impulses. The impulses produce rhythms that are known as brain waves. The brainwave activity (Fig. 2) can be visualised on an electroencephalogram or brain map. The brain map is also referred to as Quantitative Electroencephalography (digitised or computerised analysis) of brain activity. Brainwaves are the very low amplitude electrical activities produced by neurons within the human brain. There are five types of brain waves: Delta waves (1 to 3 Hz), Theta waves (3.5 to 8 Hz), Alpha waves (8 to 13 Hz), Beta waves (12 to 32 Hz), and Gamma waves (25 to 100 Hz).

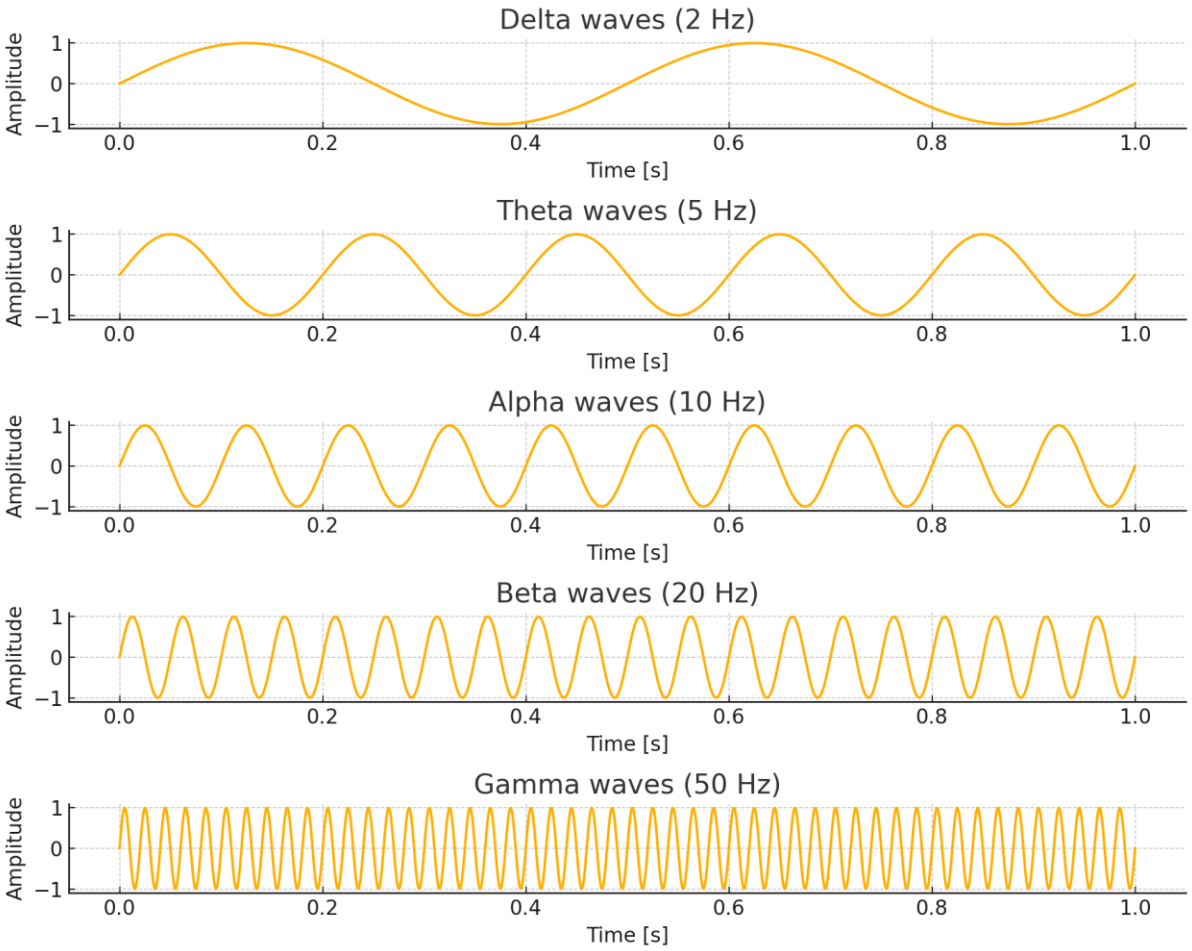

Fig. 2. Brainwave activity.

Brain data is extremely sensitive due to its intimate and personal nature. Brain data, obtained through techniques such as functional magnetic resonance imaging (fMRI), electroencephalograms (EEG), and other forms of neuroimaging, can reveal profound aspects of our thoughts, emotions, mental states, and health conditions. Because of this sensitivity, it is crucial to implement robust security measures to protect this data from unauthorised access, alteration, and misuse.
In this paper it is important to highlight how we can see the analogy of how the brain could be considered as if it were a computer, the Computational Theory of Mind.

Computational Theory of Mind (CTM) holds that the human mind is, in essence, a computer-like information processing system. According to this theory, mental processes can be understood as the manipulation of symbols according to formal rules, analogous to how a computer processes data. Jerry Fodor (1975) proposes the idea that the human mind operates similarly to a computer, using an internal representation system that he calls the language of thought or Mentalese. This language is hypothetical and is supposed to have a specific syntax and semantics, allowing thoughts to be manipulated and processed in a formal way. The components of CTM are:

- Mental Representations. Symbolically encoded thoughts, beliefs, desires, perceptions etc.
- Algorithms and Manipulation Rules. Formal procedures and rules for processing mental representations.
- Memory System. Short-term and long-term memory for storing representations and rules.
- Input and Output Mechanisms. Sensory perception (sight, hearing, touch, etc.) and generation of actions or responses (movements, language).}
- Executive Control. Coordination and regulation of mental activity; decision making on what algorithms to apply and how to manage representations.

The table 1 containts the comparative between CTM and the computers.

Table 1. CTM versus Computers.

Component CTM	Computer
Mental Representations	Data stored in bits, files, and documents in the file system.
Algorithms and Manipulation Rules	Software, programs, and algorithms that process data.
Memory System	RAM (random access memory) and hard disk/SSD storage.
Input and Output Mechanisms	Input devices (keyboard, mouse, sensors) and output devices (monitor, printer, speakers).
Executive Control	CPU (central processing unit) that executes and controls program operations.

Turing (1936) introduced the concept of abstract models of computation that manipulate symbols on an infinite tape according to a set of formal rules. Based on this idea, the mind is conceived as a system that processes symbols, with thoughts being internal symbolic representations and mental processes involving the manipulation of these symbols.
Chomsky (1957) suggested that mental processes follow formal rules or algorithms, similar to computer programs. This principle derives from his work in linguistics, where he applied computational ideas to understand human language through formal grammatical rules and syntactic structures. This idea is fundamental to CTM, as it states that the human mind operates in a similar way to a computer in manipulating symbols and processing information.

Fodor (1975) developed the concept that the mind represents information from the external world in an internal form that can be manipulated computationally. CTM postulates that human thought has a language-like structure with specific syntax and semantics, allowing mental processes to operate computationally.

Putnam (1967) was a leading proponent of functionalism, the idea that mental states are defined by their function or causal role in the cognitive system, rather than by their physical composition. A central tenet of CTM is functionalism, which suggests that the mind could be implemented in any system capable of performing the necessary functions, not just in the biological brain.
The central idea is that psychological states and processes are computational in nature, which has led to a focus on taxonomies of psychological states that depend on the intrinsic properties of individuals (Kersten, 2016).

The model of the mind as a computational system has been fundamental in cognitive science, where the analogy between the brain and computers has been used to investigate how information is organised and stored (Gómez & Orbe, 2016). This analogy suggests that humans act as symbol processors, which implies that cognition can be decomposed into computational processes that operate independently of the physical medium (Gómez & Orbe, 2016; Müller, 2009). However, some critics argue that this view may be too reductionist and does not capture the complexity of cognitive processes (Brattico, 2008).
Furthermore, CTM is closely related to computational theory, as it involves the ability to attribute mental states to oneself and others, which is essential for social interaction (Resches et al., 2010; Zegarra-Valdivia & Vilca, 2017). ToM has been studied in the context of education and social development, where it has been found that a poor understanding of ToM may be correlated with aggressive and bullying behaviours (Portillo et al., 2023).

On the other hand, it is argued that the mind does not only reside within the individual, but is also influenced and mediated by the environment and the technological tools we use (Aydin, 2013; Merrill & Chuang, 2019). This perspective challenges the traditional notion of the mind as a closed system and suggests that cognition is a dynamic process that extends beyond the boundaries of the human body.

2 Brain Data Security and Neurosecurity

A Neurotechnology, which includes devices capable of reading and, in some cases, influencing brain activity, poses significant ethical and legal challenges. The regulation of these devices is crucial to prevent the exploitation of brain information, which could be used for unethical purposes, such as the manipulation of decisions or the invasion of mental privacy (Sánchez, 2024; Tello, 2024). In this sense, the creation of a regulatory framework that contemplates neuro-rights is fundamental to ensure that individuals maintain control over their mental information and that their fundamental rights are respected (Tello, 2024).

Ware (1973) introduces key concepts of computer security, stressing the need for security controls that address technical, administrative, and physical aspects to protect computer systems. Ware defines computer security as protection against unauthorised access to and misuse of computer resources. Modern computer security (Stallings, 2018) refers to the practice of protecting systems, networks, and software from digital attacks. Attacks are often aimed at accessing, changing, or destroying sensitive information, extorting money from users, or disrupting normal business processes. There are two fundamental concepts, physical security and logical security:

- Physical security (National Bureau of Standards, 1977) refers to practices and procedures designed to protect computer resources and data processing infrastructure against physical damage and unauthorised access.
- Logical security (Ware, 1973) is defined as the set of controls and measures implemented to protect computer systems against unauthorised access and unauthorised modification of data.

It is necessary to build on the original concept of Data Security and Computer Data Security. Ware (1973) defined data security as the set of practices and procedures designed to protect information systems against unauthorised access, unauthorised modification, and accidental or intentional destruction. Computer data security refers to the set of practices and technologies designed to protect data stored, processed, and transmitted by computer systems against unauthorised access, alteration, and destruction. Computer data security encompasses several key dimensions: confidentiality, integrity, and availability. With this definition, in this paper we propose new definitions of Brain Data Security and NeuroSecurity.

In order to correctly define the term Brain Data Security it is necessary to mention the concept defined by Bonaci et al. Bonaci et al. (2015) define neurosecurity as the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will. This definition underscores the critical need for robust security measures as neurotechnologies become more integrated into healthcare and daily life. In this paper we define and redefine some concepts:

- ***Brain Data Security*** refers to the set of practices and technologies designed to protect data stored, processed and transmitted by a series of protocols and electrical signals that occur in the neurons of the brain against unauthorized access, alteration and destruction.
- **Neurosecurity** refers to the comprehensive protection of the brain and its functions against external threats, including the physical security of implanted devices, protection against electromagnetic interference and the integrity of mental processes.

Neurosecurity encompasses a broader range of protection measures, including physical and ethical aspects. This concept refers to the comprehensive protection of the brain and its functions against external threats, ensuring the physical security of implanted devices, protection against electromagnetic interference, and the integrity of mental processes. In contrast, brain data security focuses exclusively on the security of neural data, emphasising the protection of brain-generated information through methods such as encryption, authentication, and anonymisation. While neurosecurity addresses the holistic protection of the brain as a whole, brain data security specialises in safeguarding the confidentiality, integrity, and availability of brain data.
The rapid development of neurotechnologies, such as BCIs and neuromodulatory devices, has introduced various security risks. Markosian et al. (2020) highlight the need for neurosecurity in the context of spinal cord stimulation devices, which present documented vulnerabilities that could compromise patient safety.

In addition, the concept of brainjacking - the unauthorised manipulation of brain implants - poses unique challenges, as highlighted by Pycroft et al. (2016), who discuss how attackers can alter device parameters to induce damage.
Pugh et al. Pugh et al. (2018) explain that while the possibility of hacking BCIs in both experimental and real-world settings has been demonstrated, the possibility of interfering with the software configuration of implanted pulse generators (IPGs) in deep brain stimulation (DBS) systems raises profound ethical concerns. Once neurosafety is breached, there are several mechanisms for brainjacking, such as manipulation of voltage, current, frequency and pulse width, which can significantly affect the patient's neural functioning (Straw et al., 2022).

Wang et al. (2023) note that while the risks associated with neurosecurity are largely theoretical at present, the increasing prevalence of connected neurodevices necessitates vigilance against potential attacks. The ability to wirelessly control implanted devices opens the door to cyber-attacks, where unauthorized users can change settings or activate functionalities without consent (Ahmed et al., 2019).

The ethical implications of brainjacking are significant, particularly concerning individual autonomy. Ienca and Andorno Ienca & Andorno (2017) argue that the possibility of brainjacking raises profound concerns about the autonomy of individuals with implanted devices. Unauthorized control over a person's neural activity not only infringes on their privacy but also poses risks of

physical and psychological harm. The manipulation of neural devices can lead to alterations in mood, behavior, and cognitive function, which could have devastating effects on an individual's quality of life (Pycroft et al., 2016).
The use of encryption to protect brain data both at rest and in transit is crucial in safeguarding sensitive information. Brain data, often collected through neuroimaging techniques like MRI, EEG, or other neurotechnological methods, contains highly personal and potentially exploitable information. Encrypting this data ensures that even if unauthorized individuals gain access to the storage systems, they cannot interpret the data without the correct decryption keys. Encryption algorithms, such as AES (Advanced Encryption Standard), provide robust security measures to prevent data breaches and ensure privacy.
In addition to protecting data at rest, encryption is also essential for securing data in transit. As brain data is transmitted between devices, such as from a neuroimaging device to a cloud server or between different healthcare providers, it becomes vulnerable to interception and tampering. Implementing encryption protocols like TLS (Transport Layer Security) ensures that data remains confidential and integral during transmission. TLS encrypts the data being sent over the network, making it unreadable to anyone who might intercept it.

Moreover, encryption plays a vital role in meeting legal and ethical standards regarding patient data privacy. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States mandate the protection of personal health information, including brain data. Encrypting brain data helps healthcare organizations comply with these regulations, avoiding legal penalties and maintaining trust with patients.

The use of encryption also addresses the ethical concerns related to the handling of sensitive brain data. Ethical considerations in neurotechnology emphasize the need to respect patient autonomy and confidentiality. By encrypting brain data, researchers and healthcare providers can ensure that individuals' sensitive information is not exposed to unauthorized parties, thereby respecting their privacy rights. Ethical guidelines outlined by the International Neuroethics Society highlight the necessity of robust encryption methods to uphold ethical standards in the collection, storage, and transmission of neurological data (International Neuroethics Society, 2019).

The continuous advancements in encryption technology further enhance the protection of brain data. Innovations such as homomorphic encryption allow data to be processed without being decrypted, providing an additional layer of security. This means that sensitive brain data can be analyzed and utilized for research or clinical purposes without exposing it to potential risks. Homomorphic encryption is a type of encryption that allows certain computations to be performed on encrypted data, producing an encrypted result which, when decrypted, corresponds to the outcome of the operations as if they had been performed on the original, unencrypted data. There are several types of homomorphic encryption: Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), and Fully Homomorphic Encryption (FHE). The integration of homomorphic encryption into Neurotechnology applications can provide several benefits.

- Homomorphic encryption ensures that brain data remains confidential during processing. This is particularly crucial in clinical settings where patient data must comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States.
- Homomorphic encryption allows encrypted data to be shared without revealing the underlying information.
- The ability to perform computations on encrypted data enables advanced analytical techniques, such as machine learning and artificial intelligence, to be applied to brain data without compromising privacy.

Below is a comparative table illustrating the differences between physical and logical security for computers and other devices versus the security of brain data. Table 2 provides a comparative overview of the different security measures and considerations for physical and logical security in both computers and other devices versus brain data.

Table 2. Computers and Devices Security vs Brain Data Security.

Aspect	Computers and devices	Brain data
Physical security	Securing hardware from theft or damage Using locks, security cameras, and restricted access Ensuring physical integrity of servers and networks	Securing neuroimaging devices and storage units Controlling access to neuroimaging facilities Protecting physical data storage media

Aspect	Computers and devices	Brain data
Logical security	Implementing firewalls and anti-virus software Using secure passwords and authentication methods Adhering to data protection regulations (e.g., GDPR, HIPAA)	Encrypting brain data at rest (e.g., AES encryption) Ensuring secure data transmission (e.g., TLS protocols) Applying homomorphic encryption for data processing
Threats	Malware, phishing attacks, and unauthorized access Physical theft or destruction of devices	Data interception, unauthorized access to sensitive information Misuse of neuroimaging devices or unauthorized data collection
Compliance	Adhering to data protection regulations (e.g., GDPR, HIPAA) Implementing policies for data security and privacy	Complying with healthcare data regulations (e.g., HIPAA) and ethical guidelines Ensuring ethical handling and storage of brain data
Ethical Considerations	Protecting user privacy and data integrity Avoiding misuse of computing resources	Ensuring confidentiality and autonomy of patients Preventing unauthorized use of brain data for non-consensual purposes

On the other hand, Neurotechnology (UN, 2023) is an emerging field of knowledge that presents a broad evolution that has generated important benefits for different fields of knowledge such as medicine, biomedical engineering, neurosciences, law, public policies, through research and innovation processes focused mainly on improving the quality of life of human beings. These benefits are accompanied by risks that must be analysed with a broad perspective, supported by a broad ethical framework, as misuse could impact and change personality, individual behaviour, affecting privacy and free will. UNESCO produced a report on neurotechnology and human rights in Latin America and the Caribbean: challenges and public policy proposals. This report identifies four human rights in neurotechnology: a) mental privacy, b) mental integrity, c) personal identity and d) cognitive freedom. It also analyses the regulatory proposals of international and regional organisations and legislative bodies for the regulation of neurotechnology in the context of Latin America. In (UNESCO, 2023), it is reported that among the agreements reached at the 42nd General Conference, the Social and Human Sciences Sector was assigned the task of developing a global normative framework on ethics in neurotechnology.

At the same time, Andorno (2023) mentions four ethical and legal challenges that neurotechnologies must consider and address:

a) Mental privacy is the ethical-legal principle concerning the protection of brain data belonging to third parties, as well as the avoidance of its dissemination. International standards such as the Universal Declaration of Human Rights (UDHR) protect privacy, including the confidentiality of personal data. Other standards include the International Covenant on Civil and Political Rights of 1966, the American Convention on Human Rights of 1969, and the Universal Declaration on Bioethics and Human Rights adopted by UNESCO in 2005. Mental data obtained through brain scans open up the possibility of reading thoughts and intentions that even the owner may not be aware of. Therefore, the privacy of mental data should be considered as the right to confidentiality of such data.
b) Mental integrity, which can be altered by psychological damage, can be compromised in a manner similar to how computers are hacked. A deep brain stimulation device has the potential to alter a person's mental integrity. Memory engineering can achieve the selective erasure of a person's memories, and by applying optogenetic techniques (genetic and optical methods), specific memories can be restored or erased by

strengthening or weakening synaptic connections using lasers. Technological interventions to the brain can cause harm through the malicious use of devices; therefore, consideration should be given to developing civil and criminal law to compensate for and punish inappropriate behaviour.

c) Personal identity. In addition to monitoring the brain, neural devices can also allow information to be written to the brain. Therefore, personal identity can be altered by stimulating the brain, which could be exploited by authoritarian entities for the mind control of individuals who disagree with their proposals.

d) Cognitive freedom, which can be affected by the misuse of neurotechnology, may be compromised through the use of neurological enhancement devices that could trigger inequity in various areas of social life. Freedom of thought must be considered in legal norms that protect both the external and internal dimensions of mental activity.

2.1. Technologies to protect brain data

For brain data protection, we can consider various methods and technologies such as data anonymization, blockchain, Access Control, Data Encryption, and Intrusion Detection Systems (IDS). Each of these methods has an important role to play in ensuring the privacy and security of brain data.

2.1.1. Data Anonymization

Data Anonymization involves deleting or modifying personal information so that the data cannot be linked to specific individuals. This helps protect the privacy of brain data, especially when it is shared or analysed for research or clinical purposes. Anonymization, pseudonymization, and de-identification are techniques used to protect brain data and images (Eke et al., 2021). Some techniques include: Generalization: Changing specific data to ranges, Deletion: Eliminating parts of the data and Disturbance: Modifying the data by adding alterations. One challenge is to keep the data useful for analysis while preventing it from being re-identified using advanced techniques. Some techniques considered for data anonymization are:

- De-identification: Removes information that can identify a person.
- Encryption: Converts data into an unreadable format without the correct key.
- Synthetic Data Generation: Creates fake data that mimics real data.
- Hashing: Transforms data into a fixed, irreversible string of characters.
- K-anonymity: Ensures that each data point is not distinguishable from at least k other individuals.
- L-diversity: Ensures that the data within a group is varied.
- Differential Privacy: Adds intentional noise to protect individual identities.
- Pseudonymization: Changes names and personal data into codes.
- Downsizing: Reduces the amount of data to minimise risk.
- T-closeness: Maintains the similarity of sensitive data within any group.

2.1.2. Blockchain

Brain data and activities are recorded in a distributed manner, ensuring their integrity and transparency based on a decentralised system, which prevents unauthorised modifications. This technology is used in brain-computer interfaces to protect the connection and communication between wearable devices from attacks and to safeguard data in networks of connected medical devices (Khan et al., 2022). It is also employed to protect communication between devices that generate electroencephalograms (EEG) and prostheses available to individuals, specifically the data generated between the two devices (Bak et al., 2019). An important consideration for this technology is the handling of large volumes of data and the high consumption of resources. Some techniques and technologies within the blockchain stand out:

- Decentralized storage. Store data in multiple places instead of just one.
- Private Blockchains. Only authorized persons can view and use the information stored on this blockchain.
- Blockchain encryption. It applies encryption techniques and only authorized people access the data stored on the blockchain.
- Smart Contracts. Automatic programs that ensure data is used only under specific conditions approved by the patient.
- ChainLink (Data Oracles). It connects smart contracts with real-world data securely, allowing data to be reliably integrated.

- Decentralized Identity. People control who can see and use their digital information.
- Data management platforms. Platforms available in the cloud or on servers that allow you to control who can access the blockchain, protect data in a secure and regulated environment.
- Consensus Protocols. Mechanisms that ensure that all data on the blockchain is validated and cannot be tampered with, protecting the integrity of the data.
- Data Tokenization. It converts sensitive data into secure codes that can be easily handled on the blockchain without revealing the original information.
- Zero-Knowledge Proofs. It verifies that the data is correct without the need to reveal the exact information, thus protecting the privacy of the data.

2.1.3. Access Control

Mechanisms and policies are established to ensure that only authorised individuals can access brain data. Retinal authentication is a secure example of accessing personal or brain data (Devi et al., 2022), while electroencephalogram (EEG) data can also be used as a means of authentication (Jalaly Bidgoly et al., 2020). It is important to regularly update permissions and ensure that systems storing keys and permissions can scale as needed.Some methods or technologies are:

- Biometric authentication. This technology uses physical and biological data from a person to verify their identity. These include the use of fingerprints, facial recognition, iris scanning, voice recognition.
- Based on Roles whose access is according to the person's role.
- based on Attributes which access is according to specific characteristics. It is important to constantly update permissions and ensure that systems that store keys and permissions can grow as needed.

2.1.4. Data Encryption

This technique uses special codes to ensure that only authorised individuals can access the data. To protect data during transmission, the TLS protocol is employed. However, security depends on how keys are managed, and the process can be slow. For example, neurofeedback devices measure brain waves, and the data collected by these devices from users is encrypted to prevent interception by third parties. Additionally, brain data from an MRI can be analysed without putting the patient's personal data at risk (Liu et al., 2020). Some types of encryption:

- Symmetrical, uses the same key to encode and decode information, such as AES.
- Asymmetric that uses a public key and a private key, i.e. a key to open and another to close, such as RSA.
- Homomorphic, it uses a special key where mathematical operations are performed on the encrypted data without being decrypted, the data can be analyzed without being shown.

2.1.5. Intrusion Detection Systems (IDS)

These tools monitor and analyse unauthorised access attempts. When combined with autonomous learning, these systems provide a security option for the Internet of Medical Things (Si-Ahmed et al., 2023). There are two main types: Signature-Based, which compares data traffic with known signatures, and Anomaly-Based, which detects unusual behaviour in data. These systems can register or generate false alerts, and signatures need to be constantly updated.Other intrusion detection technologies include:

- Entity and User Behavior Analysis: They use artificial intelligence to observe how users behave. If someone does something unusual, they notify them so that it can be checked.
- Firewalls. They filter traffic according to rules and also include advanced features to detect and block intruders. They combine the functions of IDS and IPS and examine traffic in more detail.
- Security Information and Event Management (SIEM) Tools: Gather and analyze security information from many different sources. They help to find and understand suspicious events and allow you to react quickly.
- Real-Time Network Monitoring: These tools continuously monitor the network for suspicious activity. They have sensors that collect and analyze data instantly.

- Intrusion Prevention Systems (IPS): Similar to IDS, but in addition to warning, they can block unauthorized access automatically.

Current technologies used to protect brain data encompass a variety of methods designed to ensure the confidentiality, integrity, and availability of this highly sensitive information. One of the most fundamental technologies is encryption, which encodes data so that only authorised parties can read it. The Advanced Encryption Standard (AES) is widely adopted due to its robustness against attacks. AES encryption ensures that brain data stored on servers or devices is not accessible without the correct decryption key. A study by Li and Chen (2021) underscores the effectiveness of AES in safeguarding medical and neurological data, emphasising its critical role in data protection (Li & Chen, 2021).

Authentication technologies are also crucial in protecting brain data by ensuring that only authorised individuals can access it. Multi-factor authentication (MFA) adds layers of security by requiring multiple forms of verification, such as passwords, biometric scans, or security tokens. This significantly reduces the risk of unauthorised access.

In addition to encryption and authentication, anonymization techniques play a vital role in protecting brain data. Anonymization involves modifying data so that it cannot be traced back to an individual, thus protecting patient privacy. Techniques such as data masking, pseudonymization, and differential privacy are employed to achieve this. A report by the European Data Protection Supervisor (2020) discusses the importance of anonymization in healthcare data, including brain data, to ensure compliance with privacy regulations while enabling data sharing and research (European Data Protection Supervisor, 2020).

Another advanced technology used to protect brain data is homomorphic encryption. This method allows computations to be performed on encrypted data without decrypting it, thus maintaining data confidentiality throughout the processing stages. This is particularly useful for research and clinical applications where data analysis is required.

Blockchain technology is also being explored for securing brain data due to its decentralized and immutable nature. Blockchain can provide a secure and transparent method for tracking and auditing data access and modifications. It ensures that all actions taken on brain data are recorded in a tamper-proof ledger.

Data access control mechanisms, such as role-based access control (RBAC), are essential in managing who can view or manipulate brain data. RBAC assigns permissions based on user roles within an organization, ensuring that only those with a legitimate need can access sensitive data. This reduces the risk of data breaches from internal threats. A study by Ferraiolo et al. (2021) demonstrates the effectiveness of RBAC in enhancing security and compliance in medical data management systems, including those handling brain data (Ferraiolo et al., 2021).

Secure data transmission protocols are critical for protecting brain data as it moves between devices or networks. Protocols like Transport Layer Security (TLS) ensure that data transmitted over networks is encrypted and secure from interception. TLS is widely used in healthcare to protect data in transit, ensuring that sensitive information such as brain data remains confidential and untampered. The use of Transport Layer Security (TLS) is essential for securing medical communications and data transfers, especially in neuroimaging research. TLS ensures the confidentiality, integrity, and authenticity of sensitive brain data, making it a key defence against cyber threats. As the healthcare industry progresses, the implementation of strong security measures like TLS will be crucial in upholding trust and regulatory compliance in medical data exchanges.

Lastly, intrusion detection and prevention systems (IDPS) are employed to monitor and defend against potential threats to brain data. These systems can detect suspicious activities and respond to potential security incidents in real time. IDPS are essential in protecting the infrastructure that stores and processes brain data from cyberattacks.

Neuro-consent interfaces represent a crucial innovation in the field of neurotechnology, allowing individuals to have more precise and personalized control over access to their brain data. These interfaces are designed to process neurological signals in a sophisticated manner, facilitating increased research with human subjects. However, this increase in the use of human subjects necessitates the implementation of more robust ethical protections.

Neuro-consent interfaces offer an innovative solution, allowing individuals to precisely control access to their brain data by interpreting neurological signals in a sophisticated manner. These interfaces not only protect users' privacy and autonomy but also promote equitable distribution of technological benefits, ensuring that the advantages of BCI technology are accessible and

not restricted by exclusivity. As BCI technology advances, its ethical standards must continually adapt to address emerging challenges and maintain public trust.

Advances in brain and mind science enable new ways to monitor and manipulate cognitive functions, raising concerns among cognitive libertarians about threats to cognitive liberty. While protecting cognitive liberty is crucial, it can conflict with others' freedoms and restrict both neurotechnological and common intrusions into the mind. This dilemma mirrors traditional libertarian challenges in balancing individual rights with collective benefits.

To address this challenge, autonomous AI systems known as Cognitive Liberty Guardians have been proposed as a solution. These guardians are designed to safeguard neuro-rights by monitoring and regulating the use of neurotechnologies to ensure that ethical principles and mental privacy are respected. Utilizing advanced algorithms and machine learning, these systems can identify and prevent unauthorized intrusions into individuals' mental processes.

Crutchfield (2024) explains that Cognitive Liberty Guardians autonomously monitor brain-computer interfaces and neurotechnological devices to ensure responsible use, protecting users' autonomy and privacy. While these systems do not resolve all ethical dilemmas associated with neurotechnology, they mark a significant step towards safeguarding cognitive rights in an increasingly digital world. This analysis underscores the need for ethical, responsible systems and calls for more empirical research and stakeholder collaboration. Although definitive answers are elusive at this early stage, it is hoped that this article will foster debate among researchers and policymakers, offering recommendations to maximize benefits and minimize risks.

According to Livanis et al. (2023), the combination of neural implants and artificial intelligence offers significant opportunities for innovations in neurotechnology and the enhancement of existing devices. While these technologies promise substantial advancements in restoring neurological functions, they also present critical ethical challenges. Developers of AI-powered neural implants possess key knowledge about the possibilities and limitations of these technologies, but their perspectives are often underrepresented in academic literature. This study aims to explore the views of neurotechnology developers to describe the ethical implications of three types of AI-powered neural implants: a cochlear implant, a visual implant, and a brain-computer interface for decoding motor and speech intentions. In the table 3 are the operation and ethical consequences.

Table 3. Operation and Ethical Consequences

Operation	Description	Ethical Consequences
Monitoring User Activity	Cognitive Liberty Guardians monitor user activities in the metaverse to prevent unauthorized interference with their cognitive processes.	Protects users from harmful interventions but raises privacy and autonomy concerns. Balancing protection and privacy is crucial.
Preventing Unauthorized Data Access	The guardians detect and block attempts to access users' brain data without authorization.	Ensures data protection but requires robust consent mechanisms to prevent abuse and ensure user control over data.
Enhancing Cognitive Privacy	The guardians use encryption and other security measures to protect brain data transmitted within the metaverse.	Secures user trust through data security but may hinder beneficial uses of data in health and research if not managed well.
Real-Time Intervention in Neuro-Interactions	Cognitive Liberty Guardians intervene in real-time to prevent manipulative or coercive neuro-interactions.	Protects users from harm but could limit legitimate interactions and experiences, raising questions about appropriate intervention levels.
Supporting Neuro-Ethical Experiences	The guardians promote and facilitate neuro-ethical experiences, guiding users	Encourages ethical behavior but requires clear guidelines and education to prevent

	towards safe and consensual activities.	paternalism and ensure informed user choices.
Conflict Resolution and Reporting	The guardians mediate disputes related to neuro-rights violations and report incidents to the appropriate authorities.	Maintains order and accountability but must avoid over-regulation and respect due process and user rights.

3 Methodological approach used to analyse technological, ethical and philosophical aspects of brain data security

The methodological approach used to analyze the technological, ethical, and philosophical aspects of brain data security typically involves a multidisciplinary framework. This framework integrates insights from fields such as computer science, neuroethics, philosophy, and law to ensure a comprehensive understanding of the subject. This multidisciplinary approach allows for a more holistic analysis by incorporating diverse perspectives and expertise.

One of the primary methods used in this analysis is a literature review, which involves systematically examining existing research and publications on the topic. This method helps identify key themes, trends, and gaps in the current knowledge base, providing a foundation for further investigation.

Case studies are another important methodological tool used to analyze brain data security. By examining specific instances where brain data security measures were implemented or breached, researchers can gain valuable insights into the practical challenges and solutions associated with protecting this sensitive information.

Quantitative methods, such as statistical analysis, are used to assess the prevalence and impact of different security threats and measures. These methods enable researchers to quantify the effectiveness of various technologies and the frequency of security breaches, providing a data-driven basis for recommendations and policy development.

Ethical analysis is a crucial component of the methodological approach, focusing on the moral implications of brain data security practices. This involves evaluating the ethical principles of autonomy, beneficence, non-maleficence, and justice in the context of brain data protection.

Philosophical inquiry is another essential method used to explore the deeper implications of brain data security. This involves examining the fundamental concepts and assumptions underlying the protection of brain data, such as the nature of privacy, identity, and the ethical use of technology.

Regulatory analysis is also employed to understand the legal frameworks governing brain data security. This involves examining existing laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and assessing their adequacy in protecting brain data.

Technological assessment methods are used to evaluate the effectiveness and limitations of current security technologies. This involves testing and analyzing various encryption, authentication, and anonymization techniques to determine their suitability for protecting brain data. A technological assessment by Liu and Chen (2018) compared different encryption algorithms and their application in neuroimaging data protection, providing valuable insights into the most effective technological solutions for brain data security (Liu & Chen, 2018).

Comparative analysis of security strategies in computer science and brain data involves examining the similarities and differences in how each domain addresses confidentiality, integrity, and availability. This process typically starts with defining the specific security requirements and threats unique to each domain. For example, while computer systems often focus on protecting against malware and unauthorized access, brain data security must address concerns about privacy and ethical implications.

One method for comparative analysis is the use of benchmarking, which involves evaluating the performance of different security strategies against a set of standard criteria. Benchmarking can help identify best practices and highlight areas where one

domain might benefit from the approaches used in another. A study by Lee and Kim (2020) used benchmarking to compare encryption algorithms used in traditional IT systems with those applied to neuroimaging data, finding that certain algorithms performed better in terms of speed and security in the context of brain data (Lee & Kim, 2020).

Risk assessment methodologies are another important tool for comparing security strategies. These methodologies typically involve identifying potential threats, assessing the likelihood and impact of these threats, and determining the effectiveness of existing security measures. By applying risk assessment techniques to both computer systems and brain data, researchers can identify common vulnerabilities and develop strategies that address these risks comprehensively.

Threat modeling is a specific technique used in comparative analysis to understand the potential threats to a system and how they can be mitigated. This involves creating a detailed representation of the system, identifying potential attack vectors, and assessing the effectiveness of different security measures. Threat modeling for brain data must consider unique factors such as the ethical implications of data misuse and the potential for unauthorized cognitive manipulation.

Comparative studies often utilize case studies to provide real-world examples of how different security strategies have been implemented and their outcomes. Case studies can reveal the practical challenges and successes of various approaches, offering valuable lessons for both fields. For instance, a case study by Patel and Singh (2019) examined the implementation of multi-factor authentication in a neuroimaging research facility, highlighting the strengths and weaknesses of this approach compared to traditional IT environments (Patel & Singh, 2019).

Surveys and interviews with experts are also useful for comparative analysis, as they provide insights into the practical experiences and opinions of those who work with these security measures. Statistical analysis and data mining techniques can be used to identify patterns and trends in security incidents across both fields. By analyzing large datasets of security breaches and vulnerabilities, researchers can identify commonalities and differences in the types of attacks and the effectiveness of various security measures.

Cost-benefit analysis is another valuable method for comparing security strategies. This involves assessing the financial costs of implementing various security measures against the potential benefits, such as reduced risk of data breaches and compliance with regulations. Cost-benefit analysis helps organizations make informed decisions about which security investments are most worthwhile.

Comparative analysis also involves examining the scalability of security measures. Scalability refers to the ability of a security solution to handle increasing amounts of data or users without compromising performance. This is particularly important for neurodata, which can involve large volumes of complex data. Usability analysis is another important aspect of comparative studies. This involves evaluating how user-friendly different security measures are, considering factors such as ease of use, user satisfaction, and the potential for human error. Usability is crucial for ensuring that security measures are effectively implemented and maintained.

Interdisciplinary workshops and conferences provide a platform for experts from different fields to share their knowledge and discuss common challenges and solutions. These events facilitate cross-disciplinary learning and collaboration, helping to bridge the gap between IT and neurodata security. According to a report by the International Conference on Cybersecurity and Neuroethics (2019), interdisciplinary workshops have been instrumental in advancing the understanding of brain data security by bringing together diverse perspectives (International Conference on Cybersecurity and Neuroethics, 2019).

Lastly, comparative analysis benefits from continuous monitoring and evaluation. This involves regularly reviewing and updating security strategies based on new threats, technological advancements, and regulatory changes. Continuous monitoring ensures that security measures remain effective and relevant over time.

Finally, an interdisciplinary synthesis integrates the findings from all these methods to provide a comprehensive understanding of brain data security. This synthesis involves combining insights from technological, ethical, philosophical, and regulatory analyses to develop holistic recommendations and strategies.

Complementing the above, there are several philosophical questions about Personal Identity, Mental Privacy and Autonomy:

- Personal identity refers to the set of characteristics that make a person unique. In the context of brain data, the question arises as to how manipulation or alteration of this data can affect one's perception of self. Could neurotechnological interventions change who we are in a profound sense?

- Mental privacy is the right to keep one's thoughts and mental processes free from external intrusion. With the advancement of technologies capable of reading or influencing thoughts, serious challenges are posed to this fundamental right. Invasion of mental privacy can lead to manipulation of thoughts and emotions, undermining individual freedom. To keep brain data private, there are neuro-rights. Neuro-rights are the human right to keep our brain data private and inside our bodies. Roberto Adorno and Marcello Ienca (2017) have proposed the need to protect the thoughts and memories stored in citizens' brains from theft. They mention the need for protection of what they call neuro-rights. These include the right to protection against non-consensual use of human brain information, mental privacy, protection from unauthorised access to or manipulation of brain signals that may result in psychological or physical harm, maintaining personal identity and coherence of individual behaviour, and primarily preventing the addition or deletion of essential brain memories.
- Autonomy refers to the ability to make free and informed decisions about one's own life. In the context of neurotechnology, the ability to influence mental processes raises questions about the extent to which decisions remain autonomous if they can be influenced by external devices. Protecting autonomy requires ensuring that any use of brain data is consensual and free of coercion.

4 Ethical and Legal Implications: Reflection on the ethical and legal implications of protecting brain data.

Ochang, Eke and Stahl (2024) highlight that advances in neuroscience and other disciplines are producing large-scale brain data consisting of datasets from multiple organisms, disciplines, and jurisdictions in different formats. However, due to the lack of an international framework for data governance, brain data are currently produced under various contextual ethical and legal principles that may influence key stakeholders involved in the generation, collection, processing, and sharing of brain data, posing ethical and legal challenges. The research responds to the call for a cross-cultural study of global brain data governance, and the results of the study will help to understand the issues and concerns that arise in brain data governance.

On the other hand, Alon, Bussod & Ravitsky (2024) highlight that preimplantation genetic testing (PGT) has attracted considerable ethical, legal, and social scrutiny, but academic debate often does not reflect clinical realities. To address this gap, a review of 506 articles from 1999 to 2019 in humanities and social sciences was conducted to synthesize the ethical, legal, and social implications (ELSI) of PGT. Findings reveal that global research production on PGT ELSI multiplied tenfold between 1999 and 2019, indicating growing interest and concern. Despite intense theoretical discourse on optimal offspring selection, such practices were scarcely reported in clinical settings. Conversely, critical issues like PGT funding and family impacts remain underexplored. Notably, 86% of ELSI literature originates from only 12 countries, highlighting research concentration.

This review underscores the urgent need for ELSI research to align more closely with clinical practice, fostering collaborations among ethics specialists, physicians, policymakers, and economists. Such efforts are crucial for grounding debates in practical relevance and ultimately guiding PGT towards ethical integrity, social acceptance, and equitable access. By harmonizing PGT research with real-world clinical concerns, the review enhances the relevance and impact of future ethical debates, echoing the need for robust governance frameworks that protect individual rights while fostering technological innovation in neurotechnology.

At the same time, Sun & Ye (2023) argue that the growth of research and applications of brain-computer interfaces (BCIs) has stimulated extensive discussion on their ethical implications. However, most existing research has primarily examined ethical issues related to BCIs from a general perspective, paying little attention to the specific functions of the technology. This has led to a mismatch between governance and ethical issues, due to the lack of differentiation between written and read BCIs. By providing detailed descriptions of the functions and technical approaches of written and read BCIs, we propose that ethical governance of BCIs should follow the principle of precise governance and develop refined strategies tailored to different functional types of BCIs. This approach ensures that ethical considerations keep pace with technological advancements, addressing concerns about the security, privacy, and responsible use of brain data in the evolving landscape of neurotechnology.
Also, Bublitz (2024) explores the provocative assertion that artificial intelligence (AI) can be integrated into human beings in a profound way, examining three ethical and legal implications. This argument builds on a robust legal concept of persons as holders of rights and subjects of heightened protection, broad enough to encompass prevailing philosophical views of personhood. The claim centers on a specific technology: devices that link human brains to computers and operate using AI algorithms. Under plausible philosophical and empirical conditions, these devices and their AI components become integral parts of the person, akin to limbs, organs, or cognitive capacities. This transformation is termed empersonification, with

significant normative consequences, particularly in legal contexts, where persons have greater responsibilities towards other persons (and their integrated parts) than towards mere objects.

Three consequential implications include: (i) AI devices lose their status as independent legal entities and instead receive special legal protections similar to those afforded to persons; (ii) as a result, third parties such as manufacturers or software developers relinquish intellectual property rights over the device and software; (iii) individuals assume liability for the actions of empersonified AI devices to the same extent as they do for desires or intentions originating from their subconscious. Empersonification represents a significant milestone in the ongoing history of human-machine interaction, necessitating profound ethical deliberation and urging the development of these technologies in alignment with core human values.

Rainey (2024) argues for the inclusion of imaginative future scenarios in the development of neurotechnology, particularly for legal and political considerations. Integrating detailed imaginative explorations of potential future uses of neurotechnology can help anticipate and address ethical, legal, and political challenges that may arise as brain stimulation research moves into consumer domains. Futurist methodologies, combining artistic creativity with scientific advancement, have long advocated for envisioning potential futures shaped by current technological trajectories.

In this sense, embracing this creative approach within neurotechnology development transcends mere functional considerations of safety and regulatory compliance, encouraging proactive engagement with emerging dynamics that neurotechnology could introduce. Imagined scenarios can anticipate consumer applications that might pose legal or political dilemmas, offering insights into their implications and complexities. This approach advocates for a shared responsibility in shaping policies that govern technological advancements. Ultimately, it provides a framework for neurotechnology development that aims to preempt ethical and legal crises, fostering balanced political responses that align knowledge advancement with regulatory safeguards and innovation protection.

Finally, Ochang, Eke, and Stahl (2024) state that advances in neuroscience and other disciplines are generating large-scale brain datasets comprising data from multiple organisms, disciplines, and jurisdictions in various formats. However, due to the lack of an international data governance framework, brain data is currently being produced under various contextual ethical and legal principles, which may influence key stakeholders involved in the generation, collection, processing, and sharing of brain data, thereby posing significant ethical and legal challenges.

5 Conclusions

Imagine a future where advanced technology allows the direct modification of brain data, including the insertion of false memories, such as murders or traumatic events, into the mind of a person who has never experienced them. This scenario raises profound ethical and philosophical implications:

1. Personal identity is largely constructed from our experiences and memories. Inserting false memories of murder or trauma could radically alter one's perception of oneself, creating an identity based on fictitious events. This can lead to confusion about one's own history and personality, affecting self-esteem and internal coherence.
2. The insertion of traumatic memories can have devastating effects on a person's mental health, leading them to experience post-traumatic stress, depression and severe anxiety. These memories may trigger inappropriate emotional and behavioural reactions based on experiences that never occurred.
3. Modifying brain data without a person's consent raises serious ethical and legal issues. Invasion of mental privacy and manipulation of memory undermine personal autonomy and integrity. It is essential to develop ethical and legal frameworks to protect individuals from such practices.

We propose ideas on Mental Privacy and Neuro-Rights:

- Advanced Encryption for Brain Data. In the future, advanced encryption algorithms could be developed specifically for brain data, ensuring that any information read from or written to the brain is secure from unauthorized access. This could involve biometric encryption keys that are unique to each individual’s neural patterns.
- Brain Firewalls. Similar to computer firewalls, brain firewalls could be designed to protect against unauthorized intrusions. These would be software and hardware solutions implanted in the brain to monitor and block any unauthorized attempts to access or manipulate neural data.
- Neuro-Consent Interfaces. Neuro-consent interfaces could allow individuals to control who accesses their brain data and for what purposes. These interfaces might involve advanced neural interfaces that require conscious approval before any data exchange or manipulation can occur, ensuring that all actions are consensual.

- Cognitive Liberty Guardians. In a futuristic society, there could be cognitive liberty guardians-autonomous AI systems tasked with monitoring and protecting individuals' neuro-rights. These guardians would ensure that no unauthorized or harmful manipulations of brain data occur and could alert authorities in real-time if violations are detected.
- Neuro-Rights Legislation. Governments worldwide might adopt comprehensive neuro-rights legislation, ensuring the legal protection of mental privacy and brain data. Such laws would explicitly prohibit non-consensual use, unauthorized access, and manipulation of brain signals, and would provide severe penalties for violations.
- Electromagnetic Shielding. The use of electromagnetic shielding technologies protects the brain from electromagnetic interference and unauthorised access to neural signals. A practical example would be a Faraday cage cap is an electromagnetic shielding technology designed to protect the brain from electromagnetic interference and unauthorised access to neural signals. The cap is made of conductive materials (fabrics woven with metal wires such as silver or copper) that create a barrier around the brain, blocking any incoming or outgoing electromagnetic signals.
- Integrated Security Implants. Development of brain implants with advanced security features, such as interference detection and self-deactivation mechanisms in case of unauthorised tampering attempts.
- Neural Signal Encryption. Ensuring that any communication between implanted devices and external systems is encrypted to prevent unauthorised access.
- Biometric Authentication. Use of multi-factor authentication for any interaction with implanted devices, ensuring that only authorised users can access or modify settings.
- Neural Intrusion Detection Systems. Implementation of systems that continuously monitor neural signals and detect anomalous activity or unauthorised access attempts.
- Automatic Intrusion Response. Development of automatic responses to detected intrusions, including deactivation of implants or isolation of compromised signals.

Some possible future work on NeuroSecurity and Brain Data Security: development of Encryption Protocols for Brain Data, Neural Intrusion Detection Systems, Electromagnetic Shielding and Physical Protection of the Brain, Ethical and Legal Impact of Neurosecurity (Brain Data Security), Neuro-Consent and Advanced Biometric Authentication, Brain Implant Security, Mental Privacy and Neuro-rights.

References

Ahmed, I., Bykov, A., Попов, А. П., Meglinski, I., & Katz, M. (2019). Optical wireless data transfer through biotissues: practical evidence and initial results. Lecture Notes of the Institute for Computer Sciences, *Social Informatics and Telecommunications Engineering*, 191-205. https://doi.org/10.1007/978-3-030-34833-5_16.

Alon, I., Bussod, I., & Ravitsky, V. (2024). Preimplantation genetic testing (PGT) has attracted considerable ethical, legal, and social scrutiny, but academic debate often does not reflect clinical realities. *Journal of Assisted Reproduction and Genetics*, 41, 1153–1171. https://doi.org/10.1007/s10815-024-03076-y.

Andorno, R. (2023). *Neurotechnologies and Human Rights in Latin America and the Caribbean: Challenges and Public Policy Proposals*. Montevideo: UNESCO. Retrieved from https://www.unesco.org/es/articles/neurotecnologias-y-derechos-humanos-en-america-latina-y-el-caribe-desafios-y-propuestas-de-politica-publica.

Aydin, C. (2013). The artifactual mind: overcoming the 'inside–outside' dualism in the extended mind thesis and recognizing the technological dimension of cognition. *Phenomenology and the Cognitive Sciences*, 14(1), 73-94. https://doi.org/10.1007/s11097-013-9319-x.

Bonaci, T., Calo, R., & Chizeck, H. (2015). App stores for the brain : privacy and security in brain-computer interfaces. *IEEE Technology and Society Magazine*, 34(2), 32-39. https://doi.org/10.1109/mts.2015.2425551.

Brattico, P. (2008). Shallow reductionism and the problem of complexity in psychology. *Theory and Psychology*, 18(4), 483-504. https://doi.org/10.1177/0959354308091840.

Bublitz, J. C. (2024). Might artificial intelligence become part of the person, and what are the key ethical and legal implications? *AI & Society*, 39, 1095-1106. https://doi.org/10.1007/s00146-022-01584-y 7.

Crutchfield, P. (2024). Mental privacy, cognitive liberty, and constraints. Bioethics Research. https://doi.org/10.1007/s11673-024-10344-0.

Devi, R. M., Keerthika, P., Suresh, P., Sarangi, P. P., Sangeetha, M., Sagana, C., & Devendran, K. (2022). Chapter 5 - Retina biometrics for personal authentication. In P. P. Sarangi, M. Panda, S. Mishra, B. S. P. Mishra, & B. Majhi (Eds.), *Machine Learning for Biometrics* (pp. 87-104). Academic Press. https://doi.org/10.1016/B978-0-323-85209-8.00005-5.

Díaz-Parra, O., Ruiz Vanoye, J. A., Barrera-Cámara, R. A., Fuentes-Penna, A., & Sandoval, N. (2014). Soft systems methodology for the strategic planning of the enterprise computer security. *International Journal of Combinatorial Optimization Problems and Informatics*, 5(1), 2–14. Retrieved from https://ijcopi.org/ojs/article/view/87.

European Data Protection Supervisor. (2020). *Anonymization techniques in healthcare data protection*. EDPS Report, 19(1), 67-80. Retrieved from https://edps.europa.eu/sites/edp/files/publication/20-01-28_anonymisation_techniques_en.pdf.

Ferraiolo, D., Kuhn, R., & Chandramouli, R. (2021). Role-based access control in medical data management. *IEEE Security & Privacy*, 19(2), 43-55. https://doi.org/10.1109/MSP.2021.3058302.

Gómez, G. V. and Orbe, F. J. B. (2016). Pedagogía cognitiva: la educación y el estudio de la mente en la sociedad de la información. *Education in the Knowledge Society* (EKS), 1(1). https://doi.org/10.14201/eks.14032.

Hernández Sánchez, M. L., Cordero Pulido, L. M., Romero Sánchez, E. K., & Mis Linares, C. M. (2024). El avance la inteligencia artificial en la regulación de los neuroderechos. *LATAM Revista Latinoamericana De Ciencias Sociales y Humanidades*, 5(4). https://doi.org/10.56712/latam.v5i4.2291.

Ienca, M. and Andorno, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy*, 13(1). https://doi.org/10.1186/s40504-017-0050-1.

Ienca, M., & Andorno, R. (2017). *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy, 13(1), 5. doi:10.1186/s40504-017-0050-1.

Jalaly Bidgoly, A., Jalaly Bidgoly, H., & Arezoumand, Z. (2020). A survey on methods and challenges in EEG based authentication. Computers & Security, 93, 101788.

Kellmeyer, P. (2021). Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices. *Neuroethics*, 14(1), 83-98.

Kersten, L. (2016). A mechanistic account of wide computationalism. *Review of Philosophy and Psychology*, 8(3), 501-517. https://doi.org/10.1007/s13164-016-0322-3.

Khan, A. A., Laghari, A. A., Shaikh, A. A., Dootio, M. A., Estrela, V. V., & Lopes, R. T. (2022). A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF). *Neuroscience Informatics*, 2(1), 100030.

Lavazza, A. (2018). Freedom of thought and mental integrity: The moral requirements for any neural prosthesis. *Frontiers in Neuroscience*, 12, 82.
Liu, Y., & Chen, Z. (2018). Technological assessment of encryption algorithms for neuroimaging data. *Journal of Information Security*, 27(2), 58-73.

Liu, Y., Huang, H., Xiao, F., Malekian, R., & Wang, W. (2020). Classification and recognition of encrypted EEG data based on neural network. *Journal of Information Security and Applications*, 54, 102567.

Livanis, A., Martinez, G., & Chen, P. (2023). Ethical considerations in brain-computer interfaces. Neuroethics Journal, 14(3), 123-138.

Markosian, C., Taruvai, V., & Mammis, A. (2020). Neuromodulatory hacking: a review of the technology and security risks of spinal cord stimulation. *Acta Neurochirurgica*, 162(12), 3213-3219. https://doi.org/10.1007/s00701-020-04592-3.

Merrill, N. and Chuang, J. (2019). Models of minds. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3290607.3310427.

Müller, V. C. (2009). Symbol grounding in computational systems: a paradox of intentions. *Minds and Machines*, 19(4), 529-541. https://doi.org/10.1007/s11023-009-9175-1.

National Bureau of Standards. (1977). *Federal Information Processing Standards Publication (FIPS PUB) 31: Guidelines for Automatic Data Processing Physical Security and Risk Management*. Washington, D.C.: U.S. Department of Commerce.

Ochang, P., Eke, D. & Stahl, B.C. Perceptions on the Ethical and Legal Principles that Influence Global Brain Data Governance. *Neuroethics* 17, 23 (2024). https://doi.org/10.1007/s12152-024-09558-1.

Patel, R., & Singh, K. (2019). Multi-factor authentication in neuroimaging research: A case study. *Journal of Medical Ethics and Technology*, 21(4), 145-160.

Portillo, J. G., Arbeláez, J. S., Camacho, S., & Cubillos, S. M. S. (2023). Perfil socio familiar y cognición social de un grupo de actores de acoso escolar en una institución educativa del departamento del quindío - colombia. Ustasalud, 22(1).

Pugh, J., Pycroft, L., Sandberg, A., Aziz, T. Z., & Savulescu, J. (2018). Brainjacking in deep brain stimulation and autonomy. *Ethics and Information Technology*, 20(3), 219-232. https://doi.org/10.1007/s10676-018-9466-4.

Pycroft, L., Boccard, S., Owen, S., Stein, J., FitzGerald, J. J., Green, A. L., … & Aziz, T. Z. (2016). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurgery*, 92, 454-462. https://doi.org/10.1016/j.wneu.2016.05.010.

Rainey, S. An Anticipatory Approach to Ethico-Legal Implications of Future Neurotechnology. *Sci Eng Ethics* 30, 18 (2024). https://doi.org/10.1007/s11948-024-00482-4.

Reche Tello, N. (2024). Cuaderno n.º 2. mens iura fundamentalia: la neurotecnología ante la constitución. https://doi.org/10.69592/978-84-1194-394-9.

Resches, M., Serrat, E., Rostán, C., & Esteban, M. (2010). Lenguaje y teoría de la mente: una aproximación multidimensional. *Infancia y Aprendizaje*, 33(3), 315-333. https://doi.org/10.1174/021037010792215136.

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2023). Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing*, 140, 110227.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.

Straw, I., Ashworth, C., & Radford, N. (2022). When brain devices go wrong: a patient with a malfunctioning deep brain stimulator (dbs) presents to the emergency department. *BMJ Case Reports*, 15(12), e252305. https://doi.org/10.1136/bcr-2022-252305.

Sun, Xy., Ye, B. The functional differentiation of brain–computer interfaces (BCIs) and its ethical implications. *Humanit Soc Sci Commun* 10, 878 (2023). https://doi.org/10.1057/s41599-023-02419-x.

Thompson, R., & Lee, P. (2020). Usability analysis of authentication methods. *Journal of Cybersecurity and Usability*, 23(2), 145-160.

UNESCO. (2023, December 8). New report on neurotechnology addresses its advancements and challenges in Latin America and the Caribbean. Retrieved in June 2024, from International Conference on the Ethics of Neurotechnology: https://www.unesco.org/en/articles/new-report-on-neurotechnology-addresses-its-advancements-and-challenges-in-latin-america-and-the-caribbean?hub=85592.

United Nations. (2023, June 6). Urgent need to establish an ethical framework for neurotechnology on an international scale. Retrieved from https://news.un.org/en/story/2023/06/1521747.

Wang, J., Wang, T., Liu, H., Wang, K., Moses, K., Feng, Z., … & Huang, W. (2023). Flexible electrodes for brain–computer interface system. *Advanced Materials*, 35(47). https://doi.org/10.1002/adma.202211012.

Ware, W. H. (1973). *Security controls for computer systems (U): report of Defense Science Board Task Force on computer security*. RAND Corporation.

Zegarra-Valdivia, J. and Vilca, B. C. (2017). Mentalización y teoría de la mente. *Revista De Neuro-Psiquiatria*, 80(3), 189. https://doi.org/10.20453/rnp.v80i3.3156.