GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

RESEARCH BRIEF

NEURODATA: NAVIGATING GDPR AND AI ACT COMPLIANCE IN THE CONTEXT OF NEUROTECHNOLOGY

EXECUTIVE SUMMARY

Neurotechnology — electronic devices or methods that read or modify neural activity — lies at the intersection of diverse scientific disciplines, including (cognitive) neuroscience, clinical medicine, (bio) engineering, and computer science. It is principally concerned with the mitigation of symptoms stemming from neurological disease, cognitive disorders and mental health conditions. As the technology has developed, further uses have been identified, giving rise to a burgeoning market for 'consumer' neurotechnology, including non-invasive brain monitoring apparatus, stimulation devices, and brain-computer interface. Both medical and consumer NT devices produce rich and complex brain information called 'neurodata'. This data is collected to facilitate the operation of a NT device, and/or fed back into the algorithms that power NT devices, enhancing their speed, efficiency and accuracy. This 'virtuous circle' of data production and use is responsible for much of the recent advancement in NT, leading many scientists to advocate for enhanced data sharing and open access frameworks.

The indispensability of neurodata to fuelling progress in the sector needs to be balanced against the risks to individual data owners. Indeed, neurodata is distinctive compared to more conventional forms of data due to a combination of specific inherent features. In particular, processed neurodata can reveal sensitive information, including on health status, mental states, cognition and behaviour. While the granularity of mental information that can be gleaned using current technology is relatively low, decoding techniques facilitating the translation of neurodata into these other forms of information are advancing rapidly.

The sensitive nature of neurodata raises questions around whether current regulatory frameworks offer adequate protection against incursions on mental privacy and the safeguarding of neurodata. While there is no supranational regulation that specifically addresses neurodata, regional instruments such as the EU's General Data Protection Regulation (2018) offer a framework against which a protection analysis is possible. The main observation is that while neurodata will generally classify as personal data, its nature imbues it with many characteristics of 'special data', thus warranting a higher level of protection. Applying many of the basic principles of data protection to neurodata however, may be difficult:

DECEMBER 2024 | TIMO ISTACE

This publication has been externally peer-reviewed

THE GENEVA ACADEMY A JOINT CENTER OF GENEVA GRADUATE INSTITUTE
INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES
UNIVERSITÉ DE GENÈVE
FACULTY OF LAW

1. The processing of personal or special category data generally requires the owner's informed consent. This is problematic in the case of neurodata because: (i) the complex algorithmic processing involved makes it difficult to explain to an owner *what* data is actually held and/or *how* it might be used, (ii) individuals cannot regulate the volume or type of neurodata that they disclose, creating a risk that they disclose subconscious data (i.e. that they did not know they held) (iii) power balances, for example where NT devices are employed in the workplace, may be in play.
2. Guaranteeing an individual's privacy and protecting data from misuse or illegitimate transfer generally requires that 'repurposing' is prohibited without explicit consent. As noted however, repurposing is integral to the development, advancement and finetuning of NT devices.
3. Data protection generally requires that the collection of data and its processing is tied to an explicitly stated purpose. Again, this is challenging in the case of neurodata as (i) 'purpose' will not always be clear and easily definable (ii) current technology does not allow for the delimiting of purpose-specific data within a large neurodata set.
4. Data protection standards usually uphold the right of owners to access personal information collected/processed, for this information to be accurate, and for it to be corrected/erased if inaccurate. The difficulty of defining what processed neurodata comprises, coupled with the fact that this data may include subconscious data, will make it hard for an owner to access their information, or know if it is accurate. Even if this were possible, erasure would be difficult. The nature of NT device optimisation means that even if one data point was removed, traces would remain in the functioning of the algorithm.

Against these challenges, as states and regional bodies move towards crafting comprehensive, multi-level data governance frameworks that integrate neurodata, the following should be considered:

1. Data governance frameworks and technical approaches should ensure Privacy by Design (PbD) in the development and innovation process of NTs. In all cases the rules regulating how neuroprivacy is upheld and how neurodata is processed, stored, and shared need to be seen as intertwined and mutually reinforcing.
2. The different forms of data generated and processed by NT devices should influence the degree of protection these data require and the form it should take, taking into account the dynamic nature of neurodata. An explicit recognition as a special data category may be warranted for reasons of clarity.
3. Guaranteeing free and informed consent in the collection and processing of neurodata processing may require a bespoke approach, such as opt-in mechanisms or an expiry term on the validity of neurodata.
4. Competent authorities should develop specific guidance to assist data controllers on how AI processing may impact their approaches to accountability and data protection. This might include mandatory risk assessments for the processing of neurodata, facilitating a mapping and mitigation of the risks to individuals' autonomy, equality and authenticity.
5. The growing use of neurodata in commercial contexts underscores the need for clear boundaries on the interference with mental content, traits, and processes that individuals do not explicitly externalise. Whether such data should never be collected or processed for commercial or political purposes, or limits set, are fundamental ethical questions that must be addressed in data protection frameworks.

PART 1. NEURODATA, PRIVACY AND DATA PROTECTION IN A NUTSHELL

1.1 WHAT IS NEUROTECHNOLOGY AND HOW IS IT USED?

Neurotechnology refers to "devices and procedures designed to access, monitor, investigate, assess, manipulate, and/or stimulate the structure and function of the neural systems of natural persons" [52]. NT can be divided in two general categories: neuroimaging and neuromodulation. Neuroimaging maps the structure and functioning of the brain, while neuromodulation influences the functioning of the brain by applying, *inter alia*, electrical currents or magnetic fields. Neurotechnology is principally used therapeutically, to treat neurological disease, cognitive disorders and mental health conditions. There is also a rapidly growing market for 'consumer' neurotechnology, including non-invasive brain monitoring apparatus, stimulation devices, and brain-computer interfaces (BCIs) [72]. While the efficacy of such devices is not comprehensively established, examples include headsets that monitor brain activity in the workplace[1] (e.g. to detect fatigue[2] or as a tool to enhance productivity),[3,4] and BCIs (that allow a user to control an external device such as a computer or smart device in gaming or for entertainment ends).[5]

1.2 WHAT IS NEURODATA AND HOW IS IT COLLECTED?

Much of the recent advancement in neurotechnology has been enabled by an increase in the volume and diversity of neurodata available [36]. These broad neurodata-sets have been used to train Artificial Intelligence (AI) and Machine Learning (ML) models, and the insights gleaned leveraged to improve devices' accuracy and speed [57]. The modality for the collection of neurodata is neuroimaging, which can be invasive (i.e. involving the surgical placement of electrodes directly on the brain[6]) or non-invasive (for example a head set or skull cap).[7] The vast majority of neuroimaging (and thus the collection of neurodata) takes place in research settings and clinical practice. The monitoring of epilepsy patients, for example, has provided a particularly rich source of longitudinal neurodata. As noted above however, a growing source of neurodata is that generated by commercial neurotechnology [60], including in the wellness, entertainment, employment and education sectors [43], and that collected as part of neuromarketing research i.e. when neuroimaging is leveraged to design more effective consumer targeting based on intentions, preferences, and beliefs [11].

THE MANY FORMS OF DATA GENERATED BY NEUROTECHNOLOGY: THE CASE OF BCI-ENABLED ROBOTIC ARMS

BCIs are technological devices designed to establish a link between the brain and an external device. Utilising neuroimaging, BCIs capture brain activity signals, which are translated into technical commands capable of controlling external devices, such as prosthetic/robotic arms [28]. In a first step, the robotic arm relies on EEG to collect *raw brain data* through sensors placed on the scalp,[8] holding data on electrical activity in certain brain areas and ambient noise. This sensorial information is processed by computational and statistical algorithms into *neurodata*,[9] the output of EEG imaging holding information on brain activity patterns. The AI algorithms in BCI technology are trained to link these brain activity patterns to motor intentions, such as the intention to reach out to a cup and grasp it. The BCI is thus trained to generate *mental information*, reflecting motor intentions, by linking them to brain activity patterns. In a last phase, these motor intentions are translated into technical commands which operate the robotic arm that eventually realises the physical movement e.g. grasping a cup.

1.3 NEURODATA'S DISTINCTIVE CHARACTERISTICS AND ITS RELEVANCE FOR REGULATORY DISCUSSIONS

- Specificity to the individual: Neurodata are representations of an individual's unique brain structure and functioning [58], making it not only a suitable method of biometric identification [42], but one that is even more precise than traditional biometric markers, such as genetic data or fingerprints. [10]
- Potentiality for function-creep: Processed neurodata can reveal information on brain activity, an individual's health status and mental states. Today, the granularity of mental information that can be gleaned is relatively low, and needs to be harvested under strict laboratory conditions. In the future however, more advanced decoding techniques will expand such scope, including in ways that cannot currently be conceived. Mental information that remains indecipherable today could potentially be decoded in the future with the application

of more advanced algorithms to existing data. This 'function creep' is a specific characteristic of neurodata that imbues it with a degree of non-predictability that needs to be factored into regulation.

- The sensitivity of neurodata is not static: While raw brain data might be seen as 'first order' data, when subjected — repeatedly — to (algorithmic) processing, 'second order' inferences can be drawn, revealing information on an individual's physiological status, cognition, mental states or behaviour [34]. In short, while first order data may be considered data that is not uniquely sensitive (compared to other forms of data pertaining to bodily functions), because it may be further decoded, first and second order neurodata may require equally strong protection.
- Data aggregation: Much of the work on brain decoding and diagnosis involves combining neurodata with other forms of data, such as behavioural or physiological data, to make inferences on mental and physical status. For example, studies into obsessive compulsive disorder overlay neurodata recordings with time-stamped reporting of symptoms [64].[11] The take away is that even where neurodata is on its face innocuous, its sensitivity value needs to be understood against the possibility that it can be combined with other data available.
- Involuntariness: Insofar as it is generated subconsciously or involuntarily, individuals have limited active control over the information embedded in, and thus decipherable from, their neurodata [75]. As such, individuals may inadvertently disclose mental information, including on predispositions or subconscious emotional or intentional states that are unknown, even to themselves. Moreover, even in situations where individuals are aware that their neural data is being monitored or recorded, because they cannot always mask or regulate the information disclosed, the pool of data amassed may include elements that extend beyond the remit of the treatment/experiment.
- Predictive nature: Neurodata can assist in predicting an individual's likelihood of developing neurological or psychiatric disorders, and (when analysed concurrently with contextual information) future mental states and behaviours. [36]. This creates scope for use in, for example crime prevention, [70], including by revealing characteristics or predispositions unknown to the individual themself and, critically, which may never materialise or be acted upon.
- Difficulty anonymising data: While neurodata can currently be anonymized, as AI decoding mechanisms progress and datasets expand, eliminating the possibility of subject re-identification may become challenging [38]. Chiefly, conventional methods for anonymising data may not be effective when applied to neurodata [39]. Moreover, applying effective anonymization techniques may interrupt the workability of certain neurodevices [56]. Commercial BCI devices, for example, need to be customised to a user through training on their individual brain activity patterns, creating a link between data sets and individual users with each use of calibrated algorithms.

It is important to highlight that while neurodata is distinctive compared to more conventional forms of data [27], many of these characteristics are not unique to neurodata. Genetic data, for instance, can identify individuals, while physiological data such as blood pressure can reveal information on moods or stress levels. Analysis of 'digital exhaust'— the data that can be gleaned from digital activities like web browsing, social media usage or wearable devices — is perhaps most revealing. Especially when combined with other datasets, this can provide insight into an individual's emotions, intentions, and preferences (such as religious or political beliefs) [36, 67]. Thus, neurodata is not inherently unique in these aspects. The special, distinctive nature of neurodata has to be understood in combination with all the characteristics listed above. Many assert that this necessitates stringent data protection safeguards to mitigate the risk of privacy violations resulting from neurodata (mis) use.

1.4 WHAT ARE THE PRIVACY AND DATA PROTECTION IMPLICATIONS?

How and through which modalities access to and processing of neurodata should be regulated has become the subject of staunch debate. On the one hand, the indispensability of neurodata to support ongoing progress in NT has led to calls for *enhanced* data accessibility, facilitated for instance through sharing platforms.[12] Such essentiality, however, needs to balanced against the importance of protecting such data from a privacy perspective. Indeed, some forms of neurodata can reveal highly personal physiological information (for example on brain lesions), be used as biomarker for the diagnosis of neurological disorders (such as Parkinson's Disease),[13] or indicate a predisposition for the development of disorders (such as cognitive decline) [66]. In the future, it is likely that further attributes will be able to

be identified [5]. Brain-decoding — a separate area of research focused on extracting mental information from neurodata — is also advancing rapidly. Here, AI-powered algorithms analyse neurodata to infer mental states[14] around cognition and behaviour [13],[15] and reveal semantic knowledge [31], dreams [29], memories [6], inner speech [46], emotions [30], visual perceptions [49, 69], intentions [4] and beliefs[16] [62].

The risk is that these technologies could be misused to unveil an individual's private information. Ultimately, such information could, for instance, be used to enhance methods for influencing mental states and/or manipulating behavioural responses. Understanding how individuals process stimuli, for example, could enable marketing engineers or political campaigners to tailor messages to specific 'neuroprofiles' [65]. As neurodata becomes increasingly commodified, [76] these risks will only escalate, with spillover impacts for mental autonomy, personal identity, free will, and agency [38]

It follows that the protection afforded to the data generated and processed by neurotechnological devices, should reflect what that data might be used for and the type of information that can (or might, in the future) be extracted. Certainly, the privacy risks associated with brain data (which can unmask sensitive personal information, such as on mental health) are significantly serious when viewed through the lens of conventional notions of informational privacy. Moreover, as neurodata becomes integrated into the 'big data ecosystem', more generalized risks — including hacking, privacy-sensitive data mining, and unauthorized use — need to assessed against this heightened gravity lens.

AN IMPORTANT CAVEAT: DECODING IS NOT MINDREADING.

It is important to underscore that the advancements made in brain decoding should not imply that *mindreading* is a current possibility. Decoding technologies demonstrate statistically significant relationships between neural patterns and occurrences of certain mental states, which allow for reverse inferences, and predictions, on some mental information. They cannot, however, decode complex cognitive, affective or perceptual states in a way that resembles an individual's personal mental experience in a detailed or reliable way, nor is such technology expected in the near term. This said, given the trajectory and pace of advancement in NT, it is prudent to anticipate that their capacity to make precise and dependable inferences about an increasing array of mental states will improve and broaden.

PART 2. NEURODATA WITHIN THE GDPR

The rapid expansion and commercialisation of NT has raised questions around whether current regulatory frameworks offer adequate protection against incursions on neuroprivacy (the safeguarding of neurodata) and mental privacy (the protection of mental information) [16]. Currently, there is no international or supranational data protection regulation that specifically addresses neurodata.[17] Nevertheless, existing data protection regulations such as the EU's GDPR[18] apply to neurodata processing. The GDPR is a comprehensive regional data protection framework, upon which many national data regulations have been crafted.[19] It applies to the processing of 'personal data' (defined as data relating to an identifiable natural person), by a natural or legal person, public authority, agency or other body (defined as the 'data processor'). Anonymous data — data that does not relate to an identified or identifiable natural person or personal data that does no longer enable the identification of the data subject — falls outside the scope of the GDPR. In principle, the processing of personal data is prohibited, unless this falls under one of the legitimate grounds listed in article 6. 'Special categories' of data, which are enumerated in article 9, are accorded a higher level of protection with strict rules applying to processing. The following sections discuss the extent to which the GDPR is sufficient to address the privacy challenges arising from the development and utilisation of NTs.

3.1 THE CLASSIFICATION OF NEURODATA UNDER THE GDPR

Neurodata will generally be classified as personal data
Irrespective of the purpose for which it is collected or processed, data that enables the identification of a natural person qualifies as personal data, and thus falls within the scope of the GDPR [61]. As discussed above, when combined with other datapoints neurodata can already be used for individual identification, and identification based solely on neurodata — albeit technologically difficult — has shown to be possible and will be increasingly feasible in the future [32]. An alternate line of logic is the *difficulty of anonymising*

neurodata (also discussed above); on this basis, recital 26 GDPR, which sets out that data protection safeguards and obligations for data processors do not apply to anonymised data, could not be invoked. Finally, article 4(1) GDPR stipulates that factors "specific to the (...) mental (...) identity of that natural person *are to be considered* an identifier". While mental identity remains undefined, the fact that neurodata can be correlated with an individual's mental states [34] implies a notional link.

Neurodata might also be classified as a special category of data

While it is not explicitly listed, neurodata may also meet the criteria of a 'special category' as defined in article 9(1) of the GDPR. For example, when it is processed for the purpose of identifying an individual, neurodata would qualify as biometric data under article 9(1).[20,21] Neurodata might also be considered health data, which is defined in recital 35 as data "pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject"; and includes "information derived from the testing or examination of a body part or bodily substance". It follows that personal data must hold information on a person's good or ill health [9]. The key elements in the definition that complicate delineating the scope of health data are 'relating to' and 'health'. The concept of 'health' should not be interpreted narrowly.[22] The European Commission, for instance, has indicated that well-being and health, while not being synonymous, show considerable overlap [19]. It includes information on both medical conditions and the absence of any medical condition. Indeed, neurodata can reveal information on an individual's (mental) health status. Structural imaging, for example, can show/expose the presence or absence of potential brain abnormalities, while functional imaging can indicate biomarkers of a neurological or neuropsychiatric condition or the lack thereof.

The more challenging issue is determining whether and when neurodata *relates to* health status under the GDPR's definition of health data. Drawing from CJEU case law and EDPB guidance, Taka proposes four criteria to establish whether data relates to health: 1) content, 2) context and purpose, 3) usage, and 4) effects [68]. Importantly, in assessing these criteria, the link to information on health can be indirect, and may need intellectual effort to be established [10].

- With respect to **content**, there seems to be a straightforward argument that because neurodata serves as a biomarker for numerous neurological disorders, it does contain information pertaining to an individual's health status. On this basis, it should classify as health data, irrespective of its context, purpose, usage, or effects. [23]
- With respect to **context and purpose,** it is the case that a vast majority of NTs process data for a health-related purpose; this concerns even commercial neurotechnologies, for example EEH headsets designed to inform users on their stress levels (which would be part of a broad definition of health). There are some NTs, however, that do not serve a health purpose, for example when neurodata is collected to create a BCI-based gaming experience.
- With respect to **use,** some NTs merge data to make inferences about an individual's well-being or health — for example, pairing neurodata with age information to assist in diagnosing normal or abnormal neurological development. Such fusion can transform data that does not inherently disclose health information into health data.
- With respect to **effects,** the processing of neurodata may result in a specific treatment related to an individual's health status, with knock on effects for their rights and interests. For example, employers may use EEG headsets to monitor the brain activity of employees as a tool to measure focus and productivity. If this data influences management practices, for instance, reducing the workload of a specific employee where it was deemed excessive, this implies that the data is used in support of the well-being and mental health of the employees, and thus is health-related.

Taking these criteria together, when NTs are used in a medical context and for medical purposes, the data generated and processed are clearly health data. Even when the data is generated and processed by a device that is not medical[24] in nature, but rather marketed for purposes of well-being and lifestyle, the data would classify as health data. While the GDPR itself does not define lifestyle or well-being data, the parameters outlined above — set out against the fact that 'health' is interpretated in a broad way — indicate that neurodata collected by well-being and lifestyle devices will constitute health data [68]. Much like data on one's heart rate or blood pressure, the inherent ability to generate health information, and contribute to the health of an individual, make that data collected and processed by, for instance, EEG headbands monitoring stress levels or moods in order to

enhance well-being, health data.

Whether neurodata collected for purposes unrelated to health or well-being would classify as health data remains a contested subject. Some scholars argue that such neurodata should not be considered health data due to the absence of a medical purpose [56] or context [37]. Such an interpretation arguably creates risks, particularly against the growing availability non-medical commercial NTs that collect neurodata, the misuse of which could result in "loss of autonomy, discrimination, chilling effects and personal distress on a personal level" [34]. An alternate view is that the 'content' of neurodata inherently contains information on an individual's health status. Even if this health information is collected incidental to the NT's intended purpose (i.e. because health information cannot be excluded from the data harvest) the neurodata remains health data and the stricter conditions outlined in Article 9(2) GDPR should apply.

A final question is whether mental information inferred from neurodata should be classified as health data. Ienca and Malgieri [37] opine that mental data alone will not always fall under Article 9 GDPR, for example when it does not link to a distinct special category such as religious or political beliefs. However, when mental information, such as emotions or intentions, is inferred from neurodata, it retains the sensitive (health) data classification throughout processing. For instance, if a company collects neurodata to infer their moods or preferences for marketing purposes, this mental information remains intertwined with the neurobiological information it originated from.

3.2 THE LAWFUL BASES FOR PROCESSING PERSONAL DATA

To process personal data, the GDPR requires that processors specify a lawful basis (as outlined in Article 6 GDPR); for special data categories, an additional basis under Article 9 is required.

Informed consent as a lawful basis for processing neurodata

Informed consent of the data subject constitutes a lawful basis (article 9(2) and 6(1)a) GDPR). For consent to be informed, the information provided should indicate the purpose for which the neurodata will be processed, the period for which it is retained, and the actors it might be shared with (article 13 GDPR). The complex and emergent nature of NTs, however, problematizes the granting of such consent. First, the fact that neurodata is often repeatedly processed by AI algorithms, makes it difficult to understand what information a processor actually holds and processes. Second, because the full extent of potential interpretations is somewhat unknown [34] it is difficult for processors to articulate (and thus for individuals properly understand) the implications of disclosing their neurodata. A third issue is that because users of NT cannot regulate the volume or type of neurodata that they disclose, they may 'agree' to share data they were not even aware they held. A fourth issue is whether consent can be considered free when it is necessary to obtain an optimal benefit from a neurotechnological service/products, or in situations of power imbalance such as workplaces or medical settings. A final issue specifically concerns commercial devices that record neurodata and share it with a processing or owner company. Such products may be sold to consumers (for example a wellness device), be provided (for example in a workplace) or form part of a service agreement (for example users agreeing to share neurodata in exchange for online services). In each of these scenarios, the Terms of Use users are required to accept rarely guarantee informed decisions [51], principally because of difficulties understanding the nuances of how data might be used [40] and the risks of its misuse [22]. This is exacerbated by the 'privacy paradox', a phenomenon whereby consumers tend to prioritize/value the perceived benefits that attach to sharing personal information, over the attendant privacy/data protection concerns such sharing creates [24, 47].[25] The GDPR lacks clear guidance on addressing these concerns [56].

Other lawful bases for processing personal data

Importantly, consent is not the only basis for legally processing neurodata. However, the alternate grounds outlined in Articles 6 and 9 of the GDPR pose challenges in the context of NT. For instance, when AI models process an individual's neurodata to train NTs tailored to a specific consumer or consumer group, ownership of that data is typically transferred to the neurotech company for the purpose of optimizing the AI and ML algorithms.[26] It is unlikely that such optimisation would be considered necessary for fulfilling the contract between the consumer and the neurotech company (Article 6(1), b) GDPR). Likewise, pursuing a legitimate interest (Article 6(1), f) GDPR) would be difficult to argue given the sensitive nature of neurodata, potential harmful effects for the data subject, and the attendant necessity and proportionality assessment that would apply.[27]

In medical contexts, grounds for neurodata processing are easier to identify. It is arguably unrealistic to obtain the informed consent of every patient each time a data set

containing their data is used to train AI algorithms that can be integrated in NT devices.[28] This form of processing might, however, be done on the basis of: substantial public interest i.e. to avoid discrimination by eliminating bias (Article 9(2), g GDPR), necessity for scientific purposes[29] (Article 9(2), j) GDPR) or for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices (Article 9(2), i) GDPR).[30] Nevertheless, the unfettered use of neurodata for research purposes or reasons of public health would be hard to justify under this exception due to lack of proportionality. The same will hold true for the use of mental data in a context of behavioural or psychological research [37].

3.3 PURPOSE LIMITATION AND DATA MINIMIZATION

Article 5(1),b) and c) of the GDPR stipulate that personal data must be processed for explicitly stated legitimate purposes, and that data controllers cannot collect personal data that is unnecessary or irrelevant to achieving that purpose. Complying with these principles raises challenges when they are applied to NT devices.

First, the complex and emergent nature of neurotechnology means that its purpose will not always be clear and easily definable. Explicitly describing each step of a data processing cycle, for example, may not be possible due to the unknowns involved. For AI models with self-learning capabilities, the opacity and open-ended capabilities of algorithms (the 'black box' problem) means that the purpose of processing may not be clear, and defining how an algorithm will utilise a data set impossible [57].

A second issue is that data repurposing is a key part of the NT development process. For example, neurodata collected from a BCI gaming device is commonly be fed back to the developing company who then use it to train AI algorithms and as part of an ongoing optimization loop. Likewise in medical contexts, neurodata collected for the development of a model for diagnosing Parkinson's disease, could also be used to diagnose the disease in the individual person. Under the GPDR, both instances would constitute repurposing and thus require a separate lawful basis and communication to the user, such as additional consent.

A third challenge is the difficulty of limiting data collection to that which is strictly necessary to achieve the objective. Many devices, including EEG caps, inevitably monitor data that does not contribute to the achievement of the base objective. Pre-emptively delineating purpose-specific data within a large set of collected neurodata is not currently possible.

SHOULD THE REPURPOSING OF NEURODATA BE PERMITTED IN CERTAIN CONTEXTS?

An important question is how to balance the risk of privacy violations against the importance of managing neurodata to optimally contribute to advancements in NT. As neurodata becomes an increasingly valuable commodity, the risk of malign repurposing also grows. A particular concern is when neurodata is collected in contexts of power imbalance, such as in the workplace (for example to monitor fatigue) and then resold to neuromarketing or insurance companies to support commercial objectives [14]. The counterargument is that the repurposing or use of redundant neurodata, *ought to be* permitted as this is how the algorithms integrated in NT are developed, trained and optimized. Moreover, obtaining access to longitudinal and diversified brain data is the only way to ensure that NT devices are free from bias and do not discriminate. Currently, only the further processing of data collected for research purposes is not considered re-purposing (Article 5(1), b) GDPR).[31] If (commercial) data processors want to share their data or further process these for research purposes, the conditions for research-related processing must be fulfilled, including a lawful basis (such as public interest or a public task), necessity, fairness, and satisfactory safeguards.[32]

3.4 DATA SUBJECTS' RIGHTS

GDPR Article 15 stipulates that the data subject has the right to access personal information collected, processed, or retained. Moreover, article 5(1), d) requires that personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." Read jointly, several challenges arise in the context of neurodata. As noted, especially when it has been repeatedly processed by AI algorithms, what neurodata a processor actually holds can be difficult to define. Even when this is possible, neurodata's complexity means that it would be challenging for individuals to assess whether information stored is accurate or needs to be corrected (Article 16 GDPR). The right to have one's personal information erased may be especially difficult to apply to neurodata (Article 17 GDPR). Neurodata will most often contain 'unconscious'

information, meaning that the data subject will never be fully aware what the processor actually holds (making it impossible to request erasure). The algorithmic processing of neurodata is likewise at odds with article 17. Neuro-devices are driven by AI models that are trained on and optimized by the reprocessing of many data subjects' neurodata. Thus even if a data subject requested that their data be erased, some trace would be left in the functioning of the algorithm [57], making it unclear whether full deletion could ever be accomplished.[33]

3.5 ADDITIONAL SAFEGUARDS

AI processing

The complex algorithmic processing used in many NT devices may be deemed 'automated processing', [34]34 thus triggering the stricter safeguards stipulated in Article 22 GDPR. It follows that if automated processing were applied to neurodata as a special category of data (as indicated above), such processing would require the explicit consent of the data subject, or would need to be the subject of substantial public interest.

Risk assessments

Where the processing of personal data is likely to pose significant risks to human rights and fundamental freedoms, article 35 GDPR requires a data protection impact analysis (DPIA).35 The upshot is that a DPIA will likely be required for the development and use of NTs due to their reliance upon AI algorithmic processing and innovative nature, and perhaps more broadly, based on the fact that neurodata may contain "sensitive data or data of a highly personal nature" [38; 20]. Recital 6 of the GDPR explicitly refers to privacy and freedom of thought — human rights that are particularly put at risk by the development and use of NTs. Other areas of risk would include: bias in the AI algorithms that power neurotech devices spilling over into discrimination, and where neurodata is used for large-scale profiling, biometric identification, or for targeted marketing towards vulnerable groups such as children. A DPIA must cover (i) a description of the processing and the purposes pursued, (ii) a proportionality assessment, (iii) an assessment of the risks to the rights and freedoms of the data subject, and (iv) the measures envisaged to mitigate the potential harm of data processing. Mitigating factors might include effective safeguards (e.g. creation of policy on strict purpose limitation, access control, retention limitation, consent management, incident reporting, DPO consultation and the establishment of clear procedures for erasure and correction of data, and retention of consent). Other mitigating measures e.g., anonymisation, transparency of processing methods, and data minimisation, may prove more difficult to apply to NT.

Hence, even in cases where neurodata and mental information would not be considered a special category of data, different factors may render its processing high risk, making extra safeguards applicable. In this way, DPIAs enable a focus on a broader range of possible adverse effects on individuals or society, beyond data protection laws, encompassing physical, material or non-material aspects [33].

3.6 COMPLEMENT TO THE EU AI ACT

The EU's new AI Act also contains provisions on data protection and data governance that relate to personal data processed by AI systems (Article 2(7) AI Act).[36] Operating as a complement to the GDPR, the regulation reaffirms both general data protection principles, such as accuracy and quality, transparency and legality, as well as specific norms around data minimisation and protection by design (Recital 69 AI Act). It also sets out obligations for providers and deployers of AI-systems, including on risk management, transparency and security, documentation, incident reporting, CE marking, and conformity assessment. With respect to data protection, Recital 29 states that "the right to privacy and the protection of personal data must be guaranteed throughout the lifecycle of the AI system". This is especially relevant in the context of neurodata, as NT applications such as BCI and neurofeedback devices generally apply some form of AI processing to the collected neurodata.

A main difference between the AI Act and GDPR relates to scope. The AI Act applies to all actors within the value chain, including providers and users, while the GDPR specifically applies to EU-based controllers and processors handling personal data within their activities, or to controllers and processors dealing with the personal data of EU data subjects. In short, AI systems that do not process personal data or that process personal data of non-EU data subjects do fall under the AI Act, but not under the GDPR. A further difference is compensation. A restoration or compensation of a data subject's rights (e.g. to have data erased or corrected) can only be achieved under the GDPR; under the AI Act, unlawful AI systems that use personal data can only be stopped [41].

With respect to the processing of neurodata, the

GDPR and AI Act can be seen as mutually reinforcing in the following areas:

1. The classification of personal data as a special category of data in the sense of Article 9(1) GDPR contributes to the classification of AI systems as high risk systems under the AI act, as "the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed" is a criterion to be taken into account when the Commission wants to amend the catalogue of high-risk uses of AI system (Article 7(2), c) AI Act).
2. The AI Act reiterates and confirms the applicability of the GDPR provisions and fundamental principles within the lifecycle of AI systems that process neurodata. This includes general principles (such as lawfulness, fairness, transparency, purpose limitation, accuracy, and storage limitation, Consideration 94 AI Act), as well as specific provisions (including the applicability of article 9(1) GDPR to the processing of biometric data) (Recital 39 AI Act).
3. The AI Act impacts, facilitates and complements the DPIA obligation of article 35 GDPR by:
   - Identifying uses of AI systems as posing significant risks to the health, safety, or fundamental rights (e.g. AI systems that are used in high-risk use-cases that imply profiling within the meaning of Article 4(4) GDPR), and thereby guiding the scope of the DPIA obligation (Recital 53 AI Act).
   - Ensuring that the relevant information on high-risk AI systems — as collected and provided to deployers under the obligation of Article 13 AI Act — is accessible to controllers of personal data to conduct the DPIA under article 35 GDPR (Article 26(9) AI-Act).
   - Indicating that the human rights impact assessment — an obligation entrenched in Article 27 AI Act — is complementary to the DPIA ex Article 35 GDPR (Article 27(4) AI Act).
   - Stipulating that deployers of high-risk AI systems should provide a summary of the DPIA ex Article 35 GDPR when registering high-risk AI-systems in accordance with article 49 AI Act (Annex VIII, section C, 5 AI Act).
4. The AI Act prohibits certain uses of AI-systems; uses for which NT — and the processing of neurodata — could be deployed, e.g. emotion recognition in educational or professional contexts.
5. The AI Act stipulates conditions for the processing of personal data for developing certain AI systems in the public interest in an AI regulatory sandbox (Article 59 AI Act). This may facilitate future neurotechnological innovation, while safeguarding fundamental interests such as privacy in contexts where these may be at odds with processes necessary for technological innovation.

CONCLUDING REMARKS

Trends around the collection and processing of neurodata, along with its increased economic and political value, create new and important risks. Against such risks, the GDPR together with the AI Act, set out important safeguards for protecting privacy and preventing exploitation. The distinctive characteristics of neurodata, however, require that some principles be further elaborated and tailored, specifically those relating to the AI processing of neurodata. Such goals need to be balanced against a framework that promotes responsible innovation, including data collection to underpin scientific and technological progress. The following issues might be considered or factored into future regulatory discussions:

- There is an urgent need for governments and regional bodies to develop comprehensive, multi-level data governance frameworks that ensure responsible data processing throughout its lifecycle, from collection, storage, processing, curation, sharing and use, to deletion [16]. It should include data protection legislation, human rights-based soft law instruments, and technical approaches that ensure PbD in the development and innovation of NTs.[37] In all cases the rules regulating how neuroprivacy is upheld and how neurodata is stored need to be seen as intertwined and mutually reinforcing.
- The data generated and processed by neurotechnological devices takes several different forms. Such differences should influence the degree of protection these data need, and the way in which such protection is construed. Where it is considered health data, neurodata will generally benefit from the highest data protection standards. An explicit recognition of neurodata as a special data category, however, may be warranted with a view to promoting clarity.
- The notion of free and informed consent in the collection and processing of neurodata processing may require a bespoke approach; proposals such as opt-in mechanisms or an expiry term on the validity of neurodata [12, 26,

74], should be considered.

- Data protection bodies and other competent authorities might issue specific guidance to guide data controllers and data subjects on how AI may impact their accountability and data protection respectively. A further tool would be to mandate DPIAs for the processing of neurodata; this would provide a framework for mapping and mitigating risks to individuals' autonomy, equality and authenticity.
- The growing use of neurodata in commercial contexts underscores the need for clear boundaries on the interference with mental content, traits, and processes that individuals do not explicitly externalise. The AI Act's ban on AI emotion recognition systems in certain contexts is an important indictor in this regard, as it reflects the EU legislator's concern around the monitoring and processing information on individuals' mental content. Whether such data should never be collected or processed for commercial or political purposes, or limits set, [73] are fundamental ethical questions that must be addressed in data protection frameworks.

REFERENCES

[1] Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data, WP 136 (20 June 2007).

[2] Article 29 Data Protection Working Party: Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193 (27 April 2012).

[3] Bernhard, D., Lovejoy, J.P., Horn, A.-K., Brittany, M.A., Hughes, N.: Facebook and online privacy: Attitudes, behaviors, and unintended consequences. J. Comp. Comm. 15, 83–108 (2009).

[4] Bles, M., Haynes, J.-D.: Detecting concealed information using brain-imaging technology. Neurocase 14(1), 82-92 (2008).

[5] Carrier, J., Land, S., Buysse, D.J., Kupfer, D.J., Monk, T.H.: The effects of age and gender on sleep EEG power spectral density in the middle years of life (ages 20-60 years old). Psychophsiol. 38, 232-242 (2001).

[6] Chen, J. Leong, Y.C., Honey, C.J., YongC.H., Norman, K.A., Hasson, U.: Shared memories reveal shared structure in neural activity across individuals. Nature neurosci. 20(1), 115-125 (2017).

[7] Christen, M., Domingo-Ferrer, J., Draganski, B., Spranger, T., Walter, H.: On the Compatibility of Big Data Driven Research and Informed Consent: The Example of the Human Brain Project. In; Mittelstad, B.D., Floridi, L. (eds.) The Ethics of Biomedical Big Data, pp. 199-217, Springer (2016).

[8] CJEU 6 November 2003, Bodil Lindqvist, C-101/01, §49-50.

[9] CJEU 31 May 2005, Triantafyllia Dionyssopoulou v. Council of the European Union, T-05/03, §33..

[10] CJEU 1 August 2022, OT v. Vyriausioji tarnybinés etikos komisija, C-184/20, Opinion of AG Pikamaé, §85.

[11] Cruz, C., Fleith De Medeiros, J., Hermes, L.C.R., Marcon, A.:Neuromarketing and the advances in the consumer behaviour studies: A systematic review of the literature. *Internat. J. Buss. Glob.* 17(3),330-351 (2016).

[12] Dasgupta, I., Assessing current mechanisms for the regulation of direct-to-consumer neurotechnology. In: Bárd, I., Hildt, E. (eds.) Developments in neuroethics and bioethics, pp. 233-265, Elsevier (2020).

[13] Défossez, A., Caucheteux, C., Rapin, J., Kabeli, O, King, J.-R. : Decoding speech perception from non-invasive brain recordings. Nature Machine Intelligence 5, 1097–1107 (2023).

[14] DH-BIO: Common Human Rights Challenges Raised by Different Applications of Neurotechnologies in the biomedical field (Report by M. Ienca) (2021).

[15] Eke, D., Aasebø, I.E.J., Akintoye, S., Knight, W., Karakasidis, A., Mikulan, E., et al.: Pseudonymisation of neuroimages and data protection: Increasing access to data while retaining scientific utility, *Neuroimage: Report* 1(4) (2021).

[16] Eke, D., Bernard, A., Bjaalie, J.G., Chavarriaga, R., Hanakawa, T., Hannan, A.J., et al.: International Data Governance for Neuroscience. *Neuron* 110(4), 600–612 (2022).

[17] EU Regulation 2016/679 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. OJ L 119/1.

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

[19] European Commission: Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century, COM(2012)736 final.

[20] European 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 (October 2017).

[21] European Data Protection Supervisor: Opinion 1/2015 Mobile Health- Reconciling Technological Innovation with Data Protection (May 2015).

[22] Farahany, N.: The Battle for Your Brain. Defending the Right to Think Freely in the Age of Neurotechnology. St. Martin's Press, New York (2023).

[23] Field, R.I.: The Data We Leave behind: Limits of Legal Protections for Neurotechnology and Genomic Data, Drexel L Rev 15(4),101-151 (2023).

[24] Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Comp. Sec. 77,226–261 (2018).

[25] Giancardo, L., Sánchez-Ferro, A., Arroyo-Gallego, T., Butterworth, I., Mendoza, C.S., Montero, P., et al.: Computer keyboard interaction as an indicator of early Parkinson's disease,.Sci. Rep. 6(34468) (2016).

[26] Goering, S., Klein, E., Sullivan, L.S., Wexler, A., Agüera Y Arcas, B, Bi, G., et al.: Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics* 14(3), 365-384 (2021).

[27] Hallinan, D., Schütz, P., Friedewald, M., de Hert, P.: Neurodata and Neuroprivacy: Data Protection Outdated? Surveill. Soc. 12(1), 55-72 (2014).

[28] Hochberg, L.R., Bacher, D., Jarosiewicz, B., Masse, N.Y., Simeral, J.D., Vogel, J. et al.: Reach and Grasp by People with Tetraplegia Using a Neurally Controlled Robotic Arm. Nature 485, 372-375 (2012).

[29] Horikawa, T, Tamaki, M;, Miyawaki, Y, Kamitani, Y.: Neural decoding of visual imagery during sleep, Science 340(6132), 639-642 (2013).

[30] Huis in't Veld, De Gelder, B.: From personal fear to mass panic: The neurological basis of crowd perception. Hum. Brain Mapp. 36(6), 2338-2351 (2015).

[31] Huth, A. G., de Heer, W.A., Griffiths, T.L., Theunissen, F.E., Gallant, J.L.:Natural speech reveals the semantic maps that tile human cerebral cortex. Nature 532(7600), 453–458 (2016).

[32] IBM: Privacy and the connected mind (November 2021).

[33] ICO: AI Guidance (Updated 15 March 2023).

[34] ICO: ICO tech futures: neurotechnology (1 June 2023).

[35] Ienca M, Andorno R.: Towards new human rights in the age of neuroscience and neurotechnology. Life Sci. Soc. Policy 13(5), 1–27 (2017).

[36] Ienca, M., Fins, J.J., Jox, R.J., Jotterland, F., Voeneky, S., Andorno, R., et al.: Towards a Governance Framework for Brain Data. Neuroethics 2022;15:20.

[37] Ienca, M., Malgieri, G.: Mental data protection and the GDPR. J. Law Biosci. 9(1), 1–19 (2022).

[38] Interamerican Judicial Committee: Declaration on Neuroscience, Neurotechnologies and Human Rights: New Legal Challenges for the Americas, CJI/DEC. 01 (XCIX-O/21) (August 2021).

[39] Jwa, A., Poldrack, R.: Addressing privacy risk in neuroscience data: from data protection to harm prevention, J Law Biosci. 9(2) (2022).

[40] Kellmeyer, P.: Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices. Neuroethics 14, 83–98 (2021).

[41] Knibbeler, D., Zadeh, S.: International: The interplay between the AI Act and the GDPR - AI series part 1 (November 2023).

[42] Kumar, K., Toews, M., Chauvin, L, Colliot, O., Desrosiers, C.: Multi-modal brain fingerprinting: a manifold approximation based framework. NeuroImage 193, 212-226 (2018).

[43] Landhuis, E.: Neuroscience: Big brain, big data. Nature 541(7638), 559–561 (2017).

[44] Lee, J.A., Bai, L., Esfstratiou, C.: OSN Mood Tracking: Exploring the Use of Online Social Network Activity as an Indicator of Mood Changes. In: UbiComp '16: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 1171–1179 (2016).

[45] Lippert-Rasmussen, K.: Brain Privacy, Intimacy, and Authenticity: Why a Complete Lack of the Former Might Undermine Neither of the Latter! Res Publica 23(2), 227–244 (2017).

[46] Moses, D. A., Leonard, M.K., Makin, J.G., Chang, E.F.: Real-time decoding of question-and-answer speech dialogue using human cortical activity. Nature Comm. 10(1), 3096 (2019).

[47] Mwesiumo, D., Halpern, N., Bråthen, S., Budd, T., Suau-Sanchez, P.: Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports. Transportation Research Part A: Policy and Practice 171(103659) (2023).

[48] Nicolen M., Hrincu, V., Illes, J.: Privacy Challenges to the Democratization of Brain Data. ISCIENCE 23(6), 101134 (2020).

[49] Nishimoto S., Vu, A.T., Naselaris, T., Benjamini, Y., Yu, B., Gallant, J.L.:Reconstructing visual experiences from brain activity evoked by natural movies. Curr. Biol. 21(19), 1641-1646 (2011).

[50] O Projeto de Lei 522/22 regulamenta a proteção do uso e do tratamento de dados neurais. https://www.camara.leg.br/propostas-legislativas/2317524.

[51] Obar, J.A., Oeldorf-Hirsch, A.: The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Infor, Comm. & Soc. 23(1), 128–147 (2020).

[52] OECD: Recommendation on Responsible Innovation in Neurotechnology (11 December 2019).

[53] Panel for the Future of Science and Technology of the EPRS: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020).

[54] Peth, J., Sommer, T., Hebart, M.N., Vossel, G., Büchel, C., Gamer, M.: Memory detection using fMRI—Does the encoding context matter? NeuroImage 113, 164-174 (2015).

[55] Qiong, G., Jin, Z., Xu, W.: Exploring EEG-Based Biometrics for User Identification and Authentication. In: 2014 IEEE Signal Processing in Medicine and Biology Symposium, IEEE SPMB 2014 – Proceedings 1(1) (2014).

[56] Rainey, S., McGillivray, K., Akintoye, S., Fothergill, T., Bublitz, C., Stahl, B.: Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology. J. Law Biosci. 27(7) (2020).

[57] Rainey, S.: Philosophical Perspectives on Brain Data. Palgrave Macmillan, Delft (2023).

[58] Ravindra, I., Drineas, P., Gramma, A.: Constructing Compact Signatures for Individual Fingerprinting of Brain Connectome. Front. Neurosci. 15 (2021).

[59] Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans. Plos One 8(2), 2013.

[60] RHC: Report on Neurotechnology Regulation (November 2022).

[61] Rocher, L. Hendrickx, J.M., de Montoye, Y.-A.: Estimating the success of re-identification in incomplete datasets using generative models. Nature Comm. 10(1) (2019).

[62] Shreiber, D., Fonzo, G., Simmons, A.N., Dawes, C.T., Flagan, T., Fowler, J.H.: Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans. Plos One 8(2) (2013.

[63] Singh, A.K., Sahonero-Alvarez, G., Mahmud, M., Bianchi, L.: Towards Bridging the Gap Between Computational Intelligence and Neuroscience in Brain-Computer Interfaces With a Common Description of Systems and Data. *Front Neuroinform.* 15(699840) (2021).

[64] Stangl, M., Maoz, S.L., Suthana, N.: Mobile cognition: imaging the human brain in the 'real world'. Nat. Rev. Neurosci. 24, 347-362 (2023).

[65] Stanton, S. J.,, Sinnott-Armstrong, W., Huettel, S.A.: Neuromarketing: Ethical Implications of Its Use and Potential Misuse. J. Bus. Ethics 144(4), 799-811 (2017).

[66] Steenland, K., Zhao, L., Goldstein, F., Cellar, J., Lah, J.: Biomarkers for Predicting Cognitive Decline in those with Normal Cognition. J. Alzheimers Dis. 40(3), 587–594 (2014).

[67] Susser, D., Cabrera, L.: Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy? AJOB Neurosci. 15(2), 122-133 (2023).

[68] Taka, A.M.: A deep dive into dynamic data flows, wearable devices, and the concept of health data. Int. Data Priv. Law 13(2) (2023).

[69] Takagi, Y, Nishimoto. S.: Improving visual image reconstruction from human brain activity using latent diffusion models via multiple decoded inputs (2023).

[70] Tortora, L., Meynen, G., Bijlsma, J., Tronci, E., Ferracuty, S.: Neuroprediction and A.I. in Forensic Psychiatry and Criminal Justice: A Neurolaw Perspective. Front. Psychol. 11 (2020).

[71] UNESCO: Unveiling the Neurotechnology Landscape Scientific Advancements Innovations and Major Trends (2023).

[72] Wexler, A., Reiner, P.B.: Oversight of direct-to consumer neurotechnologies. Science 363(6424), 234-235 (2019).

[73] Wolpe, P.R.; Is my mind mine? Neuroethics and brain imaging. In: Ravitsky, V, Fiester, A., Caplan, A.L. (eds.) The Penn Center Guide to Bioethics, pp. 86-93, Springer, New York (2009).

[74] Yuste, R., et al., Four Ethical Priorities for Neurotechnologies and AI, *Nature* 2017;551.

[75] Yuste, R.: Advocating for neurodata privacy and neurotechnology regulation. Nature Prot. 18, 2869–2875 (2023).

[76] Zuboff, S.: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York, (2019).

ACKNOWLEDGEMENTS

I would like to express my gratitude to Erica Harper, Jonathan Andrew and Reidar Riveland for their insightful input.

END NOTES

1 https://www.emotiv.com/mn8-eeg-headset-with-contour-app/.

2 SmartCap, for instance, offers the EEG-based Lifeband headband that is marketed to employers in order to monitor the fatigue levels of workers. https://www.smartcaptech.com/.

3 For instance: MN8 (Emotiv) https://www.emotiv.com/mn8-eeg-headset-with-contour-app/, Flow (Kernel) https://www.kernel.com/

4 For instance: Foc.us https://foc.us/brain-stimulation/ ; Liftid https://www.getliftid.com/.

5 https://www.emotiv.com/

6 For example Electrocorticography, or ECoG.

7 For example, Electroencephalogram or EEG, Magnetoencephalography or MEG, Functional magnetic resonance imaging or fMRI, Functional near-infrared spectroscopy or fNIRS) and Positron emission tomography or PET). Note that the neurodata collected from non-invasive NT devices can be less granular as such devices need to deal with the challenges inherent to physical barriers such as hair, skin, and the skull.

8 Brain data: a complex set of data including both electrical brainwave activity, and the electrical activity of nearby muscles, electrode motion interference and "ambient noise" (caused by electrical supplies and appliances in the room).

9 Neurodata: Raw brain data that has been recorded and processed by algorithms and statistical models to produce information on brain activity or structure (e.g. the output data generated by neuroimaging technologies such as EEG or fMRI).

10 Indeed, the IBM has opined that: "Although identification of individuals based solely on their collected personal neurodata is likely to be a difficult challenge, it has been shown to be possible with relatively little data (less than 30 seconds-worth) within a laboratory setting, and some experts believe that such identification is feasible, if not today, then in the near-term" [32].

11 Likewise, the decoding of visual perception requires data gleaned from patients reacting to actual visual stimuli to train the decoding algorithms that link brain states to perceptive states

12 The sharing of such data in a research context comes with significant challenges, such as diverging conceptual underpinnings of datasets [63]

13 This is evidently no unique feature of neurodata. Other clinical tools are available that diagnose disorders such as Parkinson's disease on the basis of other data sets. Moreover, a study showed that even patterns of keyboard interaction might enable the diagnosis of Parkinson's Disease [25].

14 Mental states is interpreted in a broad way, encompassing both mental states, mental processes, and mental traits/dispositions

15 A 2011 study was able to demonstrate decoding visual perception from brain activity patterns using fMRI [49]. Participants watched movie clips while their brain activity was recorded. This data was used to train an AI model, that subsequently enabled the reconstruction of their visual experiences of new movie clips.

16 One study indicated that political beliefs can be decoded from brain activity.

17 There are, however, various national and regional privacy frameworks that explicitly incorporated neurodata in their privacy legislation, including Colorado (US) and California (US). Brazil, a legislative proposal has been submitted that aims at explicitly including neurodata in the Brasilian data protection framework, as to ensure that this framework can aptly address the privacy risks that come with increasing availability and use of NTs such as BCIs [50].

18 The scope of application of the GDPR extends beyond the EU to the Member States of the European Economic Area (EEA).

19 For some interesting analysis on the status of neurodata under US data protection laws, see [23].

20 Biometric data is defined by the Article 29 Data Protection Working Party as "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability" [1].

21 In addition, regardless of the context in or the purpose for which it is collected, neurodata will qualify as biometric data in the sense of article 4(14) GDPR, which contributes to its qualification as personal data.

22 This would be consistent with opinions cited by the CJEU [8], European Data Protection Supervisor (and its predecessor the Working Party 29) [21], as well as recital 35, which support a wide interpretation of health data.

23 Such a conclusion, however, sits somewhat in tension with statements issued by some expert bodies. The WP29 [68], for example, while it broadly defines health information to include data that could imply a person's well-being, it clarifies that heart rate data within a normal range, by itself, would not qualify as health data. Counterarguments certainly exist. First, any determination of a 'normal' heartrate would require co-processing alongside other information such as age and sex. Moreover, heart rate data that falls within a normal range automatically infers information on the health status of the person. Logic therefore demands that data on heart rate be regarded as health data, regardless of the purpose or context it is collected or processed in; the same applies to neurodata.

24 Whether or not data is processed by a medical device is irrelevant in the context of the GDPR. The EU Medical Device Regulation stipulates that a device's manufacturer determines, by indicating an intended purpose for the device, whether or not a device is a medical device or a well-being/lifestyle device [18].

25 For instance, perceived benefits for air travel passengers who are willing to share personal data for non-compulsory digital services (such as flight notifications or access to online customer service) increases their inclination to disclose personal data. Similarly, (perceived) advantages of sharing personal information with social media services often trump data protection concerns.

26 Research also shows that the vast majority of neurotech companies that target consumers have far reaching Terms Of Use, stipulating that they have ownership over the collected neurodata and reserving the right to share with and sell to third parties [75].

27 The AI Act specifically indicates that legitimate interest is not a sufficient lawful ground as such for the processing of a special category of data, also not for the detection and correction of bias.

28 In contexts of big data driven research, the notion of 'broad consent' is often used as to obtain consent for data processing. In this form of research, not all hypotheses can be communicated to the patients as not all are known at the beginning of the research. Broad consent would allow for the use of data for an unlimited amount of time and factual research, allowing for the perpetual recycling of collected data [7, 36].

29 The development of algorithms to be incorporated into medical NT for diagnosing and treating patients suffering from neurological disorders might be considered such a scientific purpose.

30 This does not take away from the fact that satisfactory safeguards ought to be in place, such as pseudonymisation of the personal data, and data security measures.

31 This is unless the lawful basis for the initial processing was consent. In that case, consent is needed for further processing for research purposes.

32 The Panel for the Future of Science and Technology of the EU Parliament notes that while there's tension between AI processing and the principle of purpose limitation, AI processing of personal data is not inherently incompatible with GDPR requirements, thanks to a flexible application of purpose compatibility [53].

33 This issue is not unique to neurodata.

34 The ICO has observed that 'sufficiently complex algorithmic processing may be considered as solely automated processing due to its complexity and lack of transparency for the device's users'.

35 A list of indicators to guide such an assessment has been drafted by the European Data Protection Board [20].

36 In total, there are 23 mentioning of the GDPR throughout the AI Act; see Consideration 69 AI Act.

37 For instance, by looking into the most performant ways for encryption and anonymisation of neurodata, or looking into differential privacy approaches for the processing, retention and transferring of neurodata; see for instance [21]: and https://uxmag.com/articles/brain-computer-interfaces-bcis-banner.

THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

DISCLAIMER

The Geneva Academy of International Humanitarian Law and Human Rights is an independent academic centre. Our publications seek to provide insights, analysis and recommendations, based on open and primary sources, to policymakers, researchers, media, the private sector and the interested public. The designations and presentation of materials used, including their respective citations, do not imply the expression of any opinion on the part of the Geneva Academy concerning the legal status of any country, territory, or area or of its authorities, or concerning the delimitation of its boundaries. The views expressed in this publication represent those of the authors and not necessarily those of the Geneva Academy, its donors, parent institutions, the board or those who have provided input or participated in peer review. The Geneva Academy welcomes the consideration of a wide range of perspectives in pursuing a well-informed debate on critical policies, issues and developments in international human rights and humanitarian law.

The Geneva Academy of International Humanitarian Law and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch