Brain Computer Interface: a Data Protection Perspective

A legal analysis of Brain-Computer Interface technology

in mobile gaming and life-style apps

LL.M Law and Technology,

Tilburg Law School,

Tilburg Institute for Law, Technology and Society

Tilburg University

2018

Student:

Alessandro Dato

ANR: 996909

SNR: 2017615

Supervisor:

dr. Tommaso Crepax

Second supervisor:

Prof. Sabrina Röttger-Wirtz

Table of Contents

1. Introduction

1. 1. Background

In "The Culture series" Scottish novelist and science fiction writer Iain M. Banks imagines a distant future where a device called "neural lace", a form of brain-computer interface, is implanted into the brains of young people to allow them to interface wirelessly with AIs and to create backups of their mind. The neural lace also permits the AIs to read and store thought of any being.[1]

To a less extent, this once-far-fetched idea of connecting humans to computers is turning into concrete facts. Today advances in neuroscience and neurotechnology are giving rise to devices that resemble the capabilities of the neural lace, thus apparently closing the gap between science fiction and reality. In particular, scientists developed a method for connecting humans to computers (aka: Brain-Computer Interface) in order to treat physically challenged or locked-in patients with a view to facilitating the restoration of their movement ability.[2] On the one hand, by mapping the brain of their patients through the use of neuroimaging techniques, scientists could understand the human brain functions and detect the correlation between mental states and behaviour.[3] On the other hand, patients could "simply" use their thought to issue commands and complete the interaction with the machine without any need of muscles intervention.[4] Essentially, a new technological method to improve people's quality of living.

Remarkably, however, the Brain-Computer Interface (BCI) is expanding its field of application outside the medical area to target healthy individuals. Not only is the possibility to control external devices as well as virtual objects in a completely new way a tantalizing suggestion for consumers,

[1] I. M. Banks, *The Culture Series*, (Orbit Books, 1987); See also Annalee Newitz, 'Elon Musk is Setting Up a Company That Will Link Brains and Computers', (Ars Technica, 28 March 2017) <https://arstechnica.com/information-technology/2017/03/elon-musk-is-setting-up-a-company-that-will-link-brains-and-computers/ > accessed 22 October 2017.

[2] L. Bi, X.A. Fan and Y. Liu, 'EEG-Based Brain-Controlled Mobile Robots: a Survey', (2013), Volume 43, Issue 2, IEEE Transactions on Human-Machine System, available at <https://ieeexplore.ieee.org/document/6461528/> accessed 22 October 2017.

[3] L. Carelli, F. Solca, A. Faini, p. Meriggi, D. Sangalli, P. Cipresso, G. Riva, N. Ticozzi, A. Ciammola, V. Silani and B. Poletti, 'Brain-Computer Interface for Clinical Purposes: Cognitive Assessment and Rehabilitation', (2017), Volume 2017, BioMed Research International, available at <https://www.hindawi.com/journals/bmri/2017/1695290/> accessed 12 February 2018.

[4] See N. Abdulkader, A. Atia and M. S. M. Mostafa, 'Brain Computer Interfacing: Applications and Challenges', (2015), Volume 16, Issue 2, Egyptian Informatics Journal, 214, available at <https://www.economist.com/science-and-technology/2017/04/01/analysing-brain-signals-to-let-a-patient-control-his-arm> accessed 15 October 2017.

but it is also an affordable one in light of the inexpensive cost of the neuroimaging techniques. In particular, contrary to other neuroimaging techniques (fMRI or MEG), [5] the electroencephalography (EEG) method of recording brain activities as electric signals using electrodes placed around the scalp, is the technology that achieved broader utilization. In fact, this technology is cheap, portable and easy to use.

As a matter of fact, the BCI based on the EEG method is already used in the neuroergonomics and smart environment, neuromarketing and advertising, games and entertainment, education and self-regulation, and security and authentication fields.[6] To give but one example, several companies such as Emotiv and Neurosky not only offer consumer-grade BCIs and software development kits, but they have already introduced the concept of "app stores" where mobile applications, provided by different actors/developers, can be used through BCI devices.[7]

In such a context, brain-data[8] generated by consumer-grade BCI are sent to a connected app and they are then stored in the cloud, or in other data store endpoints.[9] In fact, as a powerful communication system between the brain and the environment, the BCI derives its functionality from the collection of data related to users' brain activities. It collects them through sensors and transfer these data to computers which, in turn, translate such data into digital form.[10]

In light of these characteristics of the BCI and, especially, because it allows to gain fair and better insights into people's intentions, perception and attitudes,[11] many scholars analysed the ethical and legal issues this new technology brings about. Quite alarmingly, ethics scholars agree that the use

[5] Where fMRI stands for functional magnetic resonance imaging and MEG for magnetoencephalography.
[6] S.N. Abdulkader, A. Atia and M.S.M. Mostafa, (n. 5).
[7] See Neurosky official website, 'Apps', available at <https://store.neurosky.com/collections/apps> accessed 22 October 2017; and Emotiv official website, 'Consumer Insight Solutions', available at <https://www.emotiv.com/consumer-insights-solutions/> accessed 22 October 2017. Notice that Neurosky has 100+ applications for BCI devices.
[8] When there is a reference to data collected by the BCI the paper always uses a plural form. This is to emphasize the massive amount of data collected by the BCI.
[9] See Emotiv official website, 'Privacy policy', available at <https://id.emotivcloud.com/eoidc/privacy/privacy_policy/> accessed 13 June 2018.
[10] See D. J. McFarland and J. R. Wolpaw, 'Brain Computer Interfaces for Communication and Control', (2011), Volume 54, Issue 5, Communications of the ACM, 60-66, available at <https://cacm.acm.org/magazines/2011/5/107704-brain-computer-interfaces-for-communication-and-control/fulltext> accessed 22 October 2017; S. N. Abdulkader, A. Atia and M. S. M. Mostafa, (n. 5), 214.
[11] See D. Schreiber, G. Fonzo, A.N. Simmons, C.T. Dawes, T. Flagan, J.H. Fowler, M.P. Paulus, 'Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans', (2013), Volume 8, Issue 2, PLoS One, available at <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0052970> accessed 23 October 2017. A successful research experiment on the possibility to infer the political views of the users through BCI technology.

of the BCI can undermine individuals' cognitive process by affecting their personality and personhood and it can also pose problems related with the possibility to read people's minds.[12] Unsurprisingly, legal scholars advocates for the introduction of new human rights such as the right to mental privacy and cognitive liberty to tackle the privacy challenges created by the BCI.[13]

Apart from a possible infringement on individual privacy – which is tangential rather than central to this work - it is remarkable that this technology, if applied in the mobile game, entertainment and smart environment fields has the potential to disseminate an extraordinary volume and variety of brain information for purposes other than care, much like any other bit of information circulating in the digital ecosystem.[14] However, contrary to the latter type of information, data extracted from the BCI relate to the more intimate sphere of individuals as they may contain private data about users' memories, prejudices, religious and political beliefs, as well as about their possible neurophysiological disorders.[15]

Therefore, as the separation between science fiction and reality gets closer, questions about the legitimacy and legal treatment of the BCI appear all the more appropriate. In this regard, since the BCI is based on the process of data extraction from human brains, in the form of neural signal, an examination through the lens of data protection law appears to be an important aspect to address legal issues related with the introduction of such technology in the society.

[12] F. Nijboer, J. Clausen, B. Z. Allison and p. Haselager, 'The Asilomar Survey: Stakeholders' Opinions on Ethical Issues Related to Brain-Computer Interfacing', (2011), Volume 6, Issue 3, Springer Online, 541-578, available at <https://link.springer.com/article/10.1007/s12152-011-9132-6> accessed 23 October 2017.
[13] M. Ienca and R. Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology', (2017), Volume 13, Issue 5, Life Sciences, Society and Policy, available at <https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> accessed 23 October 2017.
[14] Ibid.
[15] T. Bonaci, R. Calo and H. J. Chizeck, 'App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces', (2014), IEEE International Symposium on Ethics in Science, Technology and Engineering, available at <https://ieeexplore.ieee.org/document/6893415/> accessed 23 October 2017.

1. 2. Problem Statement

In the EU the legal framework to address concerns related to the processing of personal information is provided through a technologically neutral legislation, [16] the General Data Protection Regulation (GDPR).[17] The main objective of this law is to ensure, on the one hand, the protection of natural persons with regard to the processing of their personal data and, on the other hand, to respect the freedom to conduct business for those actors who need data to run them.[18] In other words, the GDPR builds a legal framework where individuals' personal data can be processed provided that a certain set of rules and principles are followed.[19] As it has been put by Burkert the rules and principles of the GDPR are not meant to address "the material normative issue of what is acceptable to be processed for which purpose".[20] Quite the contrary, the data protection legislation has always intended to set a number of procedures to render any processing of personal data as legitimate.

Notwithstanding, the introduction of the BCI as a consumer product, especially its application in the mobile world for gaming and relaxation purposes, creates the risk of legitimizing a processing operation which is fundamentally incompatible with the GDPR. Already Hallinan *et al.* demonstrated how brain data extracted by the BCI challenges essential concepts of the EU data protection law, ultimately finding that these data contrast with the rules of the relevant legislation.[21]

However, a consumer-grade BCI that can read and store an extraordinary volume and variety of brain information for purposes other than care, also appears to challenge the basic principles of the

[16] See Recital 15 of the GDPR.
[17] See recital 3 of the GDPR.
[18] See Recital 4 of the GDPR.
[19] L. A. Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits', (The Hague, Kluwer Law International, 2002); see also P. De Hert, 'Citizens' Data and Technology: An Optimistic Perspective', (2009), The Hague, Dutch Data protection Authority, available at <https://www.researchgate.net/publication/241858150_Citizens'_data_and_technology_An_optimist_perspective > accessed 16 July 2018.
[20] H. Burkert, 'Data-Protection Legislation and the Modernization of Public Administration', (1996), Volume 62, International Review of Administrative Sciences, 557-559, available at <http://journals.sagepub.com/doi/abs/10.1177/002085239606200407?journalCode=rasb> accessed 16 July 2018.
[21] D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, 'Neurodata and Neuroprivacy: Data Protection Outdated?', (2014), Volume 12, Issue 1, Surveillence & Society, available at <http://journals.sagepub.com/doi/abs/10.1177/002085239606200407?journalCode=rasb> accessed 22 October 2017.

GDPR. In the same way someone subscribing for an online journal expects that only certain personal data are required to access and read news online, a BCI user would expect that only some of his or her personal data are processed to access and play the mobile game. This fundamental expectation on the part of data subjects has been translated into legal principles in the GDPR which, indeed, provides for the principle of purpose specification and data minimization for any data processing operation.[22]

Thus, this research aims to provide a clear answer as to whether this fundamental expectation of data subjects is respected when their data are processed through the BCI for mobile gaming and relaxation purposes.

1. 3. Research Question

As a result of the above discussion the following research question has been identified:

To what extent does the BCI comply with the principles of purpose specification and data minimization enshrined in the GDPR?

To answer this question, three different sub-questions have been established:

- *What kind of data does the BCI "read and detect" from the brain? And to what extent?*
- *What is the legal nature of brain data detected and read by the BCI technology?*
- *How does the GDPR's principles of purpose specification and data minimization impact on the processing of brain data through BCI technologies?*

[22] See Article 5 (1)(b) and (c) of the GDPR.

1. 4. Methodology

From the outset, this paper applies a traditional type of legal research to answer the research question. It adopts a research method composed of doctrinal analysis, limited, however, to the examination of key laws such as the EU General Data Protection Regulation, relevant publications and interpretations of Article 29 Working Party (Art. 29WP). Since, as of now, there are no rulings specifically concerning the data protection issues stemming from the processing of personal data through the BCI, the analysis is limited to an examination of key legal concepts. In particular, the relevant legal concepts are personal data, sensitive data as well as the principles of purpose specification and data minimization.

As a matter of fact, the only research paper directly posing the issue of data protection in the context of BCI is elaborated by Hallinan et *al.*[23] In this paper, the authors analysed the compatibility of data drawn directly from the human brain, which they classify as neurodata, with the European data protection law. Their main argument was that the current EU legal framework is not equipped to deal with such data because concepts such as anonymity, accuracy and sensitivity may not apply to neurodata.

Therefore, an extensive use of articles concerning technical aspects of the BCI technology are of the utmost importance in this analysis. In fact, this is a necessary first step to establish a clear understanding of the type and possible uses of data that can be extracted from the BCI device. Notice, also, that where the comprehension of such technical research papers has been deemed insufficient by the author, a helpful – albeit limited - clarification has been obtained by relevant BCI manufacturers.

1. 5. Literature Review

A first approach to the research was to find academic articles giving a general overview of the topic of "Brain-Computer Interfaces". Various keywords such as: 'dual use of brain-computer interface', 'brain-computer machine', 'ethical aspects of BCI', 'legal issue of BCI' were used in

[23] D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 22).

search engines and legal databases such as Google Scholar, Lexology and the SSRN databases in order to clarify which authors were relevant to the topic. Amongst others, the most relevant authors were D. Hallinan, T. Bonaci and M. Ienca. In particular, the work of D. Hallinan and T. Bonaci were fundamental in establishing the focus of this paper on the EU protection of brain data. Once the topic was decided, a further search was conducted and 'neuroprivacy' and 'neurodata' were added to the keywords.

The preliminary findings suggest that BCI technology is mostly studied from a technical point of view and, to a lesser extent, from an ethical perspective. While from a purely scientific perspective most of the experts point out at the limitations of such technology, ethicists develop further on the possible development of BCI and the consequence it would have on people's autonomy, dignity and freedom of thought. On the other hand, legal authors mostly focused on the possibility to introduce neuroimaging techniques used by BCI in the criminal legal system. When the focus is not criminal law, legal authors take the issue of BCI from a privacy perspective.

1. 6. Significance

From an academic perspective, this legal analysis contributes to fil the gap in the existent legal literature about the BCI. Legal scholars have, indeed, focus their attention on the use of BCI as a lie detector machine to be adopted in the criminal justice system [24] or have pointed out the limitation of the current framework for the protection of human rights in light of the development of this new neuro-technology.[25] Only few tackle issues of BCI from a privacy perspective,[26] and even less from a data protection point of view.[27]

[24] F. X. Shen, E. Twedell, C. Opperman, J. D. S. Krieg, M. Brandt-Fontaine, J. Preston, J. McTeigue, A. Yasis and M. Carlson, 'The Limited Effect of Electroencephalography memory recognition Evidence on Assessment of Defendant Credibility', (2017), Volume 4, Issue 2, Journal of Law and Biosciences, 330-364, available at <https://academic.oup.com/jlb/article/4/2/330/3796509> accessed 22 October 2017.
[25] M. Ienca and R. Adorno, (n. 14).
[26] See A. Greenberg, 'Inside the Mind's Eye: an International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces', (2018), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180941> accessed 21 July 2018; and K. Wahlstrom, N. B. Fairweather and H. Ashman, 'Privacy and Brain-Computer Interfaces: Identifying Potential Privacy Disruptions', (2016), Volume 46, Issue 1, ACM SIGCAS Computers and Society, 41-53, available at <https://dl.acm.org/citation.cfm?id=2908223> accessed 25 October 2017.
[27] D. Hallinan, P. Schutz, M. Friedewald and p. De Hert, (n. 22).

However, even where legal scholars analyze the BCI through the lens of data protection law their scope of research is either limited to an investigation of the legal concepts embedded in the relevant legislation, or it is confined to an abstract examination of the brain data itself rather than the processing operation of the BCI.

By taking a step further this paper investigates two principles of the GDPR and the effect they have on a more concrete processing operation of the BCI; namely, its uses in the mobile apps for gaming and relaxation purposes. In this regard, this paper humbly aims to contribute to the contemporary literature in the following way:

1) Establishing a framework for the processing of personal data through the BCI that complies with the principles of purpose specification and data minimization of the GDPR. In doing so, it is possible to appreciate the limitations of these two principles with regard to the BCI.
2) By analysing a concrete application of the BCI the objective is to provide a clear answer as to whether, when, how and why the data collected by the BCI can be considered personal and sensitive data. In this regard, it can be appreciated the discrepancy between the contemporary literature and this work. In particular, given the characteristics of the BCI and the fact that its application is outside the medical field, it is generally more complicated to assume that the data the BCI collects are personal and even more so sensitive.
3) Demonstrates why it is important for the EU legislator to provide a clear definition of brain data in the law.
4) Highlighting the discrepancies between data protection and privacy in terms of risks for data subjects. Albeit similar, from a data protection perspective the result is that certain types of BCI appear riskier for data subjects while from a privacy perspective other and different types of BCI are more critical.
5) Providing suggestion for alternative forms of remedies in line with the EU data protection law.

1. 7. Limitation and scope

As already stated, this paper starts from the assumption that the rules of data protection of the GDPR are in stark contrast with the personal data extracted through the BCI. In fact, this problem has already been demonstrated by Hallinan *et al.*[28] Thus, the analysis takes the suggestion of Professor B. J. Koops - who proposed to pay more attention on the main underlying principles of data protection law in "The Trouble with the European Data Protection Law"-[29] and investigates whether the processing of data through the BCI complies with the principles of purpose specification and data minimization enshrined in the GDPR.

The reason to focus on only two principles of the GDPR is not simply because of time constraint, but it is also determined by other considerations. In particular, the principle of purpose specification has always been considered at the cornerstone of the EU's data protection law.[30] It provides for transparency and legitimacy of data processing operation,[31] it determines whether data are necessary and accurate as well as their storage period.[32] Simply put, all the principles of the GDPR are intertwined with the principle of purpose specification which indeed fosters transparency, fairness and lawfulness of the processing operation. On the other hand, given the vast amount of data collected by the BCI, the principle of data minimization appears to be the most relevant for this analysis.

However, in light of the fact that these two principles are of direct interest to the data protection law only on the condition that the BCI processes personal data, the scope of this thesis is further extended to an analysis of the type of data processed by the BCI. With regard to the peculiarities of this kind of information the paper does not claim to be complete. It mainly defines when the BCI data turn into either personal or sensitive information by studying the scientific experiments

[28] D. Hallinan, P. Schutz, M. Friedewald and p. De Hert, (n. 22).
[29] B. J. Koops, 'The Trouble with European Data Protection Law' (2014), International Data Privacy Law, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed 25 October 2017
[30] T. Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', (2017), Volume 47, Seton Hall Law Review, available at <https://scholarship.shu.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1606&context=shlr> accessed 21 July 2018.
[31] F. Coudert, J. Dumortier and F. Verbuggen, 'Applying the Purpose Specification Principle in the Age of "Big Data": The Example of Integrated Video Surveillance Platforms in France', (2012), ICRI Working Paper, available at <https://core.ac.uk/download/pdf/34557376.pdf> accessed 21 July 2018.
[32] See Article 5 of the GDPR.

in the relevant literature. Nevertheless, it must be stated that these experiments do not directly allow to determine the nature of the data (personal or sensitive) collected by the BCI in the specific application chosen in this thesis; nor do they permit to fully comprehend the complexity of the data extracted from the brain. In this regard, it would be essential to have more technical literature so that legal scholars can better grasp issues posed by the BCI.

For what concern the technology, this paper is limited to the examination of a specific type of BCI; namely, a non-invasive BCI. However, to be able to conduct this research without overflowing the reader with the many possibilities of neuroimaging techniques using non-invasive BCI, this thesis only focuses on electroencephalography (EEG) technology, which is a method of recording brain activities as electric signals using electrodes placed around the scalp. The main reason to concentrate this analysis on EEG only is that this technology is cheap, portable and easy to use. Therefore, contrary to other neuroimaging techniques (fMRI or MEG),[33] EEG may expand its possible applications outside of research laboratories and become more accessible and attractive for businesses and consumers alike.

1. 8. Thesis Outline

Chapter two serves as a clarification of what data the BCI based on EEG imaging technique can read and detect. In this chapter, the reader is further introduced into the method that leading neuro-technology companies use to collect and store data through an EEG application in the leisure field. In particular, the attention is on how brain-data generated by consumer-grade BCI are sent to a connected app and are subsequently stored in the cloud or other data store endpoints.

Chapter three investigates the legal nature of brain data detected and read by the BCI technology. Its aim is to point out the limitation of the concept of personal and sensitive data of the GDPR in light of the data extracted by the BCI. By focusing on whether the GDPR applies to such data, the chapter argues that certain characteristics of the BCI data either challenge provisions of the GDPR like anonymization and pseudonymization; or render the application of the GDPR more complicated due to the lack of a precise definition of brain data.

[33] Where fMRI stands for functional magnetic resonance imaging and MEG for magnetoencephalography.

Chapter four provides an analysis of how the principles of purpose specification and data minimization impact on the processing of personal data through the BCI. Here, it is demonstrated that even these basic principles of the GDPR have a little role to play in the processing of personal data through the BCI. It is argued that the principle of purpose specification must be closely linked with the type of BCI technology, since different BCI based on different control paradigms needs only certain data to functions. Interestingly enough, such analysis highlights how taking the issue of BCI from a data protection perspective rather than privacy yield different results.

Chapter five sums up the most significant findings of the thesis and answers the main research question. Also, it contributes to the clarification of the issues and limitations found in this thesis and it provides recommendations for policy-makers.

2. The Brain-Computer Interface and Personal Information

2. 1. Introduction

A Brain-Computer Interface (BCI) offers an alternative to natural communication and control. In particular, it provides a powerful communication system between the brain and the environment. It collects data related to users' brain activities through sensors and transfers these data to computers. In doing so, it does not require any external devices or muscle intervention to issue commands and complete the interaction.[34]

The concept of BCI was first developed by J.J. Vidal in his seminal research paper on brain-computer communication [35] through the observation of neuronal activity in the brain. Fundamental to his discovery was the use of electroencephalography (EEG) technique which is a method of recording brain activity as electrical signals, using electrodes placed around the scalp. Indeed, as information within the brain is processed and transmitted by neurons in the form of electrical and chemical signaling, such brain activity can be measured with EEG.

Originally, it was developed for connecting humans to computers in order to treat physically challenged or locked-in patients with a view to facilitating the restoration of their movement ability.[36] Today, BCI still is the only option for facilitating communication ability of people with severe physical disabilities, provided that cognitive functions are preserved. In the medical area, this technology substantially improved the quality of life of people affected by paralysis and motor disabilities, with news on such accomplishment that constantly fills the newspaper.[37]

Slowly BCI technology left the medical field to enter the commercial market [38] and, as its scope of application further widen, concern for privacy measure amount. [39] Such concern for privacy is also emphasised by media coverage of this new technology which often overstates the actual

[34] See See D. J. McFarland and J. R. Wolpaw, (n.11); S. N. Abdulkader, A. Atia and M. S. M. Mostafa, (n. 5).
[35] J. J. Vidal, 'Toward Direct Brain-Computer Communication', (1973), Brain Research Institute, University of California, available at <http://web.cs.ucla.edu/~vidal/BCI.pdf> accessed 26 November 2017.
[36] L. Bi, X.A. Fan and Y. Liu (n. 3).
[37] See James Wu and Rajesh P. N. Rao, 'How Close are We to Elon Musk's Brain-Computer Inerface?', (The Conversation, April 12, 2017), available at <https://edition.cnn.com/2017/04/12/health/brain-computer-interface-partner/index.html> accessed 26 November 2017.
[38] See Neurosky official website and Emotiv official website, (n. 8).
[39] See A. Stopczynki *et al.*, 'Privacy for Personal Neuroinformatics', (2017), Technical University of Denmark and 2 MIT Media Lab, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427564> accessed 26 November 2017.

functional capacity of BCI devices, apparently depicting the latter as a mind-reading machine.[40] After all, a machine that can listen to brain activity and can recognize and interpret the intent of the user closely resemble the science-fiction vision of mind-reading machine. However, the BCI technology, still suffers from many technical limitations, lack of knowledge about the human brain and is ultimately a technology which, although promise to transform how people interact with computers, still is in its infancy.

This statement, nevertheless, does not mean to underestimate the potential infringement on people privacy of such technology, given that its expansion into the entertainment and leisure field has the potential to disseminate an extraordinary volume and variety of brain information for purposes other than care, much like any other bit of information circulating in the digital ecosystem.[41] Indeed, recently introduced small, head-mounted wireless EEG amplifiers and their confirmed applicability in real-life situations create new paradigms for out-of-the-lab setups.

The purpose of this chapter is to contextualize and comprehend how the BCI function in order to discern what type of information it collects and stores. In particular, it prepares the ground for consideration about whether personal information is processed by this device which is discussed in Chapter three. To do so, the first paragraph of this chapter provides an overview of BCI applications in the mainstream industry, with particular emphasis on "neurogaming" and "neuroapp". The second paragraph analyses technical specifications of how BCI measure brain activity through EEG technique. The third paragraph explains what can be inferred from the EEG signal. Eventually, the fourth paragraph concludes by summing up the principal arguments of the whole chapter and gives some insight on whether personal information is collected and stored by BCI devices.

[40] Genevieve Roberts, 'Mind-Reading Headsets Could Revolutionise Our Interaction With the World', (Independent, 9 December, 2015), available at <https://www.independent.co.uk/life-style/gadgets-and-tech/features/mind-reading-headset-could-revolutionise-our-interaction-with-the-world-a6766856.html> accessed 27 November 2017.
[41] M. Ienca and R. Andorno, (n. 14).

2. 2. Brain-Computer Interface: Overview of applications

Recent announcements of successful entrepreneurs like Elon Musk (Neuralink)[42] and Mark Zuckerberg [43] about the application of BCI technology are just the latest headlines in an ongoing science-fiction-becomes-reality story. Other claims on possible BCI application include spelling devices, computer games, environmental control, navigation in virtual reality, intelligent transportation, neuromarketing and security and authentication.[44, 45, 46, 47] Although these announcements share the common promise to achieve mind reading and remote communication outside the medical area, very little is known about the technology behind such advancements. Indeed, when analyzing such claims one thing is clear, the type of BCI widely differ in the degree of invasiveness to individual body and in the method used to measure brain activity. In particular, these differences are of special interest in this thesis because the information extracted and stored by this technology broadly diverge from each other in term of quantity and quality of data. Thus, a brief explanation is due.

Generally, an initial distinction is made between invasive and non-invasive BCI. The invasive technique requires surgery to implant the necessary sensor, composed of electrodes, which are placed on the surface of the cortex in order to record the brain activity. The signal recorded from these electrodes is called electrocorticogram (ECoG) whilst the signal recorded from within the brain is called intracortical recording. These invasive methods have many advantages compared

[42] Alex Heath, 'Elon Musk Has raised 27 Milion to Link Human Brains with Computers', (Business Insiders, 25 August, 2017), available at https://www.businessinsider.nl/elon-musk-neuralink-raises-27-million-2017-8/?international=true&r=US> accessed 26 November 2017.
[43] Josh Constine, Facebook is Building Brain-Computer Interfaces for Typing ans Skin-Hearing', (Techcrunch, April 19, 2017), available at <https://techcrunch.com/2017/04/19/facebook-brain-interface/?guccounter=1> accessed 27 November 2017.
[44] D. S. Tan, A. Nijholt, 'Brain-Computer Interfaces: Applying Our Minds to Human-Computer Interaction', (2010), Springer.
[45] T. Kim, S. Kim, and D. Shin, 'Design and implementation of smart driving system using context recognition system', (2011), Computers & Informatics (ISCI), 2011 IEEE Symposium on. IEEE, 84–89, available at <https://ieeexplore.ieee.org/document/5958889/> accessed 20 November 2017.
[46] G. Vecchiato, L. Astolfi, F. De Vico Fallani, S. Salinari, F. Cincotti, F. Aloise, D. Mattia, M.G. Marciani, L. Bianchi, R. Soranzo *et al*., 'The study of brain activity during the observation of commercial advertising by using high resolution EEG techniques', (2009), Engineering in Medicine and Biology Society, Annual International Conference of the IEEE. IEEE, 57–60, available at <https://www.ncbi.nlm.nih.gov/pubmed/19965113> accessed 15 March 2018.
[47] D. T. Karthikeyan and B. Sabarigiri, 'Enhancement of multi-modal biometric authentication based on iris and brain neuro image coding' (2011), Volume 5, Issue 5, Int. J. Biometrics Bioinform (IJBB), 249-256, available at <http://www.cscjournals.org/library/manuscriptinfo.php?mc=IJBB-136> accessed 15 March 2018.

to non-invasive one because they are in direct contact with neurons and may record the integrated activity of a much large number of neurons. Indeed, excellent signal quality, outstanding spatial resolution and a higher frequency range ensure the better functioning of the BCI.[48] However, such advantages are counterbalanced by serious drawbacks such as limited usability rising from surgery requirement, a risk of infection due to the long-term use of the device, financial costs but also ethical consideration.[49] Thus, this type of BCI is normally confined to the medical field.

Non-invasive technique offering an alternative to natural communication and control are various. The most important neuroimaging technique for BCI utilization are magnetoencephalography (MEG) which measures magnetic fields produced by electrical current occurring naturally in the brain, functional magnetic resonance imaging (fMRI) which recognize the changes in blood flow determined by the neural activity in the brain and the functional near-infrared spectroscopy (fNIRS) which, through the use of light in the near-infrared range, map blood dynamic in the brain in order to detect neuronal activity. Lastly, but most importantly, Electroencephalography (EEG) records brain activity as electrical signals, using electrodes placed around the scalp.

These non-invasive techniques differ not only in the method employed to record brain activity but also in term of portability and imaging capabilities; which, in turn, affect the information that can be collected by the BCI and its potential market distribution. For example, while fMRI captures information from deep parts of the brain that cannot be gathered by electrical measuring,[50] the EEG offer either higher temporal resolution, portability capacity and a low level of technical requirement that render such method fit for commercial use.

Because the characteristics of EEG method render such device cheap, portable and easy to use, this thesis only analyzes this type of BCI. Moreover, as the EEG is more apt to commercial use than other neuroimaging technique, the potential to disseminate an extraordinary volume and variety of brain information is much more reasonable.

---

[48] B. Graimann, '*Brain-Computer Interface: a Gentle Introduction*', in B. Graimann et al. (eds.), 'Brain-Computer Interfaces, (The Frontiers Collection', Springer, 2010), 8.

[49] G. Tamburrini, 'Brain to Computer Communication: Ethical Perspectives on Interaction Models', (2009), Volume 2, Issue 3, Springer, available at <https://link.springer.com/article/10.1007/s12152-009-9040-1> accessed 15 March 2018.

[50] B. He, S. Gao, H. Yuan, J.R. Wolpaw, 'Brain-computer interfaces', (2013), Neural Engineering, Springer, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4082720/> accessed 15 March 2018.

2. 2. 1. Brain-Computer Interface: the EEG application

Recently, with the arrival of low-cost, user-oriented BCI devices based on the EEG method, which are further combined with powerful mobile devices, software programs and cloud services, the processing and storage of brain data has become easier than ever before. In particular, several companies offer this consumer-grade device that is used for a variety of applications, such as video games and hands-free keyboards, together with application stores (AppStore) similar to the one used for smart phones, where application developers (app developers) also have access to brain data in order to deliver their services.[51] It may also be possible to imagine databases of EEG data collected from users of such application stores, for the purpose of providing services and building applications.[52]

In this new reality, given the strict limitations provided by the General Data Protection Regulation (GDPR) on the processing of personal data, which will be addressed in the next chapter, questions about the protection of such data arise. For the moment it is necessary to underline that the GDPR only protect personal data, which is any information related to an identified or identifiable natural person.[53] This means that if the information collected and stored by the BCI do not directly or indirectly identify a natural person, data protection issues may not originate.

2. 3. Brain-Computer Interface: the EEG method

A BCI based on EEG technique has, apparently, a simple structure composed of six operations. The first step involves the measurement of brain activity in order to acquire the raw signals of the individual. In a second step, specific filters are employed to reduce noise caused by muscles movements so that a better signal is extracted in the third phase. The extracted signal (also called feature) is then classified (fourth step) and translated into a command recognizable by the machine (fifth step). Usually, feedback is provided to the user in the last step to inform him/her of the recognized brain activity pattern (sixth step).

[51] T. Bonaci, R. Calo and H. J. Chizeck, (n. 16).
[52] Ibid.
[53] Art. 4 of the GDPR.

As it is clear from this description, the acquisition of EEG is the first step in the functioning of BCI. The EEG is a method to record the neuronal activity of the brain through the use of a number of electrodes placed on the scalp which measures the oscillating electrical potential recorded from the scalp surface. There are, however, three main brain activity patterns that can be measured by the EEG and which are triggered by different mental strategies. In fact, while the Event-Related Potential (ERP) and the Steady State Evoked Potentials (SSEP) are both electrical responses to visual stimuli, they differ in that the former requires a number of visual stimuli that flash in succession in the form of letters or symbols, while the latter needs constant exposition to stimuli. Also, the ERP captures the brain reaction about 300ms after the stimulus is presented (so-called P300 component), which represent a positive peak, while the SSEP is elicited when the frequency of the brain activity patterns matches the frequency shown during the stimulus. The Event Related Desynchronization (ERD) reflects the cortical activation of neurons, it does not necessitate of visual stimuli and it can be observed during Motor Imagery (which is the imagination of movement).

Albeit differences between EEG patterns affect the type of BCI functionality,[54] they do not require to be used in isolation but can be combined together. This hybrid BCI is still merely used for clinical applications but, since they may overcome the disadvantages of a traditional BCI, it is expected an extension of such device outside the research lab. Furthermore, for the purpose of this thesis, this is a fundamental aspect because it is already provided that EEG based BCI devices are already used, or proved to be adapt, for user authentication and identification purposes.[55]

[54] S. G. Mason, A. Bashashati, M. Fatourechi, K.F. Navarro, and G. E. Birch, 'A comprehensive survey of brain interface technology designs', (2007), Volume 2, Issue 35, Ann. Biomed. Eng, 137–169, available at <https://link.springer.com/article/10.1007/s10439-006-9170-0> accessed 3 February 2018.
[55] K. Revett, S. T. De Magalhaes, 'Cognitive biometrics: Challenges for the future', (2010), in Global Security, Safety, and Sustainability, Springer, 79–86, available at <https://link.springer.com/chapter/10.1007/978-3-642-15717-2_10> accessed 3 February 2018.

2. 3. 1. Brain-Computer Interface: commercial use in gaming and mobile applications

A BCI exploits the constant brain activity as an input in order to deliver a specific signal output. In particular, the BCI directly measures brain activity associated with the user's intent and translates the recorded brain activity into corresponding control signals for BCI applications.[56] From this description, the BCI appears to be a futuristic technology that promises to read people's intentions, perception and attitudes. However, the reality is much different and it is useful to state from the outset that a BCI cannot read the mind nor read thoughts (at least for now). This technology can only detect and classify specific patterns of activity in the ongoing brain signals that are associated with specific tasks or events and its functions are generally limited by the number of commands recorded through the EEG.

This means that when BCI technology is applied in the gaming industry, through the use of consumer-grade EEG device, the user's game experience is hindered by a long training time, low reliability and, above all, limited control functions.[57] Therefore, most games are not very challenging or multipurpose but they are very simple in their nature and objective. For example, a common game developed by Crooked Tree Studios called "Throw Truck With Your Brain" exploits the ability of a player to focus his thought on a single object to indeed through the truck. This game uses a neuro headset to interpret the electrical activity of the brain to pick up and hurl objects at opponents.[58] Another challenging application that uses neuro headset is called "Art of Zen" which measures your inner zen level by analyzing the EEG brain wave and then displays it in the monitor. In doing so, it is supposed to help the user to reach a full meditative state.[59]

Although the aim of the games and apps *per se* may not be exciting, their end purposes are varied and range from education and health to wellness and simple entertainment. That is why it is expected that demand for neurogaming and wellness or fitness apps will increase over the next 5

[56] B. Graimann, (n. 49), 2.
[57] M. Ahn, J. Choi and S. Chan Jun, 'A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users', (2014), Volume 14, Issue 8, Sensors, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4178978/> accessed 4 February 2018.
[58] See Neurosky official website, 'Content', available at http://developer.neurosky.com/wp-content/uploads/2016/07/Throw_Trucks_With_Your_Mind_Revolutionizing_Entertainment_with_Neurogaming.pdf > accessed 22 October 2017.
[59] NeuroSky official website, 'Store', available at <https://store.neurosky.com/products/art-of-zen> accessed 22 December 2017.

to 10 years.[60] Moreover, being the gaming industry a very competitive market, innovation and advancement of the BCI technology are easily predictable.

2. 3. 1. 1. The Promise of the BCI is an Infinite Brain Databases.

Be that as it may, all these apps and games have in common the fact that to function properly they constantly need to extract EEG data, require user subscription as well as IP address and store all these information into a specific database.[61] It is relevant to recall that the extraction process of the BCI does not discriminate between the data needed for the commanding operation and other less critical data, because it is the raw EEG data that are being sent and stored in the processing operation. Such a statement was taken as a *contrario* argument from the fact that many scholars developed technical means to limit the quantity of EEG information sent to the BCI device.[62] Also, being the BCI technology fundamentally based on a neuroimaging technique, it must be taken into account that the amount of information shared with the device are massive by default and unknown to users, as only small parts of the brain activity are under voluntary control. The app "Art of Zen" is just a perfect example of the quantity of information shared with the device, because it uses such neuroimaging technique as the core element to provide its "service".

Conversely, by turning the argument on the quality of the information - meaning what can actually be inferred from the EEG signal when using such app or playing these games - the amount of information sent to the device appears to decrease. Many scholars explain this particular event by pointing at the mechanism behind the interpretation of EEG data. In fact, two elements are necessary for an accurate reading and, thus, a proper understanding of the information. These two elements, which need to be read in a synchronized way, are the EEG data itself and the video/behavioural data (hereinafter dataset); the latter referring to either the actual stimulus being

[60] M. Ahn, J. Choi and S. Chan Jun, (n. 58).
[61] See Emotiv official website, (n. 10).
[62] See A. Stopczynki et al., (n. 40), who demonstrated how an openPDS software, integrated into a BCI device, safeguard the privacy of the user by limiting the information sent to the latter. For the same concept, but technically different, see H. J. Chizeck and T. Bonaci, 'Brain-Computer Interfaces Anonymizer', (February, 2014), US Patent Application, available at <https://patents.google.com/patent/US20140228701> accessed 22 December 2018

shown or the motor movement of the user, depending on the mental strategies used to measure the brain activity (ERP, SSEP or ERD).[63]

These opposite arguments, together with the additional information shared with the manufacturer of the device and the app or game developer, are further analyzed in the next chapter, where the information collected are put in the specific context of the neurogaming and the "neuroapp" industry, in order to better analyze whether personal information is collected and stored by the BCI.

For the moment, however, it is essential to understand what can be inferred from the EEG signal, given that the BCI collects the whole activity of the brain. Therefore, in the next paragraph, it is presented what information are implied in the EEG data as such.

2. 4. The Characteristics of EEG data

From the outset, it is important to note that in the following analysis the information inferred through an EEG signal is not specifically related to app or gaming field. However, this is relevant because the signal extracted and stored through the BCI has the same characteristics as any other EEG signal, being the different functionality of the technology merely a consequence of what is analysed in a specific circumstance. Moreover, despite the already mentioned limitation of such technology, EEG data is an extremely rich signal which may capture significant brain activity of the user. Obviously, as technology continues to evolve, it is just a matter of time before that more and qualitative better information will be extracted and analysed.[64]

Starting with the most sensitive information voluntarily disclosed by the individual, many different brain-related studies highlighted how traces collected through EEG signal may be used for prevention, detection and diagnosis purpose in the medical field. In fact, some scholars have investigated how an increase of alpha activity, detected through EEG signal, is found when taking

[63] I. Simanova, M. Van Gerven, R. Oostenveld and P. Hagoort, 'Identifying Object Categories from Event-Related EEG: Toward Decoding of Conceptual representations', (2010), Volume 1, Issue 5, PloS, available at <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0014465> accessed 22 January 2018.
[64] B. E. Moore, 'The Brain Computer Interface Future: Time for a Strategy', (2013), a research report submitted to the Air War College, Air University of the USAF, available at <http://www.au.af.mil/au/awc/awcgate/cst/bh_2013_moore.pdf> accessed 22 January 2018.

antidepressants and addictive drugs like morphine, heroin and marijuana,[65] while other studies demonstrated that alcoholics increase the occurring of beta waves. [66] Even more interesting - or alarming, depending on the purpose and use of such information – is the diagnostic value of EEG.

If willing, BCI can detect brain tumor,[67] epilepsy seizure,[68] sleep disorder [69] and schizophrenia diseases.[70]

EEG recording can also be used for identification and authentication of users. It has been shown that a characteristic of EEG signal is to be unique for every individual, meaning that any two persons have different EEG signal, which is stable over time and resistant to experimental change in both closed eyes and open eyes conditions.[7172] Thus, different experiments then successfully demonstrated that such EEG characteristic can be used for either identification (with an accuracy of 80-100%) [73] or authentication purpose.[74]

---

[65] Z. M. Hanafiah, M. N. Taib, N. Hamid, 'EEG Pattern of Smokers for Theta, Alpha and Beta Band Frequencies', (2010), Research and Development (SCOReD), IEEE Student Conference on. IEEE, available at <https://ieeexplore.ieee.org/document/5704025/> accessed 23 January 2018.

[66] D. Di, C. Zhihua, F. Ruifang, L. Guangyu, L. Tian, 'Study on Human Brain after Consuming Alcohol Based on EEG Signal', (2010), Volume 5, Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference IEEE, 406–09, available at <https://ieeexplore.ieee.org/abstract/document/5564084/> accessed 23 January 2018.

[67] V. S. Selvam, S. Shenbagadevi, 'Brain Tumor Detection Using Scalp EEG with Modified Wavelet-Ica and Multi-Layer Feed Forward Neural Network', (2011), Engineering in Medicine and Biology Society, Annual International Conference of the IEEE, 6104–09, available at <https://www.ncbi.nlm.nih.gov/pubmed/22255732> accessed 23 January 2018.

[68] S. F. Liang, F. Z. Shaw, C. P. Young, D. W. Chang, Y. C. Liao, 'A Closed-Loop Brain Computer Interface for Real-Time Seizure Detection and Control', (2010), Engineering in Medicine and Biology Society, Annual International Conference of the IEEE, 4950–53, available at <https://www.ncbi.nlm.nih.gov/pubmed/21096670> accessed 23 January 2018.

[69] H. Koch, J. A. Christensen, R. Frandsen, L. Arvastson, S. R. Christensen, H. B. Sorensen, P. Jennum, 'Classification of Irbid and Parkinson's Patients Using a General Data-Driven Sleep Staging Model Built on EEG', (2013), Engineering in Medicine and Biology Society, 35th Annual International Conference of the IEEE, 4275–78.

[70] C. N. Karson, R. Coppola, D. G Daniel, D. R. Weinberger, 'Computerized EEG in Schizophrenia', (1988), Volume 14, Issue 193, Schizophrenia Bulletin, available at <http://psycnet.apa.org/record/2005-26897-010> accessed 25 January 2018.

[71] L. De Gennaro, C. Marzano, F. Fratello, F. Moroni, M. C. Pellicciari, et al., 'The Electroencephalographic Fingerprint of Sleep is Genetically Determined: a Twin Study', (2008), Volume 64, Annals of neurology, 455–460, available at <https://www.ncbi.nlm.nih.gov/pubmed/18688819> accessed 25 January 2018.

[72] J. Lynch, D. Paskewitz, and M. Orne, 'Intersession Stability of Human Alpha Rhythm Densities', (1974), Volume 36, Issue 5, Electroencephalographic Clinic Neurophysiological, 538–540, available at <https://www.sciencedirect.com/science/article/pii/0013469474902119> accessed 25 January 2018.

[73] M. Poulos, M. Rangoussi, N. Alexandris, 'Neural Network Based Person Identification Using EEG Features', (1999), Volume 2, Acoustics, Speech, and Signal Processing, IEEE International Conference on. IEEE, 1117–1120, available at <https://ieeexplore.ieee.org/document/759940/> accessed 25 January 2018.

[74] S. Marcel, J. D. R. Millan, 'Person Authentication Using Brainwaves (EEG) and Maximum a Posteriori Model Adaptation', (2007), Pattern Analysis and Machine Intelligence, IEEE Transactions, 743–752, available at <https://ieeexplore.ieee.org/document/4107576/> accessed 26 January 2018.

What is essential to note, is that such sensitive information can be obtained with a low number of electrodes and using a non-invasive method which is a relatively cheap method.

Eventually, EEG signal may reveal further sensitive information such as PIN numbers, date of birth, religious and political beliefs even against the will or awareness of individuals. In fact, in a lab experiment, Martinovic *et al* illustrated how the brain's response to a particular stimulus (P300 paradigm explained in 2.3) can be used to infer these sensitive information.[75] Paradoxically, by employing such technique, it is possible to efficiently collect the most sensitive information, since an involuntary response is stronger when a stimulus recalls the most important pieces of individual experience. In other words, the more a stimulus is related with an individual the easiest it is to capture the sensitive information, because the response captured by the BCI is sharper. These security problems are considered so tangible that they forced scholars from different backgrounds to call for an interdisciplinary approach and to develop technical means to tackle neurosecurity problems (i.e. the protection of neural devices from malicious attackers trying to exploit, block, eavesdrop or generally endangering the safety of users),[76] while other scholars already attached the label of a new generation type of cybercrime.[77]

[75] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, 'On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces', (2012), the Proceedings of the 21st USENIX Security Symposium, USENIX, available at <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf> accessed 24 October 2017.
[76] T. Denning, Y. Matsuoka and T. Kohno, 'Neurosecurity: Security and Privacy for Neural Devices', (2009), Volume 27, Issue 1, Journal of Neurosurgery, available at <https://www.ncbi.nlm.nih.gov/pubmed/19569895> accessed 1 August 2018.
[77] See M. Gasson and Bert-Jaap Koops, 'Attacking Human Implants: A New Generation of Cybercrime', (2014), Volume 5, Issue 2, Law, Innovation and Technology, 248-277 available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485301> accessed 18 March 2018.

2. 5. Conclusion

The Brain-Computer Interface device have come a long way since its first development in 1973 by Professor J. J. Vidal. Its value now appears to be recognized even outside the medical field and, in particular, in the gaming and app industry. Such development has caused some scholars to question the ethical and philosophical consequences of the introduction of such new technology,[78] while others have focused on whether the privacy of individual users is affected and how it may be better protected.[79] However, there is no literature on the data protection issues that the BCI raises.[80]

Nonetheless, by an analysis of the technology behind the commercial application of BCI, this chapter highlighted why data protection legislation may come into play. The fact that the output of a BCI is dependent on an input constituted of brain activity/data, almost inherently begs the question about the kind and extent to which such technology detects and reads such information. This is an essential step in assessing whether personal information are collected and, therefore, whether EU data protection legislation may be called upon to limit indiscriminate dissemination of brain data.

In this regard, three elements have been found relevant in this chapter. Firstly, the BCI does not limit the collection of brain data to the one necessary for the required functional performance, but it collects and stores the whole raw EEG data. Secondly, these EEG data reveal a vast amount of involuntary information about the health condition and – potentially – about everything an ill-intentioned person wants to find out about data subjects. Thirdly, in the specific context of neurogaming and "neuroapp", a combination of EEG data and data required to access the "service" may give to the app's developers and device's manufacturers a tremendous amount of information about an individual.

[78] G. Tamburrini, 'Brain to Computer Communication: Ethical Perspectives on Interaction Models', (2009), Springer, available at <https://www.researchgate.net/publication/225735446_Brain_to_Computer_Communication_Ethical_Perspectives_on_Interaction_Models> accessed 25 April 2018.
[79] See T. Bonaci, R. Calo and H. J. Chizeck, (n. 16); and A. Stopczynki et al., (n. 40).
[80] The only paper concerned with specifically data protection issues is the one of D. Hallinan,P. Shutz and M. Friedewald and P. De Hert, (n. 22).

However, it has also been pointed out that technology limitation decreases the quality of these information. In particular, a correct interpretation of EEG data may only be based on the analysis of a given dataset. In this concluding remark it is useful to emphasize that although many doubts rest on how singular is a user in these databases and how much can be inferred about him, it is certainly true that these information relate to the most private sphere of individuals and, as such, must be legally protected from an indiscriminate dissemination.

Experience tells us that what we thought to be merely science-fiction a decade ago often becomes the science fact of today. Therefore, similar to the experience with computer and networking technology, rapid advancements in neurotechnology will render brain data regulation outdated with the consequence of increasing risks for individuals.

3. Brain-Computer Interface and personal data in the GDPR

3. 1. Introduction

Although the BCI has not reached the level of maturity to substantially affect our daily life, it undoubtedly presents certain characteristics to potentially change the way we live. Emerging ethical debates correctly point out issues concerning the exponential use of this technology such as excessive use, personality and personhood, mental integrity and mind reading. [81] Notwithstanding, given the quality and quantity of the information extracted by the BCI, it is essential to pay more attention to the shifting potential of BCI data in the society.

In this regard, the right framework to limit an unregulated and unprotected diffusion of BCI data is provided by the General Data Protection Regulation (GDPR). The latter is an instrument that may address from the outset the shifting potential of BCI data and reduce their negative impact on individuals. The GDPR is a legislation based on the principle of technological neutrality thus, in theory, equipped to take on issues arising from new developments in the technology field.[82] In fact, the principle of technological neutrality aims to protect personal data regardless of the technology used or how the personal data is stored to prevent circumvention of the law.[83] Essentially, it promotes and affirms the futureproofing essence of the GDPR in order to provide benefits to all parties.

Therefore, despite the technological leap of the BCI, this chapter examines whether the processing of information by the BCI falls under the scope of the GDPR and whether the heightened protection provided by such legislation applies to it. Eventually, it points out what are limitations and challenges of the EU data protection legislation in light of such processing operation.

[81] F. Nijboer, J. Clausen, B. Z. Allison and p. Haselager, (n. 13).
[82] See Recital 15 of the GDPR.
[83] See European Commission, '*The GDPR: New Opportunities, New Obligations'*, publication Office of the European Union, 2018, available at <https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf> accessed 19 July 2018.

3. 2. The Concept of Personal data in the GDPR

In EU law, classifying information as personal data bears a great deal of (legal) consequences, being the material scope of the GDPR closely determined by such a notion. For every time personal data are processed the data protection principles, rights and obligations come into play; with some exceptions.[84] Under Article 4 of the new Regulation personal data means:

> *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*

From the outset, by reading this Article it appears that different definitions must be clarified in order to consider an information as falling under the scope of the GDPR; namely, "identification and identifiability", "any information", "relating to", "natural person" and "anonymization". However, for what concerns the BCI and the purpose of such analysis, it is appropriate to dive deep in the examination of the notions of "identifiability", "any information" and "anonymization" only. This is so because the other terms are less problematic in the context of the BCI.

For one, it is clear that the information extracted by the BCI relates to a "natural person". For another, the concept of "relates to" has been interpreted in a broad sense by A29WP and then by the CJEU. The former stated that the elements that constitute the relation with a natural person are content, purpose and result, yet they do not need to be cumulative present; [85] the CJEU adopted a broad approach in Novak.[86]

Conversely, by having regard to the findings outlined in Chapter 2, "identification and "identifiability", the concept of "any information" and "anonymization" are of more direct interest to this paper. Firstly, it is not clear when a natural person is identified. [87] The common

[84] See Article 2 of the GDPR. Notice that exceptions are not analyzed because falls outside of the scope of this thesis.
[85] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, ('WP136'), 2007.
[86] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017].
[87] European Union Agency for Fundamental Rights, Council of Europe, Handbook on European data protection law, (2014), at 39.

understanding among legal scholars is that identification requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognizable as an individual.[88] For example, depending on the context, a person's name may suffice whilst in other circumstances other identifiers such as date and place of birth may be needed to identify a natural person. At the same time, and even more controversial, the notion of an identifiable natural person also appears to be problematic. In this regard, Recital 26 GDPR tries to clarify when a person is identifiable by establishing another context-dependent analysis for deciding when personal data are present.[89]

Secondly, the initial notion of "any information" must be clarified in light of either a semantic understanding of this concept and the lack of a clear judgement by the CJEU.[90] In particular, it is necessary to understand whether information as such fall under the scope of the GDPR, or whether only information that bears a kind of significance or knowledge is taken into account by the EU Regulation.[91] This is particularly relevant in the BCI since the data collected are a mere sequence of wave lines that do not yield information, unless interpreted and analyzed further.

Thirdly, if BCI data are anonymized the GDPR does not apply. However, it has been highlighted in chapter 2, that a characteristic of the EEG signal is to be unique for every individuals' EEG data. This certainly challenges the application of the GDPR to such data so that a clear standard should be set.

Therefore, since it is through the interpretation given to these concepts that EEG extracted data can fall under the scope of the GDPR, they are further analyzed by interpreting the opinion of the

[88] Ibid.
[89] It states that:
'*To ascertain whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.*
[90] L. Floridi, 'Is Information Meaningful data?', (2005), Volume 70, Issue 2, Philosophy and Phenomenological Research, 351-370, available at <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1933-1592.2005.tb00531.x> accessed 19 July 2018; see also an interesting analysis of this concept in N. Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law', (2015), Volume 35, Issue 1, Law, Innovation and Technology, available at <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 19 April 2018.
[91] L. Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight', (2015), Volume 35, Issue 1, Oxford J. Legal Studies, 91-120, available at <https://academic.oup.com/ojls/article-abstract/35/1/91/1530306?redirectedFrom=PDF> accessed 19 April 2018.

Article 29 Working Party (from hereafter A29WP),[92] the European Court of Justice (ECJ) and relevant literature.

3. 2. 1. Anonymization and Pseudonymization

"Unlike blood pressure data that would have many individuals falling within identical measurement numbers, electrophysiological brain signals will never be identical for any two individuals".[93]

Anonymization refers to the process of masking, removing or altering determinate elements of the data to make it impossible to trace back a certain person. The GDPR, albeit quite silent on this, underlines that "anonymized data are personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[94] Different from anonymized data, the GDPR recognizes and defines pseudonymous data as personal data.[95] Simply put, pseudonymous data is information that no longer allows the identification of an individual without additional information and is kept separate from it.[96] Thus, where pseudonymized data falls under the scope of the GDPR, anonymous data gives a leeway to controllers as no data protection rules apply to this form of information. A question with EEG data is whether the anonymization technique suffices to render these data anonymous, in light of their unique link with data subjects and the fact that A29WP heightened the threshold by declaring that anonymization must be irreversible.[97]

For one, even where EEG data can be stripped of their identifier the data are not anonymous because of their intrinsic capability to single out an individual. For another, the quality of EEG data may reduce the capability of singling out an individual through such data, as the experiments proving the uniqueness of the data have been tested under certain determinate conditions.[98] Notwithstanding, it is arguable that the constant collection of EEG data through BCI apps would undoubtedly render data subjects directly or indirectly identifiable, despite the anonymization

[92] The Article 29 Working Party is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The European Data Protection Board (EDPB) will replace the Article 29 Working Party under the EU GDPR.
[93] A. Greenberg, (n. 23).
[94] See recital 26 of the GDPR.
[95] See Article 4(5) and Recital 26 GDPR.
[96] Ibid.
[97] Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, ('WP216'), 2014.
[98] L. De Gennaro, C. Marzano, F. Fratello, F. Moroni, M. C. Pellicciari, et al., (n. 72).; J. Lynch, D. Paskewitz, and M. Orne, (n. 73).

technique. In this regard, it is useful to remind that controllers can combine another dataset – for example, Facebook dataset for when data subjects log in through their Facebook credentials – so that identification of individuals can be efficiently achieved.[99] Moreover, the inappropriateness of anonymization techniques for this type of data EEG data is further demonstrated by the availability of EEG dataset in the public domain for research purposes as well as of other datasets.[100] This certainly reduces the irreversibility of anonymization requirement enshrined by A29WP.

Another point suggesting the incompatibility of the anonymization technique for EEG data is the fact that, at the EU level, technological developments must be taken into account when assessing a dataset as anonymous.[101] As Hallinan *et al*. put it: "neurodata not judged to be uniquely identifying today, may not be judged so tomorrow".[102]

Finally, to clarify that EEG data can uniquely identify data subject as of today, it is useful to read the privacy policy of Emotiv, a BCI manufacturer. Emotiv provides an updated version of its privacy policy where it does not claim to anonymize EEG data anymore. Rather, it now claims these data to be pseudonymized.[103] It is therefore evident that EEG data collected through the BCI cannot be anonymized, but merely pseudonymized. As such they are personal data and fall under the scope of the GDPR.

For all these reasons a privacy policy like the one of Neurosky, claiming that an aggregation of EEG data renders their data anonymous, is debatable[104] As a research paper highlighted how easy it was to identify individuals through aggregate mobility data, by linking together short journey segments as people make very similar journeys every day,[105] it is useful to again remind that because EEG data are not identical for any two individuals, it is sufficient to link together short recording to identify an individual in the aggregate data.

---

[99] See Article 29 Working Party Opinion WP216, (n. 98).
[100] Some websites providing publicly accessible EEG data are available at <https://github.com/meagmohit/EEG-Datasets> accessed 19 May 2018
[101] See Article 29 Working Party Opinion WP216, (n. 99), 9; See also Opinion 4/2007 of the Article 29 Working Party, (n.86), 15.
[102] D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n.22), 65.
[103]See Emotiv official website, (n. 10).
[104] Neurosky official website, 'Privacy policy', available at <https://effectivelearnercloud.com/el/policies/?privacy> accessed 19 July 2018.
[105] F. Xu, Z. Tu, P. Zhang, X. Fu and D. Jin, 'Trajectory recovery From Ash: User Privacy is Not Preserved in Aggregated mobility Data', (2017), Proceedings of the 26th International Conference on World Wide Web, 1241-1250, available at <https://arxiv.org/abs/1702.06270> accessed 19 july 2018.

However, complete anonymization strictly depends on the concepts of "identification and identifiability" because the central tenet of the GDPR is that data are not anonymized as long as an individual is identifiable. Therefore, the two concepts are to be analyzed further.

3. 2. 2. Identifiable Natural Person

According to Article 4 GDPR, personal data shall mean 'any information relating to an identified or identifiable natural person ('data subject')'. An identified person is an individual who can be distinguished from all other persons while an identifiable natural person refers to an individual who is not yet identified, but identification is possible by conducting further research. Such an individual may be identified or identifiable; directly or indirectly. He or she is directly identified if he or she is described in this information through unique identifiers such as personal name in a familiar context; for example, a person's name in a small group such as a classroom is information that directly identifies the individual.

Conversely, a person is indirectly identified where additional identifiers such as date and place of birth are needed to identify the individual; for example, a person's name may not suffice to (directly) identify an individual in a large city like London as indeed additional identifiers (or further research) need to be used to ensure that an individual is not confused with someone else.[106] One is indirectly identifiable if the combination of not unique identifiers allow the individual to be distinguished. For example, an individual who monitors and surveilles the web may be able to take certain decisions about a web user even if the latter has not disclosed his or her identity in the narrow sense (unique identifiers). In other words, the necessity to have unique identifiers in order to pinpoint the identity of a person is no longer valid as EU law appears not to require high-standard of identifiability in view of its neutral approach to technology. At the same time, a mere hypothetical possibility to single out the individual is not enough for a person to be identifiable.[107]

According to both the A29WP and the CJEU, in order to assess whether identifiability is merely hypothetical or not depends on the context. In particular, the assessment must take into account all the factors at stake (the purpose of processing, the advantage expected by the controller, the interest

[106]European Union Agency for Fundamental Rights, (n. 88), 40.
[107] A29WP Opinion 4/2007, (n. 86).

at stake for individuals, the way the processing is structured, as well as the risk of confidentiality breached and anonymity), including technology and future development that would facilitate identification.[108] In light of this findings, especially once the CJEU declared dynamic IP address as personal data,[109] scholars pointed out a broad definition of personal data in the GDPR.[110]

In the context of this analysis, nevertheless, a point is crucial. In fact, while there is little doubt that EEG data collected by mobile apps using BCI technology are personal data, given that – inter alia – the purpose of processing EEG data only makes sense if the individual is identified or else the BCI would not recognize the brainwave signal, thus hindering the functionality of the BCI;[111] some questions may arise as to whether app developers are processing EEG personal data. It is indeed demonstrated that such entities, that own multiple mobile apps within the AppStore, acquire EEG data.[112]

However, in view of the limitation underlined in *Breyer* to the broad definition of personal data, such entities may claim that they would experience a disproportionate effort in terms of time, cost and man-power - especially if the law bans such procedure - so that the risk of identification from EEG data appears, in reality, to be insignificant. In fact, despite some legal scholars claimed that the *Breyer* case broadened the scope of data protection by declaring that even a dynamic IP address is personal data;[113] some others interpreted the decision of the CJEU as indeed limiting the concept of identifiability and thus the notion of personal data in the GDPR.

This quite banal affirmation stems from the fact that EEG data are merely graph simply showing a sequence of lines with no apparent significance for anyone, but specialized scientists. A question that thus arises is how the GDPR treats this type of information. In this regard, the concept of "any information" must be analyzed further.

---

[108] Ibid.; See also Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* [2016].
[109] Ibid.
[110] See N. Purtova, (n. 91); F. J. Zuiderveen Borgesius 'Breyer case of the Court of Justice of the European Union: IP addresses and the personal data definition', (2017), Volume 3, Issue 1, European Data Protection Law Review, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933781> accessed 19 April 2018.
[111] See F. Lotte, F. Larrue and C. Muhl 'Flaws in Current Human training Protocols for Spontaneous Brain-Computer Interfaces: Lessons Learned from Instructional Design', (2013), Volume 7, Frontiers in Human Neuroscience, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3775130/> accessed 19 April 2018.
[112] See H. Takabi, A. Bhalotija and M. Alohaly, 'Brain Computer interface Applications: Privacy Threats and Countermeasures', (2016), IEEE 2nd International Conference on Collaboration and Internet Computing, available at <https://ieeexplore.ieee.org/document/7809697/> accessed 22 July 2018.
[113] See F. J. Zuiderveen Borgesius, (n. 111).

3. 2. 3. Any Information

What constitutes information under the GDPR? Shall data bearing no specific significance (data with no meaning) considered to be information falling under the scope of the GDPR?

In the literature, differences emerge between a semantic view that regard information as composed of data and meaning,[114] and a modern view which makes no distinction between data and meaning as everything is to be considered information.[115] The former put emphasis on whether human beings can make sense of a given data, while the latter takes into account technological process (f.i. Big Data analysis).

As regards the law, the term 'any information' has been outstretched in *Nowak* since the Court at para. 46 pointed out that:

> "any information […] reflects the aim of the EU legislature to assign a wide scope to [the concept of personal data], which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments".[116]

In this regard, A29WP further clarifies that the GDPR applies to '*any sort of information*'[117] regardless of its format which may be 'alphabetical, numerical, graphical, photographical or acoustic' and it also adds that information stored in a computer memory by means of binary code, or on a videotape as well as sound and image data are personal data, since covering the automatic processing of information is one of the aim of the EU legislation on data protection.[118]

Overall, it appears that the concept of "any information" is construed broadly and thus in line with the objective of the EU legislature to provide a neutral approach to technology. In this circumstance, also the app developers are processing personal data.

---

[114] L. Floridi, (n. 91).
[115] See N. Purtova, (n. 111); see also M. Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics', (2017), Volume 10, (forthcoming) University of Toronto Law Journal, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2983045> accessed 21 July 2018.
[116] Case C-434/16, *Nowak v Data Protection Commissioner*, [2017].
[117] Emphasis added.
[118] Op. cit. supra 11 at 7.

3. 3. A Preliminary Conclusion on BCI and Personal Data

The BCI has the particular characteristic to extract data from the brain that are unique to any individual. In the specific field of mobile apps, it not only collects a vast amount of information over time, it also necessarily shares it with other entities. According to the GDPR, the information gained by these controllers are personal data regardless of the protection provided by the anonymization techniques.

It must be noticed that not only EEG data are intrinsically challenging to anonymize, but the constant collection of such data together with the availability of other datasets certainly tip the balance toward considering anonymization technique as inadequate. Also, since the concept of identifiability has been stretched in the GDPR and requirements of irreversibility of anonymization heightened, EEG data can always be considered personal data. In this regard, confirmation has been definitely provided by Emotiv privacy policy which considers EEG data as pseudonymous and, thus, personal data. It is therefore evident that protection of individuals' data cannot be attained through anonymization technique, since any processing of EEG anonymized data must be considered as processing personal data.

However, as chapter 2 has demonstrated, EEG data are highly dimensional that often carry extremely private information of the individual. In fact, information contained in such neuro signals potentially relates to health conditions of data subjects, mental states as well as bank information, PIN codes, individuals' preferences, religion and political beliefs. Although some of these information can only be extracted by actively presenting the right stimuli, this fact alone does not render the risks less topical since app developers collect EEG data and impart the stimuli.

Additionally, because the EEG data are synchronized with the video/behavioral data input presented within the apps (stimuli), the reading and understanding of EEG signal is facilitated (see Chapter 2). Also, the limitation provided in *Breyer* shall not be taken by such entities to claim that they do not process personal data. The GDPR considers any type of data, regardless of it bearing significance, as personal data from the outset. Therefore, even a graph of the EEG data which is – *per se* – either personal data or a source of personal data in the future, must be considered as falling under the scope of the GDPR. The old tenet related to genetic data for which only the use of

biological samples are personal data,[119] cannot be adapted to the EEG graph given the broader concept of personal data enshrined in the GDPR and in *Breyer*.

In this regard, it is necessary to analyze whether the highest level of protection accorded by the GDPR to sensitive data applies to these EEG data. In particular, since the GDPR has not categorized these data, it is useful to underline the consequences of such carelessness from the EU legislator.

3. 4. Sensitive Data in the GDPR

The GDPR not only protects the processing of personal data but it also ensures a higher level of protection for the processing of special categories of personal data (sensitive data). Its Article 9 gives a comprehensive - albeit non exhaustive - list of personal data that must fall within this special categories; including data that reveal racial or ethnics origin, political opinions, religious or philosophical beliefs, or trade union membership as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The higher level of protection for the processing of these special categories of personal data is established through a general prohibition to process such information. Therefore, personal data that refers to one of the special categories of personal data may only be processed where one of the exceptions apply.[120] The rationale behind this stricter legal regime stems from the nature of the personal information processed and a general presumption that misuse of these information is likely to have more severe consequences for the individual's fundamental rights;[121] including the right to privacy and non-discrimination.

Considering the extremely singular characteristics of brain data and their link to information that may reveal health condition of data subjects as well as religion, political beliefs and individual's personality, they should be treated as particular sensitive data within the meaning of Article 9 of

[119] A29WP Opinion 4/2007, (n. 86), 9.
[120] Article 9 of the GDPR; see also Article 29 Working Party, *Advice paper on special categories of data (sensitive data)*, 20.04.2011.
[121] Ibid.

the GDPR and, thus, processed only under the provided exceptions and safeguards. In particular, data concerning health fits within definition of health elaborated in the GDPR because EEG data can be considered as information derived from the testing or examination of a body part or bodily substance, including biological samples;[122] while the other data fall under the definitions of racial or ethnic origin, political opinions, religious or philosophical beliefs as well as trade union membership.

Through this simple line of reasoning it appears that the brain data are protected and issues of privacy and non-discrimination are excluded or, at least, minimized. Nevertheless, the legal realm often differs from the real one. From a legal perspective, indeed, it can be logically inferred that EEG data are legally valued as any other type of personal data simply because since there is no mention of brain data nor EEG data in the EU legislation. This implies that the processing of EEG data has no different form of relationship to fundamental rights than the processing of any normal personal data.[123]

In this regard, apart from this logical conclusion, the next chapter provides a legal analysis of why brain data are legally treated as personal data rather than sensitive, despite their clear importance put data subjects at high risks.

3. 4. 1. A Missed Opportunity for the EU Legislator

In the context of neurogaming and neuroapps, both manufacturers and app developers collect and store EEG personal data. However, these data are still raw because they do not provide such entities with sensitive information about data subjects. In fact, mental diseases are difficult to extract since a specific algorithm must be employed.[124] In general, interpretation and inference of these data are

[122] See Recital 35 of the GDPR.
[123] An argument that has been put forward in the literature with regard to genetic data before the introduction of the GDPR. See D. Hallinan, M. Friedewald and P. De Hert, 'Genetic Data and the Data Protection Regulation: Anonymity, Multiple Subjects, Sensitivity and a Prohibitionary Logic Regarding Genetic Data', (2013), Volume 29, Computer Law & Security Review, 317-329, available at <https://www.sciencedirect.com/science/article/pii/S0267364913001040> accessed 21 July 2018.
[124] See, for what concern epileptic seizures, D. Gajic, Z. Djurovic, S. Di Gennaro and Fredrik Gustafsson, 'Classification of EEG signals for detection of epileptic seizures based on wavelets and statistical pattern recognition', (2014), Volume 2, Issue 26, Biomedical Engineering: Applications, Basis and Communications, available at <http://liu.diva-portal.org/smash/get/diva2:746664/FULLTEXT01.pdf> accessed 15 March 2018.

far from trivial since they require a combination of knowledge from different fields.[125] The EEG data must, thus, be analyzed and further processed to infer sensitive information about an individual.

Even the definition of health data appears to be clear in this regard since it considers health data only the information derived from the testing or examination of a body part. The relevant element in the definition is the term "derived". In the Oxford dictionary, derive is explained as: obtain something from. With the BCI, controllers obtain raw personal data; the graph. The sensitive information are[126] not there yet, but they must be obtained from a further process. Therefore, only the inference is protected, rather than EEG data *per se* which, indeed, appears to be as a raw personal data in the eyes of the EU law. In the same line, the other sensitive data are also raw personal data.

3. 4. 2. A Complicated Framework for a Simple Problem

In the GDPR, in order to understand whether the raw EEG data collected through wearable technology are to be considered sensitive data, one of the criteria that must be taken into account is the intended use for such data.[127] By reading the privacy policy of the principal manufacturers, it is possible to grasp this relevant criterion.[128]

It appears that they process these data to – *inter alia* – provide 'information regarding [the] overall cognitive performance relative to other users of similar age or other characteristics', to 'better

[125] P. Arico', G. Borghini, G. Di Flumeri, A. Colosimo, S. Bozzi and F. Babiloni, 'A passive brain–computer Interface Application for the Mental Workload Assessment on Professional Air Traffic Controllers During Realistic Air Traffic Control Tasks', (2016), Epub, available at <https://www.ncbi.nlm.nih.gov/pubmed/27590973> accessed 15 March 2018.

[126] The use of the plural form is intentional. A characteristic of EEG data processed through the use of BCI is to not only yield one type of sensitive data (health or religious beliefs) but multiple types of sensitive data at the same time.

[127] Article 29WP, *ANNEX – Health Data in Apps and Devices*, February 2015 available at <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> accessed 15 March 2018.

[128] Four main privacy policies of four BCI manufacturers were analyzed, namely: Emotiv, Neurosky, Muse and OpenBCI. However, this paper will mainly refer to the Emotiv one for various reasons. First, not every manufacturer has a privacy policy (OpenBCI). Second, only Emotiv directly refers to EEG data and makes a clear distinction about how it treats such information. Both Muse and Neurosky have a general privacy policy that do not allow to draw a comprehensive claim.

understand [individuals] needs and interest', and they eventually share individualized and aggregated EEG data for 'scientific, medical and historical research purposes'.[129]

By taking the perspective of individual users, the processing of EEG data by these companies for their own purposes appear to be riskier; since the processing for scientific, historical and medical purpose is typically done by applying certain safeguards [130] and it is demonstrated by the GDPR itself, which offers an exception to provide a legal basis for the re-purposing of such data. A comment can be made about whether such research institutions are to be private or public held, since the purpose of processing and, thus, the intended use of data may change between the two.

Therefore, as the intended use of EEG data is to analyze and compare it with EEG data from other people or to understand individuals' needs and interest better, it is safe to say that manufacturers definitely held sensitive health information about their users. First, the accumulation (trained and further EEG data) and the combination of a vast amount of biometric and other personal data of the same individual facilitate the understanding and reading of neuro-signal.[131] Moreover, because the EEG data are synchronized with the video/behavioral data input presented within the apps (stimuli), an interpretation yielding sensitive information is speeded up (see Chapter 2). Second, when comparing EEG data of different individuals, small changes in the intensity of the brain waves may give information about particular mental diseases or addictions.[132] Third, according to A29WP data must not necessarily be accurate or performed in a medical context to be considered health data.[133]

This framework gives to controllers extensive leeway since the higher protection and tailored restrictions to the processing of sensitive data do not come into play from the outset; but it rest on the willingness and interpretation of controllers to provide better protection of data subjects. Although an *a posteriori* assessment by the data protection authority would certainly result in

[129] Emotiv official website, (n. 10).
[130] Article 89 GDPR.
[131] For example, Emotiv considers that EEG data are: electrical biosignals collected using EMOTIV devices and any related monitoring equipment, motion sensor outputs, associated data such as event timing markers, mouse, touchscreen, gestural, and keyboard events, eye movements, survey responses, choices, and preferences, tactile, audio, visual, and other sensory stimuli, reaction times, self-assessment, and cognitive performance. It also includes information that may be inferred from the foregoing sources, either alone or in any combination
[132] Z. M. Hanafiah, M. N. Taib, N. Hamid, (n. 66)' D. Di, C. Zhihua, F. Ruifang, L. Guangyu, L. Tian, (n. 67)..
[133] Article 29WP, ANNEX – *Health Data in Apps and Devices,* (n.128).

higher fines for controllers that consider sensitive data as merely personal information, the EEG data may have already been used by the controller or sold to other entities.

The situation is even less desirable if someone takes into account that such seemingly innocuous data are held by app developers, who base their business model on selling tailor-made ads.[134] Furthermore, such entities do not inform data subjects about the potential sensitive inference that can be captured by the EEG data and it can be questioned whether they take this responsibility once the further processing yielded the sensitive information.

Therefore, it can be concluded that extremely sensitive information of data subjects are being treated as any other bit of information. Although these data acquire the status of sensitive information only if further processed, this fact alone should not be a reason to ensure lower protection. First, this is an incentive to the transfer and selling of such data which, if not appropriately tracked, would be lost to the advantage of companies and to the detriment of data subjects. Second, it complicates the work of data protection authorities as they need to assess on a case by case basis whether such data are sensitive or not. Arguably, a definition of brain data within the GDPR would be more than helpful in this framework.

3. 5. Conclusion

The BCI has the particular characteristic to extract data from the brain that are both unique and highly sensitive. In the specific field of mobile apps, it not only collects a vast amount of information over time, it also necessarily shares it with other entities. However, despite the shifting potential of BCI data, the legislator did not provide a legal framework capable of reducing or eliminating the risks stemming from the processing of such data.

Notwithstanding the broadened scope of the concept of personal data in the GDPR, BCI data either challenges provisions of the GDPR like anonymization and pseudonymization; or render the application of the GDPR more complicated due to the lack of a definition of brain data. The latter issue is clearly recognizable when considering the sensitive nature of BCI data from a legal point

[134] C. Feijo, J. L. Gomez-Barroso, j. M. Augado and S. Ramos, 'Mobile gaming: Industry Challenges and Policy Implications', (2010), available at <https://core.ac.uk/download/pdf/148663771.pdf> accessed 15 April 2018.

of view. In fact, the sensitive nature of the data extracted from the BCI is not recognized by the GDPR from the outset. This is linked with an additional peculiarity of the BCI that is the capability to hide the sensitive information in a graph; at least from a data protection perspective.

In this framework, the lack of strict rules limiting the opportunities for using EEG data clearly risks infringing upon the fundamental rights of individuals. In fact, the protection of the right to health is conditional upon the assurance that no brain data may be known to third parties, who might use it to discriminate against the data subject. In other words, the protection of brain data is a *condition sine qua non* for any individual to not only protects his private lives but his very freedom.

4. Brain-Computer Interface and the Principle of Purpose Specification

4. 1 Introduction

As chapter 3 lays the groundwork for applying the GDPR to the processing of data through the BCI, this chapter provides an analysis of how the principles of purpose specification and data minimization impact on such data processing. The reason to focus on these two principles stems from the fact that, on the one hand, the principle of data minimization is of the outmost importance in light of the vast amount of personal information processed by the BCI while, on the other hand, the purpose specification is one of the most important principle for the protection of personal data,[135] proven by its recognition in the European Charter of Fundamental Rights.[136] Nonetheless, there are also other considerations.

First, there is a general call in the legal doctrine to focus more on the underlying principles of data protection law, rather than stifling the processing of information with complex and lengthy rules.[137] Second, in "Neurodata and Neuroprivacy: Data Protection Outdated?" professors P. De Hert *et al*. have already demonstrated an incompatibility of the processing of brain data with the rules of the GDPR [138] due to the fundamentally peculiar characteristics of such information. Third, whereas consent can generally provide protection to data subjects by placing them in control of their own personal data, this legal ground can only attain this important function if data subjects can clearly understand the consequences of a given data processing operation.[139] In the context of BCI, this is not the case because the intrinsic characteristic of EEG data is to yield information that are[140] unknown to data subjects as well as to controllers. [141]

Despite the clear incompatibility of the BCI with the rules of the GDPR, new BCI applications are already targeting consumers in conspicuous way. These BCI applications are not restricted to a

[135] T. Z. Zarsky, (n. 31).
[136] Article 8 of the Charter provides – *inter alia* - that "[personal data] must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
[137] B. J. Koops, (n. 30).
[138] See D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 22).
[139] See Article 7 of the GDPR entitled conditions for consent.
[140] The use of the plural form is intentional. A characteristic of EEG data processed through the use of BCI is to not only yield one type of sensitive data (health or religious beliefs) but multiple types of sensitive data at the same time.
[141] See A. Stopczynki *et al.*, (n. 40), 3.

small niche of individuals like patients where interest for patients' rehabilitation outweigh the interest in the protection of their data; and where personal data enjoy better protection. Rather, brain data are being constantly processed by BCI's manufacturers and app developers[142] and treated like any other bit of information. Therefore, it is useful to understand whether EEG data processed by the BCI can at least comply with the basics principles of the GDPR.

Therefore, since the legislator embedded general principles of data protection law within the GDPR, an examination of them appear to be more appropriate. However, in this author's view, there are no reasons to examine all the principles of the GDPR extensively. The principles of purpose specification and data minimization determine which personal data can be used by the controller to achieve his aim/s and they are the very first step in applying data protection laws and safeguards for any processing operation.[143] On the one hand, by specifying the purpose, the controller bounds itself to process only the data that are necessary and accurate for a determinate period to achieve its aims.[144] On the other hand, declaring the purpose for processing personal data provides data subjects with information and expectation about the handling of their personal data (transparency).[145]

Therefore, given the tight connection between the principles of purpose specification and data minimization with the other principles of the GDPR, a decrease of the effectiveness of these principles clearly results in an erosion of all principles of the GDPR.

Arguably, if it is found that certain differences in the characteristics of the data impact the effectiveness of even these broader principles, it can be asserted that the law must bring remedies since the neutrality of the legislation is lost, i.e., the qualities of futureproofing and benefits for all parties of the GDPR. One of such remedies can be the application of the legitimate interest principle as developed by Moerel and Prins.[146] In simple terms, such theory provides that applying

[142] See H. Takabi, A. Bhalotiya and M. Alohaly, (n. 113)..
[143] See Article 29WP, *'Opinion 03/2013 on purpose limitation'*, ('WP 203'), 2013.
[144] See Article 5 of the GDPR.
[145] See N. Forgo', S. Hanold and B. Schutze, 'The Principle of Purpose Limitation and Big Data', (2017), Springer; see also J. A. Cannataci and J. P. Misfud Bonnici, 'The End of the Purpose Specification Principle in Data Protection?', (2010), International Review of Law, Computers & Technology, available at <https://www.tandfonline.com/doi/abs/10.1080/13600861003637693> accessed 17 July 2018; see also F. Coudert, J. Dumortier and F. Verbuggen, (n. 32).
[146] L. Moerel and C. Prins, 'Privacy for Homo Digitalis: Proposal for a new Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', (2016), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 17 July 2018.

the legitimate interest principle as the only test for all the various phases of the life cycle of the personal data processing, where all the legal grounds established in the GDPR are no longer applicable as independent legal grounds, would ensure a better protection of individuals.[147]

Moreover, an implementation of such principle does not rule out the application of the usual legal grounds or principles for processing personal data. This is the reason why a framework of how the processing of EEG data in the BCI should be realized has been put forward in this paper. It is also highlighted how a difference emerges between the interested protected by data protection and privacy in the context of BCI.

4. 2. The principle of purpose specification in the GDPR

Amongst the basic principles of the GDPR, the principle of purpose specification always played a central role for the protection of personal data of individuals.[148] It formally originated from Convention 108 of the Council of Europe [149] and it is now enshrined in Article 8 of the European Charter of Fundamental Rights.[150] For what concern EU secondary law, Article 5 (1)(b) of the GDPR provides that personal data shall be:

> "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')"

In simple terms, the principle of purpose specification aims to protect data subjects by setting limits on how data collected by controllers are to be used or reused.[151] For example, personal data collected in the course of customer relations management by one company cannot be transferred and used by another company for marketing purpose, albeit it is accepted that the same company

[147] Ibid. at 2.
[148] A29WP, '*Opinion 03/2013'*, (n. 144), 4.
[149] 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (Adopted 28 January 1981, Entered into Force 1 October 1985) ETS No.108, available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> accessed 17 July 2018.
[150] See Article 8 of the EU Charter of Fundamental Rights.
[151] A29WP, '*Opinion 03/2013*', (n 144).

can use the collected data for marketing its own products. It is thus evident that purpose specification contributes to transparency, legal certainty and predictability of data processing by ruling out the use of personal data in a way that individuals may find unexpected.

At the same time, it also concedes a degree of flexibility to controllers in that it allows them to process even further the same data for purposes that they deem to be compatible with the initial one.[152] Therefore, purpose limitation has two conflicting main elements: the requirements of the collection of personal data where data must be collected for specified, explicit and legitimate purpose only (purpose specification); and a flexible limitations on further use (compatible use).[153]

In the relevant literature, it is generally held that these conflicting building blocks of purpose specification are at odds in the age of Big Data.[154] For one, the requirements of the first building block - which is meant to let any individual to reasonably understand which kinds of processing will be done on the data - cannot be attained where the main purpose of Big Data analyses is to find hidden usage patterns from the data being analysed and for which not even the entity collecting the data is aware of.[155] For another, the double negation provided in the second building block leaves a leeway to controllers to further exploit the collected data for a purpose which is different from the initial one.[156] Moreover, it is no mystery that companies take as a starting point a broad purpose for the processing of personal data in their privacy policy;[157] a custom that is not going to disappear with the entry into force of the GDPR.[158]

---

[152] Ibid.
[153] Ibid*;* see also L. Moerel and C. Prins, (n. 147).
[154] See T. Z. Zarsky, (n. 31); See L. Moerel and C. Prins, (n. 147).
[155] See M. Hildebrandt, 'Slaves to Big Data: or Are We?', (2013), Volume 17, IDP. Revista De Internet, Derecho Y Politica, available at <https://www.raco.cat/index.php/IDP/article/viewFile/303366/393038> accessed 18 July 2018.
[156] See L. Moerel and C. Prins, (n. 147); see also the statement made by the UK Information Commissioner's Office in 2014 arguing that: "The DPA does not say that processing for a new purpose is not permissible, nor does it say that the new purpose must be the same as the original purpose, nor even that it must be compatible with the original purpose: it says that it must not be incompatible with it."
[157] See Mayer-Schonberger and Padova, 'Regime Change? Enabling Big data Through Europe's New Data Protection Regulation', (2016), Volume 17, The Columbia Science & Technology Law Review, 322, available at <http://informationaccountability.org/wp-content/uploads/SchonbergerPadova.pdf> accessed 18 July 2018. The authors analyzed Facebook terms of service and privacy policy.
[158] Max Schrems filed lawsuit against Facebook based on the fact that Facebook acquires more data than needed and it requires a form of consent as take it or leave it. See Derek Scally, 'Max Schrems files first cases under GDPR against Facebook and Google', (The Irish Times, May 25, 2018), available at <https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177> accessed 18 July 2018.

As regards compatible use, the GDPR introduced a sort of legitimation of practices that enable the controller to re-use data for purposes incompatible from the one for which data was first collected, by requiring the consent of data subjects to allow for further processing.[159] However, if an individual cannot understand how his data is treated it is at least questionable the validity of his further consent. This is even more exacerbated in the context of BCI, since an understanding of the information that can be inferred by the EEG is limited to experts only.

Overall, while scholars criticize the practice of companies that do not respect the formal requirements of the principle of purpose specification,[160] practitioners strongly suggest the demise of the principle of purpose specification.[161] Whereas the former support a somewhat old concept of privacy and data protection, where individuals are aware (transparency) and in control of their data (informational self-determination), the latter support a more practical view that takes as a starting point the complexity of the information society within which individuals have lost control about their data; and propose new legal concepts to protect them. This is so despite the fact that EU data protection authorities focus on information requirements to be provided to data subjects and thus on the belief that data subjects are autonomous and able to make decisions.[162]

In this respect, this paper takes the view of practitioners and argues that, to protect data subjects using BCI technology, the theory developed by Moerel and Prins about the use of legitimate interest in determining whether a certain processing of personal data complies with the GDPR, should be preferred over the principle of purpose specification.

---

[159] See recital 50 of the GDPR.

[160] See E. Kosta, 'Enabling Valid Informed Consent for Location Tracking through Privacy Awareness of Users: A Process Theory', (2017), Volume 33, issue 4, Computer Law and Security Review,available at <https://www.sciencedirect.com/journal/computer-law-and-security-review/vol/33/issue/4> accessed 20 July 2018; see also I. Kamara and E. Kosta, 'Do Not Track Initiatives: Regaining the Lost User Control', (2016), Volume 6, Issue 4, International Data Privacy Law, available at <https://academic.oup.com/idpl/article-abstract/6/4/276/2571288?redirectedFrom=fulltext> accessed 20 July 2018. The authors, albeit focusing on consent, start with the assumption that a valid consent can only stems from a valid specification of purpose specification. An extract of the paper read as follow "The practices followed by app developers on the collection of information about users via mobile apps, the conditions and *purposes* of processing as well as their further transfer to third parties are often in conflict with their legal obligations (emphasis added)"; and again later "[…] privacy awareness will lead to valid informed consent only under certain conditions […] these conditions include that the user possesses an appreciation and understanding of the facts and implications of the consent for this particular application that will track location; an understanding of the location processing purpose served by the application.

[161] See L. Moerel and C. Prins, (n. 147); T. Z. Zarsky, (n. 31).

[162] See the French Commission Nationale de L'Informatique and de liberte' (CNIL) which requires Google, whose privacy policy provides for an extraordinarily broad purpose specification, to offer clear information about its handling of personal data.

The main reason for choosing such an approach is that the data controller can, by itself, establish the purpose for collecting data which, given its commercial interest, will always be broader than necessary. The BCI is no exception to such standardized practice. Secondly, in the BCI, the requirement of consent to process personal sensitive data do not sufficiently protect data subjects, given either the broad purpose with which controllers process their data and an evident lack of transparency in the type of information that can be inferred from the EEG data.[163] Thirdly, the requirements of purpose specification and data minimization do not provide for a prohibition of processing personal data whenever data subjects are at high risks of harms. Rather, they aim at providing procedural justice for data subjects where, nevertheless, controllers always have a right to process their personal data. [164]

However, as Hallinan *et al.* argue, "for procedural justice to be legitimate and effective, the framework needs to be capable of recognizing all the rights and interest which could be affected".[165] As brain data are not mentioned in the GDPR, it is debatable whether the legislator expertly balanced and recognized the rights at stake in the course of processing brain data. This is why the principle of legitimate interest is more appropriate in the context of BCI, because a new and context-specific balance of the rights at stake can be accommodated.

Finally, since the data minimization principle is strictly linked with the principle of purpose specification data subjects are not protected and more information than necessary are processed. Moreover, although it is possible to limit the collection and storage of EEG data for certain BCI types, this is only a limited solution. Meditative apps are booming,[166] and it can easily be imagined – given the interest showed by millennials for self-care app -[167] that such trend will continue and shift on a more advanced technique for individuals to take care of themselves. BCI technology indeed provides one of such advanced method.

[163] See, for a general critic about the failure of consent practices, D. J. Solove, 'Privacy Self-Management and the Consent Dilemma', (2013), Volume 126, Harvard law Review, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018> accessed 20 July 2018; and B. Koops, (n.30).
[164] See D. Hallinan, P. Schutz, M. Friedewald and P. De Hert, (n. 22).
[165] See D. hallinan, M. Friedewald and P. De Hert, (n. 124), 318.
[166] Sarah Perez, 'Self-care Apps are Booming', (Techcrunch, 3 April, 2018), available at <https://techcrunch.com/2018/04/02/self-care-apps-are-booming/?guccounter=1 > accessed 20 July 2018.
[167] Christianna Silva, 'The Millenial Obsession With Self-Care', (NPR, 4 June, 2017), available at <https://www.npr.org/2017/06/04/531051473/the-millennial-obsession-with-self-care?t=1530652863090&t=1533272999543> accessed 20 July 2018.

4. 3. Purpose Specification in the Context of BCI

Certainly, the purpose of collecting EEG data acquired through the use of BCI in neurogaming and meditative apps is to provide the users with the capacity to play or use the apps (first purpose). The purpose for storing such data is to provide users with the capacity to evaluate and improve their performance (second purpose). In legal terms, the first purpose can be translated into enabling communication between human and machine so that users acquire control function. The second one can be translated into recognition and evaluation of users' data for improving the control performance. Moreover, for every purpose, controllers must reduce the processing of data accordingly.[168]

In this context, if someone takes into account the criteria established by the A29WP for the compatibility test, no further processing of EEG data for a compatible purpose shall be allowed, given – principally - the absolute sensitive nature of these data and the impact that such processing may have on individuals.[169] Following the example that was given about the data collected in the course of customer relation management, the EEG data collected and stored shall not even be used to market the products of the controller; regardless whether the data subjects have given a general or separate consent. Imagine a BCI manufacturer that by analysing user's brain wave and possibly combining it with the social media data of the user, understands when that specific individual is more prone to buy online. In this circumstance, a manufacturer like Emotiv, which has already developed its own apps, may advertise any app to such individual at the right time and then manipulate such user to buy its own product.

However, all the BCI manufacturers analysed for this thesis state in their privacy policy that they use EEG data to profile users and do not limit the purpose of processing brain data to merely provide their service. Although the term profiling is not mentioned in any of their privacy policy, in practice BCI manufacturers use general sentences which closely resembles profiling purposes. For example, Emotiv affirms that they use personal information to: provide, administer, and improve the Services; (ii) better understand your needs and interests; (iii) fulfill requests you make; (iv) personalize your experience, such as to provide you with information regarding your overall

[168] See Article 5 (1)(c) of the GDPR.
[169] See A29WP, '*Opinion 03/2013', (*n. 144) 23-28.

cognitive performance relative to other users of similar age or other characteristics; (v) provide announcements; (vi) provide you with information and offers from EMOTIV; (vii) protect, investigate, and deter against fraudulent, harmful, unauthorized, or illegal activity; and (viii) comply with legal obligations.[170]

Although providing such EEG data to comply with legal obligation creates enormous data protection issues for individuals whose data are provided for legal enforcement purposes, an analysis of this topic is outside the scope of this work. Nonetheless, what is relevant is that not only such bio-informatics companies use EEG data for profiling purposes, they do not even comply with the requirements of a specific and explicit purpose. For one, a specific purpose for the collection of personal EEG data would require such company to provide the data subject with more information about which factors the controller uses to understand needs and interests better. For example, does the controller use health information inferred by the EEG data and profile the user accordingly? Would these inferences be used by such company in case it will bring forth different services than merely BCI technology or in case the company is acquired by another company selling (say) pharmaceuticals?[171]

As regard compatible use, data subjects are not shielded in the protection of their data by the purpose specification as enshrined in the GDPR. Where the initial purposes of collection and storage are to enable data subjects to play or use the apps and to evaluate and improve their performance, profiling shall not be allowed under the compatibility test of A29WP; in particular, because of the extremely sensitive nature of the EEG data and the impact that such further processing may have on data subjects.[172] Nevertheless, Recital 50 as recently introduced by the GDPR would allow the processing to go through in case data subjects give a separate consent,[173] despite the questionable argument about whether the data subject is really able to grasp how the information handed out will be treated. Arguably, the same contention can be made about the remaining purposes underlined above.

[170] Emotiv official website, (n. 10).
[171] As already stated in Chapter 3, the manufacturers of BCI analyzed in this paper declare that the collected EEG data are retained indefinitely and can be pass over in case the company is acquired by another entity.
[172] See the factors that A29WP considers in assessing the compatibility test of the purpose specification at (n. 144), 23-27.
[173] See Recital 50 of the GDPR.

4. 3. 1. Data Minimization in the context of BCI

The principle of data minimization requires controllers to process only that personal data that are adequate, relevant and necessary to the purpose for which the data are initially collected.[174] In other words, controllers must identify the minimum amount of personal data needed to fulfil their purpose and they must delete anything that is no longer relevant or adequate for that purpose. For processing operation involving sensitive data, the principle of data minimization requires controllers to limit even further both the amount of information processed and the duration of the storage of the data.[175] However, despite the amenable intention of such principle which aims to substantially reduce the amount of personal data processed, in the context of BCI it does not bear any significance.

On the one hand, since data minimization is strictly linked with the principle of purpose specification, the quantity of personal data processed is not limited. In fact, it has been clarified that BCI controllers tend to affirm a broad purpose for their operation with the consequence that the data needed for the processing of personal data increases proportionally. On the other hand, being the BCI based on a neuroimaging technique, the amount of data shared with the device is massive by default.

However, where the principle of purpose specification is constructed and broken down into two different operations (*see* section 4.2), data minimization may still provide a limited protection to data subjects. In this regard, it can be argued that there is one way for controllers to reduce the amount of data shared with their device. This claim stems from an analysis of BCI technology which, depending on which different control paradigms is based on, it may need fewer data to be processed. In such framework, data subjects would enjoy a better protection of their data, due to the limitation of the amount of data processed by the BCI.

[174] See Article 5 (1)(c) of the GDPR.
[175] See the recommendation on how to apply the principle of data minimization, provided by the UK Information Commissioner officer, here <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/> accessed 20 July 2018.

4. 4. A Data Protection Framework for Processing Personal Sensitive Data through the BCI

Arguably, an accurate implementation of these two basic principles of the GDPR would require controllers to not only clearly and better specify the purposes of their processing by identifying two different purposes for processing personal data; these purposes must also relate to the type of BCI technology, since different BCIs, based on different control paradigms, need only certain data to function.

Where the control paradigm of BCI is based on the P300 component, which is a specific method based on Event-Related Potential (ERP) to measure brain activity patterns consisting of specific sensory, cognitive and motor events, the data minimization principle may still provide a sort of protection to data subjects. In fact, as the necessary EEG data needed to input command to the machine is merely the time-locked response to stimuli, it is possible to say that the BCI controllers must store only such specific data, while the whole raw neural signals must not be retained; albeit it can be initially collected (first purpose is about enabling control function). As professor Bonaci has demonstrated, such a statement does not affect the functioning of this type of BCI. In this regard, she submitted a patent application for the invention of a particular device that by acting before the feature extraction process of the BCI, but after the signal acquisition and noise filtering process (thus between the second and third steps of BCI operation)[176] permits the BCI to implement the commands function while ensuring a better protection of data subjects because the whole raw EEG data is never transmitted or stored; but anonymized.[177]

As argued in Chapter 3, however, full anonymization of EEG data cannot be attained. Nevertheless, it is interesting to note that both principles of the GDPR can, in theory, limit the data processed by this type of BCI application (notice that only for storage purpose data can be limited, not collection) for when the whole raw EEG data is not only rendered anonymous but completely deleted; and where only the relevant neurosignal is stored. In doing so, the procedural justice

[176] See Chapter 2 of this paper.
[177] See T. Bonaci, J. Herron, C. Matlack and H. J. Chizeck, 'Securing the Exocortex: a Twenty-first Century Cybernetics Challenge', (2014), IEEE, available at <http://brl.ee.washington.edu/eprints/1/1/2014_Securing_Exocortex.pdf> accessed 16 July 2018; See also the US patent application publication (n.63).

objective of the GDPR and its principles can be achieved, although data subjects are not protected even where the requirements of the two principles of the GDPR are strictly implemented.

In fact, a natural characteristic of every type of BCI is to necessitate a calibration phase in order to then recognize the relevant brain patterns of data subjects and, thus, permit controls output.[178] An essential aspect of this calibration phase is that the necessary trained EEG data are stored in order for the machine to identify the relevant signal corresponding to the command function (recognition). Additionally, since every subject has specific neural responses to even the same stimulus,[179] it is not possible for the machine to merely store a generic neurosignal valid for everyone and artificially created. In this regards, it is to be reminded that the EEG data are highly dimensional and even a limited amount of this data always yield important sensitive information about data subjects. Therefore, even where BCI controllers are willing to adopt such an approach to their data processing it is essential to inform data subjects that a simple time-locked P300 wave can be used to infer a disabling disease such as multiple sclerosis (apparently, the P300 wave would appear longer than normal);[180] and with the continuous advancement in technology and science other inferences about other sensitive information are not to be excluded. You can also imagine these controllers extrapolating information such as 4-digit PINs, bank information, months of birth and locations of residence.[181]

As regards an active BCI, users modulate brain signal actively and they must imagine motor movement to control the machine. The control paradigm of an active BCI is the ERD neural oscillation.[182] Similarly to the reactive BCI, the machine needs to monitor the relevant part of the

[178] See F. Lotte, 'Signal processing approaches to minimize or suppress calibration time in oscillatory activity-based Brain-Computer Interfaces', (2015), Volume 103, Issue 6, Proceedings of the IEEE, Institute of Electrical and Electronics Engineers, 871-890, available at <https://ieeexplore.ieee.org/document/7109822/> accessed 16 July 2018. Reported *verbatim:* It should be noted that although the necessary long calibrations mentioned above affect all types of BCI, ERP-based BCI, e.g., spellers, do not suffer from this issue as much as oscillatory activity-based BCI do; See also for BCI based on ERD, J. Faller *et al*., 'Autocalibration and recurrent adaptation: towards a plug and play online ERD-BCI', (2012), Volume 20, Issue 3, IEEE, 313-319, available at <https://ieeexplore.ieee.org/document/6177271/> accessed 16 July 2018; See for a BCI based on ERP, D. Wu *et al.*, 'Online and Offline Domain Adaptation for Reducing BCI Calibration Effort', (2017), IEEE, available at <https://arxiv.org/pdf/1702.02897.pdf%20> accessed 17 July 2018..

[179] F. Lotte, (n. 179).

[180] I. Martisius and R. Damasevicius, 'A Prototype SSVEP Based Real Time BCI Gaming System', (2016), Comptational Intelligence and Neuroscience, available at <https://www.hindawi.com/journals/cin/2016/3861425/> accessed 17 July 2018.

[181] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, (n. 76).

[182] See S. Fialek and F. Liarokapis, 'Comparing Two Commercial Brain Computer Interfaces for Serious Games and Virtual

brain and thus collect all the EEG data (first purpose), but the only data needed to control the BCI is again a time-locked response to the relevant internal stimulus of the user.[183] However, differently from the reactive BCI, an active BCI normally has low performance [184] and it thus requires an extensive training for the user, constant calibration and neurofeedback. It is therefore clear that even where it is possible to merely store (second purpose) the relevant EEG data, it is not functional or reasonable to require an erasure of these data as in the reactive BCI. In fact, apart from the required EEG data for the calibration process of the machine, neurofeedback is an essential part of every active BCI; because data subjects are taught to influence the relevant brain waves to improve performance. Accordingly, the whole EEG data must be stored to be presented to these users. Thus, an active BCI creates more issues for the data subjects as long as the whole EEG data must be stored and continuously updated.

As regard passive BCI, users' mental state is automatically monitored by the machine and, once the selected mental state is quantified (f.i. concentration, relax and workload), users are facilitated in their communication with the machine and can also control aspects of the game.[185] Similar to an active BCI, it needs constant calibration and must provide users with neurofeedback to improve reliability in the detection of mental states.[186] In fact, a passive BCI can be seen as a technology that constantly needs to be filled with information in order to learn to adapt to its user.[187] Therefore, in this circumstance, it is not possible to merely retain relevant data, but the whole EEG signal has

Environments', (2016), Springer Internation Publishing Switzerlands, available at <https://www.fi.muni.cz/~liarokap/publications/EIG2016.pdf> accessed 17 July 2018; see also F. Nijboer, J. Clausen, B. Z. Allison and p. Haselager, (n. 13); see also K. Whalstrom. B. Fairweather, H. Istance and H. Ashman, 'Privacy and Brain-Computer Interfaces: clarifying the risks', <http://search.ror.unisa.edu.au/record/UNISA_ALMA51108695480001831/media/digital/open/9915910186601831/12143338660001831/13143337400001831/pdf> accessed 17 July 2018.

[183] See S. Fialek and F. Liarokapis (n.183).

[184] F. Lotte and D. Cichocki, 'What are the best motor tasks to use and calibrate SensoriMotor Rhythm Neurofeedback and Brain-Computer Interfaces? A preliminary case study' (2017), Real-time functional Imaging and Neurofeedback conference, available at <https://hal.inria.fr/hal-01656745/document> accessed 17 July 2018.

[185] See an application of a passive BCI to videogame by B. Van de Laar, H. Gurkok, D. Plass-Oude Bos, M. Poel, A. Nijholt, 'Experiencing BCI Control in a Popular Computer Game', (2013), Volume 5, Issue 2, IEEE Trans Comput Intell AI Games, 176–184, available at <https://ieeexplore.ieee.org/document/6484110/> accessed 17 July 2018.

[186] S. Fialek and F. Liarokapis, (n. 183). 'Comparing Two Commercial Brain Computer Interfaces for Serious Games and Virtual Environments', in K. Karpouzis and G. N. Yannakakis (eds.), 'Emotion in Games, Socio-Affective Computing', 4 Springer 2016.

[187] See Thorsten O. Zander, The First Meeting of the Community for Passive BCI Research', (2014), Technical University of Berlin, available at <http://www.pressrelease.brainproducts.com/passive_bci/> accessed 17 July 2018.

to be stored. Again, the result is that a passive BCI is as risky as an active one; but less than the reactive BCI.

From this analysis, it can be established that the principles of purpose specification and data minimization only play a limited role in the processing of EEG data through the BCI, even in the remote case controllers are willing to comply with them closely. In particular, purpose specification is not capable to provide transparency, legal certainty and predictability of data processing because EEG data inherently yield information unrelated with the purpose of providing the service. On the other hand, data minimization can achieve its objective only for a certain type of BCI. The result is that data subjects are always negatively impacted by the processing of their data through the BCI and, as such, are at high risks of harms.

There are two main reasons for such observation. First, the functionality of BCI that measure EEG data of individuals closely depends on the collection and storage of a vast amount of information. Second, the unique characteristics of EEG data (the potential to single out every individual and the prospect of inferring extremely sensitive information from a short recording) only ensure an insufficient protection of individuals.

Moreover, it is interesting to note the discrepancies between the protection afforded by data protection and privacy, which brings to the fore divergent perspective. Whereas from a privacy perspective the most critical BCI types for individuals are the reactive and passive ones, from a data protection perspective the active and passive BCI are riskier.[188]

4. 5. Applying the Principle of Legitimate Interest to the BCI

In the end, what should be chosen between purpose and legitimate interest? Looking at a problem from these two perspectives may evoke different feelings. Imagine that BCI is used by private companies to enable individuals to control an app with their thought alone or that the BCI is used by neuroscientists - in the same way as private companies' do - in order to prevent neurological diseases. The purpose of the processing of data for these two operations would be the same, but

[188] In K. Wahlstrom, N. B. Fairweather and H. Ashman, (n. 27). The authors identified four types of BCIs (active, passive, reactive and Hybrid) and underlined that reactive, passive and hybrid BCIs are the kind of BCI applications most capable to disrupt privacy.

the public opinion would undoubtedly differ widely. As Moerel and Prins rightly put it: "*it is not so much the **purposes** for which personal data might be used that is the primary consideration here, but rather the **interests** that are served by the use of the data collected".*[189]

With this in mind, they developed a legal theory based on the principle of legitimate interest as the only single test for all the various phases of the life cycle of the personal data processing (collection, storage, use, reuse etc.), where all the legal grounds and principles established in the GDPR are no longer applicable as independent legal grounds, but they are treated as secondary elements that may tip the balance toward considering the whole operation as legitimate or not. In their words, personal data processing is permissible: "if this is necessary for a specified, explicit and legitimate interest (including wider societal interest) pursued by the controller or by a third party to whom the data are provided, except where the interests or fundamental rights and freedoms of the data subject as well as the interests of society as a whole, in particular the constitutional right to privacy, prevail."[190]

Here, however, a clarification is needed. It is argued that the fundamental rights of data protection must be at the center of the test; rather than the right to privacy. The latter should play a secondary role in the assessment test. In fact, as underlined in the last part of paragraph 4.3, taking into account privacy or data protection yields different results. Similar to the *Schrems* case,[191] the right to data protection does not come into play only secondarily in order to minimize the negative impact of the use of technology. Rather, as a fundamental right of its own, it provides the framework from which privacy infringement can be established. In other words, the right to data protection comes into play even before any infringement of privacy is verified. The jurisprudence of the CJEU clearly demonstrated this in *Schecke*, where it has been underlined that if the legal conditions to process personal data are met there is no interference with the right to data protection. Notwithstanding, any subsequent improper disclosure or use of such personal data may still infringe on the privacy of individuals.[192]

[189] See L. Moerel and C. Prins, (n.)147
[190] Ibid. at 76.
[191] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, [2015].
[192] See Case C-92/09, *Volker Und Markus Schecke GBR v. Land Hessen*, and C-93/09, *Eifert v. Land Hessen and Bundesantsalt fur Landwirtschaft und Ernahrung*, [2010]; See also an explanation about the differences between privacy and data protection by J. Kokott and C. Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', (2013), Volume 3, Issue 4 International Data Privacy Law, 226.

In the context of BCI, this is not only important to set the criteria from which to assess the risks for data subjects, *i.e.* BCI's control paradigms as opposed to the type of BCI (active, passive, reactive and hybrid); but it also protects individuals from the outset. In fact, since privacy requires an interference with the internal sphere of an individual before an infringement is established, it is arguable whether a brain signals reading machine actually causes such interference that - also due to the *de minimis* rule - reaches a certain threshold of harm.[193] Conversely, data protection rules out the processing of sensitive data – at least information on health-related aspects of individuals –[194] from the outset in case exceptions do not apply.

Coming back to the theory of legitimate interest, the test to be applied closely resemble the one put forward by A29WP in its opinion on the notion of legitimate interests.[195] In particular, it provides the balancing of the different interest of the controller, data subjects and society as a whole through a proportionality test that takes into account different factors (the nature of the data, the implications for individual and society, the way data are processed, the status of the controller and individuals).[196] In this framework, the test better contributes to ensuring the procedural justice objective of the GDPR.

First, since the legislator has not considered the processing of brain data, this test provides a context-specific analysis that is helpful for either the controller or data subjects as well as for the public and authority charged with the competence to ensure the fairness of a given data processing operation. There are still many issues with the information extracted by the BCI and how data are used so that a broader perspective may set the right standards for the processing of personal data with the BCI.

Second, in light of the difficulties of data subjects to make sense of how and for what purpose their data are used, delegating such task to competent authority surely has its advantage.

---

[193] See Case C-92/09, *Volker Und Markus Schecke GBR v. Land Hessen*, and C-93/09, *Eifert v. Land Hessen and Bundesantsalt fur Landwirtschaft und Ernahrung*, [2010]; See Case C-594/12, *Digital Rights Ireland ltd. v. Ireland*, [2014] Judgement of the Court para. 29-32;

[194] This should reflect what I have said in Chapter 3 i.e. health data are sensitive by default because the modification brought about by the GDPR, whereas other sensitive information are protected only depending on the intended use of the controller.

[195] See Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* ('WP' 217), WP217.

[196] See Cit. Supra n. 45 at 77.

Third, the collective interests are taken into account. There is indeed the necessity to balance the collective interest in helping scientists to uncover the mystery of the brain and, thus, prevent or treat neuronal diseases; with the collective interest to preserve the mystery of their mind.[197]

Fourth, the fundamental rights and freedoms of data subjects are newly assessed against the interest of the controller. This is arguably the most important aspect of applying such test because there is an independent evaluation, regardless an initiative of data subjects; and because not only data protection and privacy come into play, but also principles such as freedom of expression and non-discrimination. This is indeed essential in view of the particular information extracted by the BCI that may be used to steer people's behavior or treat them differently because of natural characteristics.

Fifth, this test would account for how the data are processed. This is a fundamental aspect in the neurogaming and neuroapp, since it involves the sharing of such critical data with app developers.[198] It is especially important, as the legitimate interest test may assess whether such entities are trustworthy and implement the necessary security measures if they are to process these types of sensitive data. As it has been shown by Martinovic *et al*. and prof. T. Bonaci, these app developers may well present certain stimuli to users for which any of their response yield determinate sensitive information.[199]

Eventually, a broader test capable of providing a context-specific assessment would better account for the singularity of the BCI. Coming back to the initial question about a BCI application used for scientific or commercial purposes, a clear differentiation between the interests served would give different results also in legal terms. In this regard, not only high fines may be imposed in case certain procedures and safeguards are not addressed and implemented by controllers, but the processing operation may be declared unlawful. In fact, a specific prohibition of the processing operation can be affirmed for when the fundamental rights of individuals outweigh the interest of controllers. Although one must be cautious, given the objective of data protection law, the protection of individual data must not be seen as a trivial exercise; especially where sensitive

[197] The terms brain and mind are intentionally used differently.
[198] See H. Takabi, A. Bhalotiya and M. Alohaly, (n. 113).
[199] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the feasibility of side-channel attacks with brain-computer interfaces," (2012), Proc.21st USENIX Security Symp., USENIX, 2012; and T. Bonaci, R. Calo and H. J. Chizeck, (n. 16).

data[200] are involved. As the Schrems case demonstrated, there is space to declare a certain data processing operation unlawful where infringements of the fundamental right of data protection are substantial and can be linked with the right to privacy.

4. 6. Conclusion

In the context of BCI applications for neurogaming and neuroapp purpose, the principles of purpose specification and data minimization merely play a limited role; even where controllers formally and strictly implement them. On the one hand, the objectives to provide transparency, legal certainty and predictability of data processing through a specification of purpose is undermined by the fact that by default data subjects unconsciously yield information unrelated with the purpose of providing the service. On the other hand, data minimization can achieve its objective only for a specific type of BCI. The main reason for such conclusion stems from the combined unique characteristic of the BCI and the data extracted by this device.

This particularity clearly demands a new approach to data protection law; at least for the specific field of BCI. It provides the right framework from which to assess in a legal way the data processing operation of the BCI. Although such theory as applied here has placed significant attention on the right to data protection rather than privacy, the ultimate result is that data subjects would find better protection of their interest through such legitimate interest test. In fact, not only does such a test provide for a case by case analysis of the relevant operation, but it also ensures that the objective of a neutral legislation is preserved. By balancing the different interests at stake, the objective of providing benefits for all parties is preserved; since the legislator has apparently missed this opportunity. The additional and most important value of this approach resides in the possibility to declare unlawful the processing operation of the BCI in the context of neurogaming and neuroapp, depending on whether not only the fundamental right of data protection of data subjects is infringed by controllers, but also on whether other relevant fundamental rights and freedoms are violated through the processing of personal data. Moreover, as Ray Kurzweil rightly

[200] The use of the plural form is intentional. A characteristic of EEG data processed through the use of BCI is to not only yield one type of sensitive data (health or religious beliefs) but multiple types of sensitive data at the same time.

put it: "exponential trends themselves have experienced exponential growth".[201] In light of this, it is necessary to tackle the issue raised by the BCI from the outset, rather than waiting for a new legislation

[201] R. Kurzweil, 'The Law of Accelerating Returns', (2001), Essays, available at <http://www.kurzweilai.net/the-law-of-accelerating-returns> accessed 20 July 2018

5. Concluding Remarks

The primary drive in writing this thesis is a simple thought: "what if" the path to the future of Brain-Computer Interface imagined by neurotech pioneers - however arduous - is achievable? More importantly for a legal scholar, "what if" the main law which is supposed to protect individuals when they share their personal data, simply lags behind technological developments? After all, experience tells us that what we thought to be merely science-fiction a decade ago often becomes the science fact of today.

In light of these doubts, the paper investigated the data protection issues stemming from the out-of-the-lab use of BCI. In particular, its actual application in the mobile world for gaming and recreational purposes. In this regard, it has been assumed and to some extent demonstrated with the help of relevant literature that the BCI functioning is in stark contrast with the rules enshrined by the GDPR.[202] Therefore, this thesis aims to clear the following doubt: *To what extent does the BCI comply with the principle of purpose specification enshrined in the GDPR?*

The description of the technical functioning of the BCI allowed an understanding of why data protection legislation comes into play. Not only because of the obvious reason that the output of a BCI is dependent on an input constituted of brain activity data; but, especially, because of the high dimensionality of EEG data. A characteristic of this EEG data is, indeed, to be highly unique for every individual containing a vast amount of involuntary information about health conditions and – potentially – about everything an ill-intentioned person want to finds out about data subjects.

Examples include diagnosing mental disorders as well as disclosure of other strictly personal information such as PIN numbers, date of birth, religious and political beliefs of data subjects. Moreover, in the context of the commercial application of BCI analysed for this paper, a combination of EEG data and data required to access the "service" may give to the app's developer and device's manufacturer a tremendous amount of information about an individual.

However, it has also been pointed out that technology limitation decreases the quality of this information. In particular, the fact that this type of BCI is used for different purposes than a medical

[202] See See D. Hallinan, p. Schutz, M. Friedewald and P. De Hert, '*Neurodata and neuroprivacy: data protection Outdated?* 12 (1) Surveillance and Society, 2014.

one – where this application aim to specifically diagnose mental disorders of patients - certainly reduces the capacity of the BCI to extrapolate sensitive information about data subjects.

Limitation, potential and actual capability of such technology to extract personal information directly from the brain have all been factors that have been considered in the third chapter and put in the perspective of the relevant law. Despite technical limitations of the BCI and the shortsightedness of the EU legislator in defining brain data into the law, the long arm of the GDPR still lures such brain data under its scope.

On the one hand, the fact that the EEG data are unique to every individual and are constantly collected by controllers each time data subjects access the service are clear indications toward a finding of these data as personal ones. On the other hand, since the concept of identifiability has been stretched in the GDPR and requirements of irreversibility of anonymization heightened, EEG data can always be considered personal data. Essentially, once controllers collect these EEG data, they must always treat them as information relating to individuals, regardless of the protection provided by the anonymization technique.

However, the shortsightedness of the EU legislator is clearly visible when someone, in light of the extremely delicate information extracted by the BCI, would want to afford the highest protection accorded by the GDPR to sensitive data. In particular, because the data collected by the BCI are initially in a raw status - in the form of a simple graph - and they must be processed and interpreted further to gain different sensitive information about data subjects, the brain data cannot be considered as sensitive by default.

Instead, the GDPR provides a complicated framework for a simple problem where it must be taken into account the intended use of controllers. Although an examination of the intended use of controllers often results in a consideration of brain data as sensitive, this framework gives extensive leeway to controllers. In fact, the higher protection and tailored restrictions to the processing of sensitive data do not come into play from the outset, but it rests on the willingness and interpretation of controllers to provide better protection of data subjects. Essentially, extremely sensitive information of data subjects are being treated as any other bit of information whereas the risks of infringing upon the fundamental rights of individuals are clearly visible.

It is in light of this finding and the fact that new BCI applications are already targeting consumers in a conspicuous way that the principle of purpose specification has a critical role to play. In fact, in determining the amount, the type, the duration and safeguards to be applied in the processing of personal data; the principle of purpose specification provides for the transparency, fairness and legitimacy of a given data processing operation. In other words, it shields data subjects against the often unlimited appetite of controllers to secure their intimate information.

Notwithstanding, in the context of the BCI, the principle of purpose specification does not provide protection to data subjects given the particular characteristic of this technology. On the one hand, the fact that data subjects must yield, at the same time, data necessary and unnecessary to access the service without any possibility to minimize the sharing of the latter data constitute an insurmountable incompatibility with the principle of purpose specification. On the other hand, the objectives to provide transparency, legal certainty and predictability of data processing through a specification of purpose are undermined by the fact that the information collected by the BCI are unknown to data subjects as well as controllers. It thus appears that rather than a shield, which is an essential instrument against aggression, the EU legislator provides data subjects with a simple sword. Although at first sight it seems an excellent instrument, it is quite inconvenient when your only move is to defend yourself.

Because of these particularities, it would be beneficial considering a new approach to data protection law; at least for the specific field of BCI. In this regard, it is argued that the application of the legitimate interest principle as developed by Moerel and Prins would better serve the interest of data subjects. Although such theory has been modified by placing significant attention on the right to data protection rather than privacy, the additional result of such theory would be the possibility to approach issues of data protection in a technologically neutral way. Moreover, the ultimate effect of this theory is to declare the processing operation as unlawful; depending on whether controllers infringe not only the fundamental right of data protection of data subjects, but also on whether other relevant fundamental rights and freedoms are violated through the processing of personal data.

Overall, a simple answer to the initial “what if” dilemma of this author is that the law will always lag behind technological development. Not only because it is already tricky to foresee what comes next, but also because the law, to be law, must rightly undergo through a lengthy legislative process.

What is essential is to have basic principles that can always act as a shield against the unknown. When, however, also the basic principles are rendered meaningless in light of new technology developments, an entirely different approach must be envisioned, designed and provided.

Bibliography

Books

Banks I. M., *The Culture Series*, (Orbit Books, 1987)

Bygrave L A*, 'Data Protection Law: Approaching Its Rationale, Logic and Limits'*, (The Hague, Kluwer Law International, 2002)

B. Graimann, 'Brain-Computer Interface: a Gentle Introduction', in B. Graimann et al. (eds.), '*Brain-Computer Interfaces*, (The Frontiers Collection', Springer, 2010)

Tan D S, Nijholt A, '*Brain-Computer Interfaces: Applying Our Minds to Human-Computer Interaction'*, (Springer, 2010),

European Union Agency for Fundamental Rights, Council of Europe, *Handbook on*

European data protection law, (2014)

Articles and Papers

Abdulkader N, Atia A and Mostafa M S M, 'Brain Computer Interfacing: Applications and Challenges', Volume 16, Issue 2, Egyptian Informatics Journal, 2015

Ahn M, Choi J and Chan Jun S, 'A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users', Volume 14, Issue 8, Sensors, 2014

Arico' P, Borghini G, Di Flumeri G, Colosimo A, Bozzi S and Babiloni F, 'A passive brain–computer Interface Application for the Mental Workload Assessment on Professional Air Traffic Controllers During Realistic Air Traffic Control Tasks' Epub, 2016

Bi L, Fan X. A, and Liu Y, 'EEG-Based Brain-Controlled Mobile Robots: a Survey', Volume 43, Issue 2, IEEE Transactions on Human-Machine System, 2013

Bonaci T, Calo R and Chizeck H J, 'App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces', IEEE International Symposium on Ethics in Science, Technology and Engineering, 2014

Bonaci T, Herron J, Matlack C and Chizeck H J, 'Securing the Exocortex: a Twenty-first Century Cybernetics Challenge', IEEE, 2014

Burkert H, 'Data-Protection Legislation and the Modernization of Public Administration', Volume 62, International Review of Administrative Sciences, 1996

Bygrave L, 'Information Concepts in Law: Generic Dreams and Definitional Daylight', Volume 35, Issue 1, Oxford J. Legal Studies, 2015

Carelli L, Solca F, Faini A, Meriggi P, Sangalli D, Cipresso P, Riva G, Ticozzi N, Ciammola A, Silani V and Poletti B, 'Brain-Computer Interface for Clinical Purposes: Cognitive Assessment and Rehabilitation', Volume 2017, BioMed Research International, 2017

Cannataci J A and Misfud Bonnici J P, 'The End of the Purpose Specification Principle in Data Protection?', International Review of Law, Computers & Technology, 2010

Coudert F, Dumortier J and Verbuggen F, 'Applying the Purpose Specification Principle in the Age of "Big Data": The Example of Integrated Video Surveillance Platforms in France', ICRI Working Paper, 2012

De Gennaro L, Marzano C, Fratello F, Moroni, M. C. Pellicciari, et al., 'The Electroencephalographic Fingerprint of Sleep is Genetically Determined: a Twin Study', Volume 64, Annals of neurology, 2008

De Hert P, 'Citizens' Data and Technology: An Optimistic Perspective', The Hague, Dutch Data protection Authority, 2009

Denning T, Matsuoka Y and Kohno T, 'Neurosecurity: Security and Privacy for Neural Devices', Volume 27, Issue 1, Journal of Neurosurgery, 2009

Di D, Zhihua C, Ruifang F, Guangyu L, Tian L, 'Study on Human Brain after Consuming Alcohol Based on EEG Signal', Volume 5, Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference IEEE, 2010

Feijo C, Gomez-Barroso J L, Augado and S. Ramos, 'Mobile gaming: Industry Challenges and Policy Implications', 2010

Fialek S and Liarokapis F, 'Comparing Two Commercial Brain Computer Interfaces for Serious Games and Virtual Environments', Springer Internation Publishing Switzerlands, 2016
Floridi L, 'Is Information Meaningful data?', Volume 70, Issue 2, Philosophy and Phenomenological Research, 2005

Faller J et al., 'Autocalibration and recurrent adaptation: towards a plug and play online ERD-BCI', Volume 20, Issue 3, IEEE, 2012

Forgo' N, Hanold S and Schutze B, 'The Principle of Purpose Limitation and Big Data, Springer, 2017

Gajic D, Djurovic Z, Di Gennaro S and Fredrik Gustafsson, 'Classification of EEG signals for detection of epileptic seizures based on wavelets and statistical pattern recognition', Volume 2, Issue 26, Biomedical Engineering: Applications, Basis and Communications, 2014

Gasson M and Koops B J, 'Attacking Human Implants: A New Generation of Cybercrime', Volume 5, Issue 2, Law, Innovation and Technology, 2014

Greenberg A, 'Inside the Mind's Eye: an International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces', 2018

Hallinan D, Schutz P, Friedewald M and De Hert P, 'Neurodata and Neuroprivacy: Data Protection Outdated?', Volume 12, Issue 1, Surveillence & Society, 2014

Hallinan D, Friedewald M and De Hert P, 'Genetic Data and the Data Protection Regulation: Anonymity, Multiple Subjects, Sensitivity and a Prohibitionary Logic Regarding Genetic Data', Volume 29, Computer Law & Security Review, 2013

Hanafiah Z M, Taib M N, Hamid N, 'EEG Pattern of Smokers for Theta, Alpha and Beta Band Frequencies', Research and Development (SCOReD), IEEE Student Conference on. IEEE, 2010

He B, GaoS , Yuan H, Wolpaw J R, 'Brain-computer interfaces', Neural Engineering, Springer, 2013

Hildebrandt M, 'Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics', Volume 10, (forthcoming) University of Toronto Law Journal, 2017

Hildebrandt M, 'Slaves to Big Data: or Are We?',Volume 17, IDP. Revista De Internet, Derecho Y Politica, 2013

Ienca M and Andorno R, 'Towards new human rights in the age of neuroscience and neurotechnology', Volume 13, Issue 5, Life Sciences, Society and Policy, 2017

Kamara I and Kosta E, 'Do Not Track Initiatives: Regaining the Lost User Control', Volume 6, Issue 4, International Data Privacy Law, 2016

Karson C, Coppola R, Daniel D G, Weinberger D R, 'Computerized EEG in Schizophrenia', Volume 14, Issue 193, Schizophrenia Bulletin, 1988

Karthikeyan D T and Sabarigiri B, 'Enhancement of multi-modal biometric authentication based on iris and brain neuro image coding', Volume 5, Issue 5, Int. J. Biometrics Bioinform (IJBB), 2011

Kim T, Kim S, and Shin D, 'Design and implementation of smart driving system using context recognition system', Computers & Informatics (ISCI), 2011 IEEE Symposium on. IEEE, 2011

Koch H, Christensen J A, Frandsen R, Arvastson L, Christensen S, Sorensen, Jennum P, 'Classification of Irbid and Parkinson's Patients Using a General Data-Driven Sleep Staging Model Built on EEG', Engineering in Medicine and Biology Society, 35th Annual International Conference of the IEEE, 2013

J. Kokott and C. Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', Volume 3, Issue 4 International Data Privacy Law, 2013

Koops B J, 'The Trouble with European Data Protection Law', International Data Privacy Law, 2014

Kosta E, 'Enabling Valid Informed Consent for Location Tracking through Privacy Awareness of Users: A Process Theory', Volume 33, issue 4, Computer Law and Security Review,available, 2017

Liang S F, Shaw F X, Young C P, Chang, Y. C. Liao, 'A Closed-Loop Brain Computer Interface for Real-Time Seizure Detection and Control', Engineering in Medicine and Biology Society, Annual International Conference of the IEEE, 2010

Lotte F, Larrue F and Muhl C'Flaws in Current Human training Protocols for Spontaneous Brain-Computer Interfaces: Lessons Learned from Instructional Design', Volume 7, Frontiers in Human Neuroscience, 2013

Lotte F, 'Signal processing approaches to minimize or suppress calibration time in oscillatory activity-based Brain-Computer Interfaces', Volume 103, Issue 6, Proceedings of the IEEE, Institute of Electrical and Electronics Engineers, 2015

Lotte F and Cichocki D, 'What are the best motor tasks to use and calibrate Sensori Motor Rhythm Neurofeedback and Brain-Computer Interfaces? A preliminary case study' (2017)
Lynch L, Paskewitz D, and Orne M, 'Intersession Stability of Human Alpha Rhythm Densities', Volume 36, Issue 5, Electroencephalographic Clinic Neurophysiological, 1974

Marcel M, Millan J D R, 'Person Authentication Using Brainwaves (EEG) and Maximum a Posteriori Model Adaptation', Pattern Analysis and Machine Intelligence, IEEE Transactions, 2007

Martinovic I, Davies D, Frank M, Perito D, Ros T, and Song D, 'On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces', the Proceedings of the 21st USENIX Security Symposium, USENIX, 2012

Martisius and Damasevicius R, 'A Prototype SSVEP Based Real Time BCI Gaming System', Comptational Intelligence and Neuroscience, 2016

Mason S G, Bashashati A, Fatourechi M, Navarro K F, and Birch G E, 'A comprehensive survey of brain interface technology designs', Volume 2, Issue 35, Ann. Biomed. Eng, 2007

Mayer-Schonberger and Padova, 'Regime Change? Enabling Big data Through Europe's New Data Protection Regulation', Volume 17, The Columbia Science & Technology Law Review, 2016

McFarland D J and Wolpaw J R, 'Brain Computer Interfaces for Communication and Control', Volume 54, Issue 5, Communications of the ACM, 2011

Moerel L and Prins C, 'Privacy for Homo Digitalis: Proposal for a new Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', 2016)

Moore B E, 'The Brain Computer Interface Future: Time for a Strategy', a research report submitted to the Air War College, Air University of the USAF, 2013

Nijboer F, Clausen J, Allison B J and Haselager P, 'The Asilomar Survey: Stakeholders' Opinions on Ethical Issues Related to Brain-Computer Interfacing', Volume 6, Issue 3, Springer Online, 2011.

Poulos M, Rangoussi M, Alexandris N, 'Neural Network Based Person Identification Using EEG Features', Volume 2, Acoustics, Speech, and Signal Processing, IEEE International Conference on. IEEE, 1999

Purtova N, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law', Volume 35, Issue 1, Law, Innovation and Technology, 2015

Revett S, De Magalhaes S T, 'Cognitive biometrics: Challenges for the future', in Global Security, Safety, and Sustainability, Springer, 2010

Schreiber D, Fonzo G, Simmons A N, Dawes C T, Flagan T, Fowler J H, Paulus M P, 'Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans', Volume 8, Issue 2, PLoS One, 2013

Selvam V S, Shenbagadevi S, 'Brain Tumor Detection Using Scalp EEG with Modified Wavelet-Ica and Multi-Layer Feed Forward Neural Network', Engineering in Medicine and Biology Society, Annual International Conference of the IEEE, 2011

Shen F X, Twedell E, Opperman C, Krieg J D S, Brandt-Fontaine M, Preston J, McTeigue J, Yasis A and Carlson M, 'The Limited Effect of Electroencephalography memory recognition Evidence on Assessment of Defendant Credibility', Volume 4, Issue 2, Journal of Law and Biosciences, 2017

Simanova I, Van Gerven M, Oostenveld R and Hagoort P, 'Identifying Object Categories from Event-Related EEG: Toward Decoding of Conceptual representations', Volume 1, Issue 5, PloS, 2010

Solove D J, 'Privacy Self-Management and the Consent Dilemma', Volume 126, Harvard law Review, 2013

Stopczynki A et al., 'Privacy for Personal Neuroinformatics', Technical University of Denmark and 2 MIT Media Lab, 2017

Takabi H, Bhalotija A and Alohaly M, 'Brain Computer interface Applications: Privacy Threats and Countermeasures', IEEE 2nd International Conference on Collaboration and Internet Computing, 2016

Tamburrini G, 'Brain to Computer Communication: Ethical Perspectives on Interaction Models', Volume 2, Issue 3, Springer, 2009

Van de Laar B, Gurkok H, Plass-Oude Bos D, Poel, Nijholt A, 'Experiencing BCI Control in a Popular Computer Game', Volume 5, Issue 2, IEEE Trans Comput Intell AI Games, 2013

Vecchiato G, Astolfi L, De Vico Fallani, S. Salinari, F. Cincotti, F. Aloise, D. Mattia, M.G. Marciani, L. Bianchi, R. Soranzo et al., 'The study of brain activity during the observation of commercial advertising by using high resolution EEG techniques', Engineering in Medicine and Biology Society, Annual International Conference of the IEEE. IEEE, 2009

Vidal J J, ‘Toward Direct Brain-Computer Communication’, Brain Research Institute, University of California, 1973

Wahlstrom K, Fairweather N B and Ashman H, ‘Privacy and Brain-Computer Interfaces: Identifying Potential Privacy Disruptions’, Volume 46, Issue 1, ACM SIGCAS Computers and Society, 2016

Xu F, Tu Z, Zhang P, Fu X and Jin D, ‘Trajectory recovery From Ash: User Privacy is Not Preserved in Aggregated mobility Data’, Proceedings of the 26th International Conference on World Wide Web, 2017

Zander T O, ‘The First Meeting of the Community for Passive BCI Research’, Technical University of Berlin, 2014

Zarsky T Z, ‘Incompatible: The GDPR in the Age of Big Data’, Volume 47, Seton Hall Law Review, 2017

Zuiderveen Borgesius F J ‘Breyer case of the Court of Justice of the European Union: IP addresses and the personal data definition’, Volume 3, Issue 1, European Data Protection Law Review, 2017

Other Online Materials

Alex Heath, ‘Elon Musk Has raised 27 Milion to Link Human Brains with Computers’, (Business Insiders, 25 August, 2017), accessed via https://www.businessinsider.nl/elon-musk-neuralink-raises-27-million-2017-8/?international=true&r=US

Annalee Newitz, ‘Elon Musk is Setting Up a Company That Will Link Brains and Computers’, (Ars Technica, 28 March 2017) accessed via <https://arstechnica.com/information-technology/2017/03/elon-musk-is-setting-up-a-company-that-will-link-brains-and-computers/ >

Chizeck H G and Bonaci T, ‘Brain-Computer Interfaces Anonymizer’, (February, 2014), US Patent Application accessed via https://patents.google.com/patent/US20140228701

Christianna Silva, ‘The Millenial Obsession With Self-Care’, (NPR, 4 June, 2017),

Genevieve Roberts, ‘Mind-Reading Headsets Could Revolutionise Our Interaction With the World’, (Independent, 9 December, 2015), accessed via https://www.independent.co.uk/life-style/gadgets-and-tech/features/mind-reading-headset-could-revolutionise-our-interaction-with-the-world-a6766856.html

James Wu and Rajesh P. N. Rao, ‘How Close are We to Elon Musk’s Brain-Computer Inerface?’, (The Conversation, April 12, 2017), accessed via https://edition.cnn.com/2017/04/12/health/brain-computer-interface-partner/index.html

Josh Constine, Facebook is Building Brain-Computer Interfaces for Typing ans Skin-Hearing', (Techcrunch, April 19, 2017), accessed via https://techcrunch.com/2017/04/19/facebook-brain-interface/?guccounter=1

Sarah Perez, 'Self-care Apps are Booming', (Techcrunch, 3 April, 2018), accesses via https://techcrunch.com/2018/04/02/self-care-apps-are-booming/?guccounter=1

Opinions

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, ('WP136'), 2007

Article 29 Working Party, Advice paper on special categories of data (sensitive data), 20.04.2011

Article 29WP, 'Opinion 03/2013 on purpose limitation', ('WP 203'), 2013.

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, ('WP216'), 2014

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, ('WP' 217), WP217

Article 29WP, ANNEX – Health Data in Apps and Devices, February 2015

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (Adopted 28 January 1981, Entered into Force 1 October 1985) ETS No.108

European Commission, 'The GDPR: New Opportunities, New Obligations', publication Office of the European Union, 2018

Case Law

Case C-434/16 Peter Nowak v Data Protection Commissioner [2017]

Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016]

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, [2015].

Case C-594/12, Digital Rights Ireland ltd. v. Ireland, [2014]

Case C-92/09, Volker Und Markus Schecke GBR v. Land Hessen, and C-93/09, Eifert v. Land Hessen and Bundesantsalt fur Landwirtschaft und Ernahrung, [2010]

Websites

https://store.neurosky.com/collections/apps

https://www.emotiv.com/consumer-insights-solutions

Websites providing publicly accessible EEG data accessed via https://github.com/meagmohit/EEG-Datasets

https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177