IS NIGERIA READY FOR NEUROTECHNOLOGY? A BRIEF LEGAL ASSESSMENT

Kwame-Okpu Aghoghovwia*

Abstract

Nigeria's data protection regime, while robust in many respects, must expand to adequately address neurotechnology and the protection of neural data. Neurotechnology refers to devices that interface with the nervous system for medical, research, or consumer purposes, while neural data are the signals generated through such interfaces and processed to infer neural activity. Neural data can reveal highly sensitive information, including thoughts and health status. It presents privacy risks beyond conventional categories of personal data and challenges traditional notions of privacy. This paper assesses Nigeria's legal readiness for neurotechnology by examining whether existing constitutional and statutory frameworks are sufficient to address the privacy risks posed by neurotechnological applications. The analysis considers the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Nigeria Data Protection Act 2023 and its 2025 Guidelines, the National Mental Health Act, the National Health Act, and the Cybercrimes (Prohibition, Prevention, etc.) Act. The study finds that although these instruments provide a general foundation for privacy and data protection, they contain little to no express recognition of neurotechnology or neural data and lack sufficient interpretive guidance to address the distinctive privacy risks associated with neurotechnological use. As adoption accelerates, these gaps may undermine effective protection. The paper concludes that Nigeria must address the absence of explicit recognition of neurotechnology and supplement its existing framework with targeted interpretive measures. It recommends clarifying the legal status of neural data within Nigeria's data protection regime and adopting incremental regulatory guidance issued by the Nigeria Data Protection Commission.

Key - Words: Data Protection, Privacy, Neurotechnology, Neural Data, Mental Privacy

*LLB (Benson Idahosa University) BL (Lagos), LL.M, Ph.D (Afe Babalola University), Senior Magistrate Gd II, Delta State Judiciary
email:akwameokpu@gmail.com.

1.**Introduction**

In the years since 1973, when Sweden passed the world's first national data protection law,[2] global efforts to safeguard personal data have expanded significantly. As a result, numerous countries across continents have taken steps to protect their citizens' data by enacting data protection laws.[3] Data protection laws define personal data as any information that can be used to identify an individual, directly or indirectly.[4] In addition, these laws create rights for individuals referred to as data subjects, obligations for those who control and process data, as well as sanctions for non-compliance. Data protection law also provides clear guidelines for data subjects to obtain remedies in the event of unauthorised collection and processing of personal data.Data protection law also establishes a special regime for processing special categories of data, like sensitive data and data belonging to vulnerable groups like children.[5] Sensitive data can be data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records, or any additional sensitive personal information that can identify a data subject.

Modern data protection takes many forms, ranging from regulations like the European Union (EU) General Data Protection Regulation (GDPR)[6] to continental treaties like the Malabo Convention[7] to municipal statutes like the Nigerian Data Protection Act of 2023 (NDPA)[8] and sector-specific regulations like the People's Republic of China Regulations on

[2]Swedish Data Act No 289 of 1973. Today Sweden is a part of the European Union and data protection in Sweden is regulated under the General Data Protection Regulation of 2016.

[3].Douwe Korff and Marie Georges, 'The Origins and Meaning of Data Protection' (2020) <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3518386_code1098072.pdf?abstractid=3518386&mirid=1&type=2>accessed 23 November 2025.

[4]Mark Burdon, *Digital Data Collection and Information Privacy Law* (1st Edition, Cambridge University Press 2020) 161.

[5]Gloria González Fuster, The Emergence Of Personal Data Protection As A Fundamental Right Of The EU (Vol 16 *Springer Science & Business* 2014) 63; Kaitlin Asrow and Spirow Samonas, 'Privacy Enhancing Technologies: Categories, Uses Causes and Considerations' <https://bit.ly/3SdbLC5> accessed 24 November 2025.

[6]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) OJ 2016 L 119/1.

[7]African Union Convention on Cyber Security and Personal Data Protection Adopted by the 23rd Assembly of Heads of States and Governments held in Malabo, Equatorial Guinea,June 27, 2014 (Malabo Convention) <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> 23 November.2025.

[8] Nigeria Data Protection Act (NDPA) 2023, Act No. 37 of 2023.

the Protection of Children's Personal Information Online of 2019.[9] The best data protection regimes establish an independent and fully funded supervisory Data Protection Agency/Authority to oversee enforcement[10] and coordination. Today, across jurisdictions, data protection has become a national issue encompassing public and private entities that handle personal data, which requires laws as well as coordinated campaigns for spreading awareness and ensuring implementation.[11]

Despite these milestones and global progress, data protection continues to face pressure from emerging technologies. The next major challenge and arguably the most disruptive is neurotechnology.[12] Therefore, advocates for data protection must not rest on their oars as the next frontier is upon us.

Neurotechnology broadly refers to any device that interfaces with the nervous system (of which the brain is a major component) to monitor and regulate its activity.[13] Neurotechnologies such as electroencephalogram (EEG) headsets, Magnetic Resonance Imaging (MRI) scanners, and brain–computer interfaces (BCIs) now make it possible to collect, decode, and transmit signals to and from the nervous system. These technologies, although useful when applied properly and once confined to laboratories, are increasingly being adapted for education, gaming, leisure, healthcare, workplace monitoring, and even

[9]Regulations on the Protection of Children's Personal Information Online, 2019 <http://www.cac.gov.cn/2019-08/23/c_1124913903.htm> accessed 21 November 2025.

[10]. Fuster (n 5) 262. These agencies are headed by officials known diversely as Commissioner, Chairperson, Ombudsman, or Registrar.

[11] Ewan Sutherland, 'The Governance of Data Protection in South Africa' (2021) <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3922218_code927092.pdf?abstractid=3922218&mirid=1> accessed 23 November 2025; Fuster (n 10); Shawn Marie Boyne, 'Data Protection in the United States', *The American Journal of Comparative Law*, (2018) (66) (1) 29–343 <https://doi.org/10.1093/ajcl/avy016>accessed 23 November 2025; Justin Bryant, 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights' *Stanford Technology Law Review* (2021) (24) (2) 389<https://law.stanford.edu/wpcontent/uploads/2021/05/.BryantAfricaInTheInformationAge.pdf> accessed 23 November 2025.

[12]. Damain Eke, 'Ethics and Governance of Neurotechnology in Africa: Lessons From AI' *JMIR Neurotechnology*.(2024) (3<doi:10.2196/56665> accessed 23 November 2025.

[13]*Ibid*; Rae Silver, and others, 'Neurotech for Neuroscience: Unifying Concepts, Organizing Principles, and Emerging Tools' *Journal of Neuroscience (*2007) (44) (27) 11
807 <https://doi.org/10.1523/JNEUROSCI.3575-07.2007> accessed 23 November 2025; , Shona Haston, and others, 'A Horizon Scan of Neurotechnology Innovations.' *Internatio*
nal Journal of Environmental Research and Public Health (2025) (22) (5) 811 <https://doi.org/10.3390/ijerph22050811> accessed 13 November 2025.

marketing.[14] The data they generate (neural data) and the patterns of neural activity they record (also neural data), can reveal emotions, intentions, and preferences at a level of intimacy previously unimaginable.[15] Therefore, Nigeria must prepare before adoption accelerates any further.

Neurotechnology and neural data raise urgent questions for law and policy. How should such data be classified? Should neural data be classified as a form of sensitive personal data or as a distinct category altogether? What constitutes consent? And how can individuals retain autonomy over their own thoughts in contexts where cognitive activity becomes observable? There are also questions on the ethical use of neurotechnology[16] and whether neural data should be considered an extension of bodily integrity.[17]

When the rise of neurotechnology is considered alongside the advent of Artificial Intelligence (A.I.),[18] we can understand why attention must be drawn to the worrisome reality of a lack of solid governance and regulation in this area. In this regard, UNESCO has sounded an alarm that the convergence of neurotechnology and A.I. presents new challenges with ethical and human rights implications.[19]

Against this backdrop, this paper asks a fundamental question: Is Nigeria legally prepared for the rise and adoption of neurotechnology? While the NDPA and the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (CFRN), provide foundational safeguards, they do not explicitly address neural data or the unique risks associated with neurotechnological systems. This is a critical gap when it comes to neural data-specific safeguards.

[14]Siga Samuel, 'Your brain may not be private much longer' *Vox* (17 March 2023) <https://www.vox.com/future-perfect/2023/3/17/23638325/neurotechnology-ethics-neuro feedback-brain-stimulation-nita-farahany> accessed 13 November 2025; Eke (n 12); Nita A. Farahany, The Battle For Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology (St Martin's Publishing, 2023) 8.
[15]*Ibid.*
[16]Eke (n.11).
[17]Sjors Ligthart, and others, 'Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights'' *Cambridge Quarterly of Healthcare Ethics* (2023) (32) (4) 461–481 <doi:10.1017/S0963180123000245> accessed 1 November 2025.
[18]*Ibid* 462; Farahany(n.13) 5, 8.
[19]United Nations Educational, Scientific and Cultural Organization (UNESCO), 'Ethics of Neurotechnology' <https://www.unesco.org/en/ethics-neurotech> accessed 1 November 2025.

To achieve its target, this paper is divided into sections, the first houses the introduction and provides a general overview of the emergence and concept of data protection, while positioning the advent of Neurotechnology. The next section provides an overview of neurotechnology. Then the paper situates the issue of Neurorights and Neurotechnology within the broader data protection discourse by pointing to the challenges neurotechnology poses to privacy and data protection. Thus, the paper analyses the current legal landscape of data protection in Nigeria and the readiness of existing Nigerian laws to handle the emerging issue of neurotechnology. Thereafter, the current gaps in the legal system are highlighted. Thereafter, the paper makes policy and legislative recommendations based on the findings in the previous section. Finally, the paper concludes by reaffirming the opportunity Nigeria has to lead the continent in regulating this area, as well as stressing the urgency of the situation.

2. Overview of Neurotechnology and Neurorights

Neurotechnology refers to a broad category of devices, tools and systems that measure the structure or function of the nervous system or intervene in its activity.[20] The Organisation for Economic Co-operation and Development (OECD) defines neurotechnologies as devices or procedures that access, monitor, investigate, assess, manipulate, and/or emulate the structure and function of neural systems.[21] In some discourses, neurotechnologies are also referred to as neural interfaces.[22] The core feature of neurotechnology is its ability to transform patterns of neural activity into meaningful information. As noted by the Royal Society,[23] "advances in computational neuroscience and machine learning enable the decoding of intentions, emotions, and mental states

[20]Ligthart and others (n.16) 462; Damain Eke (n 11);UNESCO, 'Ethics of neurotechnology: UNESCO adopts the first global standard in the cutting-edge technology' <https://www.unesco.org/en/articles/ethics-neurotechnology-unesco-adopts-first-global-standard-cutting-edge-technology> accessed 21 November 2025.

[21] Organisation for Economic Co-operation and Development (OECD), 'Neurotechnology Toolkit To support policymakers in implementing the OECD Recommendation on Responsible Innovation in Neurotechnology' (July 2025)<https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf> 21 November 2025.

[22] Nicholas G. Hatsopoulos, and John P. Donoghue. 'The science of neural interface systems.' Annual review of neuroscience (2009) (32) (1) 249-266 <https://doi.org/10.1146/annurev.neuro.051508.135241> 21 November 2025; John P. Donoghue, 'Bridging the Brain to the World: A Perspective on Neural Interface Systems' Neuron, (60) (3) 511 - 521

[23]The Royal Society of London for Improving Natural Knowledge, 'iHuman: blurring lines between mind and machine' <https://royalsociety.org/-/media/policy/projects/Ihuman/report-neural-interfaces.pdf> 21 November 2025.

that were previously inaccessible without verbal or behavioural expression."

Academics have opined that established human rights, such as the rights to bodily integrity, privacy, personal identity, freedom of thought, and protection against discrimination, apply to many conceivable scenarios of neurotechnological use.[24] Similarly, it can be argued that the operation of neurotechnology can be regulated by existing data protection laws.

However, there is considerable proof in the available literature that there have been calls for a widening of existing rights to safeguard neural data since the new millennium, and for the introduction of so-called "neurorights".[25] Neurorights refer to the rights and protections afforded to individuals regarding neural data, mental privacy and cognitive autonomy.[26] In this sense, it is concerned with the following:

1. Protecting neural data from unauthorised access, use, or manipulation
2. Freedom to control one's thoughts, emotions, and behaviours.
3. Safeguards against misuse, exploitation, or unauthorised sharing of brain data.
4. Protection against discrimination based on brain data, neurological characteristics, or cognitive abilities.

2.1 Categories of Neurotechnology

These devices can be grouped into three categories, to wit: those that can monitor and/or record neural activity, those that can intervene in or stimulate neural activity and those that perform both functions.[27] It is important to note that some devices straddle different categories. In use, these devices can be invasive or non-invasive.[28] The invasive kinds are placed or used inside the body, whereas the non-invasive kinds are placed outside of the body. With this understanding, it is important to highlight the current categories of neurotechnologies as follows:

[24] Ligthart and others (n.16) 464.
[25] *Ibid.*
[26] *Ibid.*
[27] Ligthart and others (n.16) 463.
[28] *Ibid*; Ujwal Chaudhary, E*xpanding Senses using Neurotechnology* (Springer 2025)1-23; Benjamin Collins and Eran Klein, 'Invasive Neurotechnology: A Study of the Concept of Invasiveness in Neuroethics' *Neuroethics* (2023) (16)(11)<https://doi.org/10.1007/s12152-023-09518-1> accessed 13 November 2025.

2.1.1 Brain-Computer Interfaces (BCIs)

These devices and systems enable direct communication between the brain and external devices by translating neural signals in the cerebral cortex into commands. The cerebral cortex is the wrinkled, outermost layer of the cerebrum responsible for higher-level functions like consciousness, thinking, memory, and voluntary movement. BCIs can take invasive and non-invasive forms. An example of invasive BCI is the Utah Array, which uses a grid of microelectrodes inserted into the brain, specifically the cerebral cortex to record brain signals and stimulate neurons. These signals can then be translated into commands. Although initially developed for application in visual prosthesis, the translation of signals into commands to and from computers has raised the potential applicability of the Utah Array to now extend to thought-controlled prosthetic limbs and decoding speech from thoughts. It is also used for studying neurological diseases like epilepsy.[29] Non-invasive BCIs have the same application but use electrodes which are woven together to form a web or designed like a cap and then placed on the scalp to record EEG signals. Due to their nature, they are reported to have lower signal quality compared to their invasive counterparts.[30]

Beyond clinical and medical applications, there has been an uptick in the production and marketing of consumer-grade BCI devices for workplace productivity, educational analytics and gaming by companies such as Emotiv.[31] Research has shown that these consumer-grade devices can infer emotional and cognitive states.[32]

[29]Florian Solzbacher, 'Medical Design and Outsourcing;How the Utah Array is advancing BCI science' *Blackrock Neurotech* (31 October 2022) <https://blackrockneurotech.com /insights/how-the-utah-array-is-advancing-bci-science/> accessed 21 November 2025.

[30]José del R Millán, Pierre W Ferrez and Anna Buttfield, 'Non Invasive Brain-Machine Interfaces: Final Report' (Ariadna Study 05/6402, European Space Agency Contract No 19708/06/NL/HE, IDIAP Research Institute) <https://www.esa.int/gsp/ACT/doc/ARI/ARI%20Study%20Report/ACT-RPT-BIO-ARI-056402-Non_invasive_brain-machine_interfaces_-_Martigny_IDIAP.pdf> accessed 21 November 2025.

[31]Emotiv, 'Scientific Research' *Emotiv* (2025) <https://www.emotiv.com/pages/scientific-research> accessed 21 November 2025.

[32]Eke (n11); Ligthart and others (n.16) 470.

2.1.2 Neuroimaging Technologies

These devices and systems use non-invasive technological processes to visualise the nervous system to show its structure and functions. In simpler terms, it is different kinds of scans to reveal images of the nervous system. Beginning with the popular versions like Computed Tomography (CT) scans and MRI scans, to more advanced versions like Functional Magnetic Resonance Imaging (fMRI) and Magnetoencephalography (MEG).

An fMRI is performed with the patient lying down in a large scanner, which measures blood-oxygen responses in the brain to decode visual imagery, map decision making and infer preferences and emotional reactions.[33] Similarly, a Magnetoencephalography (MEG) is performed by a non-invasive helmet-shaped brain imaging device that measures the magnetic fields produced by electrical activity in the brain. The captured magnetic signals allow researchers to map neural activity with high temporal and spatial resolution. The MEG reveals more accurate readings than the EEG.

There is also the Functional Near-Infrared Spectroscopy (fNIRS), which is a portable, non-invasive neuroimaging technique that uses near-infrared light to measure blood oxygenation in the brain.[34] Neural activity is detected by the change in the near-infrared light.

While neuroimaging is often used to study neurological disorders, cognitive processes, and brain function, it has started to find applications outside medicine. This is often the case with technology in general, where inventions find applications outside the field they were originally developed for. This phenomenon is often referred to as technology transfer or technology spin-offs. As a result, smaller wearable fNIRS devices are currently used in neuromarketing to measure consumer preferences[35] and in the field of product design to figure out which

[33]Peter A Bandettini, 'fMRI: Blood Oxygen Level-Dependent Contrast and Its Value for Understanding Functional Brain Networks' in V.A Diwadkar and S.B Eickhoff (eds), *Brain Network Dysfunction in Neuropsychiatric Illness* (Springer, 2021) 19–44 <https://link.springer.com/chapter/10.1007/978-3-030-59797-9_2>accessed 21 November 2025; Ligthart and others (n.16).

[34]Eleonora Gentile and Antonio Casas Barragán, 'EEG/fNIRS' in Massimiliano Valeriani ans Marina de Tommaso(eds) *Neuromethods* (Springer, 2023) 181–202 <https://link.springer.com/protocol/10.1007/978-1-0716-3545-2_9> accessed 21 November 2025.

[35]Shinya Watanuki, 'Identifying distinctive brain regions related to consumer choice behaviors on branded foods using activation likelihood estimation and machine learning' *Frontiers in Computational Neuroscience* (2024) (18) 1310013 <https://pubmed.ncbi.nlm.nih.gov/38374888/> accessed 21 November 2025.

designs trigger reward or stress responses.[36] In educational research, it is used to study learning, attention and memory patterns. Currently, it is also used by some employers to monitor employees' fatigue, attention, and cognitive load, with the aim of optimising performance.[37] This raises concerns about privacy, consent, and potential misuse of neural data.[38]

2.1.3 Neurostimulation Technologies

Neurostimulation refers to technologies that deliver electrical, magnetic, or ultrasonic energy to targeted areas of the nervous system to either activate, inhibit, or modulate neural activity.[39] Technologies for neurostimulation can either be invasive or noninvasive, and they are used to treat various conditions such as movement disorders (tremors, Parkinson's disease), chronic pain, and depression.[40] Major examples of neurostimulation devices are Transcranial Magnetic Stimulation (TMS), Transcranial Electric Stimulation (TES), and Deep Brain Stimulation (DBS).

TMS is non-invasive, and it is done by placing a handheld coil with copper windings over the scalp so as to generate a magnetic field that induces an electric current in the brain. The transcranial electric stimulation is also non-invasive, and it involves the use of electrodes in a cap-like design to deliver direct and alternating electrical currents to the brain. DBS is an invasive process, and it involves surgically implanting electrodes deep in the brain and pulse generators under the collarbone.[41] The electrodes deliver a mild electrical current directly to the brain. The purpose is to use the current to improve how those parts of the brain work by stimulating the brain cells in that area, which may have become

[36]Sujin Bak, and others 'Analysis of consumer purchase intentions using functional near-infrared spectroscopy (fNIRS): A neuromarketing study on the aesthetic packaging of Korean red ginseng products.'(2005) *PLoS ONE*, (20) (6) e0326213. <10.1371/journal.pone.0326213> accessed 19 November 2025.

[37] Muhl Ekaterina , Andorno Roberto, 'Neurosurveillance in the workplace: do employers have the right to monitor employees' minds?' *Frontiers in Human Dynamics* (2023) (5) <10.3389/fhumd.2023.1245619> accessed 19 November 2025; Ligthart and others (n.16) 464.

[38]*Ibid.*

[39]Science Direct 'Nuerostimulation'<https://www.sciencedirect.com/topics/medicine-and-dentistry/neurostimulation>accessed 19 November 2025; Christine A. Edwards and others, 'Neurostimulation Devices for the Treatment of Neurologic Disorders.' (Mayo Clinic proceedings, 2017)) 1427-1444. <doi:10.1016/j.mayocp.2017.05.005> accessed 19 November 2025.

[40]Edwards *Ibid*; Pain Management Specialist 'Types Of Neurostimulation Devices & Treatments' <https://painandspinespecialists.com/types-of-neurostimulation-devices-and-treatments/> accessed 19 November 2025.

[41]Cleveland Clinic, 'Deep Brain Stimulation' <https://my.clevelandclinic.org/health/treatments/21088-deep-brain-stimulation> accessed 19 November 2025.

inactive due to a medical condition.[42]Like other neurotech devices, those under this heading are also finding use outside medical and clinical purposes, for cognitive enhancement, gaming and virtual reality immersion, treatment of fatigue and mood regulation.[43]

3.**Privacy,Data Protection and Challenges Posed by Neurotechnology**

The fulcrum of privacy in the Human Rights context is that individuals be 'let alone'.[44] As Westin put it, privacy is 'the claim of an individual to determine what information about him or herself should be known to others.'[45] In addition to this 'right to be let alone', privacy is also conceptualised along the following categories, namely: limited access to the self, secrecy, control of personal information, personhood and intimacy.[46] Whatever category a definition of privacy falls into, the power an individual has to decide what happens to himself is one of the themes that runs through all definitions.[47] It is upon this accepted notion that privacy came to protect bodily autonomy and serve as the basis for data protection.[48]

Data protection emerged to address the intricacies of privacy issues raised by developments in ICT, which were beyond the contemplation of early privacy protection laws as contained in preexisting rules and

[42]*Ibid.*

[43]Ligthart and others (n.16) 464.

[44]. Samuel D Warren and Louis Brandeis, 'The Right to Privacy' Harvard Law Review (1890) (4) (5) 193-220 <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf >accessed 6 November 2025. While the authors popularized this phrase, they were not the ones to coin it, that recognition goes to Thomas Cooley who had done so in 1879. Thomas M Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Callaghan 1879) 29

[45]. Alan Westin, 'Social and political dimensions of privacy' *Journal of Social Issues* (2003) (59) (2) 2.

[46]. DJ Solove, 'Conceptualizing privacy' *California Law Review* (2002) (90) (4) 1132-1140, 1094

[47]. For more definitions of privacy, please see; MR Konvitz, 'Privacy and the Law', *Law and Contemporary Problems* (1966) (31) (2) 272-286; Jozsef Hajdu, *Protection of the Privacy rights of Employees* (Elemer Polay Foundation 2005) 8; Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008); Alan Westin, *Privacy and Freedoms* (IG Publishing 2018); Yinka Olomojobi 'Right to Privacy in Nigeria' *SSRN* (2017) https://dx.doi.org/10.2139/ssrn.3062603> accessed 25 November 2025; Bert-Jaap Koops and Maša Galič 'Unity in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions' *South Carolina Law Review* (2021) (73) (2) 1-36

[48]. Orla Lynskey, 'Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order' *International and Comparative Law Quarterly* (2014) (63) (3) 569-597.

provisions on privacy.[49] Although an offshoot of the right to privacy with considerable overlaps, data protection diverges from the right to privacy because it sets legal bases for collecting and processing personal data in technical ways. In contrast, the right to privacy, in a strict sense, is oriented towards protecting the home, family life, and correspondence from intrusion.[50] For example, recording personal information without doing anything further cannot be considered an intrusion into personal space. However, this activity involves collecting personal data and is within the ambit of data protection.[51] Situations such as this motivated Lynskey to state that data protection offers individuals more rights over more types of information than the right to privacy when applied in processing personal data.[52]

Data protection also regulates the legal ability of an individual to determine what personal data in an ICT system can be shared with third parties.[53] Furthermore, it is used as a phrase to designate the laws which protect personal data.[54] While the phrase "data protection" is popular due to European influence, personal data protection has also developed in the United States of America (hereinafter the USA) under the nomenclature of information privacy.[55]

As highlighted earlier in this paper, the challenge posed by neurotechnologies to human rights is primarily because it creates new

---

[49]. Adrienn Lukacs, 'What Is Privacy? The History and Definition of Privacy' (2016)<http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> accessed 17 November 2025

[50]Raphael Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection', *Computer Law and Security Review,* (2013) (29) (5) 522-530 <https://works.bepress.com/serge_gutwirth/107/> accessed 7November 2025; Jan Holvast, 'History of Privacy' in Matyáš V *et al* (eds),*The Future of Identity* (Springer 2009) 14,28.

[51]Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (PhD Thesis, Faculty of Law University of Pretoria 2016)
<https://repository.up.ac.za/bitstream/handle/2263/53129/Abdulrauf_Legal_2016.pdf?sequence=1> accessed 3 November 2025.

[52]Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 90.

[53]Privacy International, 'A Guide for Policy Engagement on Data Protection Part 1: Data protection, explained' <https://privacyinternational.org/sites/default/files/2018-0monitor 9monitormonitor/Part%201%20-
%20Data%20Protection%2C%20Explained.pdf>accessed 5 November 2025.

[54]*Ibid.*

[55]B Garbin and K Staunton and M Bourdon, 'Tracking Legislative Developments in Relation to "Do Not Track" Initiatives' in MG Michael and K Michael *(*eds), *Uberveillance and The Social Implications Of Microchip Implants: Emerging Technologies* (IGI Global, 2014) 235-259; Lynskey, (n.51)26.

forms of collecting, processing, sharing, manipulating, influencing, and storing information about individuals which were previously private and inaccessible. These include thoughts, intentions, emotions and cognitive states. This creates questions that were not within the contemplation of lawmakers when the current Human Rights laws were enacted.[56]
For example, privacy traditionally protects the individual from physical or tangible intrusion, but neurotech can infringe upon privacy through intangibles like attention, emotion, stress, and intention. Let us also consider the freedom of thought, which is a right guaranteed globally in statutes, conventions and treaties.[57] Neurotechnology poses a threat to this because devices can sense what a person is thinking, and this creates possibilities for interfering with (either by changing or correcting) the thought held by that person. Also, neurotech is used to assess cognitive ability, and this raises concerns because it can be used to sort people based on neurological differences, which can be the basis for discrimination based on those differences.[58] With the continued use of neurotechnology in the workplace, one can envisage a future of excessive productivity monitoring and tracking, which can lead to coercive consent and power imbalance between employees and employers, where the latter can infer the mental state of the former indiscriminately.

Any discussion on challenges to Human Rights is incomplete without mention of how children will be affected. On this issue, children are an especially vulnerable group because their brains are still developing and they are unaware of the long-term risks when they engage with neurotech, for example, playing video games with a BCI.

In the area of criminal justice and due process, neurotechnology poses a serious challenge. In India, EEG-based tools are used during investigations by the police, with the results used to generate leads, corroborate findings, and screen suspects.[59]Although such evidence has not been admissible in Indian courts since 2010, there are a handful of court judgments in which brain tests appear to have influenced judges'

[56]Ligthart and others (n.16).
[57]Freedom of thought is guaranteed under Art 18 of the Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217A(III))and Art 18 (1) International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.
[58]Ligthart and others (n.16) 467.
[59]Jonathan Moens, 'Indian police are trying to "read minds" of suspects, over neuroscientists' objections', *Science* (7 May 2025) <https://www.science.org/content/article/indian-police-are-trying-read-minds-suspects-over-neuroscientists-objections#> accessed 7 November 2025.

decisions about whether suspected rapists and others should be released on bail.[60] This has raised concerns about coerced participation and violation of mental privacy. Specifically, it risks compelling the mind to 'testify', which undermines the principles of fair trial, specifically the right against self-incrimination. In the United States, defence lawyers have tried to use brain scans in conjunction with the insanity defence to argue for diminished responsibility.[61] Both of these examples combine to show how neurotech can become a legal tool.

There is also the matter of what den Hoven describes as 'informational injustice'.[62] This happens when personal information provided in one sphere or context (for example, healthcare) may change its meaning when used in another sphere or context (such as commercial transactions). Informational injustice may lead to discrimination and disadvantages for an individual through targeted adverts, targeted disinformation, or misuse, for example, by employers who may use online information to avoid hiring certain groups of people.

Some of these challenges are present while others will materialise in the near future as we continue to witness the growth of and adaptation of different forms of neurotechnology, coupled with A.I, the expansion of telemedicine and increased private sector interest. In the African context and specifically in Nigeria, most of these technologies are not built with us in mind,[63] and if we continue to import them without the necessary legal framework or sensitisation to guide usage, we run the risk of

[60]*Ibid*; D.A Puranik and others, 'Brain Signature profiling in India. It's status as an aid in investigation and as corroborative evidence – as seen from judgments.' (Proceedings of XX All India Forensic Science Conference, Jaipur, November 15 – 17 2009) 815 – 822 . <https://axxonet.pro/wp-content/uploads/2019/06/BEOS_IN_CASES.pdf> accessed 7 November 2025.

[61]Michael J. Vitacco, and others, 'Neuroscience and the insanity defense: Trying to put a round peg in a square hole' *Forensic Science International: Mind and Law*, (2024) (5) 100131 <https://doi.org/10.1016/j.fsiml.2024.100131> accessed 3 November 2025.; Susan E. Rushing 'The Admissibility of Brain Scans in Criminal Trials: The Case of Positron Emission Tomography' *Court Review: The Journal of the American Judges Association* (2014) (494) 62 <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1464&context=ajacourtreview> accessed 3 November 2025.

[62] J Van den Hoven, 'Information technology, privacy, and the protection of personal data', in J Van Den Hoven and J Weckert (eds), *Information technology and moral philosophy* (Cambridge University Press 2008) 301–322.

[63]Eke (n.11); Cris Micheli, Jacopo Micheli and Maurizio Compiani, 'An Introduction to Neurocolonialism: A Challenge for Emerging Economies Like Nigeria' in Ikechukwu Anthony Kanu, Timothy Dokpesi Adidi, Catherine Chiugo Kanu, Philip Osarobu Isanbor (eds), Philosophy of Entrepreneurship: Intersections and Insights (Veritas University Press, 2025) 17.

playing catch-up and having a reactive body of laws on the subject matter.

4.Examination of the Current Framework for Neurorights Protection In Nigeria

Nigeria has a rapidly expanding tech sector (inclusive of neurotech), and although neurotechnology adoption (asides the use of CT Scans and MRI scans) is still at a nascent stage, a rapidly expanding tech sector means we can expect an uptake. Currently, there are fewer than a handful of registered neurotech or neuroscience-adjacent startups/projects in Nigeria, and there is a possibility that we might witness more in the near future. These include AI-enabled health tools and cross-border neurotechnology partnerships.[64] All of these make it more important to consider, from a legal aspect, how ready Nigeria is for neurotechnology.

4.1 The Constitution of the Federal Republic of Nigeria 1999 (as amended)

Section 37 of the CFRN guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. Despite the somewhat archaic wording about telegrams and other outdated technologies,[65] the provisions of Section 37 have been expanded upon by the courts and by laws to address privacy in the modern context. Before the advent of the NDPA and its precursor, the Nigerian Data Protection Regulations,[66] the courts had to consider and interpret the scope of this provision in light of the more modern concept of privacy. In one of such instances, in the case of *Incorporated Trustees of Digital Rights Lawyer Initiative v The National Identity Management Commission,*[67] the court commented that the right a person has to privacy as provided for in section 37 CFRN also includes the protection of personal information from others. And that, 'This right to privacy is not limited to his home but extends to anything private and personal to him, including communication and personal data.'

Section 37 of CFRN has served as the constitutional anchor for statutory data protection initiatives, including the NDPA. In the context of neurotechnology, the protection it offers will, in practice and by inference, extend to neural data, as such data constitutes personal

[64]Eke (n.11) 4.
[65]C Izuogu, 'Personal Data Protection in Nigeria' *World Wide Web Foundation* (2018) <https://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf> accessed 28 November 2025.
[66]Nigeria Data Protection Regulation of 2019 (NDPR) which has been repealed by the Nigeria Data Protection Act General Application and Implementation Directive (GAID), 2025.
[67]Unreported Suit No. AB/83/2020.

information belonging to and capable of identifying an individual. However, having to infer rather than having a direct protection creates uncertainty and creates a scenario where the courts may have to state explicitly that Section 37 covers neural data.

The CFRN also guarantees the right to the dignity of human persons and freedom of thought, conscience and religion in Sections 34 and 38, respectively. Research[68] shows that neuroethics increasingly links human dignity to protection against intrusive neurotechnological interventions, especially those capable of manipulating cognition or emotional states. Similarly, comparative scholarship suggests that freedom of thought may form a constitutional basis for protecting cognitive liberty in the face of advancing neurotechnologies.[69] While Nigerian jurisprudence has not yet applied Section 34 or 38 to neurotechnological contexts, it could support emerging arguments[70] against coercive or exploitative uses of neurotechnology, particularly in workplaces, law enforcement, or healthcare.

4.2 The Nigerian Data Protection Act

The Nigeria Data Protection Act[71] (NDPA) was passed in 2023 to replace the Nigeria Data Protection Regulation of 2019 (NDPR), which until then was the primary legal regulation for data protection in Nigeria. The NDPA establishes a comprehensive framework for the processing and safeguarding of personal data processed in Nigeria, or that of a data subject in Nigeria, where processing occurs outside Nigeria.[72]

The NDPA mandates that all processing be lawful, fair, and transparent. It protects all personal information, including sensitive data and requires explicit consent, purpose limitation, data minimisation, and robust security measures for processing. Key provisions include the appointment of a certified Data Protection Officer, mandatory Data Protection Impact Assessments (DPIAs) for high-risk activities, strict cross-border transfer rules, and enhanced rights for data subjects.[73]

Personal data is defined in Section 65 of the NDPA as any information relating to an identified or identifiable natural person. The Act also covers biometric data[74] which it defines to include personal data

[68]Ligthart and others (n.16) 462, 467.
[69]*Ibid.*
[70]Ligthart and others (n 16) 465-466.
[71]Nigeria Data Protection Act (NDPA) , Act No 37, Volume 110, No. 113, 2023.
[72]*Ibid* s 2 (2) (a) - (c).
[73]*Ibid* s 28, Part VI and Part VIII.
[74]*Ibid* s 65.

resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual. Under the NDPA, these specific technical processes include but are not limited to physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis.[75]

The NDPA classifies personal data as sensitive[76] if it relates to an individual's genetic and biometric data and if it reveals race or ethnic origin, religious or similar beliefs, reflects conscience or philosophy, health status, sex life, political opinions or affiliations and trade union memberships.[77] As an added level of security, the NDPA in Section 30 (1) generally prohibits the processing of sensitive personal data, allowing it only in clearly defined situations. Such as where the data subject has given valid consent for specific purposes,[78] where it is necessary to fulfil obligations or exercise rights under employment or social security laws,[79] or where it is required to protect the vital interests of the data subject or another person when consent cannot be given.[80]

The Act also permits the processing of sensitive data in specific organisational and legal contexts. These include processing carried out by non-profit organisations in the course of their legitimate activities, provided it relates to members or persons in regular contact with the organisation and is not disclosed externally without consent.[81] Processing is further allowed where it is necessary for legal advice, legal proceedings, or the establishment, exercise, or defence of legal claims.[82] In addition, sensitive personal data may be processed where it is required by broader public or societal needs and supported by law. This covers processing for substantial public interest, public health, medical care, or community welfare by professionals bound by confidentiality, as well as processing for archiving in the public interest or for historical, statistical, or scientific research, provided appropriate safeguards are in place.[83]

---

[75]*Ibid.*
[76]*Ibid.*
[77]S.30 (2) (a) of the NDPA, gives the NDPC the authority to prescribe other categories of personal data as sensitive personal data.
[78]. NDPA s 30 (1) (a).
[79]. *Ibid* s 30 1 (b).
[80]. *Ibid* s 30 1 (c).
[81]. *Ibid* s 30 (1) (d).
[82]*Ibid* s 30 (1) (e).
[83]*Ibid* s 30 (1) (f) - (i).

In line with best practices, the NDPA established the Nigeria Data Protection Commission (NDPC),[84] and charged it with overseeing the implementation of the NDPA. The NDPC is also empowered to issue guidelines and can impose administrative sanctions on defaulters. Penalties range from fines of up to ₦10 million (or 2 % of annual turnover, whichever is higher) for minor breaches to ₦50 million (or 4 % of turnover) for serious violations, plus possible revocation of licences.[85] The NDPC also handles complaints, conducts audits, and can issue enforcement notices to ensure adherence to the NDPA. In administering the NDPA, the NDPC is empowered to issue regulations and codes of practice.[86]

In March 2025, the NDPC issued the Nigeria Data Protection Act General Application And Implementation Directive (GAID) pursuant to Section 37 of the CFRN and Sections 1(A), 6(C), 61 & 62 of the NDPA.[87] The directive became effective on the 19th of September 2025. In reality, it is an addendum to the NDPA with 52 articles and 10 schedules. Some of them expand on issues already provided for under the NDPA, while others tackle fresh topics like A.I, internet of things (IoT) and 'emerging technologies' which the NDPA is silent on.[88] The GAID has been described as operationalising the NDPA with precision and authority.[89]

The following is a cursory look at some of the key provisions in the GAID.

i. Expanded duties for data protection officers (DPO)
ii. Stricter rules for cross-border transfer of personal data
iii. DPIAs are made mandatory for high-risk processing (profiling, automated decision-making, sensitive data, etc.) and processing by new technologies/techniques or directives which mandate the processing of personal data on a large scale, and the assessment must be signed by a certified DPO.

[84] *Ibid* s 1(g), s 4.
[85] *Ibid* s 46.
[86] *Ibid* ss 3 (4), 42 (5).
[87] See Authority and Preamble to Nigeria Data Protection Act – General Application and Implementation Directive (GAID) 2025. NDPC/NDP ACT-GAID/01/2025.
[88]. The GAID generally aims to tighten oversight, raise compliance costs for large data handlers, and further align Nigeria's data protection framework with global standards
[89]. Patience Aliu, 'GAID 2025 Takes Effect: A New Data Privacy Compliance Era for Nigeria Businesses' *Businessday* (*30, September 2025) 12 <https://drive.google.com/file/ d/1gl2WmsQVh9rB5VtYgReRdrv5rtyV-IaK/view>*accessed 2 November 2025

iv. Storage limitation: Personal data generally cannot be kept longer than six months after the purpose for collection is fulfilled, unless a lawful exception applies .
v. Safeguards for vulnerable data-subjects: There is the introduction of extra protections for the young, elderly, disabled, financially distressed, or low-literacy individuals.
vi. Legitimate-interest assessment (LIA): Controllers must conduct a LIA when relying on legitimate interest as a lawful basis for processing personal data.
vii. Standard Notice to Address Grievance (SNAG): Data subjects can issue notices to lodge complaints directly with controllers/processors, which must respond within the stipulated time frame.
viii. Repeal of NDPR 2019: The GAID officially repeals the NDPR and its 2020 Implementation Framework, but provides that actions taken under the old regime remain valid.

While there is no express mention of neurotechnology and neural data within the NDPA and GAID. Several provisions easily come to mind as at least providing implicit and incidental protection.
For starters, one can argue that neural data is health data and therefore some level of protection already exists within the NDPA, which classifies personal data relating to an individual's health status as sensitive.

However, the NDPA is silent on what constitutes health data, and as this paper has shown, neurotech is increasingly finding usage outside of health and clinical contexts. So, neural data generated by consumer BCI and EEG devices, workplace monitoring systems, or educational tools may fall outside traditional health data interpretations, leaving regulatory gaps.
Another level of protection may also reside within the NDPA[90] and GAID[91], requiring controllers to first carry out DPIAs where (i) the processing of personal data may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes. And (ii) where processing is by new technologies/techniques or directives which mandate processing of personal data on a large scale. Due to their nature, neurotechnological processes, which clearly involve new or innovative data processing mechanisms, are likely candidates to undergo such an assessment. So in practice, this could serve as a safeguard.

[90]S 28 (1) NDPA.
[91]Art 28 GAID.

GAID goes further in Article 43 to require that data controllers, considering the deployment of Emerging Technologies (ETs) such as AI, blockchain, or IoT, must take into account the NDPA, public policy, and comply with technical and organisational safeguards to protect data subjects. Neurotechnologies can be classified or understood as "emerging technologies" in this provision, especially when they involve AI, predictive analytics, or BCIs. So this is another safeguard that could function in practice. Thus, even without a specific mention of neurotechnology or neural data, the NDPA and the GAID indirectly regulate neurotechnology.

4.3 The National Mental Health Act

The National Mental Health Act (MHA)[92] of 2021 is primarily focused on promoting, protecting, and regulating mental health care in Nigeria through a rights-based framework. It seeks to ensure access to mental health services, protect the dignity and autonomy of persons with mental health conditions, and prevent discrimination, abuse, and inhumane treatment.[93] Key provisions address voluntary and involuntary admission, consent to treatment, confidentiality, community-based care, and the integration of mental health into primary healthcare,[94] as well as provisions on persons with mental health and criminal proceedings.[95]

The Act introduces important innovations, including the formal recognition of the rights and protection of persons in need of mental health services.[96] The Act also emphasises a shift away from archaic models of care to modern and integrated mental health treatment.[97] The Act also establishes oversight mechanisms[98] to ensure accountability and standards in mental health facilities.

With regards to privacy and data protection, the Act provides implicit but significant safeguards by emphasising confidentiality of mental health information, informed consent, and respect for personal autonomy, which together function as protections for highly sensitive personal data. With specific regards to neurotechnology, section 37 of the MHA prohibits a person or institution from the performance of electroconvulsive therapy (ECT), psychosurgery and other irreversible treatments, where it is not in the best interest of the person with a mental

[92] National Mental Health Act (MHA), Act No. 46 Vol 109, 229 2021.
[93] *Ibid* ss 1 and 12.
[94] *Ibid* ss 5 (i), 21, 24 (5), 26 – 28.
[95] *Ibid* s 46.
[96] *Ibid* ss 12-23.
[97] *Ibid* s 24.
[98] *Ibid* s 11.

health condition except (a) with a valid license ; (b) with the informed consent of the person with mental health condition and (c) in accordance with the prescribed clinical guidelines. Section 38 also prohibits using a person with a mental health condition for teaching, experimentation or research purposes except in accordance with the National Health Act and the National Code on Health Research Ethics.

The MHA in Section 5 establishes a Department of Mental Health Services in the Federal Ministry of Health to supervise compliance and service delivery. The MHA also provides for sanctions and penalties for violations of rights[99] or breach of duties imposed on mental health practitioners and institutions,[100] thereby reinforcing accountability and the protection of fundamental rights within Nigeria's mental health framework.

4.4 National Health Act

The National Health Act of 2014 (NHA) lays the guidelines for the management, development, and control of a national health system and establishes requirements for providing healthcare in Nigeria.[101] It regulates users of health services, healthcare personnel and health establishments in Nigeria.[102] A user of a health service is a person receiving treatment in a health establishment or using a health service. Health establishments are obliged to maintain health records, with examination, disclosure and access granted only on certain grounds.[103] Although the NHA does not explicitly define what constitutes health records, Section 26 (1) provides that all information concerning a user, including information relating to health status, treatment or stay in a health establishment, be kept confidential.

Information relating to health status is clearly personal data, and when the provisions of the NDPA are taken into consideration, they are afforded an extra layer of protection because they further qualify as sensitive personal data. This points to the importance of the NHA in data protection discourse in Nigeria. The NHA does not use the term neurotechnology, but it has provisions that regulate the construction, quality, use and development of new applications of "health

[99] *Ibid* s 51.
[100] *Ibid* 2 52- 55.
[101] National Health Act (NHA), Act No. 8 of 2014 s 1.
[102] Technology Advisors, 'Keeping Personal Health Information Safe and Secure: A guide to privacy and data security laws in nigeria' (2015) <https://ehealth4everyone.com/wp-content/uploads/2016/01/Nigeria-Health-Data-Security-Guide.pdf> accessed 1 November 2025
[103] NHA s 25, s 28 and s 29.

technology".[104] Health technology is defined under the Act as machinery or equipment that is used in the provision of health services. Neurotechnology is certainly a kind of health technology, and this provision captures it even though it is limited to the use of these technologies in health services. In operation, the NHA will apply to neurotechnology used for the provision of health services, and it can be argued that it will govern how neural data (in the form of health status) is stored and who can access it. However, it must be noted that even though the NHA mentions "health technology," it does not do the following:

A. Define or expressly recognise neural data as a distinct category;
B. Address mental privacy, cognitive autonomy, or inferred mental states;
C. Regulate non-health uses of neurotechnology (workplace, education, consumer devices);
D. Provide rules on the analysis of neural data.

The emphasis of the NHA is on the tool, not the data or the nervous system. So, although it provides a framework for assessing the safety and quality of health technologies, its focus remains on governing these technologies and service delivery, leaving questions of neural data protection and mental privacy to be addressed under Nigeria's data protection regime.

4.5 Cybercrimes (Prohibition, Prevention, etc.) (Amendement) Act

The Cybercrimes (Prohibition, Prevention, etc.) Act was passed into law in 2015 and amended in 2024. While national cyber security forms part of the motivations behind the passing of the law in 2015, the law also sought to answer repeated calls for legislation to tackle offences committed against and through computer systems.[105] Nine years later, in response to evolving threats, the need to correct omissions in the 2015 Act and with the aim of strengthening the legal framework for combating cyber crimes, an amendment was passed in the form of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act of 2024.

The Cybercrimes Act in its current form, criminalises offences[106] that can be committed with and through information systems, these include identity theft, publishing/making false and misleading posts,

[104] *Ibid* ss 12, 13, 19 and 64.
[105] BO Awoyemi and OA Omotayo and J Mpapalika, 'Globalization and Cyber Crimes: A Review of Forms and Effects of Cyber Crime in Nigeria' *International Journal of Multidisciplinary Research and Modern Education*, (2021) (7) (1) 18-25.
[106] Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act of 2024 (Cybercrimes Act) part III.

impersonation, computer-related fraud and forgery, wilful misdirection/interception of electronic communications, and electronic money transfers. The Cybercrimes Act also mandates service providers who are dealing with subscriber information for law enforcement purposes, to do so in accordance with the provisions of the NDPA.[107] As a result of its cyber security motivations, and the need to curb the trend of offences committed through information systems, which often involve the manipulation of personal information and violation of data privacy,[108] the Cybercrimes Act is situated in the intersection between security and personal data. Flowing from the above, the Cybercrimes Act will apply where neurotechnology systems are hacked, or neural data is unlawfully accessed.

Although the Cybercrimes Act strengthens Nigeria's cybersecurity regime, it does not expressly address neurotechnology or neural data. Its focus remains on unlawful access and cyber offences rather than the privacy implications of lawful but sensitive data processing. As a result, even in its amended form, the Act offers no direct regulatory response to the mental privacy or cognitive autonomy concerns raised by neurotechnological applications.

5. **Challenges to Nigeria's Legal Readiness for Neurotechnology**

Nigeria's legal framework provides important foundational protections, particularly through the CFRN, the NDPA and the MHA. However, these laws were not designed with neurotechnology in mind and therefore do not explicitly recognise neural data or mental privacy. As neurotechnology develops, this absence creates uncertainty regarding classification, consent, enforcement, and accountability.

With the coming into force of the NDPA in 2023, Nigeria joined the ranks of countries with comprehensive data protection laws, and the addition of GAID in 2025, with its provision on emerging technologies and mandatory DPIAs, Nigeria now has detailed operational guidance that brings its legal framework closer to global standards.[109]
Despite this progress, significant gaps remain, and challenges to adequate regulation of neurotechnology have emerged, primarily because neurotechnology has a complex, technical, and constantly evolving

[107] *Ibid* S 38 (1).
[108] JL Hernández-Ramos *et al*, 'Toward a data-driven society: A technological perspective on the development of cyber security and data-protection policies' *IEEE Security & Privacy* (2019) (18) (1) 28-38.
[109] Aliu (n.88).

nature where innovation can outpace regulation.[110] This means that gaps stem not from a complete absence of legal protection, but from the fact that current laws were designed for existing/conventional data-processing contexts and did not anticipate the distinctive characteristics of neurotechnology and neural data. This section identifies the key legal and regulatory challenges Nigeria faces as neurotechnology develops.

5.1 Absence of Explicit Recognition of Neural Data

Under Nigerian law, there is no explicit reference, recognition or definition of neural data. The definition of personal data under Nigerian law is any data that can identify an individual.[111] While this broad definition can be said to reasonably encompass neural data where such data identifies an individual, the situation is not ideal. Also, for neural data to qualify for protection as sensitive personal data as 'health records', it would require that neural data be processed within healthcare contexts. The fact that protection of neural data has to be read implicitly into existing legal provisions offers limited practical guidelines for regulators, data controllers and data subjects.

With the absence of an explicit reference, classification and definition of neural data, there is the possibility that neural data processed outside healthcare contexts, for example, using consumer EEG headsets or workplace monitoring tools, may fall into regulatory grey areas.

5.2 Lack of Legal Protection for Mental Privacy and Cognitive Autonomy

As mentioned earlier, Nigeria's constitution guarantees the individual's privacy, dignity and freedom of thought. These are traditional notions of privacy and autonomy, which are challenged by advancements in technology and updated by the more sophisticated notion of data protection.[112] Neurotechnology challenges both of these notions by enabling access to mental processes without outward communication or visible interference/intrusion. It bears reiterating that privacy developed as an antidote to the action of physical/visible intrusion/interference into personal space.[113] Unlike conventional information or even personal data, neural data can be collected subconsciously without the individual's

[110]A. Shaji George, 'Protecting Brain Privacy in the Age of Neurotechnology: Policy Responses and Remaining Challenges.' *Partners Universal Innovative Research Publication,* (2024) (2) (5), 18–33 <https://doi.org/10.5281/zenodo.13942131> accessed 3 November 2025.
[111]See s 65 NDPA.
[112]Gloria Adeola-Adedipe and Prudence Okparavero, 'Data Protection and the Right to Privacy in the Digital Era: A Complex Twin' *African Journal of Law and Human Rights* (2022) (6) (1) 14-22.
[113]Warren and Brandeis (n.43).

awareness or an overt intrusion. This challenge has given birth to new notions and safeguards like mental privacy, mental integrity, and cognitive liberty/freedom.[114] These notions currently drive the relationship between neurotechnologies and human rights as well as debates in this area.[115]

In Nigeria, the absence of express legal safeguards for mental privacy and cognitive liberty means that individuals may have limited recourse where neural inferences are drawn from their data, even if no overt data breach occurs. Therefore, existing privacy and data protection frameworks are ill-suited to protect against intrusions into the mental domain.

5.3 Challenges to Meaningful Consent

Consent is the bedrock of data protection, and it is no different under Nigerian law, where it forms the first of the lawful bases of personal data processing.[116] Consent is simple, it is an individual's freely given, specific, informed, and unambiguous indication where he agrees to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent.[117] Nevertheless, neurotechnology complicates things because neural data processing often involves complex inference mechanisms that are not easily understandable to data subjects. As a result, consent given and obtained for neurotechnology applications, particularly in consumer, workplace, or educational settings, may fail to meet the threshold of being fully informed. Nigerian law currently offers no neurotechnology-specific consent standards to address this challenge.

5.4 Weaknesses of Neurotechnology Specific Risk Assessment Frameworks

Before the entering into force of the GAID, there was an absence of detailed, binding risk assessment guidance on new and emerging technologies comparable to that issued by the European Data Protection Board (EDPB).[118] As noted earlier, the GAID, specifically in Articles 28 and 43, significantly strengthens risk-based data protection in Nigeria.

These provisions bring Nigeria closer to international best practice by introducing clearer *ex-ante* risk-assessment obligations akin to those

---

[114] Sjors Ligthart and other (n.16) 463.

[115] *Ibid.*

[116] NDPA S s 25 (1) (a).

[117] *Ibid* ss 26 (7) (a), 31, 35 and 65.

[118] European Union Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' <https://ec.europa.eu/newsroom/article29/Items /611236/en> accessed 25th November 2025.

developed under EU data protection law.[119] The European Data Protection Board (EDPB) has recognised that technologies enabling behavioural or psychological profiling warrant heightened scrutiny, often recommending they be restricted or prohibited.[120]

However, unlike the EDPB's extensive and technology-specific guidance, which mentions behavioural and psychological profiling,[121] the provisions of the GAID are general and do not provide interpretive clarity on how particular classes of emerging technologies, such as neurotechnology, should be assessed, categorised, or regulated in practice. As such, while the GAID marks a notable evolution from principle to implementation, important questions remain regarding regulatory interpretation, particularly as neurotechnology moves from experimental contexts into healthcare, education, and workplace environments.

While the Nigerian framework is not entirely silent on high-risk technologies, it has yet to articulate a coherent guide specific to neurotechnology. This creates uncertainty for organisations deploying neurotechnology and also weakens preventive safeguards.

6. **Recommendations**

Nigeria's current legal framework provides a useful starting point for regulating neurotechnology, but targeted reforms are necessary to ensure that emerging risks are addressed before neurotechnology adoption accelerates. Rather than advocating an entirely new regulatory regime, this section recommends incremental and practical reforms that build on existing constitutional and statutory foundations.

6.1 Explicit Recognition of Neural Data within Nigeria's Data Protection Framework

The broad definition of personal data adopted by the NDPA has its advantages, but the absence of an explicit recognition of neural data is a failure to capture the sensitivity of neural data. Therefore, it is recommended as a critical first step in preparing for neurotechnology that there be an explicit recognition of neural data within Nigeria's data protection regime. This can be achieved by amending the NDPA or the NDPC, issuing a regulation or guidance that defines neural data as a distinct category of personal data or classifies it as a form of sensitive data.

[119] Art 35 GDPR.
[120] EDPB Guidelines (n.121) p10.
[121] *Ibid.*

As mentioned earlier, in administering the NDPA, NDPC is empowered to issue regulations and codes of practice. This provides a regulatory entry point for the development of neurotechnology-specific regulation without the hurdles of the legislative law-making process. However, at the time of research, no NDPC code or guideline addresses neural data or neurotechnology.

6.2 Development of Neurotechnology Specific Regulatory Guidance

It is recommended that the authority granted to the NDPC under section 62 of NDPA to issue regulations, codes of practice, and guidelines be used to develop neurotechnology-specific guidance, particularly for non-clinical applications such as consumer EEG devices, workplace monitoring, and educational technologies. Guidelines such as this could help bridge the gaps quickly, particularly as amendment of the substantive act could take some time to scale the hurdles in the National Assembly. As a result, such guidelines can immediately clarify lawful bases for processing neural data, consent requirements for neurotechnology, limits on secondary use and profiling, and retention and security standards.

6.3 Strengthening Consent Standards for Neurotechnology

As highlighted earlier, traditional consent models will be inadequate where data subjects cannot reasonably anticipate the inferences that can be drawn from neural signals and, as such, cannot give informed consent. To remedy this, it is recommended that Nigeria's consent framework under the NDPA should be adapted to address the unique challenges posed by neurotechnology by:

a) Requiring enhanced consent disclosure for neurotechnology
b) Mandate plain-language explanations of risks associated with neurotechnology; and
c) Prohibit the bundling of consent for neurotechnology in employment and education. This means that data subjects cannot be made to give a single, all-or-nothing consent for neuro-tech devices. Instead, they should be able to say yes to a specific purpose while rejecting another purpose.

6.4 Strengthening Regulatory Guidance for Neurotechnology under the Framework of the Nigerian Data Protection Act

Although the GAID represents a significant advancement in Nigeria's data protection regime by expressly addressing emerging technologies and mandating DPIAs for high-risk processing, further regulatory refinement is required to ensure preparedness for neurotechnology. In particular, the NDPC should consider issuing supplementary, technology-specific guidance clarifying how neurotechnologies, such as

EEG devices, BCIs, and neural data analytics systems, ought to be assessed under the existing DPIA framework as provided by the NDPA. Such guidance could draw on the risk-based structure already established by the GAID, while providing illustrative examples of neural data processing, identifying typical risk factors, and outlining appropriate safeguards for mental privacy, cognitive autonomy, and data subject rights.

Additionally, the NDPC may adopt a soft-law approach by publishing interpretive notes or sectoral guidelines that articulate how core data protection principles apply in neurotechnology contexts. This approach would avoid premature over-regulation while ensuring legal certainty for data controllers, innovators, and regulators. By building on the foundations laid by the GAID rather than creating a parallel regulatory regime, Nigeria can incrementally develop a coherent governance response to neurotechnology that is adaptable, proportionate, and aligned with international best practices.

6.5 Integrating Neurotechnology into Health Regulation

It is recommended that the NDPC, the Ministry of Health, and relevant health regulators come together to address the use of neurotechnology for health purposes. Existing legislation, such as the NHA and the MHA provide ethical foundations but requires supplementation to address neural data. This can be achieved by:

a) Explicitly integrating neural data and neurotechnology into health legislation;
b) Clarifying accountability between data protection and health regulators, and
c) Ensuring neurotechnology complies with both health ethics and data protection standards.

6.6 Gradual Introduction of Neurorights as Interpretive Principles

Rather than an immediate constitutional amendment, it is recommended that Nigeria adopt interpretive principles on neurorights within existing legal frameworks. For example, neurorights can be recognised through policy instruments or incorporated into NDPC enforcement through flexible guidance that clarifies how existing NDPA and GAID obligations apply to neurotechnological applications.

These do not require rewriting the law, but will reshape how the law is understood and applied in light of emerging neurotechnologies. This means that when judges, regulators and other stakeholders read and interpret existing laws on privacy, dignity, freedoms and data protection, they do it through a lens that considers neurorights. It will ultimately

complement constitutional rights to privacy, dignity, and freedom of thought, and allow courts to develop jurisprudence in this area.

This incremental strategy is consistent with comparative practice, most notably Chile's phased approach to the governance of neurotechnology. Beginning with ethical and scientific discourse on the implications of neurotechnology for human dignity and mental autonomy,[122] Chile progressed to legislative action that culminated in Law No. 21.383 of 2021,[123] which amended Article 19 of the Chilean Constitution to explicitly protect both physical and mental integrity, including information derived from brain activity, and to require that scientific and technological development respect fundamental rights.

For Nigeria, building upon the NDPA and the GAID through targeted guidance offers a proportionate and institutionally realistic pathway that balances innovation with rights protection. It enables regulatory preparedness without foreclosing future legislative or constitutional reform, should the scale and societal impact of neurotechnology ultimately demand more comprehensive intervention.

6.7 Capacity Building and Public Awareness

Effective regulation requires institutional capacity and public awareness. Therefore, it is recommended that Nigeria adopts a rights-based approach which will raise levels of accountability by identifying 'rights-holders' and corresponding 'duty-bearers' as well as enhance the capacities of those duty-bearers to meet their obligations.[124] These include both positive obligations to protect and promote neurorights, as well as negative obligations to abstain from violations. For effective accountability, it is recommended that duty-bearers be given the knowledge, mandate, resources and willingness to achieve their obligations.[125] Accountability also requires transparency, awareness, as well as a competent monitoring and redress system. Transparency will ensure that people understand neurotech and neural data, how and what decisions are being made, what resources are being provided and what

[122]Rafeal Yuste, and others, 'Four ethical priorities for neurotechnologies and AI' *Nature* (2017) (551) (7679)159-163 <https://doi.org/10.1038/551159a.> accessed 10 November 2025.

[123]Full Title, Constitutional Reform Law that establishes scientific and technological development at the service of the people, October 25, 2021.

[124]Dina Craissati, and others, A Human Rights-Based Approach to Education for All (UNICEF 2007)10.

[125]Swedish International Development Cooperation Agency (SIDA), 'Human Rights Based Approach'<https://www.sida.se/en/for-partners/methods-materials/human-rights-based-approach#block-11> accessed 3 November 2025.

results have been reached.[126] Awareness is important because rights are meaningless unless those to whom the rights accrue are aware that they exist, and duty-bearers know that they have obligations with regard to their implementation.

7. **Conclusion**

This paper has identified how neurotech could transform medicine and fundamentally change how we interact with technology and each other. At the same time, they raise critical human rights, data protection and ethical concerns with how they challenge foundational notions within those same frameworks. As a result, this paper concludes that a balancing act must occur, one that allows us to enjoy the benefits that neurotechnologies provide while mitigating the drawbacks and risks associated with using them.

This paper has examined Nigeria's readiness for neurotechnology through the lens of its constitutional guarantees and data protection regime. It has shown that Nigeria is not starting from a position of legal or institutional void. The CFRN provides foundational protections for privacy, dignity, and freedom of thought, while the NDPA and the GAID establish a modern framework for personal data governance and regulatory oversight. These instruments provide a solid legal base upon which further protections can be developed.

However, the analysis also revealed that the majority of Nigeria's current framework on data protection was not designed with neurotechnology in mind. The absence of explicit recognition of neural data, the lack of protection for mental privacy and cognitive autonomy, challenges surrounding meaningful consent, and limited regulatory guidance collectively expose gaps that could undermine individual rights as neurotechnology adoption increases. These gaps are particularly significant in non-clinical contexts, where neurotechnology may be deployed without the ethical safeguards traditionally associated with medical practice.

Rather than calling for wholesale legal reform, this paper has argued for incremental and pragmatic measures. By clarifying the legal status of neural data, strengthening consent standards, mandating high-risk assessments, empowering the NDPC to issue targeted guidance, and

[126].Office of the High Commissioner for Human Rights (OHCHR), 'A Human Rights Based Approach to Data :Leaving No One Behind in the 2030 Agenda for Sustainable Development' (2016) <https://www.ohchr.org/en/issues/indicators/pages/dtheestablis hocuments.aspx> accessed 10November 2025.

gradually integrating neurorights as interpretive principles, Nigeria can adapt its existing legal framework to the reality of neurotechnology. An approach such as this balances innovation with rights protection and avoids the risks associated with regulatory overreach or delay.

Nigeria stands at a critical juncture. As one of Africa's largest digital economies and a regional leader, it has the opportunity to shape how neurotechnology is governed on the continent. Proactive engagement with the legal and ethical challenges of neurotechnology will not only protect fundamental rights but also position Nigeria as a thought leader in responsible technological governance. The question, therefore, is not whether neurotechnology will arrive in Nigeria, but whether the law will be ready when it does.