Alma Mater Studiorum – Università di Bologna
In collaborazione con LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

DOTTORATO DI RICERCA IN

Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

Ciclo XXXII – A.A.2016/2017

Settore Concorsuale: 12/H3
Settore Scientifico Disciplinare: IUS/20

TITOLO TESI

Ethical and Legal Aspects of Using Brain Computer Interface in Medicine: Protection of Patient's Neuro Privacy

Presentata da: ***Laman Yusifova***

Coordinatore Dottorato:

Prof.ssa Monica Palmirani

Supervisore:

Prof.ssa Carla Faralli

Esame finale anno 2020

Alma Mater Studiorum – Università di Bologna
in partnership with LAST-JD Consoritum
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

PhD Programme in
Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

Ciclo XXXII – A.A.2016/2017

Settore Concorsuale: 12/H3
Settore Scientifico Disciplinare: IUS/20

Ethical and Legal Aspects of Using Brain Computer Interface in Medicine: Protection of Patient's Neuro Privacy

Submitted by: ***Laman Yusifova***

The PhD Programme Coordinator:

Prof. Monica Palmirani

Supervisor:

Prof. Carla Faralli

Year 2020

To my mother Afar and father Rafael

Abstract

A growing application of invasive neuro-modulation in treating the diseases unresponsive to the conventional therapy or resuming lost motor functions requires a renewed look at the long-established conceptions of medical ethics such as privacy and autonomy. Through nano-chips embedded into the brain of a patient, this novel technology- Brain Computer Interface (BCI) traces how information is encoded and decoded by neural circuits in real time and accesses the subjective experience in a completely different way that no other medical technology could do in the past and is able to execute at present. Either in the application of the Deep Brain Stimulation (DBS), the most frequently used method of the Brain Computer Interface which involves machine brain interaction only, or during the treatment with other types of BCIs, when human to machine operation engaging both input and output communication with brain is used, the patient's privacy raises concerns at every level of the treatment.

The research looks into questions of law and ethics raised by BCI which have not yet been explored in detail in academic literature. The benchmark for the analysis is the privacy of the patient in the types of informational and decisional privacy. The issues directly relating to privacy are technical challenges in ensuring data security in this complicated technology handled through a wireless system, ethical and legal concerns such as the level of discreetness of the patient's state of mind and control over it, and the legal boundaries for its disclosure to third parties, among others.

It is the aim of the research, by referring primarily to the European context, to transmit ethical norms protecting privacy in general and in the physician-patient relationships *in particular* to the application of data protection in the field of neuro-technologies through legal regulation and to elaborate on the newly developing neuro-data conception.

Table of Contents

Acknowledgments

Firstly, I would like to thank my supervisor, Prof. Carla Faralli and LAST-JD Doctorate Programme Co-ordinator Prof. Monica Palmirani, whose guidance and support during my Ph.D. have been invaluable. In addition, I would like to extend my thanks to Dr. Marcel Mertz and Mrs. Britta Sanders at the Institute for History, Ethics and Philosophy of Medicine of Hannover Medical School for the hospitability and opportunities they have facilitated for me.

My deep gratitude is to Prof. Kevin Warwick for his insights into the actual application of BCI in real world, that has helped me immensely. My thanks also to my PhD examiners, Dr. Pietro Cipresso and Dr. Matteo Galletti, who provided me with helpful feedback on this research.

I am indebted to CIRSFID at the University of Bologna - the award of a PhD fellowship funded by the EACEA and continued support by all members of staff, specially by Mrs Dina Ferrari, made the research possible.

I would also like to thank my wonderful family and friends for their unwavering support and kindness. In particular, I am grateful to my sisters, Gular and Mehriban, my father Rafael, whose footsteps I have followed to become a lawyer. And my mother Afar, who left her own PhD Programme to take care of the family when her first child was born - thank you for your enormous encouragement, continued support and love!

Chapter I Introduction

1.1 Introduction

Advances in scientific fields have opened vast prospects for economic progress and human development, but such discoveries have also brought new challenges to the adequate protection of the rights and freedoms of individuals. Those complex challenges are tackled in scientific literature in an inter-disciplinary way with the co-operation of legal and economic scholars, sociologists, engineers, medical specialists, biologists, and others in scientific community.

Invasive neuromodulation, a subsection of neuroengineering is among technological discoveries which bring hope to life of patients with critic neural diseases, but at the same time carries risks of abuse of the individual's integrity and identity with a degree of intensity that creates qualitatively new challenges. It offers the possibility of immediate access to and control of the innermost part of human being: his thinking, intentions, memories, and emotions. Envisioned neural engineering technologies can penetrate and alter the personality and can even harm physical well-being in real time, with or without the patient's knowledge or consent. Thus, invasive and controlling power of neural technologies raises a number of novel legal and ethical questions, one of which is the patient privacy and confidentiality of brain data that is the proposed research intends to address.

Through nano-chips embedded into the brain of a patient, Brain Computer Interface (BCI), traces how information is encoded and decoded by neural circuits in real time and accesses the subjective experience in a completely different way that no other medical technology could do in the past. Accordingly, this novel technology raises qualitatively different concerns over privacy, autonomy and integrity of the patients which have been highlighted in a number of academic papers of legal,[1] ethical,[2] and scientific character. [3]

[1] Szekely, I., Regulating the future? Law, ethics, and emerging technologies, *Journal of Information, Communication & Ethics in Society*, Vol 9, 2011, pp180-194

[2] Haselager, P., et al., A note on ethical aspects of BCI, Neural Networks 22 (2009) 1352–1357; Klein, E., et al., Engineering the Brain: Ethical Issues and the Introduction of Neural Devices, *Hastings Center Report* Vol 45 No 6, (2015); pp26-35.

[3] Denning, T., et al. , "Neurosecurity: Security and Privacy for Neural Devices*," Journal of Neurosurgical Focus* Vol 27, No. 1 (2009) pp. 1-4.,

The issues directly relating to privacy are e.g. technical challenges in ensuring data security in this complicated technology handled through wireless system[4], or ethical[5] and legal concerns such as the level of discreetness of the patient's state of mind and control over it and the legal boundaries for its disclosure to third parties.[6] The European Group on Ethics in Science and New Technologies has also warned against the risk that Implantable Neural Devices can be used to control and locate people, and furthermore could provide third parties with access to information about the body and mind of the involved. On the achievements of BMI technology outside medicine, the US DARPA's recent project "Silent Talk" proves that the technology is indeed capable of reading the EEG device wear's mind.

In one hand it is highly commendable that these implantable neural chips due to its structural and functional imaging methods of high resolution and specificity, can encourage and guide neuronal regeneration and reconnection, and thus provide substantial benefit for the patient's recovery. Due to the nature of the 'data collection' at these devices however it also creates risks exposing patients to distress or discrimination, or more serious consequences, such as bodily harm.[7]

From social and ethical perspective, a scientific team at the University South Australia through experimental empirical analysis method determined that in active BCI, disruption of privacy has causes at different levels including in the social context. In passive BCI, it often arises, for instance, when controlled environment is interrupted.[8]

From technical point of view, scholars at ETH Zurich, suggested hypothesis describing vulnerability of BCIs to the cyber-hacking which could affect privacy of the patients at signal

[4] Ienca, M., Haselager, P., Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity, Ethics, Information, Technology, Vol 18 (2016) pp117–129

[5] Wahlstrom, K., Fairweather, N., and Ashman, H., Privacy and Brain-Computer Interfaces: Identifying potential privacy disruptions, *ACM Computers & Society*, Vol 46 (2016) pp41-5

[6] Schmitz-Luhn, B., et al.,Law and ethics of deep brain stimulation, International Journal of Law and Psychiatry Legal and Ethical Issues in the Regulation and Development of Engineering Achievements in Medical Technology: A 2006 Perspective, Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, Aug 30-Sept 3, 2006; Hallinan, D., et. al, Neurodata and Neuroprivacy: Data Protection Outdated? *Surveillance & Society* Vol 12 No1: 2014, pp 55-72; Szekely, I., Regulating the future? Law, ethics, and emerging technologies, *Journal of Information, Communication & Ethics in Society*, Vol 9, 2011, pp180-194

[7] U.K. Nuffield Council on Bioethics Report on Novel Neurotechnlogies, 2013

[8] Wahlstrom, K., Fairweather, N Ben & Ashman, H., 2017 'Privacy and brain-computer interfaces: method and interim findings' Ethicomp/CEPE 2017, pp. 1-26

accusation, signal processing (measurement) or signal transferring and feedback providing (output) levels which is also backed by other scholars in scientific literature.[9]

I review the privacy concerns in all medical applications of BCI, whether in Deep Brain Stimulation (DBS), most frequently used method of BCI which involves machine to brain interaction only, or during the treatment with other type of BCIs when human to machine operation engaging both input and output communication with brain is used.

I analyse the *adequacy*, *consistency* and *predictability* of relevant binding instruments for ensuring patient privacy in BCI therapeutic procedures.

[9] M. Ienca, P. Haselager, *Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity,2016;* Bonaci T, et. al, *App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces*. 2014,

1.2 Research purpose and question

The purpose of the thesis, with an emphasis on privacy, is to establish whether the current legislative framework in the EU applicable to neuro-modulation research and therapy can sufficiently protect the personal rights of patients; to examine the ways in which other jurisdictions, namely the U.S.A have responded to similar issues; and to identify problems and propose alternative solutions in relation to this specific issue, such as re-conceptualization of privacy of thought and adoption of neuro-rights to cover current developments in neuroscience field.

Specific consideration is given to whether it might be appropriate to re-evaluate or re-qualify the existing conception of privacy, in particular for formulating brain privacy. In addition, the ethical implications of consent in medicine and bioethics are explored in order to provide an insight into when access to patient's personal data can be justified.

It should be mentioned that to date, there is no European Union level regulation directly protecting the privacy of brain information or protecting against the use of such information other than general sensitive health data provisions. In the context of rapidly advancing neuro-technologies and the ethical and legal concerns that arise, this thesis examines the need for a regulatory framework to address the distinct nature of brain data collected from the patient's brain.

Two main research questions are as followings:

1. To what level patients treated with invasive neuromodulation require special or heightened confidentiality of health information and privacy protection (e.g. appropriate encryption and design constraints to eliminate hacking the sensible neural information or device's software) and are there adequate safeguards?
2. *In particular*: How the right to thought is protected in the concerned patients? Is the neuro-privacy merits special subdivision in ethics (in privacy conception and typologies) as well as in legal domain

1.3 Methodology: doctrinal analysis, comparative method and inter-disciplinary research

The research will have an inter-disciplinary character, because complex challenges emerged by the advances in biomedical field could be addressed through the cross review of medical, technical, philosophical, social and legal literature.

There are three parts in the research. The first part will be dedicated to constructing the preliminary scope of work, i.e. for defining the technical characteristics and application of brain computer interfaces in medicine which can challenge autonomy and privacy. The content analysis of literature and monographs in medical, neuroscience and social domain will answer the question of how BCI can interfere with patient's privacy and autonomy and in particular decode the BCI user thoughts and alter them.

Before examining the legal landscape, I turn to the task of identifying which philosophical considerations (ethical norms derived from assessing values and interests) are key to re-evaluating existing conceptions of privacy to frame the emerging neuro-privacy notion ethics.

Then through qualitative doctrinal methodology, I will outline the legal framework in the relevant field: i.e. by employing the doctrinal method, international legal instruments relating to data protection and privacy, health law, technological development, human rights law, and other instruments will be reviewed in order to identify the norms relevant for the regulation of health data protection in BCI use for medicine. This stage will also involve the perusal and analysis of the preparatory works, relevant case law, authentic commentaries of international instruments, soft law, draft documents and reports of international organizations, relevant national laws and the treatises of legal scholars.

As the result of scientific literature review and corresponding comparative legal analysis, information processing stages in the brain machine interface and the types of its use in medical domain as well as the interpretation of relevant legal and ethical standards applicable to development and use of BMI will be outlined to reveal the level of the protection of health data (neuro-data) in question.

The ultimate aim is to explore whether there are/ or there should be neuro-exceptional privacy provisions that make it more difficult for treating physicians or data possessing organizations to use and disclose brain data compared to other information or will consenting to an invasive neuro modulation mean consenting to diminished privacy or increased potential accessibility.

Chapter II. Brain Computer Interface

2.1 Neuroengineering achievements in medical technologies /Milestones in BCI development

Advances in scientific fields such as neuroscience, engineering and information technology open vast prospects for treating neurological disorders and understanding the brain function. Those promising new approaches are based on the ability to record and stimulate neural activity with ever-increasing precision. This precision has resulted to the rapid expansion of neural interface devices that interact with the nervous system to resume sensory and motor function.

First-time brain–computer interface (BCI)[10] technology was demonstrated in 1964 when Gray Walter using the scalp-recorded electroencephalogram achieved in remote control of a slide projector.[11]

Although already in the late 1960s experiment with monkeys conducted by Eberhard Fetz showed that by changing the firing rate of a single cortical neuron monkeys can be taught to control a meter needle, [12] systematic investigations with humans began only in the 1970s.

As such Jacques Vidal's Brain-Computer Interface Project was the first attempt to evaluate the feasibility of using neuronal signals in a person-computer dialogue that enabled computers to be a prosthetic extension of the brain, i.e. through eye gaze a person could determine the direction of a computer cursor he wanted to move.

Until 1990s, there had been only a handful of BCI research studies. In 1980, Elbert with his colleagues proved that people could learn to control slow cortical potentials.[13] In 1988, Farwell

[10] Brain-Computer Interface is also called Brain-Machine Interface. Throughout the thesis the term can be used inter-changeably.
[11]Graimann, B., Allison, B., Pfurtscheller, G., Brain-computer interfaces: a gentle introduction. In *Brain-computer interfaces*, ed. Graimann B, (Berlin: Springer, 2010) pp 1–27
[12] Fetz, E., Operant conditioning of cortical unit activity. *Science* No163 (1969) pp 955–958; Fetz, E., Finocchio, D., Operant conditioning of specific patterns of neural and muscular activity. *Science* No 174 (1971) pp 431–435
[13] He, B., Gao, S., Yuan, H., & Wolpaw, J. R., Brain–computer interfaces. In *Neural Engineering*: Second Edition (2013) pp. 87-151.

and Donchin showed how the P300 event-related potential could be used to allow normal volunteers to spell words on a computer screen.[14]

But over the past two decades, the volume and pace of implantable neural device research have grown rapidly. In 1995, there were no more than six active BCI research groups, now there are more than dozen. Early examples of sensory neuroprostheses are the retina implant for eyes[15] and the cochlear implant in the ear which transmit electrically processed acoustic signals via implanted stimulation electrodes directly to the acoustic nerve.[16] At a later stage, an implanted stimulator neuroprosthesis (DBS- devices for deep brain stimulation) was developed which is used to inhibit hyperactivity of the subthalamic nucleus to improve symptoms for individuals with Parkinson's disease, essential tremor and other motor symptoms.[17]

In 2006, a microelectrode array was embedded in the primary motor cortex of a man with complete tetraplegia after a C3-C4 cervical injury. Using the signals obtained from the implanted electrode array, a BCI system enabled the patient to perform some basic functions such as opening e-mail, operating a television, opening and closing a prosthetic hand, etc.[18]

Later in 2011, Dean Krusienski and Jerry Shih showed that signals recorded directly from the cortical surface with electrocorticography can be translated by a BCI system to enable a person to spell words on a computer screen.[19]

Over the past twenty years, increased BCI research for communication and control has been stimulated by a better understanding of brain function, powerful computer equipment, and by a growing awareness of the needs and potentials of people with disabilities.[20] It is important to

[14] Farwell L. A, Donchin E. Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials. *Electroencephalography Clinical Neurophysiology*. Vol 70 No 6 (1988) pp510- 523.
[15] Eckmiller, R., System identification of leaming retina encoders for a retina implant, Investigative. Ophthalmology. & Visual Science. No 38 (1997);
[16] Zenner et al. (2000); Merzenich et al. (1974); Pfingst (2000) cited in *Towards Brain Computer Interfacing,* ed. Dornhege, G., MIT Press, (2007)
[17] Mazzone, P., A. Lozano, P. Stanzione, S. Galati, E. Scarnati, A. Peppe, and A. Stefani. 2005. Implantation of human pedunculopontine nucleus: a safe and clinically relevant target in Parkinson's disease. *Neuro-reporting* No 16 Vol17 (2005) pp 1877–1881; Benabid, A. L., P. Pollak, C. Gervason, D. Hoffmann, D. M. Gao, M. Hommel, J. E. Perret, and J. de Rougemont. Long-term suppression of tremor by chronic stimulation of the ventral intermediate thalamic nucleus. *Lancet* 337 (1991) pp.403–406.
[18] Hochberg LR, Serruya MD, Friehs GM, et al. Neuronal ensemble control of prosthetic devices by a human with tetra-plegia. *Nature.* Vol 442 No 7099 (2006) pp.164-171.
[19] Krusienski DJ, Shih JJ. Control of a visual keyboard using an electrocorticographic brain-computer interface. *Neurorehabilitation Neural Repair*. Vol 25 No4, (2011) pp323-331.
[20] Wolpaw, J.R.: Brain-computer interfaces for communication and control. 'Clinical. Neurophysioogy. Vol 113, (2002) pp 767-791.; Kübler A, Neumann N, Kaiser J, Kotchoubey B, Hinterberger T, Birbaumer NP. Brain-computer

underline that in addition to addressing patient's clinical and quality of life issues, such interfaces constitute powerful tools for research on how the brain coordinates and instantiates human behavior and how new behavior is acquired and maintained. This is because a BCI offers the unique opportunity to investigate brain activity as an independent variable.[21] In the research process, large amounts of brain data are collected from participants. And as we can retrieve ever more detailed and voluminous information about what is going on inside the user's mind, the issues of data integrity, data security, and privacy are gaining high relevance for neurotechnology as well. At one point, the read-out of brain activity and the corresponding data processing help the person to alleviate the consequences of a disease or disability, thus restoring his or her quality of life to various degree. However, these data also become more "sensitive" the more precisely one is able to interpret the user's' intentions and internal states. [22]

Currently there are a number of ongoing national and transnational programmes which deal with the data retrieved from human brain as the major object of research. Most notables are the U.S. Brain Research through Advancing Innovative Neurotechnologies (BRAIN) initiative[23], the European Union's Human Brain Project - FP7-BRAIN project (2012)[24], and the Asian Decade of the Mind and the Strategic Research Program for Brain Sciences launched in Japan in 2008. At more specific level, worldwide more than 50 BCI research groups have been identified as active.[25] For the purpose of the mentioned projects, voluminous brain data generated from research participants are collected, stored and shared among different stakeholders.

communication: self-regulation of slow cortical potentials for verbal communication. Arch Phys Med Rehabil. Vol 82 No 11 (2001). pp 1533-1539

[21] Toward Brain-Computer Interfacing, edited by Guido Dornhege, et. al

[22] Müller, O. and Rotter, S. Neurotechnology: Current Developments and Ethical Issues, *Front System Neuroscience*.; Vol 11 No 93 (2017). See also, Nam et al, "Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, (2018), "*Brain data are a vital resource for BCI research but concerns have been raised about whether the collection and use of these data generate risk to privacy. Further, the nature of BCI research involves understanding and making inferences about device users' mental states, thoughts, and intentions. This, too, raises privacy concerns by providing otherwise unavailable direct or privileged access to individuals' mental lives. And BCI-controlled prostheses may change the way in which clinical care is provided and the type of physical access caregivers have to patients.*''

[23] http://www.nih.gov/science/brain/, last accessed on 30 October 2019

[24] http://www.brain-project.org, last accessed on 30 October 2019

[25] https://bciovereeg.blogspot.com/2017/04/bci-research-groups.html , last accessed on 30 October 2019

2.2 Brain Computer Interface Technology:

2.2.a) Overview

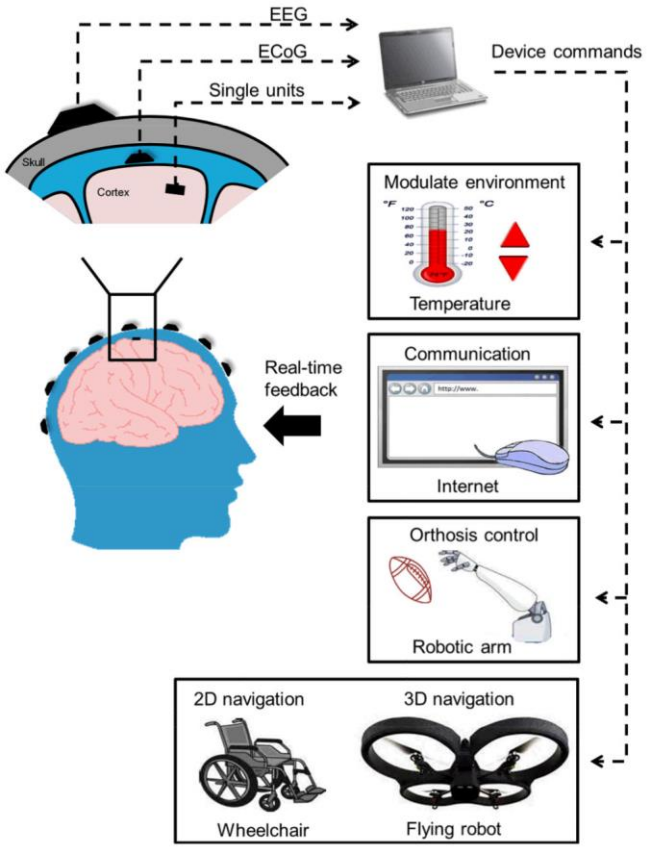
"*A Brain Computer Interface is a device that can decode human intent from brain activity alone to create an alternate communication channel for people with severe motor impairments*."[26] Translating thoughts into actions without acting physically has always been a product of human imagination in fiction literature and has fascinated scientists alike. Recent developments in brain-computer interface technology, have created opportunity for making these dreams realise. BCIs are devices that allow interaction between humans and artificial devices without using any muscular activity:[27]they rely on continuous, real-time interaction between living neuronal tissue in human brain and artificial effectors. Modern BCIs provide an additional output channel to use the neuronal activity of the brain for controlling artificial devices, for example, in restoring motor function. Neuronal activity of few neurons or large cell assemblies is sampled and processed in real-time and converted into commands to control an application, such as a robotic arm or a communication program.[28]They are focusing on brain electrical activity, recorded from the scalp as electroencephalographic activity (EEG) or from within the brain as single-unit activity, as the basis for this new communication and control technology. As such current interest in BCI development in medicine comes from the hope that this technology could be a valuable new augmentative communication option for those with severe motor disabilities—disabilities that prevent them from using conventional augmentative technologies, all of which require some voluntary muscle control.[29]

[26] "Leuthardt, E., Schalk, G., Roland, J., Rouse, A., Moran D., Evolution of brain-computer interfaces: going beyond classic motor physiology, *Neurosurgery Focus*, Vol 21 No1, (2009)

[27] Kubler et al. 2001; Lebedev, M., and Nicolelis, M., Brain–machine interfaces: past, present and future, TRENDS in Neurosciences Vol.29 No.9, (2006); Wolpaw JR, Birbaumer N, et al. Brain-computer interfaces for communication and control. *Clinical Neurophysiology*. Vol 113 No 6, (2002) pp767–791.

[28] Guido Dornhege, et. al, see also e.g., Birbaumer, N., Murguialday, A. R., and Cohen, L., Brain–computer interface in paralysis. Current. Opinion. Neurology. Vol 21, (2008) pp 634–638; Taylor DM, Tillery SI, Schwartz AB. Direct cortical control of 3D neuroprosthetic devices. *Science*. Vol 296 (2002) pp1829–1832; Hochberg LR, Serruya MD, Friehs GM, Mukand JA, Saleh M, Caplan AH, et al. Neuronal ensemble control of prosthetic devices by a human with tetraplegia. *Nature.* Vol 442, (2006); Li, Z., O'Doherty, J. E., Lebedev, M. A., & Nicolelis, M. A. Adaptive decoding for brain-machine interfaces through Bayesian parameter updates. *Neural computation,* Vol 23, (2011) pp 3162–3204. doi:10.1162/NECO_a_00207; Millán, J., Rupp, R., Müller-Putz, G.,, Murray-Smith, R., Giugliemma, C., Tangermann, M., Vidaurre C., Cincotti, F., Kübler, A., Leeb, R., Neuper, C, Müller, R., and Mattia, D., Combining brain–computer interfaces and assistive technologies: state-of-the-art and challenges, *Front Neuroscience*, 2010

[29] Wolpaw Jonathan R., Brain–Computer Interface Technology: A Review of the First International Meeting, *IEEE Transactions on Rehabilitation Engineering*, Vol. 8, No. 2, (2000)



Excerpt from: Han Yuan, Bin Hee, Brain-Computer Interfaces Using Sensorimotor Rhythms: Current State and Future Perspectives, *IEEE Trans Biomed Eng*. Vol 61 No5 (2014) pp. 1425–1435

2.2.b) Types of BCIs

A BCI system composed of 4 elements: a human agent, multi-electrode arrays, a signal processor and an application. But the application hardware itself (e.g., communication device, robotic arm, etc.) is not part of the BCI per se.

BCIs are divided into two groups according to the placement of the electrodes used to detect and measure neurons firing in the brain. The electrode arrays can be either invasive or non-invasive. Invasive electrodes consist of multi-electrode arrays implanted into the cortex of the brain or placed on the surface of the cortex (Dura). These multi-electrode arrays enable detecting both electrophysiological activity and chemical activity of single or multiple neurons in the brain or spinal cord. Such BCIs have yielded the highest information transfer rates and the best decoding performance to date, allowing human subjects to, for example, control robotic arm-and-gripper

systems for self-feeding under laboratory conditions.[30] Non-invasive electrodes are placed on the scalp, and use non-invasive electroencephalography (EEG) or magnetoencephalography (MEG) to detect neuron activity.[31]

BCIs can also be classified whether the BCI only *records* from the brain, *stimulates* brain regions (e.g. Deep Brain Stimulators), or does both ("*bidirectional*" BCIs),[32]and also according to their functional applications, those with *motor, virtual,* and *linguistic* applications.[33] As for the latter categorization, they are considered cognitive extension depending on their functionality.

Also, BCIs are divided into active, reactive, and passive BCI's based on how signals are initiated: spontaneous by the user or evoked through stimuli.[34]

An active BCI acquires and interprets neural activity elicited when a user voluntarily and intentionally engages in a pre-defined activity, whereas in reactive BCIs evoke recognition responses from users.[35] Passive BCIs applied in non-medical domain, its users acquire neural signals from spontaneous, non-evoked neural activity typically generated as the user performs a complex real-world task.

There is also a hybrid BCI, where a BCI is used with some other technology, another type of BCI to improve system performance via elicitation, acquisition and interpretation of volumized data[36] (e.g., the combination of two different types of BCI – a hybrid BCI for minimizing the effects of fatigue).[37]

Based on Clark's extended mind theory BCIs are reviewed as functionally integrated devices constituting part of human cognitive processes.[38] Attached or implanted devices of BCI can restore

---

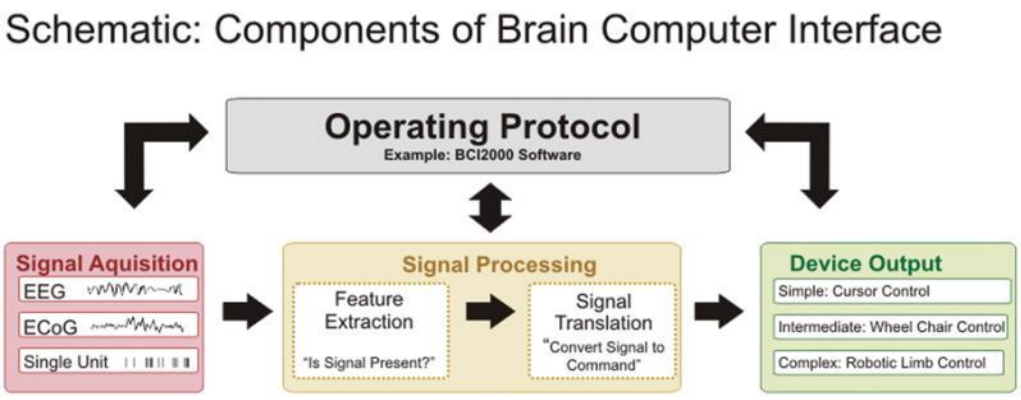
[30] Moritz C. et. al New Perspectives on Neuro-engineering and Neurotechnologies: NSF-DFG Workshop Report, *IEEE Transactions on Biomedical Engineering*, Vol. 63, no. 7, (2016)
[31] Donoghue, J.P.,Bridging the brain to the world: A perspective on neural interface systems. *Neuron* Vol 60 (2008) pp 511–521.
[32] Moritz et. al , New Perspectives on Neuroengineering, 2016
[33] Heersmink R., Embodied Tools, Cognitive Tools and Brain-Computer Interfaces, *Neuroethics,* (2013) DOI 10.1007/s12152-011-9136-2
[34] Nijholt et al, Brain-Computer Interfacing for Intelligent Systems, *Intelligent Systems*, Vol 23 No3, (2008) pp72-79,
[35]Zander et al, Enhancing Human-Computer Interaction with input from Active and Passive Brain-Computer Interfaces. In *Brain-Computer Interfaces*, Desney Tan and Anton Nijholt editors, Springer, (2010) pp181-199
[36] Allison et al, Toward Smarter BCIs: Extending BCIs through Hybridization and Intelligent Control, *Journal of Neural Engineering*, Vol 9 No1, (2012).
[37]Leeb et al, A Hybrid Brain-Computer Interface Based on the Fusion of Electroencephalographic and Electromyographic Activities. *Journal of Neural Engineering*, Vol 8 No2, (2011).
[38] Fenton, A., and Alpert, Extending our view on using BCIs for locked-in syndrome. *Neuroethics* Vol 2 No1 (2008) pp119– 132.

or enhance cognitive capacity by acquiring, storing or transmitting information to the agent. Although one can argue that moving a robotic arm, prosthetic leg, motorized wheelchair, or a cursor on a computer screen with a BCI, are mere physical actions, rather than complex cognitive actions, they may acquire functional role characteristic for cognition in the process. For instance, an LIS patient might use BCI for drawing virtual mind map which would make him to establish and better comprehend different concepts. In that case the patient delegate memory processes and abstraction functions to the BCI system and hence the BCI can be a cognitive extension.[39]

2.2.c) Essential components of BCI

BCI functions by translating neurological input signals into electrical signals, extracting features from the signals, and deriving meaningful information, and aggregating knowledge for useful purposes.[40]

As such BCI system consists of 4 sequential components: (1) signal acquisition - recorded brain signal or information input, (2) feature extraction and (3) feature translation called in combination as signal processing, (4) device output- the overt command or control functions administered by the BCI system;[41]



[39] Kyselo, M. Locked-in syndrome and BCI: Towards an enactive approach to the self. *Neuroethics*. (2011) doi:10.1007/ s12152-011-9104-x.
[40] Morshed, et al., A Brief Review of Brain Signal Monitoring Technologies for BCI Applications: Challenges and Prospects, *Bioengineering Biomedical Sciences*, Vol 4 No1 (2014)
[41] Leuthardt, et. al, Evolution of brain-computer interfaces: going beyond classic motor physiology, *Neurosurgical Focus*. Vol 27 No 1(2009).

2.3 Intracortical, subdural, and extracranial neural signal acquisition in BCI

The adult human brain consists of around 86 billions of neurons that communicate (transfer) information through action potentials- an endogenic bioelectric phenomenon and preserves this information in synapses, which are the couplings (inputs and outputs) between neurons.[42] "*An action potential is a brief and highly stereotyped fluctuation in neuronal membrane potential that occurs when excitatory synaptic input to the neuron triggers an abrupt, transient opening of channels in the cell's membrane, through which specific ions can flow. These action potentials are actively regenerated as they travel down a neuron's axon to provide synaptic input to other neurons*". [43]

Much of the membrane current from source regions remains in the local tissue and forms small current loops that may pass through the intercellular, membrane, and extracellular media. Such local source activity may be recorded as local field potential (LFP). In addition, some of the source current from localized sets of neurons and synapses may reach the cortical surface to be recorded as ECoG signal. Cortical mesoscale source current which is synchronous spike activity from very large and widely distributed sets of neurons and synapses are generators of EEG signal. [44]

Signal acquisition is a real-time measurement of this electrophysiological state of the brain. Intracortical BCIs sensors can record both field potentials (FPs) and single-neuron action potentials from the extracellular space simultaneously. Whereas non-invasive BCIs can record only synaptic activity in the form of FPs. Although the actual sources of the FP are complex, it is often referred to as a reflection of input to neurons, i.e. synaptic currents. They comprise 0–0.2

[42] Suzana, H., The human brain in numbers: a linearly scaled-up primate brain, *Frontiers Human Neuroscience*, Vol3 (2009) pp1-11
[43] Wolpaw, J.; Wolpaw, EW., editors. Brain-Computer Interfaces: Principles and Practice. Oxford University Press; Oxford: 2012
[44] *Ibid*

kHz potentials due to current flux through the somato-dendritic membranes of many neurons. In other words, EEG or ECoG signals reflect the activity of many neurons and synapses.
In contrast, spikes are the measure of neuronal output itself, the neural information-carrying product of the neurons, which often passes over long distances to other brain areas. Spikes are the brief (~1-msec) all-or-none impulses of higher frequency (~1 kHz) generated at the axon hillocks of individual neurons.[45]

Present BCIs are classified into two groups according to the nature of those signals:
First category depends on user control of *endogenous* electrophysiological activity, such as amplitude in a specific frequency band in EEG which is recorded over a specific cortical area (e.g., the sensorimotor rhythm (SMR).[46] Others depend on user control of *exogenous* electrophysiological activity, that induced by specific stimuli (e.g., amplitude of the event related potential produced in response to a letter flash).[47] Endogenous BCI systems provide a better option to a controlled model because the trained user exercises direct control over the environment. However, these BCIs require long-term training. On the other hand, exogenous BCIs may not require extensive training, but they require a somewhat structured environment (e.g., stereotyped visual input). To see the difference between exogenous and endogenous BCI systems, we can review a simple command such as moving a compute cursor: in an endogenous BCI a user can move a cursor to any point in a two-dimensional space, while in an exogenous BCI a user only have the choices presented by a display.[48]

2.3.a) Control signals in BCI

As mentioned above brain signals involve numerous simultaneous phenomena related to cognitive tasks. In general, major part of those signals are still incomprehensible and their origins are not known. However, the electrophysiological phenomena of some brain signals have been decoded in such method that people can learn to modulate them at will, to enable the BCI systems to

[45] *Ibid*
[46] Wolpaw, J., Brain–Computer Interface Technology: A Review of the First International Meeting, *IEEE Transactions on Rehabilitation Engineering*, vol. 8, No. 2, (2000)
[47] Donchin, E., *et al.*, "The mental prosthesis: Assessing the speed of a P300- based brain–computer interface," *IEEE Trans. Rehab. Eng.*, vol. 8, (2000) pp. 174–179
[48] Wolpaw, J., Brain–Computer Interface Technology: A Review of the First International Meeting, *IEEE Transactions on Rehabilitation Engineering*, vol. 8, No. 2, (2000)

interpret their intentions. These signals are referred as possible control signals in BCIs.[49] There are a number of signals that can serve as BCI control signal, but only few have been successfully employed so far. These are η (mu) and β (beta) rhythms from sensorimotor cortex, slow cortical potentials, event related potentials, P300 evoked potentials, local field potentials and action potentials/spikes (single unit activity from motor cortex or multiunit activity).

Sensorymotor rhythms

Neurophysiological rhythmic activities recorded over the sensorimotor cortex are modulated by actual movement, motor intention, or motor imagery (e.g. the execution or imagination of leg movement creates changes in rhythmic activity observed over sensorimotor cortex). The modulation is expressed as decrease in the mu (8-13 Hz, also known as the Rolandic band) and beta (14-26 Hz) frequency bands accompanied by increase in the gamma frequency band (>30 Hz). Such rhythmic brain activities referred as the sensorimotor rhythms (SMRs) can be detected on the scalp by electroencephalography (EEG) or magnetoencephalography (MEG) or on the surface of the brain by electrocorticography (ECoG). The amplitude of the sensorimotor rhythms varies when cerebral activity is related to any motor task, but as mentioned above actual movement is not always required to modulate the amplitude of sensorimotor rhythms.

As such motor intention or motor imagery can be decoded from the sensorimotor rhythms, which forms the basis of neural control in SMR-based BCIs. People can learn to increase and decrease the amplitude of sensorimotor rhythm using mental strategy of motor imagery, and thereby control physical or virtual devices. This makes it possible to use sensorimotor rhythms for the design of endogenous BCIs, which are more useful than exogenous BCIs.

The significant clinical application for SMR-based BCI is to restore or replace the lost motor function. Also, the patient with speaking difficulty could use a BCI to spell words that are afterwards spoken by a speech synthesizer. [50]

[49] He, B., Gao, S., Yuan, H., & Wolpaw, J. R. Brain–computer interfaces. In *Neural Engineering*: Second Edition. Springer US. (2013). https://doi.org/10.1007/9781461452270, pp. 87-151

[50] Wolpaw, J.; Wolpaw, EW., editors. Brain-Computer Interfaces: Principles and Practice. Oxford University Press; Oxford: 2012.

Sensorimotor rhythms have been used extensively in BCI research. For instance, Wadsworth, Berlin or Graz BCIs employ sensorimotor rhythms as control signals.

To sum up, the latest findings in the field of BCIs based on sensorimotor rhythms proved that it is possible to predict human voluntary movements before they occur based on the oscillations in sensorimotor rhythms and this prediction could be realised without the user making any movements at all. [51]

Slow cortical potentials

Slow cortical potential (SCP) is the signal caused by slow voltage shifts in the depolarization levels of pyramidal neurons in cortex. They occur from 0.5 to 10 seconds after the onset of an internal event and are thus considered an SCP. SCPs belong to the part of the EEG signals below 1 Hz. Different SCP signals convey different intents. Negative SCP generally reflects increased neuronal activity, while positive SCP generally reflects reduced cortical activation. People can learn to control SCPs and use them to operate a simple BCI. [52] For instance SCP shifts can be used to move a cursor and select the targets presented on a computer screen.[53] Patients can be trained to generate voluntary SCP changes using a thought-translation device - a tool used for self-regulation SCP training, which shows visual-auditory marks so that the user can learn to shift the SCP. It consists of a vertically located cursor on a computer screen that constantly reflects the amplitude of SCP shifts. Thought-translation devices usually show continuous feedback; however, it is possible to train SCP self-modulation in the absence of continuous feedback.[54] Typical accuracy rates achieved for SCP classification vary between 70 and 80 per cent being considered adequate, but the rates of information provided by SCP-based BCI are comparatively low.

[51] Bai, O.; Rathi, V.; Lin, P.; Huang, D.; Battapady, H.; Fei, D.; Schneider, L.; Houdayer, E.; Chen, X.; Hallett, M. Prediction of human voluntary movement before it occurs. Clinical Neurophysiology. Vol 122 (2011) pp364–372

[52] Birbaumer, N.; Elbert, T.; Canavan, A.G.; Rockstroh, B. Slow potentials of the cerebral cortex and behavior. *Physiological Reviews*. Vol 70 (1990) pp 1–41.

[53] Hinterberger, T.; Schmidt, S.; Neumann, N.; Mellinger, J.; Blankertz, B.; Curio, G.; Birbaumer, N. Brain-computer communication and slow cortical potentials. *IEEE Transactions on Biomedical Engineering*, Vol 51, (2004) pp1011–1018.

[54] Nicolas-Alonso, L., and Gomez-Gil J., Brain Computer Interfaces, a Review, *Sensors* 2012, pp1211-1279; doi:10.3390/s120201211

Event related potentials

Event-related potentials (ERP) is a distinctive pattern of positive and negative voltage deflections that occur in the EEG at a fixed time after a brain receives a particular visual, auditory, or somatosensory stimulus. The most common way to deduct ERP from EEG recording is aligning the signals according to the stimulus onset and then averaging them. The number of stimuli averaged typically are low in BCI applications. ERPs can be "exogenous" or "endogenous." [55] Exogenous ERPs are of shorter latency that can be recorded over the first 150 msec following the eliciting event. They tend to reflect activity in the primary sensory systems, and their waveforms and scalp distributions vary with the modality of the eliciting stimuli. Endogenous ERPs are of longer-latency components which reflect information-processing activity that is cognitive in nature and therefore less dependent on stimulus modality and more dependent on the significance of the eliciting event in the patient's concurrent tasks. [56]

Most commonly used ERP is the visual evoked potential (VEP), that occur in the visual cortex after receiving a visual stimulus, such as a light flash, the appearance of an image, or an abrupt change in color or pattern.[57] These brain activity modulations are relatively easy to detect since the amplitude of VEPs increases to a large degree as the stimulus is moved closer to the central visual field.[58]

Steady-state visually evoked potentials (SSVEPs)

The most frequently used VEPs - steady-state VEPs (SSVEPs) are stable oscillations in higher voltage that are elicited by rapid repetitive stimulation such as a strobe light, a light-emitting diode, or a checkerboard lattice. The successive stimulus presentations evoke similar responses, and the overlap of these responses produces a steady-state oscillation. Frequency analysis of SSVEPs normally reveals a peak at the frequency of stimulation, as well as peaks at higher harmonic frequencies.

Standard SSVEP-based BCI and other VEPs depend on the user's gaze direction requiring muscular control. To produce such signals, the user is presented with a display of concurrent

[55] He, B et al., Brain–computer interfaces. 2013

[56] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012

[57] Regan, D. Human Brain Electrophysiology: Evoked Potentials and Evoked Magnetic Fields in Science and Medicine; *Elsevier*: New York, NY, USA, (1989).

[58] Yijun, W.; Ruiping, W.; Xiaorong, G.; Bo, H.; Shangkai, G. A practical VEP-based brain-computer interface. *IEEE Transaction on Neural Systems and Rehabilitation Engineering*., Vol 14 (2006) pp234–240.

repetitive stimuli (e.g., several LEDs) that are located at different places in the visual field. Each stimulus flashes at different frequencies in the alpha or beta bands and represents a specific BCI output (e.g., type a specific letter, move the wheelchair in a specific direction, etc.). The user typically makes a selection by looking at the stimulus that represents the desired BCI output. The BCI calculates the frequency spectrum of the occipital EEG. Frequency analysis of the SSVEP shows a peak at the frequency of the object at which the user gazes. Thus, a BCI by determining the frequency of this peak can guess which object the user wants to select and produces that output.[59]

It should be mentioned that early BCI studies used VEPs as an input for BCI systems. In the first BCI developed by Vidal described above the user viewed a maze and a checkerboard stimulus. By looking at one of four fixation points surrounding the checkerboard stimulus (and thus producing a VEP that resembled which quadrant of the visual field the stimulus was in), the user could move a cursor of a computer in one of four directions and thereby move it through the maze.[60]
Currently, an SSVEP-based BCI that has been developed could control a functional electrical stimulator (FES) to initiate knee flexion.[61]

P300 event related potentials

The P300 is an endogenous ERP component in the EEG that occurs over central-parietal scalp 300msec after a rare event occurs in the context of the oddball paradigm (where the designation of "*P300*" come from). [62] In this paradigm, users are subject to events, (i.e oddball stimuli) consisting of two distinct categories. Events in one of the two categories occur only rarely. The user is presented with a task that can be accomplished only by classifying each event into one of the two categories. When an event from the rare category is presented, it elicits a P300 response in the EEG. Although this is a large positive peak that occurs usually 300 msec after event onset, the response can be elicited between 250 to 750 msec. The amplitude of the P300 component is inversely proportional to the frequency of the rare event presented, i.e the less probable is the stimulus, the larger is the amplitude of the response peak. This variability in latency reflects the

[59] Middendorf, M., McMillan, G., Calhoun, G., Jones K., Brain-computer interfaces based on steady-state visual evoked response. *IEEE Transaction on Neural Systems and Rehabilitation Engineering* Vol 8 No2 (2000) pp211–214; Ortner, R., Allison, B., Korisek, G., Gaggl, H., Pfurtscheller, G., An SSVEP BCI to control a hand orthosis for persons with tetraplegia, *IEEE Transaction on Neural Systems and Rehabilitation Engineering*, Vol 19 No1 (2011) pp1–5
[60] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[61] Middendorf et al. (2000)
[62] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012

fact that the P300 is elicited by the decision about that a rare event has occurred, and the decision latency can vary with the difficulty of the decision.[63] The P300 is usually highest over central parietal scalp and decreases gradually as distance from this area increases.

This endogenic ERP component is a natural response and therefore does not require training. The use of P300-based BCIs especially needed in cases where either sufficient training time is not available, or the patient cannot be easily trained.[64] P300-based BCIs allow users to select items displayed on a computer screen and are available for current daily use patient in their homes.

LFPs and action potentials

Two type of signals are obtained by intracortical neuron recording: spikes in the form of single-unit activity (SUA), or multi-unit activity (MUA), and local field potentials (LFPs).[65].

Spikes reflect the action potentials of individual neurons. They are used to determine the average firing rates – voltages, and functional correlations of neuronal firing based on *rate-coding hypothesis*. Temporal patterns of neuronal firing are also recorded based on *temporal coding hypothesis.* It should be mentioned that rate and temporal coding provides information where the firing rate of a neuron or neurons encodes movement information, while the synchrony between neurons encodes expectation or enhanced attention.[66] As such recording spiking activity of firing rates in different neurons, may be extremely useful for achieving multidimensional control for a BCI.

Local field potentials (LFPs) are microlevel phenomena recorded within the cortex. They represent mainly synchronized events (in the frequency range of <300 Hz) in neural populations. The major sources of FPs are synaptic currents which are also the major sources for EEG and ECoG signals. Because FPs reflect signals from many different neurons, their spatial resolution and their functional specificity are lower than that of spiking activity.[67]

[63] Kutas et al., Augmenting mental chronometry: the P300 as a measure of stimulus evaluation time. *Science (*1977)
[64] Spencer KM, Dien J, Donchin E Spatiotemporal analysis of the late ERP responses to deviant stimuli. *Psychophysiology* Vol 38 No2 (2001) pp343–358
[65] Waldert, S.; Pistohl, T.; Braun, C.; Ball, T.; Aertsen, A.; Mehring, C. A review on directional information in neural signals for brain-machine interfaces. J. *Physiology.* Vol 103Paris (2009) pp 244–254
[66] Middlebrooks et al., A panoramic code for sound location by cortical neurons. *Science*. Vol 264 1994; pp842–844
[67] He, B et al., Brain–computer interfaces. (2013)

2.3.b) Technologies for Brain Activity Monitoring in BCI

BCI technology, is based on the premise that brain signals can be decoded and used to control devices as per the desire of the user. At present, there are various technologies available for brain activity monitoring. They are classified depending on their invasiveness level which can be performed at the vicinity of neurons inside the brain cortex, on the scalp, and in some cases remotely.[68] The invasive techniques provide more reliable signal acquisition, for instance electrode embedded into the brain of the patient can record neuronal activity and convert it to motor activity in a robotic prosthetic for amputees.[69] But at the same time, they require dangerous brain surgery, and thus are utilized when there are only significant clinical needs.

Currently the three major recording modalities for BCI are electroencephalographic (EEG) scalp electrode arrays with its centimeter resolution that attached noninvasively over scalp, electrocorticographic (ECoG) electrode arrays with its millimeter resolution that are surgically positioned over the cortical surface, and miniaturized *microelectrode arrays* with their tens-of-microns resolution that are surgically inserted into the cerebral cortex to record neuronal action potentials (spikes) from individual neurons and/or local field potentials (LFPs).

All of these methods record, at microvolt-level, the extracellular potentials generated by neurons in different cortical layers, but they are sampled at different field distances and at different spatial resolutions. ECoG shares the same electrophysiological sources with EEG, i.e. the underlying field potentials - a complex product of activity in many synopses and neurons, but are measured at a closer distance to the cortex, thus providing a finer spatial resolution on the order of milli-meters as well as the ability to record higher-frequency content in the signal (up to 200 Hz). Intracortical recordings of single neuron action potentials (also called spikes) are of the highest resolution but they represent the most invasive BCI method since they record electrical activity from electrodes implanted in the parenchyma (brain tissue). [70]

[68] Chi YM, Jung T, Cauwenberghs G., Dry-contact and noncontact biopotential electrodes: methodological review, *Biomedical Engineering,* IEEE Vol 3 No 1(2010) pp06-119.
[69] Nicolas-Alonso L., and Gomez-Gil, J., Brain Computer Interfaces, a Review, *Sensors* Vol 12, 2012, pp 1211-1279;
[70] Yuan H., Hee B., Brain-Computer Interfaces Using Sensorimotor Rhythms: Current State and Future Perspectives, *IEEE Transactions on Biomedical Engineering*. Vol 61 No5 (2014) pp1425–1435

- *Noninvasive method of acquiring brain signals:* ***EEG***

Non-invasive BCIs acquire signals from electrodes located outside brain tissue (e.g., those placed on the scalp). These BCIs record field potentials (FPs), which are a complex product of activity in many synapses and neurons. Recording potentials on the scalp is called electroencephalography (EEG).[71] EEG is the most prevalent method of signal acquisition for BCIs due to the minimal risk involved and the relative convenience of conducting studies. It is easy to set up, portable, inexpensive, and has almost 80 years of past performance. The EEG recording system consists of electrodes, amplifiers, A/D converter, and a recording device. The electrodes acquire the signal over the scalp, the amplifiers process the analog signal to increase the amplitude of the EEG signals so that the A/D converter can digitalize the signal in a more accurate way. Finally, the recording device, such as a personal computer, stores, and displays the data.[72]

The EEG recording system has high temporal resolution: it is capable of measuring massive amounts of neuron firings in the brain cortex that produce many oscillatory waves. However, its spatial resolution is not as good as that of implanted methods, as signals up to 256 electrode sites can be measured at the same time. This technique is furthermore affected by background noise generated either inside the brain or externally over the scalp. The applications to date are generally limited to low-degree-of-freedom continuous movement control and discrete selection. Sensorimotor rhythms or event related potentials have been used to control cursors in several dimensions, a spelling device - visual P300 speller, conventional assistive devices, and a wheelchair. Two-dimensional cursor control has also been achieved via attention modulation.[73]

EEG analysis of the waveforms originating from various regions of the brain lobes are applied in neuroscience, cognitive science and psychology through studies that show which brain lobes are responsible for specific cognitive activities. For example, the frontal lobe is highly associated with problem solving, mental flexibility, judgment, and creativity; whereas the temporal lobe is primarily responsible for auditory sensation, perception, language comprehension, and long-term memory. EEG data can be analyzed to assess mental states and neuronal activities of patients. For

[71] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[72] Nicolas-Alonso L., and Gomez-Gil, J., Brain Computer Interfaces, a Review, *Sensors* 2012;
[73] Jerry J. Shih, Dean Krusienski J., and Wolpaw J., Brain-Computer Interfaces in Medicine, Mayo Clinic Proceedings, Vol 87 No 3 (2012); pp268-279

epileptic patients, ictal episodes captured in EEG data shows high level of uncontrolled activity of brain signals typically characterized by increases in Gamma rhythms.[74]

- *Invasive BCI monitoring technologies:*

Electrocorticography (ECoG) is an electrophysiological technique that utilizes electrodes placed intracranially on the surface of the brain, therefore it sometimes referred to as Intracranial Electroencephalogram (iEEG). ECoG is recorded by electrodes implanted inside the skull either above (epidural) or below (subdural) the dura mater, but not penetrating the brain, providing a unique balance between invasiveness and signal quality.[75] ECoG uses signals that may reflect highly local or broadly distributed changes in electrical field potential.

Many studies during the last decade have shown the functional specificity, signal fidelity, and long-term stability of ECoG activity in behavioral and cognitive tasks.[76]

Together with its spatial (coverage of distant areas of the brain on the scale of millimeters, versus the cm scale used for EEG) and temporal resolution (able to record higher gamma frequency) and, a lower vulnerability to artifacts, ECoG elucidates brain function in ways that cannot be achieved by other electrophysiological or neuroimaging techniques. For instance, compared to intracortical electrodes which induce tissue responses that may degrade or prevent neuronal recordings ECoG electrodes may provide greater long-term functional stability. Or while scalp-recorded EEG lacks functional specificity and is very prone to artifacts, ECoG because of its closer proximity to the neurons producing electrical currents has larger signal amplitude and broader bandwidth and thus is able to provide higher accuracy and shorter training times in, for example, operating external robotic control. [77]

ECoG consists of electrodes made of platinum, platinum-iridium, stainless steel, or silver embedded into a thin flexible silastic sheet. After the implantation of the electrodes, bioamplifiers with high temporal resolution and with sufficient range and resolution in voltage are required to

[74] Morshed, et al., A Brief Review of Brain Signal Monitoring Technologies for BCI Applications: Challenges and Prospects, J *Bioengineering and Biomedical Science*, Vol 4 No 1 (2014)
[75] Nam et al, "Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, 2018; See also, Dornhage et al., Toward Brain-Computer Interfacing, MIT press, 2007
[76] Schalk, G. Can electrocorticography (ECoG) support robust and powerful brain–computer interfaces? Front Neuroengineering ,Vol 3 (2010)
[77] Nam et al., "Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, 2018;

capture synchronous synaptic inputs. ECoG BCI has similar signal-processing techniques to EEG, as it uses the same features i.e. the mu and beta rhythm bands prominent in the scalp-recorded EEG over sensorimotor cortex. It also produces higher-frequency broadband gamma activity and, with depth electrodes, activity from subcortical structures that cannot be captured over the scalp. In addition, ECoG detects the local motor potentials (LMP), that encodes different aspects of movements (i.e. execution and planning) which is in a way similar to intracortical recording.

Penfield's pioneering work with epilepsy patients in the 1950s represented the first comprehensive ECoG-based effort to study the neural basis of human behavior.[78] Interest in ECoG as a control source for brain-computer interfaces (BCIs) has grown over the past decade. However, still the large majority of human ECoG studies have been restricted to patients with pre-surgical epilepsy as a part of diagnostics.

Some examples of the use ECoG include the following: In 2011, the first matrix speller using ECoG was implanted in the occipital lobe of the patient. The BCI used P300 and visual evoked potentials to spell very effectively, attaining 17 characters per minute over sustained BCI operation and 22 characters per minute when it reached the peak performance.[79] These rates were higher than those reported for EEG-based P300 spellers at that time and are still higher than typical EEG-based P300 BCIs today. Two additional studies also reported encouraging results with a similar approach.[80] Groups in other studies selected characters through a sequence of binary selections based on imagination of either tongue or hand movement.[81]

Actual two- and three-dimensional control was shown in a patient with tetraplegia resulting from a C4 spinal injury. This was the first publication that reported real-time ECoG-based robotic arm control in a tetraplegic patient.[82]

---

[78] Penfield, W., and Rasmussen, T. editors. The Cerebral Cortex of Man. MacMillan, New York, 1950.

[79] Brunner, P., Ritaccio, A. L., Emrich, J. F., Bischof, H., and Schalk, G. Rapid communication with a "P300" matrix speller using electrocorticographic signals (ECoG). *Front Neuroprosthestics*, Vol 5 No 5, (2011). pp1–9

[80] Krusienski, D., and Shih, J. J. Control of a brain–computer interface using stereotactic depth electrodes in and adjacent to the hippocampus. *J Neural Engineering*, Vol 8 No 2 (2011)
Krusienski, D. J., and Shih, J. J. Control of a visual keyboard using an electrocorticographic brain–computer interface. *Neurorehabilitation Neural Repair,* Vol 25 No4 (2011) pp323–331

[81] Hinterberger, T., Widman, G., Lal, T., Hill, J., Tangermann, M., Rosenstiel, W., Schölkopf, B., Elger, C., and Birbaumer, N. Voluntary brain regulation and communication with electrocorticogram signals. *Epilepsy Behav*, Vol 13 No2 (2008) pp300–306

[82] Wang, W., Collinger, J. L., Degenhart, A. D., Tyler-Kabara, E. C., Schwartz, A. B., Moran, D. W., Weber, D. J., Wodlinger, B., Vinjamuri, R. K., Ashmore, R. C. et al. An electrocorticographic brain interface in an individual with tetraplegia. *PloS One,* Vol 8 No2 (2013)

A recent study from 2016 utilized a fully implanted ECoG-based BCI device with subdural ECoG electrodes over cortical motor areas and a subcutaneously placed transmitter in the thorax. The patient could convey about two letters per minute by imagining hand movement or using eye-tracking system, both simultaneously and as an alternate communication tool. The BCI provided communication through an implanted device designed for chronic recording and remained effective 28 weeks after electrode placement. This study demonstrated that an ECoG BCI can provide practical communication, even in a hybrid environment with an eye-tracker, for about 7 months after implantation surgery.[83]

In addition to working with selective attention and imagined movement, ECoG studies have introduced communication options that may not be readily viable with noninvasive imaging methods such as EEG. ECoG signals may be employed to decode phonemes or words that a user speaks or even simply imagines.[84] These approaches rely on ECoG electrodes embedded in the temporal lobe since this region includes Wernicke's area and earlier auditory processing areas over superior temporal gyrus. ECoG activity reflecting speech processing has also been explored over Broca's area and nearby motor areas involved in speech.

One study used ECoG BCI to explore vocal track kinematics as six participants articulated nine vowels. The authors could predict lip kinematics based on ECoG activity from ventral sensorimotor cortical areas.[85] Advancing further to simple phrases or words, other two studies examined ongoing spatiotemporal changes in cortical activity while people openly or in silence read sentences continuously,[86] decoded complete spectro-temporal representations and even whole sentences from ECoG.[87]

---

[83] Vansteensel, M., Pels, E., Bleichner, M., Branco, M., Denison, T., Freudenberg, Z., Gosselaar, P., Leinders, S., Ottens, T., VandenEboom, M., van Rijen, P., Aarnoutse, E., and Ramsey, N. Fully implanted brain– computer interface in a locked-in patient with ALS. *The New England Journal of Medicine*, Vol 375 No 21 2016. pp2060–2066

[84] Leuthardt, E. C., Gaona, C., Sharma, M., Szrama, N., Roland, J., Freudenberg, Z., Solis, J., Breshears, J., and Schalk, G. Using the electrocorticographic speech network to control a brain–computer interface in humans. *J Neural Eng*, 8(3):036004, 2011; Martin, S., Brunner, P., Iturrate, I., Millán, J. d. R., Schalk, G., Knight, R. T., and Pasley, B. N. Word pair classification during imagined speech using direct brain recordings. *Sci Rep*, 6, 2016.

[85] Bouchard, K. E., Conant, D. F., Anumanchipalli, G. K., Dichter, B., Chaisanguanthum, K. S., Johnson, K., and Chang, E. F. High-resolution, non-invasive imaging of upper vocal tract articulators compatible with human brain recordings. *PloS One*, Vol 11 No 3: (2016).

[86] Brumberg, J. S., Krusienski, D. J., Chakrabarti, S., Gunduz, A., Brunner, P., Ritaccio, A. L., and Schalk, G., Spatio-temporal progression of cortical activity related to continuous overt and covert speech production in a reading task. *PloS One*, Vol 11 No11(2016).

[87] Herff, C., Heger, D., De Pesters, A., Telaar, D., Brunner, P., Schalk, G., and Schultz, T. Brain-to-text: Decoding spoken phrases from phone representations in the brain. *Frontiers in Neuroscience*, 9:217, 2015.

Another study explored ECoG activity while 10 patients listened to a rock song or spoken narrative.[88] The researchers could precisely and reliably identify the moments when spoken lyrics began and ended within the rock song and demonstrated that broadband gamma power over temporal areas reflected processing dynamics relating to different aspects of sound such as pitch tone and timbre.

ECoGs are used in neuromodulation together with Deep Brain Stimulation for treating, e.g. Parkinson disease or epilepsy.

For instance, Responsive Neurostimulator (RNS) developed by the NeuroPace for the treatment of intractable epilepsy has received approval in United States in 2011. The RNS System provides responsive cortical stimulation via a cranially implanted programmable neurostimulator which continually senses ECoG or LFP activity.

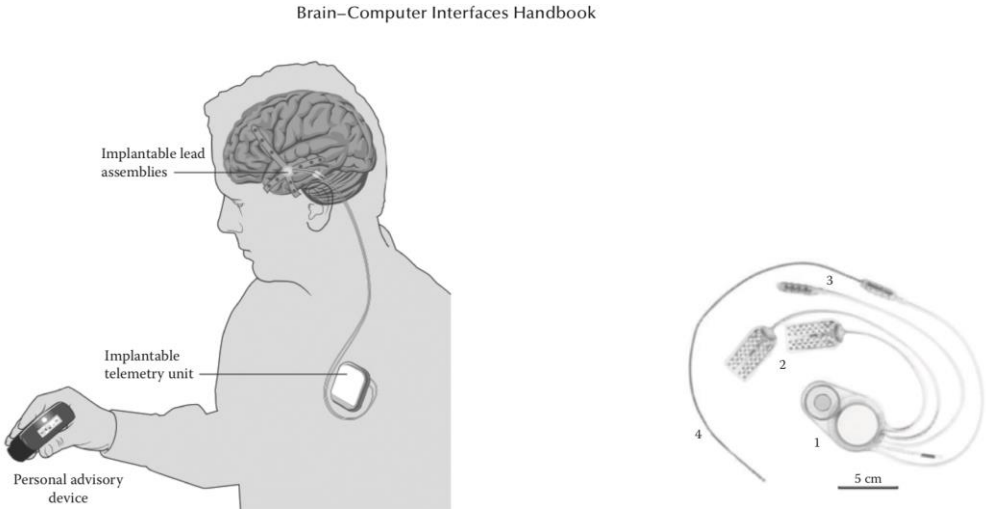
A randomized controlled trial assessing the safety and effectiveness of responsive cortical stimulation study as an additional therapy for partial onset seizures was conducted in 191 adults with medically refractory epilepsy. The study is registered on ClinicalTrials.gov and the results of the study are publicly available through the BRAIN Initiative Public-Private Partnership Program.[89]

Example to ECoG and DBS hybrid device is the German BrainInterchange system by CorTec. It is based on a fully implantable device for recording and stimulation in humans which provides 32 electrode contacts, to be used for signal recording or/and brain stimulation. The system consists of (a) the electrodes; (b) a hermetically encapsulated electronic unit that amplifies, digitizes, and broadcasts brain signals as well as directs electrical stimuli to selected electrodes; (c) a telemetric unit that is placed outside the body on the patient's skin; and (d) a wearable controller unit. The telemetric unit communicates with the implant and provides it wirelessly with energy. The controller unit (usually laptop PC) runs a software interface to custom-specific application

[88] Sturm, I., Blankertz, B., Potes, C., Schalk, G., and Curio, G. ECoG high gamma activity reveals distinct cortical representations of lyrics passages, harmonic and timbre-related changes in a rock song. *Frontiers in Human Neuroscience*, Vol 8 No798 (2014).

[89] Nam et al., Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, 2018;

software such as C++, Python II, or MATLAB for controlling brain signal data stream, analyzing the data, taking decisions, and sending commands to the implant.[90]



These new approaches open opportunities to develop BCIs based on words, sentences, or other speech-related activity that people simply imagine. As such BCIs that can directly interpret imagined words, sentences, or related mental activities at one hand would provide major advances for BCIs in terms of ease of use, practicality, flexibility, and bandwidth, on the other would pose qualitatively different ethical questions of autonomy and agency and mental privacy.

- *Intracortical recording*:

Intraparenchymal BCIs (iBCIs) are those that acquire brain signals from microelectrodes surgically implanted within brain tissue (i.e., parenchyma). These are also called *penetrating* or *intracortical BCIs*.

The pioneering studies on using electrodes to record spikes from individual cortical neurons were conducted by Fetz and colleagues in the 1960s and 1970s.[91] Later, electrodes were used to record spikes from neurons in visual, somatosensory, and motor cortices.[92]

[90] Nam et al., Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, 2018;
[91]Fetz, E.E. Operant conditioning of cortical unit activity. *Science* Vol 163, (1969) pp955–958
[92]Hubel D., Tungsten Microelectrode for Recording from Single Units, *Science*. 22;125 (1957) pp549-50; Evarts E., Pyramidal tract activity associated with a conditioned hand movement in the monkey. *Neurophysiology*, Vol 29 No 6 (1966) pp1011-27.

Nowadays, miniaturized microelectrode arrays are embedded into the cerebral cortex to record neuronal action potentials (i.e. spikes) from individual neurons and/or potentials from small localized sets of neurons and synapses that yield high information content.[93] Neuronal *action potentials* are viewed as the basic units of inter-neuronal communication and information transfer in the central nervous system. The relationship between neuronal activity (i.e., spikes) in motor and sensory areas of cortex and movements or external sensory events are revealed through intracortical recording.[94]

Intracortical BCIs are unique that due to its microelectrodes placed within neural tissue, they can measure LFPs and spikes simultaneously. In addition to recording a *single-unit activity* (SUA) (i.e., the action potentials) that reflect the output of single neurons, iBCIs can also record spikes of a cluster of neurons in the form of *multiunit activity* (MUA). Thus, in providing BCI control, an iBCI can use all-rounded information about *spiking patterns* within the central nervous system, as well as precise information about LFPs.[95]

Because the size and shape of the spikes from an individual neuron are highly stereotyped and differ from those coming from all other neurons, the spike-sorting process can be more precise if the spikes of a single neuron are recorded by more than one electrode. Therefore, a variety of invasive electrodes have been developed in the form of microwires in planar silicon probes and platforms with micro-electrode array (MEA) such as "Utah Electrode", or multisite electrode such as "Michigan Electrode". [96] The fabrication involves the use of integrated circuit technology to create dense arrays of thin film electrodes for recording neuronal spike activity and/or LFPs from the target neural population with sufficient quality, information content, reliability, and longevity to meet the demanding needs of the BCI system.[97]

Spiking is believed to be the major information output for long-distance, high-content communication for all neurons capable of spiking and to be a predominant form of coding in human nervous system. Information available from the spiking activity of even a single neuron can predict joint angles, muscle-contraction strengths, force levels, and individual or combined

[93]Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[94]*Ibid.*

[95] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[96] Kotov NA, Winter JO, Clements IP, Jan E, Timko BP et al. Nanomaterials for neural interfaces, Advanced Materials Vol 21 (2009) pp3970-4004.
[97] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012

finger actions, as well as bimanual and unimanual actions. In addition, spikes from specific neurons, if recorded properly, can provide insight not only into movements and movement parameters and but also higher-level information about future movement sequences and goals.[98]

Furthermore, populations of many single neurons can provide much more detailed information and with greater precision (i.e., with higher signal-to-noise ratio). [99] Neural populations can provide accurate predictions of ongoing limb actions, such as the trajectory of the hand during a reach or grasp. The collective information coding by populations of neurons is called a population or ensemble code. It is this code that has the proven potential to provide real-time estimates of intended movements for iBCIs. [100] To date, iBCIs are considered the best possible interface for controlling a robotic arm or prosthetic leg with several degrees of freedom.

2.4 Steps of signal processing

The purpose of a BCI is to sample and digitize characteristics of brain signals that indicate what the user wants the BCI to do, to translate these measurements in real time into the desired device commands, such as where or how to move a cursor, an arm, or a wheelchair and to provide concurrent feedback to the user. [101] For useful processing of brain signals in BCI applications (i.e. for diagnosis, prognosis, monitoring, and feedback) the brain signals captured through different recording technologies must be processed with low-noise and high-gain amplification. The processing is conducted by way of removing artifacts from the signals, extracting features of interests, and classifying with sophisticated and versatile algorithms.[102] The brain-signal characteristics used for this purpose are called *signal features*, or simply *features*.

The signal-analysis in BCI operation occurs in two steps: feature extraction and feature translation.

[98] Achtman et al. 2007; Pesaran et al. 2006; Scherberger & Andersen 2007 cited in Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[99] Georgopoulos A., et al., Neuronal Population Coding of Movement Direction, *Science*, Vol 233 1986 pp 1416-19; Maynard, E., et al. Neuronal interactions improve cortical population coding of movement direction. Neuroscience. Vol 19 (1999) pp. 8083–8093.
[100] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[101] Maureen C., Laurent B., Fabien L., Brain–Computer Interfaces, Foundations and Methods, 2016
[102] Krusienski DJ, Wentrup MG, Galán F, Coyle D, Miller KJ et al. Critical issues in state-of-the-art brain–computer interface signal processing, *Neural Engineering* Vol 8 (2011)

2.4.a) Feature extraction

The first step, feature extraction is the process of distinguishing the pertinent signal characteristics from extraneous content and representing them in a compact and/or meaningful form, amenable to interpretation by a human or computer. In order to have effective BCI operation, the electrophysiological features extracted should have direct correlations with the user's intent. The process of feature extraction prepares the signals for translation into BCI output commands by cleaning up and removing superfluous corrupting information or interference, typically referred to as noise from acquired signals in order to keep only the relevant information for measuring. It should be mentioned that both noise and artifacts can contaminate the signal. Noise is due to background neurological activity, whereas artifacts are due to sources unrelated to the neurological activity and are not intrinsic to the expected measurement of this activity.

As such in scientific literature the process of feature extraction is divided into 3 sub-steps:

- signal conditioning involves high input impedance buffer, low-noise amplification of brain signals, filtering through a band-pass filter of high order, and driving of signals to reduce common mode noise[103] (i.e. to reduce noise and to enhance relevant aspects of the signals)

- extraction of the features from the conditioned signals: The feature extraction stage identifies discriminative information in the brain signals that have been recorded. Signals are described in terms of a small number of relevant variables called "features"; e.g., an EEG or ECoG signal's strength on some sensors and on certain frequencies may count as a feature; [104] Different feature extraction methods are used for brain signals that are clearly characterized spatially, spectrally, and temporally (e.g., sensory evoked potentials or sensorimotor rhythms). For instance, because sensorimotor rhythms are amplitude modulations at specific frequencies over sensorimotor cortex, it is recommendable to extract frequency-domain features using processing parameters which are appropriate to the characteristic dynamics of these rhythms (i.e. *rate coding)*. However, in more exploratory situations, when not much is known about the optimal feature choice, it is

[103] Sanei S, Chambers JA EEG Signal Processing, John Wiley & Sons, West Sussex, (2007);
Consul Pacareu S, Morshed BI ,Power Optimization of NeuroMonitor EEG Device: Hardware/Software Co-Designed Interrupt Driven Clocking Approach, 6th Intl IEEE EMBS Neural Engineering Conf: 25-28. (2013)
[104] Bashashati A, Fatourechi M, Ward RK, Birch GE A survey of signal processing algorithms in brain–computer interfaces based on electrical brain signals, *Neural Engineering,* Vol 4. (2007)

preferable to first assess potential features in both time (i.e *temporal coding)* and frequency domains, and construct a feature vector that includes features extracted in both time and frequency domains.[105]

- feature conditioning/normalization is eliminating differences in means or dynamic rages of features which are not relevant to the BCI usage.

It should be noted that extracting features from continuously varying signals, such as those recorded by EEG, ECoG, and local field potentials (LFPs) are different from those of action potentials. It is because as described above each of these electrophysiological phenomena – EEG, ECoG signals and LFPs is a complex reflection of the activity of many different synaptic and neuronal sources, whereas each spike reflects the activity of an individual neuron. Whenever the neuron's internal state and its concurrent synaptic inputs combine to achieve a specific voltage threshold, the neuron produces an impulse called a spike train. Thus, the spike train reveals very specific information: it tells when a specific neuron fires. It does though reveal very little about what is going on in the network(s) to which that one neuron belongs. In contrast, EEG or ECoG signals provides complex information about what large populations of neurons are doing and but not much about a specific neuron. Spike trains are microscale brain activity and recorded by microelectrodes within the brain as are LFPs. Whereas, EEG recorded from the scalp and ECoG recorded on the brain surface are, respectively, macroscale and mesoscale brain activity. The timing of the spike is significant for BCI measuring and is usually measured with a resolution of 1 msec.[106]

2.4.b) Feature translation

The BMIs main function is converting thought into actions which is done by extracting motor control signals from the firing patterns of populations of neurons and using these control signals to reproduce motor behaviors in artificial actuators.[107] Ideally, these features-control signals would be in a form that could directly communicate the user's intent. However, because the features extracted represent indirect measurements of the user's intent, they must be translated into

[105] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[106] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[107] Nicolelis, M.A. Actions from thoughts. *Nature* Vol 409, (2001) pp 403–407

appropriate device commands using a translation algorithm. For instance, an amplitude (e.g. a decrease on increase) in power in a specific EEG frequency band might be translated into an upward displacement of a computer cursor, or a particular evoked potential measure might be translated into the selection of a letter on the screen. The core of a translation algorithm is a model, which is a mathematical procedure typically comprised of a mathematical equation with set of equations, and/or mapping mechanism such as look up mechanism. The selected translation algorithm must be dynamic to accommodate and adapt to spontaneous or learned changes in the user's signal features, to ensure that the possible range of the specific signal features from the user covers the full range of device control, and to make control as efficient as possible. A more complex application requires that a set of features be translated into three-dimensional spatial coordinates that are used to control the position of a robotic arm.[108]

In a BCI, the both parts of signal processing - feature extraction and feature translation should work together well. Thus, the choice of the feature type through frequency analyses or spike sorting (e.g., evoked-potential amplitude, power in a frequency band, single-neuron firing rates) and the choice of the model type of linear or nonlinear algorithms (e.g., linear discriminant, Bayesian classifier, support-vector machine, etc.) guarantee the success of the most accurate prediction of a user intent. For instance, it is advisable, to apply a two-class classification algorithm to the feature type of P300 amplitude. In contrast, if the feature type is mu-rhythm power, a linear regression may be most appropriate choice.[109]

2.4.c) Device output

Translation into a command associates an output control signal with a given brain activity pattern identified in the user's brain. E.g., when imagined movement of the left hand is identified, it can be translated into the command: "move the cursor on the screen toward the left". This command can then be used to control a given application, such as a text editor.[110]
The output might be used to operate a spelling program on a computer screen through letter selection, to move a cursor on a computer screen, to drive assistive devices, to manipulate a robotic arm or prosthetic leg.

[108] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[109] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[110] Kubler, Brain–machine interfaces: past, present and future, 2006

Feedback is afterwards provided to the patient in order to inform him about the brain activity pattern that was observed and recognized. The objective here is to help the patient learn to modulate brain activity and thus improve his control of the BCI device. Indeed, controlling a BCI device is a skill that is to be learned gradually.[111]

For some applications the output and the feedback are identical (e.g., a BCI spelling application that puts its output on a screen in front of the user, or in a robotic arm the movements of which can be seen by the user). In other applications the output and feedback are different (e.g., an environmental control application in which the output is a command for room-temperature change, and the feedback is an indication of the change that appears on the user's screen).[112]

Users can acquire selective control over certain brain areas by means of neurofeedback, with the aim of inducing behavioral changes in the brain. Neurofeedback provided by a BCI system may improve cognitive performance in elderly,[113] speech skills,[114] and pain management[115], epilepsy,[116] attention deficit,[117] depression,[118] alcohol dependence.[119]

2.5 BCI applications

BCI offers its users new communication and control channels without any intervention of peripheral nerves and muscles and have potential applications for verbal communication, activities of daily living, environmental control, locomotion, and exercise realised through the use of

[111] Allison, B. Z., & Neuper, C. Could anyone use a BCI? In Applying our Minds to Human-Computer Interaction (pp. 35-54). London: Springer Verlag. (2010).
[112] Brain-Computer Interfaces, Principle and Practices, ed Wolpaw, 2012
[113] Angelakis, E.; Stathopoulou, S.; Frymiare, J.; Green, D.; Lubar, J.; Kounios, J. EEG neurofeedback: A brief overview and an example of peak alpha frequency training for cognitive enhancement in the elderly. *Clinical. Neuropsychology*. Vol 21, 2007, pp. 110–129; Hanslmayr, S.; Sauseng, P.; Doppelmayr, M.; Schabus, M.; Klimesch, W. Increasing individual upper alpha power by neurofeedback improves cognitive performance in human subjects. Applied Psychophysiology Biofeedback, Vol 30, 2005, pp1–10.
[114] Rota et al., Self-regulation of regional cortical activity using real-time fMRI: The right inferior frontal gyrus and linguistic processing. Human Brain Mapping. Vol 30, (2009), pp1605–1614.
[115] deCharms, et. al, Control over brain activation and pain learned by using real-time functional MRI. Proceedings of the National Academy of Sciences, USA Vol 102 (2005)pp 18626–18631
[116] Walker, J.E.; Kozlowski, G.P. Neurofeedback treatment of epilepsy. *Child and Adolescent Psychiatric Clinics of North America*, Vol 14, (2005) pp163–176.
[117] Strehl et al., Self-regulation of slow cortical potentials: A new treatment for children with attention-deficit/hyperactivity disorder. *Pediatrics* Vol 118, (2006), pp1530–1540.
[118] Schneider et al., N. Self-regulation of slow cortical potentials in psychiatric patients: Depression. Applied Psychophysiology Biofeedback Vol 17, (1992), pp203–214.
[119] Schneider et al, Self-regulation of slow cortical potentials in psychiatric patients: Alcohol dependency. Applied Psychophysiology Biofeedback, Vol 18, (1993) pp23–32.

external devices such as computers, speech synthesizers, assistive appliances, and neural prostheses.[120] For instance, in non-invasive BCIs, its use for communication purposes outline an operation that typically displays a virtual keyboard on screen, where the user selects a letter from the alphabet by means of a BCI. Or for motor restoration, neuroprostheses guided by functional electrical stimulation can be managed also through an EEG based BCI.[121]

As regards monitoring or medical evaluation, brain signal recordings generated in BCIs can provide better assessment of brain functions to evaluate the patients' status in health and disease.[122] Invasive neural probe arrays used for electrophysiological recordings provide better data processing and data acquisition or closed-loop control. Their applications are numerous differing from neural prosthetics,[123] epilepsy diagnostics [124], functional electrical stimulation,[125] cochlear,[126] and retina implants,[127] to dense arrays of micro optical light sources[128] necessary for a location-specific optogenetic stimulation of neural tissue.

[120] IEEE Transactions on Rehabilitation Engineering, Vol. 8, No. 2, June 2000
[121] Nicolas-Alonso L., and Gomez-Gil, J., Brain Computer Interfaces, a Review, *Sensors* 2012;
[122] Georgopoulos et al. Synchronous neural interactions assessed by magnetoencephalography: A functional biomarker for brain disorders. J. Neural Engineering. 2007, doi: 10.1088/1741-2560/4/4/001.
[123] L. R. Hochberg *et al.*, "Reach and grasp by people with tetraplegia using a neurally controlled robotic arm," *Nature*, vol. 485, (2012) pp. 372–375,
[124] M. Cossu *et al.*, "Stereoelectroencephalography in the presurgical evaluation of focal epilepsy: A retrospective analysis of 215 procedures," *Neurosurgery*, vol. 57, pp. 706–18, (2005), pp 706–718.
[125] C. E. Bouton *et al.*, "Restoring cortical control of functional movement in a human with quadriplegia," *Nature*, 2016.
[126] I.Hochmair *et al.*, "Deep electrode insertion and sound coding in cochlear implants," *Hearing Research.*, vol. 322, (2015) pp. 14–23
[127] M. S. Humayun *et al.*, "Interim results from the international trial of Second Sight's visual prosthesis," *Ophthalmology*, vol. 119, (2012) pp. 779– 788,
[128] T. I. Kim *et al.*, "Injectable, cellular-scale optoelectronics with applications for wireless optogenetics," *Science*, vol. 340, pp. 211–216, 2013.

2.6 Conclusion: Understanding and decoding brain data: challenges and perspectives

Although engineering intracortical neural interfaces presents many challenges, they at the same time provide a unique perspective on human brain function because they allow the properties of single neurons to be evaluated.

To be useful on a long-term basis and worth the potential risks associated with surgery, implanted BCIs using micro-electrodes placed in the brain must record neural activity reliably and stimulate neural tissue safely over many years. The main challenges in achieving these goals are 1) controlling the electrode–tissue interface, i.e. implantable microelectrodes and their microscale neural interfaces, and biological information about the brain tissue surrounding microscale implants, 2) the long-term stability of the implanted hardware, 3) the sophisticated nature of neurotechnology used for developing implantable devices.[129] For instance, in the case of BCIs aiming at restoring limb or full-body movements where up to hundred thousands neurons might be required,[130] the need for a significant increase in channel count further extends the technical challenges in view of accommodating these interfaces in decidedly compact neural devices. [131]

BCI is seen as a pattern recognition system that classifies each pattern into a class according to its features. BCI extracts some features from brain signals that reflect similarities to a certain class as well as differences from the rest of the classes. The features are measured or derived from the properties of the signals which contain the discriminative information needed to distinguish their different types. One of the major difficulties in BCI design is choosing relevant features from the vast number of possible features.[132] For example neurons used for controlling devices were found to be "multipotent" in that each could represent multiple parameters of movement.[133] Another challenge is to cope with changing background of brain states and physiological as well as non-

[129] Moritz C. et. al, New Perspectives on Neuroengineering and Neurotechnologies: NSF-DFG Workshop Report *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 7, July 2016
[130] Lebedev M., and Nicolelis M.A., "Toward a whole-body neuroprosthetic," *Progress in Brain Research*, vol. 194, 2011 pp. 47–60,
[131] Moritz C. et. al, New Perspectives on Neuroengineering and Neurotechnologies: NSF-DFG Workshop Report *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 7, July 2016
[132] Nicolas-Alonso L., and Gomez-Gil, J., Brain Computer Interfaces, a Review, *Sensors* 2012;
[133] Moritz C. et. al, New Perspectives on Neuroengineering and Neurotechnologies: NSF-DFG Workshop Report *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 7, July 2016

physiological or technical artifacts. Artifacts are undesirable signals, such as heart rhythm or noises from electrode, that come into collusion with brain activity. Since the shape of neurological phenomenon is affected, artifacts along with noises may reduce the performance of BCI-based systems. Thus, BCI developers are still in a search of finding ways for either controlling rich environments, devices, and software applications using only limited and unreliable control signals or improving the signal acquisition to an advanced level.[134]

Decoding BCI user's intentions

Different thinking activities in humans result in different patterns of brain signals. BCI's artificial intelligence system can recognize a certain set of those patterns. As shown above in doing so BCI extracts some features from brain signals that reflect similarities to a certain class as well as differences from the rest of the classes. BCI relies on the recording process that measures electrophysiological activity generated by electro-chemical transmitters exchanging information between neurons which are usually monitored by electroencephalography, electrocorticography, or electrical signal acquisition in single neurons.[135] Whereas conventional neuroimaging, such as functional magnetic resonance[136] and near infrared spectroscopy, measure the hemodynamic response (a process in which the blood releases glucose to active neurons at a greater rate than in the area of inactive neurons), which, in contrast to electrophysiological activity, is not directly related to neuronal activity.[137]

These new approaches open opportunities to develop BCIs based on words, sentences, or other speech-related activity that people could simply imagine. As such BCIs that can directly interpret imagined words, sentences, or related mental activities at one hand would provide major advances in terms of ease of use, practicality, flexibility, on the other would pose qualitatively different ethical questions of autonomy and agency and mental privacy.

[134] Moritz C. et. al, New Perspectives on Neuroengineering and Neurotechnologies: NSF-DFG Workshop Report *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 7, July 2016

[135] Baillet, S.; Mosher, J.C.; Leahy, R.M. Electromagnetic brain mapping. *IEEE Signal Processing Magazine.* Vol 18, (2001) 14–30

[136] fMRI can reveal which visual image someone is viewing (Schoenmakers et al. 2013), or what implicit attitudes correlate with moral decision-making (Greene et al. 2001), and measure specific intentions at some point (Haynes et al. 2007)

[137] Laureys, S.; Boly, M.; Tononi, G.; Functional Neuroimaging. In *The Neurology of Consciousness*; Steven, L., Giulio, T., Eds.; Academic Press: New York, NY, USA, 2009; pp. 31–42

Because human brain is an organ representing personal identities and selfness, any device that might alter the brain functioning—even with the aim of restoring or improving functioning—is perceived as particularly worrisome or even threatening.

Even if BCI is designed to function well with respect to its initial engineering aims—recording brain activity, identifying salient activity, translating data into relevant control signals, and stimulating appropriately—it still have to be acceptable by potential end users, and provide a reasonable assurance with respect to pressing issues of safety, security, privacy, and respect for autonomy.

Since BCI applications potentially represent a powerful tool for revealing hidden information in the user's brain that cannot be expressed, [138] the issues of data integrity, data security, and privacy are especially important to consider. It is not disputable that better recording of brain activity and the corresponding data processing provide more help in alleviating the consequences of a disease or disability and restoring patient's quality of life. However, these neuro-data derived from patient's brain also becomes more "sensitive" the more precisely it is interpreted. [139]

As such neural technologies does not only raise questions of identity, privacy, and the like, but they do so with a degree of intensity that no other technology could have done in the past creating qualitatively new challenges. This possibility of immediate access to and control of our brain: innermost of our thoughts, intentions, memories, moods, and emotions, changes the notions of classic values such as autonomy, privacy, and personhood, etc. While drugs, prostheses, and genetic manipulations can also interfere with our identities and affect us in somehow powerful ways, no biotechnology has quite the same power to penetrate and alter our subjectivity—and the ability to do so in real time, with or without our knowledge or consent—as do these new neural engineering technologies.[140]

Chapter III Conseptualisation of privacy in an era of technological advancement

[138] Nicolas-Alonso L., and Gomez-Gil, J., Brain Computer Interfaces, a Review, *Sensors* 2012
[139] Neurotechnology: Current Developments and Ethical Issues, Oliver Müller and Stefan Rotter
[140] Engineering the brain, Ronald M. Green 10 November 2015

3.1 Introduction

Privacy is an all-encompassing at the same time ambivalent concept covering or touching, *inter alia*, freedom of thought and freedom of expression; a right to confidentiality and secrecy of communications (i.e. restriction of information about oneself) and access to information; freedom of movement, autonomy, and a right to be left alone, solitude in one's home, a right to control one's own life or control over one's body; protection of one's reputation, dignity and liberty. Therefore, for years legal scholars and philosophers have had great difficulty in framing an agreed-upon conception of privacy.[141]

Professor Miller claimed privacy is "*difficult to define because it is exasperatingly vague and evanescent.*"[142] According to Inness, the author of the intimacy concept, the legal and philosophical discourse of privacy is in a state of chaos.[143]

Gutwirth stated that, "*the notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as "our" privacy, it still finds a way to remain elusive.*"[144] Bennett similarly notes that "*attempts to define the concept of 'privacy' have generally not met with any success*".[145]

Westin rightly points out: "[how only few] *values so fundamental to society as privacy have been left so undefined in social theory.*" [146] More than half century ago, saddened by the U.S. Supreme Court's first privacy decision of Griswold v. Connecticut, Beaney wrote, "*even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right*."[147] In modern era as well, it is still valid that "*scholars have a famously*

[141] See e.g. Thomas M., The Rights of Publicity and Privacy, Thomas and Reuters, 2019, "It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts ....Like the emotive word 'freedom,' 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had."; See also, Robert G., *Does Privacy Work?* in Technology and Privacy: The New Landscape, edited by Agre P., and Rotengberg M., (1997), where he argues that privacy can be a broad and almost limitless issue.
[142] Arthur Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, 1971.
[143] Inness J., Privacy, intimacy, and isolation, Oxford University Press, 1996
[144] Gutwirth, S., Privacy and the information age, Rowman & Littlefield, 2002.
[145] Bennett C., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, 1992.
[146] Alan, W., Privacy And Freedom, 25 Wash. & Lee L. Rev. 166 (1968) https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.
[147] Beaney, W., The Right to Privacy and American Law, *Law & Contemporary. Problems*.1966.

*difficult time pinning down the meaning of such a widely used term [*that*] ...most introduce their work by citing this difficulty*".[148]

Privacy can have a protean capacity to be everything to all lawyers. Legal scholars Whitman and Solove have referred to privacy as although fundamentally important but "*an unusually slippery concept*",[149] or "*a concept in disarray. Nobody can articulate what it means.*"[150]

Some even claim that, aside from being difficult to define, privacy is usually culturally relative and has no inherent moral value per se.[151] Famous reductionist Thompson in her treatises has shown that privacy as a concept serves no useful function, according to her for what we call privacy really amounts to a set of other more primary interests.[152] In general reductionists believe the expansive conceptions of privacy are vague, ambiguous, or indeterminate. Motivated by views of what ought to be protected from violation through the recognition of rights, reductionists assert that privacy can be reduced to other concepts and rights.[153]
Privacy also describes an important aspect of one of the main, vital and constitutive dualities that shape human beings, i.e. the tension between individuals and the community.[154]

During the late XXth century, the debate on privacy has further evolved in order to address the challenges raised by the emergence of new technologies. The central issue has been how it is possible to best protect personal data, the collection and processing of which have been increased by technological advance. With advancement of machine learning and powerful processing techniques, it has become more realistic to capture values that cannot yet be measured directly. These are psychological properties and conditions measured with emerging field of neuroscience – brain-wave reading.

[148] Debbie, K., The Evolution (or Devolution) of Privacy, *Sociological Forum* Vol 20, (2005)
[149] James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, *The Yale Law Journal,* Vol 113 (2004), pp 1153-54
[150] Solove believes that privacy is not one thing, that there is no common dominator. Solove, D., Understanding Privacy, *Cambridge: Harvard University Press,* 2008
[151] See e.g. James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *The Yale Law Journal* 113 (2004), pp1153-54. "*In particular, the sense of what must be kept "private," of what must be hidden before the eyes of others, seems to differ strangely from society to society*."
[152] Thomson, J., The Right to Privacy, in Philosophical Dimensions of Privacy, 1975: "*Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."*
[153] Soma, J. et al, Privacy Law in a Nutshell, 2014
[154] Friedevald et al, Privacy, data protection and emerging sciences and technologies: towards a common framework, *The European Journal of Social Science Research*, 2010.

Despite the difficulty of encapsulating the nature and boundaries of privacy, philosophers, sociologists, anthropologists, legal and economic scholars, and jurists have developed numerous conceptions of privacy, and framed out taxonomies and typologies of it, and interpreted it in the court of law to improve our understanding of what privacy means in all its variety, including in light of current and emerging socio-technological developments.

In this chapter I review the conceptions which define privacy in general terms based on philosophical grounds of privacy as a value,[155] and a pragmatic approach that offer classifications of privacy into different types of privacy including *privacy of thoughts* which has been impacted with advent *of new technologies*. In subsequent chapters I will analyze the scope of the right to privacy, its current legal protection and relation to data protection by also covering emerging conception of neuro-data.

3.2. Predominant approaches to privacy

3.2.a) Classic conceptions of Privacy

At the outset it is paramount to differentiate between the concept of privacy and the right to privacy. As Gross observed "*the law does not determine what privacy is, but only what situations of privacy will be afforded legal protection*."[156] Privacy as a concept covers what privacy entails and its intrinsic value. Privacy as a right provides reasons that explain why privacy deserves to be achieved or/and to be protected.

While instructive and descriptive, law cannot be exclusive material for constructing a concept of privacy. Law is the product of balancing competing values and it sometimes embodies different trade-offs. In order to determine what the law should protect; we need to revisit theoretical under-standing of privacy.

Various scholars, such as Nissenbaum, Moore, and Gavison, develop a unitary conception of privacy as an over-arching category with necessary and sufficient conditions. Others offer

[155] Different scholars, such as Nissenbaum, Moore, and Gavison developed somehow unified conceptions of privacy.
[156] Gross, H., The concept of Privacy, *The New York University Law Review*, Vol 42, (1967)

pragmatic approach to conceptualizing privacy by making meaningful distinctions between different types of privacy from particular contexts.

Privacy is an issue of profound importance around the world. In every corner of the world, scholars proclaim *privacy* as a supremely important human good, as a value somehow at the core of what makes life worth living. Without our privacy, we lose "*our very integrity as persons"*[157] and it is fundamental to our *"personhood*.[158]

Gutwirth explains that privacy is "*a cornerstone of contemporary society because it affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation*."[159] There is a compelling evidence that the ability to control access to our bodies, capacities, and powers and to sensitive personal information is an essential part of human wellbeing and serves for his/her flourishing.[160]

It is helpful to start by seeking to identify those features of human life that would be impossible- or highly unlikely-without some privacy. Lack of privacy is access to, knowledge about, and observation of an individual without his/her permission.

Boulstain analyzed the effect of lack of privacy to human psychology and to the society alike: "*The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual*."[161]

---

[157] Charles Fried, Privacy, *The Yale Law Journal* Vol 475 No 477 (1968).
[158] Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, in *Philosophical Dimensions of Privacy: An Anthology, Ferdinand*, David Schoeman ed., 1984.
[159] Gutwirth, S., *Privacy and the information age*. Rowman & Littlefield, 2002.
[160] Newell et al., Privacy in the family. In *The social dimensions of privacy,* ed Edited by Roessler, B., et al, Cambridge University Press. 2015

[161] Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, *The New York University Law Review* Vol 962 No 971 (1964).

Philosopher Arendt agreed with Boulstain: "*A life spent entirely in a public, in the presence of others, becomes, as we would say, shallow. While it retains visibility, it loses the quality of rising into sight from some darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense.*"[162]

Famous anti-reductionist scholar Gavison,[163] saw the danger of non-privacy twofold. According to her the first relates to our notion of the individual, and the kinds of actions we think people should be allowed to take in order to become fully realized. To this cluster belong the arguments linking privacy to mental health, autonomy, growth, creativity, and the capacity to form and create meaningful human relations. The second cluster relates to the type of society we want. First, we want a society that will not hinder individual attainment of the goals mentioned above. For this, society has to be liberal and pluralistic. In addition, we can link a concern for privacy to our concept of democracy.

Anti-reductionists acknowledge that privacy extends beyond simply being apart from others. Limited access in Gavison's theory is divided into three aspects: "*the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.*"[164] Privacy in her view is not understood as a psychological state of an individual or as a form of control over personal information; it is rather a combination of three separate and irreducible elements: secrecy, anonymity, and solitude. A violation of any of these elements infringes upon accessibility and it is therefore a violation of privacy.

Reductionists in their turn argue that privacy is derived from other rights such as life, liberty, and property rights—there is no overarching concept of privacy but rather several distinct core notions that have been consolidated together.[165] Viewing privacy in this fashion might mean abandoning the idea altogether and reducing privacy to other fundamental concepts and rights.

For example, professor Thomson, has studied numerous cases which are usually considered to represent violations of the right to privacy, and concluded that all of the cases can be sufficiently

[162] Arendt, H., The Human Condition, *The University of Chicago Press* (1958)
[163] Gavison, R., Privacy and the Limits of Law, *The Yale Law Journal*, Vol. 89, 1980

[164] Ruth Gavison, Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, (1980)
[165] Thomson, J.,. The right to privacy. *Philosophy and Public Affairs*, (1975).

and equally explained in terms of violations of liberty, property rights, or rights over the person and she concluded that "right to privacy is everywhere overlapped by other rights."

Frederick Davis, another reductionist has argued that, "[i]f *truly fundamental interests are accorded the protection they deserve, no need to champion a right to privacy arises. Invasion of privacy is, in reality, a complex of more fundamental wrongs. Similarly, the individual's interest in privacy itself, however real, is derivative and a state better vouchsafed by protecting more immediate rights*"[166] But by treating privacy only as a label for selected aspects of other basic rights, reductionism is seen as threatening to undermine belief in the distinctness and importance of privacy for privacy's sake.

In the control-based theory of privacy Prof. Fried posits that privacy "*is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.*"[167] Moore, further developed the idea that a condition of privacy obtains when others do not have access to, and uses of, places, bodies, and personal information while "*a right to privacy affords control over access and use independently of whether condition of privacy holds*."[168]

"Informational privacy," a term brought by Westin, is an example of a control definition of privacy. Informational privacy is the interest individuals has in managing or at least significantly influencing the handling of data about themselves. In other words, privacy is the ability of determining why, when, how, and to what extent personal information is shared with others. From this definition, Westin deduces that personal information would be best understood as a form of a property right.

The scholars argue control definitions are too narrow because they exclude those aspects of privacy that are not informational, e.g., a right to make choices about reproduction.[169] Furthermore, theorists relying on control definitions often have difficulties to define what is meant by "control" over information, and the word can range from extremely narrow to extremely broad. Also, control is not a necessary condition for the existence of informational privacy because a person can lose control over information but still retain privacy.

[166] Fredrik Davis, What do we mean by 'Right to privacy'? *South Dakota Law Review* (1959).
[167] Fried, C., Privacy, Yale Law Journal, Vol 77 No 475, (1968)
[168] Moore, Privacy, Neuroscience, and Neuro-Surveillance, Springer Science+Business Media Dordrecht 2016
[169] John Soma, Privacy Law in a Nutshell, 2014

On the other hand, condition based definitions define privacy as a condition or state of affairs in which it is possible to describe changes that may be considered losses of privacy.[170] This pragmatic approach simplifies the process of finding a privacy violation because one no longer needs to focus on normative arguments. Instead, the question of whether privacy has been lost becomes a pure question of fact. The aim of the condition definition is to explain what a "loss of privacy" consists of, without addressing either the circumstances that led up to that loss or otherwise attaching any particular legal, moral, or political significance to the change in condition.

3.2.b) Taxonomies of privacy harms

As widely accepted definition of privacy remains elusive, there has instead been more consensus on a recognition that privacy comprises different dimensions, and it is best can be explained through taxonomies of privacy problems or intrusions. Solove's taxonomy, the most-cited and best-known classification in contemporary privacy literature, is not a classification of privacy types but of privacy harms.

Solove argues that privacy is too complicated concept to be boiled down to a single so instead, he aims to sketch out potentially harmful or problematic activities affecting private matters or activities. He asserts that taxonomy of privacy problems must be addressed, regardless of whether they conform to a precise definition of privacy.

Solove comprehensively outlines a list of possibly harmful actions discerning it to 'four basic groups of harmful activities': information collection (surveillance; interrogation); information processing (aggregation; identification; insecurity; secondary use exclusion); information dissemination (breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation; distortion); and invasion (intrusion; decisional interference).[171] Solove provides a clearer and more robust account of privacy - one that provides us with a framework for understanding privacy problems. Privacy violations in Solove's taxonomy are a group of related harms, each of which has received at least some recognition in the law. If courts and legislatures

[170] John Soma, Privacy Law in a Nutshell, 2014
[171] Solove, D., A taxonomy of privacy, *University of Pennsylvania Law Review*, 2006

focused instead on the privacy problems, many of these distinctions and determinative factors would matter much less in the analysis.

It should also be noted that the activities that affect privacy are not always socially undesirable or worthy of sanction or prohibition. They might involve efforts to gain knowledge about an individual without physically intruding or even gathering data directly from them (through aggregation of big data), or problems that emerge from the way that the data is handled and maintained (insecurity, flows in information technology), the way it is used (lawful or unauthorised secondary use), and the inability of people to participate in its processing (exclusion, lack of access to the information about oneself).[172] Besides, privacy harms are not all related in the same way - there is no common denominator that links them all.

A typology of privacy violations is also outlined by Kasper, who asserts that privacy cannot be understood unless examined from the inside. Kasper distinguishes between invasions by the principal activity by which privacy invaded, dividing it into extraction, observation and intrusion.[173] *Extraction*-based privacy invasions involve making a deliberate effort to obtain something from a person. *Observation*-based privacy invasions are characterised by active on-going surveillance of a person, whereas *intrusion*- based invasions cover an "unwelcome presence or interference" in a person's life. Within each primary category, there are three subcategories that further differentiate types by characteristics such as the motivation for the invasion, the method by which it is carried out, the nature of the consequences, and the invadee's awareness of the invasion.[174]

Other scholars offer typological or pluralist conceptions of privacy by making meaningful distinctions between different types/typologies of privacy in a positive way. The difference between a taxonomy of privacy harms and a taxonomy of types of privacy is that the former is reactive whereas the latter is of protective nature, i.e. pro-active.

3.2.c) Evolvement of typologies of privacy

[172] *Ibid.*
[173] Kasper, D., "The Evolution (or Devolution) of Privacy", Sociological Forum, Vol. 20, No. 1, 2005, pp.69-92
[174] *Ibid.*

Clarke was the first privacy scholar who has reframed the dimensions of privacy in a logical, and structured way:

- *privacy of the person*, sometimes referred to as 'bodily privacy' This is concerned with the integrity of the individual's body. Issues may include compulsory immunisation, compulsory provision of samples of body fluids and bodytissue, etc;
- *privacy of personal behaviour*. This relates to all aspects of behaviour, but especially to sensitive matters, such as personal preferences, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy';
- *privacy of personal communications (or* interception privacy). Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by others
- *privacy of personal data (*data privacy or information privacy). Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.[175]

He referred to privacy of personal communication and privacy of personal data together as informational privacy.
In 2013, Clarke added a fifth category:[176]

- *privacy of personal experience*. During the first decade of the 21st century, reading and viewing activities have migrated to screens and are controlled; most conversations have become 'stored electronic communications', many individuals' locations are tracked, and correlations are performed to find out who is co-located with whom and how often; etc, This massive consolidation of individuals' personal experience electronically is available for exploitation.

It can be deduced from the fifth category of privacy typology that ***the privacy of personal thought***, is indirectly under assault through the monitoring of what people read and view.

As mentioned above privacy is a developing concept and scope of it is constantly being changed by many developments in science and technology. Therefore, Clarke's updated categories had not been sufficient to cover the range of new privacy issues. In order to capture the nature and

[175] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (Xamax Consultancy,) 2006 (Clarke, Privacy Introduction and Definitions, 2006)
[176] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (Xamax Consultancy,)2016

boundaries of contemporary privacy challenges, Finn, Wright and Friedewald have outlined the privacy in seven typologies:[177]

- *Privacy of the person* encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. According to Mordini, the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values". Privacy of the person is understood to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. This aspect of privacy is shared with and somehow broader than Clarke's identical categorisation.

- *Privacy of personal behavior and action.* Clarke's notion of personal behaviour is extended to privacy of behaviour and action. This type entails sensitive issues such as religion, politics, or personal preferences. However, the notion of privacy of personal behaviour concerns activities that happen in public space, as well as private space, and Clarke makes a distinction between casual observation of behaviour by a few nearby people in a public space with the systematic recording and storage of information about those activities. The ability to behave in public, semi-public or one's private space without having actions monitored or controlled by others contributes to "the development and exercise of autonomy and *freedom in thought* and action".[178]

- *Privacy of personal communications* is the same as in Clarke's category. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector.

- *Privacy of location* refers to the right of an individual to be present in a location or space without being tracked or monitored or without anyone knowing where he or she is. 'Space' could be physical or cyber space. This conception of privacy also includes a right to solitude and a right

[177] Although these seven types of privacy may have some overlaps, they are categorized individually because they provide a number of different lenses through which one can view the effects of emerging technologies. Finn, R., Wright D., and Friedewald, M., "Seven Types of Privacy." In *European Data Protection: Coming of Age?*, edited by Gutwirth, S., Leenes, R., Hert P., et al. Dordrecht: 2013.
[178] Nissenbaum, H., Privacy in Context: Technology, Policy and the Integrity of Social Life, Stanford University Press, 2010

to privacy in spaces such as the home, the car or the office. This categorisation of privacy has evolved with the technological advancement. Clarke defined the privacy of location under his new fifth category privacy of personal experience.

- *Privacy of data and image,* includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use." Such control over personal data builds self-confidence and enables individuals to feel empowered. Like privacy of thought and feelings, this aspect of privacy has social value in that it addresses the balance of power between the state and the person.

- ***Privacy of thoughts and feelings:*** new and emerging technologies carry the potential to impact on individuals' privacy of thoughts and feelings. People have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual. This aspect of privacy may be coming under threat as a direct result of new and emerging technologies. Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body. Similarly, we can (and do) distinguish between thought, feelings and behaviour. Thought does not automatically translate into behaviour.

- *Privacy of association (including group privacy)*, is concerned with people's right to associate with whomever they wish, without being monitored. This aspect of privacy was not considered before as a number of new technologies could create qualitatively new threats to individuals' privacy of association.

Types of privacy changes by time and evolution of technology, for instance privacy of home does not bear the same type of value as it used to be, with the evolution of smart home devices. Pragmatic approach of framing typologies is thus helpful to discover which problems are arising with the development of new technologies to then consider whether there is a need for adopting new regulations to cover these new relations identified through typologies. The latest typologies developed by Dr. Koops and his team is more systematic and comprehensive than any existing model preceding it. The model consists of eight typologies, where informational privacy does not

belong to any of typologies, rather being depicted an overarching aspect of each underlying type. Koops asserts that each ideal type of privacy contains an element of informational privacy—which is, an interest in restricting access or controlling the use of information about that aspect of human life.

- *Bodily privacy*: The emphasis here is on negative freedom: being able to exclude people from touching one's body or restraining or restricting one's freedom of bodily movement.
- *Spatial privacy* is the privacy of private space, and restricting other people's access to it or controlling its use. The home is the prototypical example of the place where spatial privacy is enacted, closely associated with the intimate relations and family life that take place in the home.
- *Communicational privacy*: means a person's interests in restricting access to communications or controlling the use of information communicated to third-parties. Communications may be mediated or unmediated, which involve different ways of limiting access or controlling the communicated messages.
- *Proprietary privacy*:[179] typified by a person's interest in using property as a means to shield activity, facts, things, or information from the view of others. For example, a person can use a purse to conceal items or information they prefer to keep private while moving in public spaces.
- *Intellectual privacy*: typified by a person's interest in ***privacy of thought and mind***, and the development of opinions and beliefs. While this can have important associational aspects, it is suitable as an ideal type of the personal zone, as the mind is where people can be most themselves.
- *Decisional privacy*: typified by intimate decisions, primarily of a sexual or procreative nature, but also including other decision- making on sensitive topics within the context of intimate relationships.
- *Associational privacy*: typified by individuals' interests in being free to choose who they want to interact with: friends, associations, groups, and communities. This fits in the semi- private zone since the relationships often take place outside strictly private places in semi-public spaces such as offices or cafés.
- *Behavioral privacy*: typified by the privacy interests a person has while conducting publicly visible activities. These relate to Westin's states of anonymity. This is an ideal type of privacy where the need for control after access has been granted is most pressing. "Being oneself" in public can be achieved if others respect privacy through

[179] Koops referring to property-based interests, rather than Allen's reference to image management and reputational privacy.

> civil inattention, but otherwise control can only be exercised by trying to remain inconspicuous among the masses in public spaces.[180]

3.3 Emerging approaches to Privacy

3.3.a) Freedom of thought as brain privacy

Each of us has the right not to share our thoughts, hopes, feelings, and plans, as well as a right to control information about our lives, family, and friends. People should have the right to think whatever they like. Advocates of cognitive liberty demand that the individual should enjoy a wide range of autonomy over what is on – and in – his/her mind, as such creative freedom not only good for well-being of human, but it benefits society: "The right to control one's own consciousness is the quintessence of freedom."[181]

According to Kant's categorical imperative, as whatever happens in the interior of a person's mind never restricts the freedom of anyone else, the purview of legitimate legal coercion is therefore confined to the regulation of outward actions only.[182]

In the similar way, Mill emphasized the special role of the mind in his famous treatise "On Liberty":

> [T]he appropriate region of human liberty ... comprises, first, the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects…

In general thoughts are free because of their private character. Except the thinker, no other person else could know the exact content of thoughts in the same way as the thinker does. Thoughts are not in general directly observable for others; they can be assumed from verbal and/or behavioral expressions of the person. "In addition to this privileged epistemic access that confers authority over the knowledge of one's thoughts, privacy of thoughts can also mean that others cannot control

[180] Koops et al, A Typology of Privacy, *University of Pennsylvania Journal of International Law*, (2017).
[181] Boire, R. G., On cognitive liberty I. Journal of Cognitive Liberties, 1, 7–13. 1999/2000, Boire R.G. Searching the brain: The fourth amendment implications of brain-based deception detection devices, *American Journal of Bioethics*, (2005);
[182] Kant I., Political Writings, 2nd edition, Cambridge texts in the history of political thought, (1991)

our thoughts because they are inaccessible from the outside". [183] In ordinary circumstance it should be impossible to compel another person to contemplate a particular thought or to induce idea or form opinion.

Gavison described it as total lack of privacy if our thoughts would not be safe from intrusion by others:

> In such a state, there would be no private thoughts, … and no private parts. Everything an individual thought and planned would immediately become known to others.
> …We would probably try hard to suppress our daydreams and fantasies once others had access to them. We would try to erase from our minds everything we would not be willing to publish, and we would try not to do anything that would make us likely to be feared, ridiculed, or harmed. There is a terrible flatness in the person who could succeed in these attempts. We do not choose against total lack of privacy only because we cannot attain it, but because its price seems much too high.[184]

The moral value of privacy is foremost attached to the moral value of autonomy. And one key aspect of autonomy relevant to privacy is autonomy in decision-making. An individual requires a certain degree of privacy to arrive at his/her own evaluations, intentions, beliefs, and decisions. S/he must, at minimum, have some opportunity for contemplation removed from the influence and pressures of others.[185] Not to mention determinism and free will, free decisions imply that the preferences on which decisions are made have not been brought about through manipulative influences.[186]

As the mind is among the most essential aspects of a person, the drafters of the Universal Declaration of Human Rights called freedom of thought "the basis and origin of all other rights" and freedoms with quintessential significance. [187]

According to cognitive liberty activities of XXI century, "*if freedom is to mean anything, it must mean that each person has an inviolable right to think for him or herself. It must mean, at a*

[183] Bublitz, C., Cognitive Liberty or the International Human Right to Freedom of Thought in *Handbook of Neuroethics*, edited by Clausen J. and Levy N., 2015
[184] Gavison, R., Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, 1980
[185] Michelfelder, D., The moral value of informational privacy in cyberspace. *Ethics and Information Technology*, Vol3, (2001) pp129–135.
[186] Bublitz, C., Cognitive Liberty or the International Human Right to Freedom of Thought in *Handbook of Neuroethics*, edited by Clausen J. and Levy N., 2015
[187] Rene Cassin, quoted in Christoph Bublitz, Cognitive Liberty or the International Human Right to Freedom of Thought in Handbook of Neuroethics, edited by Clausen J. and Levy N., 2015

minimum, that each person is free to direct one's own consciousness; one's own underlying mental processes, and one's beliefs, opinions, and worldview. This is self- evident and axiomatic". [188] Freedom of thought stands behind other well-accepted human rights and freedoms which could be severely undermined without its firm protection. [189]

In ethics brain privacy is considered having both physical and informational aspects. In a locational sense, brain privacy would afford individuals the right to control access to their brains or cogitative processes whether through sound waves or electrical impulses, chemicals, or magnetic/infrared imaging, or another technology stimulating or monitoring a specific location of brain. Rights to control access to and uses of this specific brain location would be a form of physical privacy rights. On the other hand, thoughts, feelings, or preferences that can be inferred from monitoring brain are informational in nature. Brain privacy, understood as a subset of a more general right to privacy, would thus include (1) rights over access to and uses of the brain itself, and (2) over the information that may be deducted from scanning. [190]

As mentioned above, modern privacy scholars included freedom of thought in the list of privacy typologies. Finn, Wright and Friedewald, stated that "*individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual. This aspect of privacy may be coming under threat as a direct result of new and emerging technologies.*"[191] They distinguish between privacy of thought and feelings privacy of the person, in the same way that the mind can be distinguished from the body. Similarly, there is a clear difference between thought, feelings and behaviour. Thought is not automatically translated into behaviour.[192]

In Koops' typology, privacy of thought and mind is categorized as intellectual privacy. He also extends it to the interest in the development of opinions and beliefs. He posits that while intellectual privacy can have important associational aspects, it is suitable as an ideal type of the personal zone, as the mind is where people can be most themselves.

[188] Boire, R. G., On cognitive liberty, *Journal of Cognitive Liberties*, Vol 1, 1999/2000 pp7–13.
[189] Blitz, Freedom of thought for the extended mind: Cognitive enhancement and the constitution. *Wisconsin Law Review*, 2010.
[190] Moore, Privacy, Neuroscience, and Neuro-Surveillance, Springer Science+Business Media Dordrecht 2016
[191] Finn et. al, "Seven Types of Privacy." 2013
[192] Finn et. al, "Seven Types of Privacy." 2013

Privacy of the information decoded from a human brain has been defined with different terms including "brain privacy",[193] "neural privacy", [194] "cognitive privacy",[195] "thought privacy", [196] and "cognitive liberty".[197]

In scientific literature thought is referred as 'mental state'. It is rather broadly encompasses "*every aspect of an individual's psychology, including, but not limited to, personality traits and dispositions (e.g. sexual preferences, personal tastes and habits...), qualitative states (e.g. perceptions, emotions, feelings...), propositional states (e.g. knowledge, beliefs), intentions and goals, plans, memories etc*."[198]

Ayer distinguishes 4 ways in which our mental states can be secluded: [199]

1. They are private in the sense that they can be incommunicable. People can experience difficulties in adequately expressing their thoughts or feelings. There is, or there can be, a felt difference between the report and the experience of what is reported.
2. Mental states are private in the sense that individuals have a 'first person perspective' (Shoemaker 1988, 1994) on their inner mental life. Each person only has such 'special access' to his or her own mental states. One knows introspectively about one's own mental states, which is different from the way any- one else can know about them. In other words, there is a qualitative component that is inaccessible to an external viewer.
3. Mental states are private in the sense that they can be unshareable, meaning that it is impossible for two persons to entertain exactly the same thought in exactly the same way.
4. Mental states are private in the sense they can be incorrigible, for certain knowledge claims cannot be corrected or overridden.

[193] Räikkä, J. Brain imaging and privacy. *Neuroethics* Vol 3 (2010) pp5–12
[194] Schneider J., Fins J., and Wolpaw, J., Ethical issues in BCI research Brain–Computer Interfaces: Principles and Practice, ed Wolpaw, J., and Wolpaw, E., Oxford: Oxford University Press (2012); Trimper J, Root Wolpe P., and Rommelfanter, K., When 'I' becomes 'we': ethical implications of emerging brain-to-brain interfacing technologies, *Frontiers* Neuroengineering. Vol 7, (2014)
[195] Klein E, Chapter 7 Neuromodulation ethics: Preparing for brain–computer interface medicine in *Neuroethics Anticipating the Future,* ed. Illes J, Oxford University Press, 2017
[196] Illes, J. and Racine, E. Imaging or imagining? A neuroethics challenge informed by genetics. American Journal of Bioethics, Vol 5, (2005) pp.5–1
[197]Boire, R. G., On cognitive liberty, *Journal of Cognitive Liberties,* Vol 1, 1999/2000 pp7–13.
[198] Mecacci G., and Haselager P.,, Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, *Science Engineering Ethics*, 2017
[199] Ayer, 1963, quoted in Mecacci G., and Haselager P., Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, *Science Engineering Ethics*, 2017

3.3.b) Conceptualizing privacy in light of emerging technologies/BMI's impact on privacy

Beyond making classic challenges to privacy more prevalent, technology is also creating entirely new challenges. Professor Brandeis foresaw this possibility almost a century ago in his dissenting opinion from Olmstead v. United States:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[200]

Further, Justice Douglas, dissenting in the famous privacy case Osborn v. United States (1966) noted:

> The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that *his most secret thoughts are no longer his own* ... when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone.

In 1977, Bezalon also rightly predicted that "*the contents of our thoughts and consciousness, now relatively immune from observation and forced disclosure, may not always be free from discovery. Lie detectors are only one kind of technological development that could threaten this privacy*."[201]

Theoretical and legal conversations about the relationship between technology and privacy dates in further back to 19th century with the invention of a carriable photography device accessible to the wider population. As technologies continue to develop, conceptualisations of privacy have developed alongside with them, from a "right to be let alone" to attempts to encapsulate the complexity of privacy issues within frameworks that highlight the legal, social and/or political concerns that new technologies present.

[200] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[201] Bazelon, Probing Privacy, 12 Gonzaga Law Review. Vol 587, No 592 (1977)

Whether altering the definitions of privacy or facilitating gathering, retention, and use of personal information, technology challenges and reshapes privacy law and policy on a daily basis. In fact, courts recognized almost as a matter of course when adopting the privacy torts that technological advancements have altered traditional expectations of privacy. These advancements ease the aggregation, storage, and analysis of immense amounts of information about individuals; create an extraordinary capacity to track and monitor people; and permit access to, communication, and publication of this information at ever-greater volumes and speeds.[202]

According to Nissenbaum's contextual theory, privacy must be understood in social context as privacy violation depends to some extent on the relevant context, the agents involved, their relationship to one another, and the setting of the interaction.[203] The ethical dimension of information technologies which change the ways we communicate with each other and the amount of information we share relies on the fact that they are challenging previous commitments to values and principles. In other words, emerging technologies which cause change in social contexts, changes the notion of privacy consequently. Even the questions that relate to the system's technical character are often "*rooted not in an interest in the technology alone, but in a concern – and usually a dispute – over values*". Nissenbaum questions whether this new way of communicating deprives people of essential human character, and consequently of meaningful opportunities for emotional, spiritual and social growth. [204]

In the ontological theory of information ethics developed to cover issues brought by modern day information technology, Floridi views personal information as constitutive element of human:

> …an agent "owns" his or her information, yet no longer in a vaguely metaphorical sense, but in the precise sense in which an agent is her or his information. "My" in "my information" is not the same "my" as in "my car" but rather the same "my" as in "my body" or "my feelings": it expresses a sense of constitutive and intimate belonging, not of external and detachable ownership, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions."[205]

[202] See, Soma, Privacy in a Nutshell, 2014.
[203] Nissenbaum, H., Privacy in Context: Technology, Policy and the Integrity of Social Life, Stanford University Press, 2010
[204] Nissenbaum, H., "How computer systems embody values", *IEEE Computer*, Vol. 34, No. 3, (2001).
[205]Floridi, L., The ontological interpretation of informational privacy, *Ethics and Information Technology*, 2006

Privacy issues arisen from new sciences and technologies, such as radio frequency identification, social network services, the creation of large bio banks, nanotechnology, etc do not fall easily within commonly used typologies of privacy problems. Therefore, previously unconsidered types of privacy now need to be addressed in order to adequately protect individuals' rights, freedoms and access to goods and services.

One example of this is neuro-engineering technology which has unique power to penetrate and alter our subjectivity—and the ability to do so in real time, with or without our knowledge or consent.

In response to the advances in neurotechnology a new branch of bioethics – Neuroethics has emerged as an interdisciplinary area. Technical development of neuroimaging, neuropharmacology, neurogenetics, neural transplantation, and neural engineering have led to combined efforts to cope with non-scientific challenges raised by the launch of these numerous technologies. Philosophers, lawyers, neuroscientists, clinicians, social scientists, and others have engaged in an ongoing dialogue about ethical, legal, and social implications (ELSI) of neuroscience developments. As mentioned above many of the new social and ethical issues in neuroscience resulted from the ability to monitor brain function in humans with a spatial and temporal resolution sufficient to capture psychologically meaningful fluctuations of activity. Discussion about ethical issues in BCI inherits a kind of orienting framework from this larger conversation in Neuroethics, some of which have been explored at the research and policy level:[206]

Privacy of thought (Clausen 2011)
Security of brain data (Denning et al. 2009)
Changes to identity (Goering 2014)
Responsibility for action (Haselager 2013)
Access to expensive technology and post-study obligations to subjects (Schneider et al. 2012)

The focus of this thesis is the privacy and confidentiality of thought processes which threatened by those neuro-technologies that can reveal the neural correlates of an individual's innermost thoughts. Brain data is the main resource for BCI research and in the process, large amounts of brain data are generated from research participants, including intracortical, subdural, and

[206] Klein, E., & Nam, C., Neuroethics and brain-computer interfaces (BCIs), *Brain-Computer Interfaces*, Vol3No3, 2016, pp123-125

extracranial sources. The nature of BCI research involves understanding and making inferences about device users' mental states, thoughts, and intentions.[207] The direct and immediate access to the most intimate aspects of an individual's subjectivity afforded by Brain Computer Interfaces is something new. In the forms of both data collection and control of neural processes, it does not only provide otherwise unavailable direct access to people's mental lives but also substantially impacts our self-awareness and our judgments of responsibility and accountability.[208] The privacy issues derived from BCI application can be divided into three categories:

a) First, *privacy of communication* may be impacted by brain-computer interfaces, where the interception or monitoring of data streams between the BCI user and the machine could be possible. In other words, when BCIs are used to assist individuals in communicating with others, the data that passes between the user and the communication software could be intercepted and analysed. And, if the user employs the BCI to communicate with family, friends, or co-workers and complete data on BCI use are collected, the data will necessarily include these communications. This may be against the user' /patient's will to exert control over the personal conversation with the purpose of perhaps protecting a family member's feelings or because of embarrassment.

b) *Autonomy issues.* In BCI a machine learning algorithm recognizes and categorizes, an arbitrary, preferably easy to evoke and measure, neural activity pattern. The particular kind or nature of the mental state that is correlated to such activity does need to be relevant as long as it can be used to reliably drive a system or provide a user with a certain feedback. As the BCI technology is based on learning processes on both sides (human and machine), manipulation of the BCI carrier could be possible in this situation.[209]The gain in control could then easily result in a loss of the same, confronting the user with unintended and potentially devastating consequences, especially if individuals really depend on the technology linked to the BCI.

[207] Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Nam et al., Taylor&Francis Group, 2018
[208] Ronald Green, Neural Technologies: The Ethics of Intimate Access to the Mind, Hasting Centre Report, 2015
[209] McFarland and Wolpaw, Brain-Computer Interfaces for Communication and Control, *Communications of the ASM*, 2011, p. 63.

c) *Privacy of thought*: Finally, brain measurements are used to decode or interpret mental states (assess their nature and/or content). As suggested by the very word 'reading', brain reading is based on interpreting (combinations of) neuronal signs and drawing inferences about their meaning.[210] As such, through the use of neurotechnology, "*for the first time it may be possible to breach the privacy of the human mind, and judge people not only by their actions, but also by their thoughts and predilections."*[211]

3.3.c) BCI Privacy Typologies

Despite the fact that BCI research is advancing rapidly since 2000, there is still very little research dedicated to privacy considerations.[212] There are several explanations for this. First, by many researchers, device manufacturers, clinicians and even by the patients themselves and their relatives the risk of privacy might seem to be trivial in comparison to the relief and health benefits it can bring to otherwise hopeless conditions. The BCI device that would allow someone in locked-in condition to speak or someone who is tetraplegic to control a robotic limb is undeniably compelling thing. Then, there is a widespread view among clinicians, that "*informed consent*" process practiced in academic sphere as well as in clinical research can safeguard all the necessary precautions against privacy violations. But due to the specific character of BCI research, the extent to which informed consent achieves meaningful consent is questionable, especially, taking into consideration that patients using BCI usually have impaired cognitive state, also collection and usage of data in BCI are completely different from conventional treatments. In below chapters, I will explain why initial consent to treatment should not automatically amount to the loss of further aspects of privacy. In BCI, another ethical issues such as autonomy, identity and agency raise

[210] Mecacci, G., and Haselager, P., Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, *Science Engeniering Ethics*, 2017
[211] Farah, M., "Neuroethics: The practical and the philosophical", *Trends in Cognitive Sciences*, Vol. 9, No. 1, 2005, pp. 34-40
[212] Finn et al, Seven types of Privacy, 2013; Bonaci et al, Application of BCI, 2014; Prescient report; BMI Privacy Australia, 2017, BMI Principles Handbook 2018,

novice challenges too. However, taking into consideration the size of the research, only those aspects of autonomy and agency which are relevant to privacy will be touched upon.

As mentioned above there is not yet a unified concept explaining moral value of privacy in the context of BCI. Some describe a number of scenarios where BCI may affect different types of privacy. According to Finn et al, BCI "*carry the potential to impact upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of thoughts and feelings*." [213]

For example, privacy of behavior and action may be diminished if BCI information is used to predict patients' behaviors. Finn et al. also further stipulates that that communications privacy may be affected "*when the data that passes between the user and the communication software could be intercepted*". [214]

The most importantly, first time in Finn et al, it was recognized that the identified privacy typology of *freedom of thought and feelings* are coming under threat as a direct result of new and emerging technology-BCI. Because, it has now been clear that "*information from brain computer interfaces may be able to recognise and identify patterns that shed light on certain thoughts and feelings of the carrier*."[215]

Due to the proven link between neural recordings, on the one hand, and mental states and predictors of behavior, at the other, scholars from ETH Zurich too have argued that privacy challenges raised by BMIs are characterized by greater complexity and ethical sensitivity than traditional privacy issues in digital technology, and called for an ethical and legal assessment of mental privacy.[216]

Further, Bonaci et. al have recognized the need to address emerging ethical and legal questions in BCI applications, and in particular privacy and security concerns. They suggested a hypothesis describing vulnerability of BCIs to the cyber-hacking which could affect privacy of the patients at signal accusation, signal processing (measurement) or signal transferring and feedback providing (output) levels which is also backed by other scholars in scientific literature.[217]

[213] Finn et al, Seven types of privacy, 2013
[214] Finn et al, Seven types of privacy, 2013
[215] Finn et al, Seven types of privacy, 2013
[216] Ienca, M., and Andorno, R.: 'Towards new human rights in the age of neuroscience and neurotechnology', Life Sciences, Society and Policy, 2017, 13, (1), pp. 5
[217] Bonaci T, et. al, *App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces*. 2014,

Dening et. al identified potential security threats against implanted neural devices and introduced the term "neurosecurity" for "*the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will*."[218]

Koops, who has developed the latest typologies of privacy to encompass all the novice issues raised by the developments in all spheres of science and technology, typified freedom of thought as *intellectual privacy*, but also identified relevant *decisional privacy* as a separate type.[219]

Very recently, in 2018, Klein and Rubbel identified three privacy typologies affected by BCI: physical privacy, informational privacy and decisional privacy.[220]

Physical privacy- the condition in which others' access to one's person (by sight, sound, touch, and presence) is limited. Thus, for example, one may desire a degree of physical solitude or to remain free of video surveillance, regardless of whether one is concerned about information gathering. Some examples of physical privacy intrusions in BCI include physical access to skull for placement of monitoring electrodes such as EEG, ECoG or intracranial electrodes (as participation in BCI research involves the loss of some physical privacy) or being pulled aside in security screening due to metal detector. BCI at the same time gives ability to attend some activities of daily living with less intensive intervention by others.

Informational privacy- "the condition in which others' ability to learn about one, or to make inferences about one, is limited". In BCI, informational privacy derives from potential for neural recording to expose thoughts, dispositions, and intentions, also unknown inferences made from troves of data stored, and storage of intimate BCI conversations.

Issues of informational privacy can arise in different cases, when BCI might reveal incidental findings of clinical significance, or other collateral information, or neural activity patterns be used

[218] T. Denning, Y. Matsuoka, and T. Kohno. Neurosecurity: Security and Privacy for Neural Devices, *Neurosurgical Focus*, Vol 27 No1, 2009.pp1-4
[219] Koops et al, A Typology of Privacy, *University of Pennsylvania Journal of International Law*, 2017.
[220] E. Klein and A Rubel, Privacy and Ethics in Brain– Computer Interface Research in Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Nam et al., Taylor&Francis Group, 2018

to detect attention or motivation, which are critical to the success of BCI training,[221] or may reveal something about the underlying personality of the person using the BCI.

Here informational privacy is not differentiated whether it is the privacy of communications, privacy of actions or privacy of thoughts.

Decisional privacy – "is the ability of a person to make important, intimate decisions without excessive influence or control by others." Decisional privacy is about individual autonomy or in other words whether others can limit the range of important decisions a person can make for himself/herself. In the United States, decisional privacy is often discussed in the context of access to birth control,[222] abortion,[223] legal restrictions on same-sex partners, etc.[224] Participation in BCI research can require that volunteers engage in or dismiss certain activities. If a person is denied from entering studies based on exclusion criteria regarding, for example, her future reproductive decisions, this can be violation her decisional privacy.

Solove's privacy related harms categorized according to information processing (aggregation; identification; insecurity; secondary use exclusion); and information dissemination (breach of confidentiality; disclosure; exposure; increased accessibility) can be applied for distinguishing the different dimensions and nuances of data protection and privacy affected by BCI.

At the same time, Kasper's extraction and observation types of privacy invasions can also be used to explain privacy violations pertinent to BCI. Since BCIs are capable of collecting and processing personal data, extraction and even real-time observation is possible. As mentioned above due to the high quality of the data, the data processor (treating clinician, nurse, device operator) is able to gain information from the data subject (the patient) not only about his/her communication, e.g. in the case of the mental speechwriter, but also concerning more complex facts such as his/her inner-state, decisions, and preferences.[225]

[221] Curran, Eleanor A., and Maria J. Stokes. 2003. Learning to control brain activity: A review of the production and control of EEG components for driving brain–computer interface (BCI) systems. *Brain Cogn* 51 (3)
[222] Griswald v. Connecticut, 381 U.S. 479 (1965)
[223] Roe v. Wade, 410 U.S. 113 (1973)
[224] Lawrence v. Texas, 539 U.S. 558 (2003)
[225] Kasper, D., "The Evolution (or Devolution) of Privacy", Sociological Forum, Vol. 20, No. 1, 2005, pp.69-92

From social and ethical perspective, a research team at the University of South Australia through the experimental empirical analysis method determined that all four types of BCIs- active, reactive, passive and hybrid BCIs have potential for disrupting privacy of the user. They outlined privacy disruptions as followings:[226]

> In active BCIs, patients who are compelled beyond their *control* to use an active BCI in order to engage in everyday activities, will experience loss of control over the privacy communication. Example to this is a user of a BCI- controlled vocal synthesizer who is in a crowd and seeking a private conversation with another person.
>
> In reactive BCIs, if the controlled environment is interrupted, users may generate P300 event related potential signals in response to the interruption and, depending on the nature of the interruption, a privacy disruption may ensue.

The *restricted access* theory of Gavison posits that direct control over personal information is increasingly difficult or even impossible to achieve as information proliferates further. If the data acquired by BCIs is protected under regulatory frameworks, privacy will not be disrupted. But as there is not such specifically designed legal provisions, privacy disruptions may be of concern.

If we *commodify* data privacy, then potential privacy disruption applies to all four types of BCI, just as it applies to all personal data whenever secondary use of the collected data happens.

According to Floridi's ontological theory, as personal data is constitutive, technologies can either increase or decrease the traction of the infosphere, increasing or decreasing privacy accordingly.[227] Since BCIs upload a new form of personal data to the infosphere, there is a risk of decreasing the traction of the infosphere and decreasing privacy. It should be mentioned that due to the technological specification in reactive and hybrid BCIs, disruptions to privacy may be at a greater level.

[226] *Active BCIs* acquire and translate neural data generated by users who are voluntarily and intentionally engaged in pre-defined cognitive tasks for the purpose of 'driving' the BCI., *Reactive BCIs* make use of neural data generated when users react to stimuli, often visual or tactile. *Passive BCIs* acquire neural data generated when users are engaged in cognitively demanding tasks. *Hybrid BCIs* can be a combination of active, reactive or passive BCI, or combine an active, reactive, or passive BCI with some other data acquisition system. Wahlstrom, K., et al, Privacy and Brain-computer Interfaces: Identifying Potential Privacy Disruptions. SIGCAS Computer Society, Vol 46 No 1, (2016) pp.41-53; See also Wahlstrom et al, Privacy and brain-computer interfaces: method and interim findings Ethicomp/CEPE 2017, (2017) pp.1-26.

[227] Floridi, L., The ontological interpretation of informational privacy, *Ethics and Information Technology*, (2006)

Chapter IV Comparative Overview of Data Privacy Legal Frameworks

4.1 The right to privacy in international law/ Defining privacy as a fundamental right

Privacy is an issue of profound importance in all countries and is considered to be a fundamental right in many parts of the world. It has been even referred as '*fundamentally fundamental right'.* Privacy is essential to human dignity and individual autonomy which translate these moral principles in the legal sphere. As such privacy is a necessary precondition to the enjoyment of most other fundamental rights and freedoms. [228]

It is an ancient conception that has been discussed in foundational philosophical and legal treatises such as Aristotle's *Politics* from approximately 350 B.C., John Locke's *Second Treatise of Government* from 1690, and has been implemented in law for thousands of years.[229] For instance, the notion of the "private sphere", understood as the interests of individuals, distinct from a "public sphere", relating to political activities, was codified into Roman law, through the first chapter of the two sections of the Corpus Juris Civilis, issued by Emperor Justinian in 533–534 CE.[230]

The modern scholarly genesis of the right to 'informational privacy' may be traced back to Warren and Brandeis' classical Harvard Law Review article of 1890 where concept of privacy built on the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should have been reflected in the Constitution. Brandeis equated the 'right to be left alone' with the principle of an inviolate personality' when writing that "*...the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone.*''[231]

[228] H.Burkert, 'Dualities of Privacy – An Introduction to 'Personal Data Protection and Fundamental Rights", *in Privacy- New visions,* ed. Perez M., Palazzi A., Poullet, Y., Cahier du Crid, (2008)
[229] DeCew, J.: In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. *Cornell University Press*, Ithaca (1997)
[230] Smith, R., Shao, J.: Privacy and e-commerce: a consumer-centric perspective. *Electronic Commerce Research* Vol7 (2007) pp 89–116
[231] S.Warren and L. Brandeis, 'The Right to Privacy', Harvard Law Review, Vol 4 No 5, 1890. See also Solove, D., 'Conceptualizing Privacy', California Law Review Vol 90, 2001, pp. 1041–1043

Alan Westin, author of the seminal work "Privacy and Freedom," defined the right of informational privacy as: '*the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others*."[232]

In almost every nation, statutes, constitutional rights, and judicial decisions safeguard privacy. In the constitutional law of countries around the world, privacy is enshrined as a fundamental right.

Brazil's constitution promulgated that "*the privacy, private life, honor and image of people are inviolable*"; South Africa declared that "[e]*veryone has the right to privacy*"; and South Korea proclaimed that "*the privacy of no citizen shall be infringed*."[233]

Article 2 of the Italian Constitution, recognises and protects the inviolable rights of individuals, both individually and within the social groups in which they express their personality which also extends to the right to privacy.[234]

The Preamble to the Australian Privacy Charter provides, "*A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy ... Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech... .*" and "[p]*rivacy is a basic human right and the reasonable expectation of every person*."'

When privacy is not directly mentioned in constitutions, the courts of many countries have recognized implicit constitutional rights to privacy, such as in France, Germany, Japan, etc.

For example, the term "privacy" does not appear in the U.S. Constitution or the Bill of Rights. However, the U.S. Supreme Court has ruled in favor of various privacy interests - deriving the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution. For instance, in 1977 in *Whalen v. Roe*, the Supreme Court first time mentioned and somehow recognized the right to information privacy. It noted that the Constitution protected two kinds of individual interests: "*One is the individual interest in avoiding disclosure of personal*

[232] Westin A., Privacy and Freedom New York: Atheneum, 1967
[233] Privacy and Human Rights: An International Survey of Privacy Laws and Development, Electronic Information Privacy Center, 2007.
[234] The main Italian legislation for the protection of privacy is however, Legislative Decree 196/2003 (also called "The Privacy Code"), amended by Legislative Decree 101/2018 in order to adapt it to the changes introduced by the GDPR of 2016). The Privacy Code provides an illustrative list of operations describing personal data processing, such as collection, storage, recording, organisation, retrieval, consultation, erasure and dissemination of data.

matters, and another is the interest in independence in making certain kinds of important decisions".

The German Constitutional Court traced the foundations of a general 'right to informational self-determination' and of the right to privacy, to the fundamental right to "free development of one's personality" protected by Article 2.1. of the German Constitution:

> The value and dignity of the person based on free self-determination as a member of a free society is the focal point of the order established by the Basic Law. The general personality right as laid down in Arts 2 (1) i.c.w 1(1) GG serves to protect these values (. . .) [235]

It should be mentioned that governments by creating privacy legal frameworks aim to provide legal certainty where public interest are balanced against an individual's privacy rights.

Furthermore, as a modern right, privacy established a firm international recognition with the adoption of Article 12 of the Universal Declaration of Human Rights in 1948. This simple text of "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation*" established privacy's position as a fundamental human right.

Although the UDHR does not have binding legal obligations *per se*, and there is no judicial or quasi-judicial mechanism where a definitive application of the rights enshrined in it may be judged, it is still accepted as an international right to enjoying privacy without interference because of its global accession. Article 29, tries to define the scope of interference as below:

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society

It did not, however, explain how the term "privacy" shall be understood. This was left to the forthcoming international agreements with judicial oversight. Indeed, soon after the adoption of the UDHR, the European Convention on Human Rights (ECHR), a treaty that is legally binding

[235] Constitutional Court, Dec. 15, 1983, *EuGRZ*, 1983, p; 171

on its Contracting Parties and is safeguarded by the European Court of Human Rights, was signed to enforce rights enshrined in the UDHR:

> Being resolved, as the governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law to take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration.[236]

The scope of Article of 8 of the ECHR containing the right to private life and family appears to more be limited than Article 12 of the UDHR because it does not explicitly include within its scope the protection of honour or reputation.

Article 8 provides that everyone has the right to respect for his or her private and family life, home and correspondence. Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society. Article 8 of the ECHR was a cornerstone of international privacy law. It set out a robust concept of privacy, incorporating concepts of necessity, proportionality, and the functioning of a democratic state (a three-part test of interference) which have created a jurisprudence of privacy widely followed not only by European nations and institutions, but regional tribunals and countries from other parts of the world.

The International Covenant on Civil and Political Rights (ICCPR) which is an international treaty that commits its 169 parties to respecting and ensuring the exercise of individuals' civil rights, in theory, the universal binding articulation of the right to privacy. Article 17 reads as follows:[237]

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

According to General Comment 16 to Article 17 of ICCPR[238] the right to respect for privacy also encompasses a right to data protection and that each signatory state has an obligation to provide

[236] Preamble of the European Convention of Human Rights, 1950.
[237] International Covenant on Civil and Political Rights, Art. 17, 16 Dec 1966, S. Treaty Doc. No. 95–20, 999 U.N.T.S. 171
[238] General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), para. 10.

legal protection against violation of the privacy of people under its jurisdiction and those present within its territory, regardless of the origins of the violations.

It should, however, be mentioned that freedom of thought articulated in Article 18 UDHR, as "*everyone has the right to freedom of thought, conscience and religion*", and replicated in almost every human rights treaty (e.g. Article 18 ICCPR and Art 9 ECHR) does not *prima facie* protect the privacy of thought, rather create negative obligations for States not to interfere with people's political, religious and ideological and other convictions/determinations.

In 1980, the Organisation for Economic Co-operation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[239] These Guidelines contain what is known as the Fundamental Fair Information Principles which formed the basis of almost all privacy acts around the world:

Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle mentioned in Paragraph 9, except (a) with the consent of the data subject; or (b) by the authority of law.

[239] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle. An individual should have the right (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD Guidelines define "personal data" as any information relating to an identified or identifiable individual (data subject). It should be mentioned that the Guidelines do not separate "sensitive" categories of data.

The Privacy Guidelines address data transfer on an international basis and— especially since the 2013 revision—the main provisions on transborder data flows include aspects of both the accountability and adequacy principles, also adding a principle of proportionality between risks and benefits. Although the OECD Privacy Guidelines first time developed the concept of "data controller" to assign responsibility for compliance with data protection laws, they lacked proper guidance for processors in general terms or definition of technical standards for improving compliance.

Despite the fact the OECD Privacy Guidelines are non-binding in nature even within OECD member countries and referred as establishing minimum "standards", nearly all the current privacy and data sharing policies worldwide have incorporated into their provisions most of its principles.

In 2013, The Privacy Experts Group of the OECD Working Party on Information Security and Privacy (WPISP) taking into consideration the significant changes the environment has gone from the time when the traditional privacy principles are adopted identified few fields which should be analyzed and updated further.[240] Those differences contributing to the change of environment have been:

the volume of personal data being collected, used, processed and stored,

the range of analytics – algorithms based on artificial intelligence- providing insights into individual and group trends, movements, interests, the extent of threats to privacy enabled by new technologies;

the number and variety of actors capable of either putting privacy at risk or protecting it;

the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate;

and *the global availability of personal data*, supported by communication networks and platforms that permit continuous, and diverse data flows.[241]

Thus, in order to respond to the privacy questions of the changing world, the WPISP analysis report suggested, *inter-alia*, re-assessing the role of consent and individual autonomy within the current framework, counterweighing the purpose specification and use limitation in principles against innovation and value creation, and finding better technical approaches which more effectively could preserve privacy than anonymisation (de-identification) where re-identification remain a persistent risk due to the emerging technologies. In addition to the issues highlighted already, the following questions were mentioned as being worthy of further consideration:[242]

- The definition of data controller: Should this definition be updated, in light of increased diversification and cross-organisational collaboration in data usage?
- The role of other actors (e.g. system designers): should the role of actors other than data controllers be better reflected in privacy frameworks? If so, to what extent?
- The principle of collection limitation: should this principle be revised to be more precise? Should additional efforts be made to adopt technological means which both minimise the amount of information collected and

[240] "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing, Paris. 2013 http://dx.doi.org/10.1787/5k3xz5zmj2mx-en last accessed on 18 September 2019

[241] *Ibid.*

[242] *Ibid.*

increase the control of individuals? How would this operate in the context of increasing capacity for valuable re-use?

- The need for time limits on the storage of personal data: should a new principle be introduced calling for the deletion of personal data once the purpose(s) for which they have been collected has been achieved?
- The openness principle: should the duty of data controllers to provide information be enhanced to provide greater transparency, particularly in a general context of much broader data use? Should data controllers be required to provide access to data in usable format?
- The principle of individual participation: should the Guidelines specify additional criteria to determine how "challenges" from data subjects should be resolved?

In 1990, the UN too adopted the Guidelines Concerning Computerized Personal Data Files. These guidelines contain similar set of principles to the OECD Privacy Principles and contain minimum guarantees that should be provided in national legislation by a set of general principles, albeit this time at a universal level.

In 2003, the Asia-Pacific Economic Cooperation developed their own the Asia-Pacific Economic Cooperation Privacy Principles based on OECD Privacy Guidelines.

The right of privacy is also articulated in the two UNESCO declarations; the Universal declaration on the human genome and human rights of 1997 and the Universal declaration on bioethics and human rights of 2005.

Recently in 2013 and 2014, the United Nations adopted two resolutions on privacy issues entitled "the right to privacy in the digital age" in response to the development of new technologies and established a Special Rapporteur on the right to privacy, with a mandate to promote and protect this right.[243]

Privacy is instrumentally valuable, as it enables people to flourish through developing personal relationships and social participation, and it is intrinsically valuable, as it is based in moral values such as dignity, integrity, and autonomy.[244] Therefore, as also seen from the above mentioned

[243] UN, General Assembly, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18 December 2013; and UN, General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19 November 2014.

[244] Dove, E., and Phillips, M., Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, ed. Aris Gkoulalas-Divanis, Grigorios Loukides, Springer 2015

instruments, there is a universal consensus about the importance of privacy and need for its protection.

Law distinguishes between the conceptions of privacy and data protection. Privacy is a broader concept that embodies a range of rights and values, such as the right to be let alone, intimacy, seclusion, and personhood. It can cover different aspects of human life not necessarily involving information, such as a right to have family, to live solitude life, or acquire new gender identity, etc. It can also include control over personal data, but not all personal data are private. The legal right to privacy protects the intimacy as well as the autonomy and self-determination of citizens, whereas data protection is seen as a legal tool that regulates the processing of personal data. As such data protection and privacy are separate but complementary rights; data protection is a subset of the right to privacy; and data protection is also an independent right which serves a multitude of functions including, but not limited to, the protection of privacy.[245]

More specifically data protection covers concepts such as data security, data quality, non-discrimination, and proportionality. The origins of the right to data protection lie partially in the data protection rules of northern European countries, which arose in several nations in the 1970s, as well as in the Council of Europe's Resolutions on data processing. [246] Currently, data protection claimed to offer individuals more rights over more types of information than the right to privacy when applied in the context of personal data processing.

Data protection is a "*set of legal rules that aims to protect the rights, freedoms, and interests of individuals, whose personal data are collected, stored, processed, disseminated, destroyed, etc".*[247] The ultimate objective of data protection is to ensure fairness in the processing of data and in the outcomes of such processing.

[245] Linksy, O., The foundations of EU data protection law, Oxford University Press, 2015
[246] Van der Sloot, B., Legal Fundamentalism: Is Data Protection Really a Fundamental Right? in Data Protection and Privacy: (In)visibilities and Infrastructures, edited by Leenes, R., Springer, 2017.
[247] Tzanou, M., Data protection as a fundamental right next to privacy? 'reconstructing' a not so new right. International Data Privacy Law Vol 3, (2013) pp. 88–99

4.2 Overview of privacy and data protection framework in EU law

4.2.a) Privacy and data protection in EU

The human rights to privacy and data protection are not absolute and can be limited under certain conditions when specific safe-guards are taken into-consideration and the limitation is proportionate. Fundamental rights and values can also conflict with each other, such as the right to privacy and data protection versus freedom of expression, the right to information as well as to benefiting from scientific research, also transparency in decision-making processes, public interest, etc. This issue becomes even more complicated when taking into consideration the fact that the law today is more fragmented than ever as the result of the interaction of several different legal orders such as the international, regional and national regimes.

Above I have reviewed the right to privacy and freedom of thought as it is recognized in international documents. A distinction can be made in EU law between privacy and data protection, though. The European Convention on Human Rights and the EU Charter are the basis for the principles concerning the protection of privacy, personal life and personal data. The specific protection of personal data in the EU, however, is covered by the Guidelines for Data Protection Regulations of 2016, the main provisions of which will be reviewed in detail below.

At the European Level, the Lisbon Treaty[248] was the major document to introduce significant changes to the legal framework for data protection in the EU. Of particular importance was the introduction of a legal basis for data protection legislation in Article 16 of the Treaty on the Functioning of the European Union (TFEU), and the addition of a right to data protection in the EU Charter. Article 16 TFEU provides, *inter alia*, that '[e]*veryone has the right to the protection of personal data concerning them' and enables the Union to enact data protection legislation applicable to Member States 'when carrying out activities which fall within the scope of Union law*'. Article 16 TFEU explicitly states that the rules adopted pursuant to it '*shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on the European Union (TEU)*'. Article 39 TEU introduces a specific legal basis for data processing by Member States when acting on Common Foreign and Security Policy matters and in the area of Police and Judicial Co-operation.

[248] European Union (EU), Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community (2007) OJ C306/01

Data protection is now part of the provisions having general application in the founding treaties.[249]Article 8 (the right to private life) ECHR has been duplicated in Article 7 of the Charter, while Article 8 of the Charter (the right to protection of personal data) has no equivalent in the ECHR. Article 8 separates the right to data protection from the right to privacy and coins it as fundamental right. Nevertheless, inter-relationship between the right to privacy and the protection of personal data has been recognised by the case law of the Court of Justice of the European Union, where it ruled that in order for finding the infringement of the right to privacy the processing of personal data must be interpreted in light of the fundamental rights as enshrined in the ECHR.[250]

Further, Article 8 of the Charter not only distinguishes data protection from privacy, but also lays down some specific guarantees in paragraphs 2 and 3, namely that personal data must be processed fairly for specified purposes and on the basis of the consent of the person or on some other legitimate basis laid down by law; that everyone has the right of access to data collected about him or her, and the right to have it rectified; and that compliance with these rules shall be subject to control by an independent authority.[251] The fundamental right to data protection is not an absolute right as it was ruled by the CJEU.[252]

The ECHR with its Article 8 and the jurisprudence of the European Court of Human Rights provided strong protection for the right to privacy evolving its scope over the decades to encompass not only the right to private and family life, home and correspondence, but also privacy of many other values such as freedom of holding opinions, privacy of thought, autonomy, freedom of movement, and data protection including protection of health data, among others. Although wording of Article 8 puts negative obligations to State Parties, by stating that "*interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society*", from the case law of the ECtHR it can be deducted that governments bare responsibility to protect rights enshrined in Article 8 by adopting measures designed to secure respect for privacy and enacting domestic law for effective challenging any violation by third parties.

[249] 21 Art. 16, Consolidated Version of the Treaty on the Functioning of the European Union (2012) OJ C 326,
[250] Joined Cases C-465/00, 138 and 139, Österreichischer Rundfunk [2003] ECR I–4989, paras. 68–69.
[251] Kokott J., and Sobotta C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law* Vol 3 (2013)
[252] "The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society." Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. (2010) ECLI: EU: C: - 662, para 48

Article 8 ECHR is not only applicable in respect of individuals, but also legal persons.[253] The object and purpose of Article 8 ECHR is to protect the physical or legal person against arbitrary interference by public authorities. Excluded from the scope of Article 8 ECHR is the processing and disclosure of personal data which is not private in itself or not systematically collected and stored with to regard to a data subject, and where the data subject could reasonably expect the processing or disclosure.[254]

Article 8 does not explicitly mention privacy of freedom of thought, and Article 9 of the ECHR on freedom of thought, conscience, and religious matters as in the case with identical ICCPR's provision (Article 18), only governs freedom in expressing or withholding from expression of political or other ideas or practicing religion. However the European Court on Human Rights, the judicial body in charge for oversight of the ECHR implementation, in the case concerning Article9 established that disclosure of information about personal religious and philosophical convictions may engage Article 8 as well, as such convictions (determinations) concern some of the most intimate aspects of private life.[255] Thus, Article 8 can be seen as covering indirectly privacy of thought and opinion.

Besides, in cases concerning data protection, the ECtHR interpreted the concept of "private life" under Article 8 broadly within the context of the Council of Europe's Data Protection Convention108,[256] upon which the former Data Protection Directive is modelled, thus extending the scope of Article 8 to the data protection as well. Regarding the sensitive (health) information, it is obvious that signatory States are required to afford appropriate safeguards through domestic law to prevent any communication or disclosure of health data which can be inconsistent with the guarantees of Article 8 ECHR.[257]

As such within Europe, the individual's right to privacy is firmly embedded at the fundamental human rights level by the European Convention on Human Rights of 1950. With the emergence of information technology in the 1960s, however there was a growing need for more detailed rules to safeguard individuals by protecting their personal data. In the 1970s the CoE concluded that

[253] *Niemitz v. Germany*, ECtHR Judgment of 16 December 1992;
[254] Kranenborg, Herke, Access to documents and data protection in the European Union: on the public nature of personal data, *Common Market Law Review*, vol. 45, 2008, 1079–1114, at 1093
[255] Folgerø and Others v. Norway, (ECtHR 2007)
[256] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. See also *Z v. Finland*, Judgment of 25 February 1997.
[257] Z v. Finland, § 95,(ECtHR 1997); Mockutė v. Lithuania, §§ 93-94, (ECtHR, 2018)

Article 8 ECHR has had several limitations in the light of new developments - especially in the area of information technology, which were the uncertain scope of private life, the emphasis on protection against interference by public authorities, and the insufficient response to the growing need for a positive and proactive approach, also in relation to other relevant actors and interests.[258] As a result, in 1981, the CoE adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Convention 108, to date is the only legally binding international instrument in the data protection field.

The Convention 108 do not contain the word privacy in its title per se, but specifies its importance in the preamble: "*Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing; Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples*"'

Also, Article 1 of the Convention, clearly mentions that the purpose of the Convention is to protect the person's right to privacy with regard to automatic processing of personal data relating to him or her.

These wordings demonstrate that the Convention is both wider and more specific than the protection of privacy. It is wider since it also relates to other fundamental rights and freedoms of individuals, such as equality and due process derived from data protection and it also protects personal data the one which does not fall within the scope of the privacy right mentioned in the ECHR and the EU Charter. It is at the same time more specific, since it only deals with the processing of *personal data* aspect of privacy. Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. Personal data concerning the health of the data subject is also protected as sensitive data under Article 6 of Convention 108. Convention 108 protects individuals against abuses that may accompany the collection and processing of personal data. It also regulates the transborder flows of personal data.

[258] P.J. Hustinx, Data protection in the European Union, *Privacy & Informatie*, 2005

The processing of personal data by EU institutions and bodies are covered by Regulation (EC) No.45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data. The EU Institutions Data Protection Regulation applies main data protection principles to the data processing carried out by EU institutions and bodies in the exercise of their functions. It establishes an independent supervisory authority - the European Data Protection Supervisor (EDPS) to monitor the application of its provisions which also reviews complaints from the breaches of data protection rules and provides guidance to EU institutions by issuing interpretation of a data protection provision and drafts new rules when necessary. The EU Commission has proposed an amendment to the EU Institutions Data Protection Regulation to ensure its compliance with the new EU data protection regime which came into force with the adoption of the GDPR.

There are also some sectoral EU documents which deal with data protection in certain fields, such as the sector of electronic communications. Directive 2002/58/EC35 concerning the processing of personal data and the protection of privacy in electronic communications (the E-Privacy Directive) regulates the security of personal data in those networks. Article 4.1 requires electronic communication service operators to ensure that access to personal data is limited to authorised persons and take measures to prevent personal data from being destroyed, lost or accidentally damaged. Where there is a particular risk of breach of the security of the public communications network, operators are obliged to inform the subscribers about the risk (Article 4.2). When despite the security measures undertaken, a breach of security nevertheless occurs, operators must notify the competent national authority entrusted with implementation and enforcement of the E-Privacy Directive. Operators are also required to notify personal data breaches to individuals when the breach is likely to negatively affect their personal data or privacy. (Art. 4.3). The confidentiality of communications requires that the listening, tapping, storage or any type of surveillance or interception of communications and metadata is, in principle, prohibited. These negative obligations indicate that confidentiality of communications is linked to the protection of the right to respect for private life enshrined in Article 7 of the Charter and the right to personal data protection enshrined in Article 8 of the Charter.[259]

[259] Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p 34

The EU Commission proposed a new Regulation (the Regulation on Privacy and Electronic Communications) concerning the respect for private life and the protection of personal data in electronic communications to repeal the current E-Privacy Directive. The proposal aims to align the rules governing electronic communications with the GDPR. The new regulation which will be also directly applicable throughout the EU providing the same level of protection to everyone and will extend coverage to new players providing electronic communication services such as Skype, WhatsApp, Facebook Messenger and Viber. The proposed Regulation on Privacy and Electronic Communications will also apply to new players providing electronic communication services which are not covered by the e-Privacy Directive. [260] In addition, the confidentiality of both content and metadata derived from electronic communications would be protected.[261]

The European Commission also has an eHealth Action Plan 2012-2020 to provide a roadmap for empowering patients and healthcare workers through linking up devices and technologies and increasing research in the personalised medicine of the future.

4.2.b) Specifics of the General Data Protection Regulation

After a decade of discussion, the General Data Protection Regulation (GDPR) was finalised in May 2016 and entered into force on 25th May 2018. The regulation enshrines in law the principles of protection of privacy and personal data that have been internationally agreed in the OECD Privacy Guidelines and *Data Protection Directive 95/46/EC.* Because these principles have previously been expressed only in guidelines and directives, they were somehow overlooked for commercial, regulatory, and practical purposes. Now, the Regulation directly applies in Member States national law. By equalizing the rules for data protection in all western Europe, the GDPR will lead to more legal certainty, strengthen individual control of data subjects over their data and remove potential obstacles to the free flow of personal data in digital age. [262]

It should be mentioned that defining privacy in a technologically developing world is one of the most challenging issues in lawmaking. With its 99 articles and 173 interpretative recitals, the

[260] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, art. 18
[261] E-Privacy Regulation Proposal, Art. 4, no. 3a, Art 5.
[262] Voigt, P., and Von dem Bussche, A., The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017

GDPR is a complex piece of legislation which aims to achieve this task. While the ECHR and the EU Charter are providing basis for the principles concerning the protection of privacy, personal life and personal data, the GDPR covers the procedures of specific protection of personal data in the EU. The main purpose of the GDPR is to define and update a number of basic rights of data subjects regarding control of and access to their personal data, and to implement common rules for data protection in all member states. The amendments brought with the GDPR, *inter alia,* include, the need for clear and affirmative consent by the data subject, destruction of data if storage is no longer needed for the initial purpose or after withdrawal of consent by the data subject; the right to obtain rectification about personal data; the right of the data subject to transfer personal data to another service provider; the requirement to inform the data subject when his/her data is leaked.

The GDPR does not mention the right to privacy, instead it extends on the definition "data protection" given in Directive 95/46/EC. Even common terms such as "privacy by design" have been redefined as "data protection by design" and "privacy impact assessments'" have been given as "data protection impact assessments". As such data protection has been disconnected from the right to privacy in the GDPR. It is claimed that because "unlike privacy's elusive and subjective nature that makes the right different in different contexts and jurisdictions, data protection has an essential procedural nature that it makes it more objective as a right in different contexts".[263]

It should be highlighted that the GDPR has an extremely broad territorial scope capturing both controllers and processors in the EU, and those outside the EU who offer goods and services to, or monitor, EU residents.[264]

Principles of data processing

According to Article 5 of the GDPR, processing of personal data shall be carried out complying with the principles of "*lawfulness, fairness and transparency*", "*purpose limitation", "data minimization", "accuracy", "storage limitation", "integrity and confidentiality", and the data controller's "accountability"*.

Lawfulness, fairness and transparency

[263] Tzanou, M.: Data protection as a fundamental right next to privacy? 'reconstructing' a not so new right. Int. Data Priv. Law 3, 88–99 (2013)
[264] Article 3.1, GDPR

This first means the data should be processed fairly, having a clear legal basis, and in a transparent manner. Also, the principles of fairness and transparency about data processing require that the data subject shall be informed of the existence of the data processing and its purposes (Articles 13 and 14).

As data subjects have rights to access to, rectify and erase the data about themselves (subject to various restrictions however),[265] the data controller shall provide the data subject with any further information necessary to ensure the data subject rights and fairness and transparency of processing, by also taking into account the special circumstances in which the personal identifiable data is processed.

Purpose limitation: Personal data undergoing processing shall be collected and recorded for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those said purposes.[266]

Data minimization[267] stipulates that collected personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. IT systems should be configured by minimising the use of personal data or its identification, in such a way as to rule out their processing should the purposes sought in data processing are achieved by using either anonymous data or by making suitable arrangements to limit identification of data subjects only in cases of necessity.

Accuracy:

Personal data shall also be processed accurate and, when necessary, kept up to date; and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased. Also, any mistakes on the stored or processed data should be rectified without delay. This principle is also linked to fair and transparent processing.

Storage limitation

[265] Articles 15- 22, the GDPR

[266] Article 89.1 research exception applies

[267] The data "minimisation" principle has been established in national privacy laws, such as Section 3(a) of the German Bundesdatenschutzgesetz and Section 3 of the Italian Data Protection Code.

Personal data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for *inter alia* public interest, scientific research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject;

Integrity and confidentiality

The data should be processed and stored in a secure way using appropriate technical or organisational measures to avoid unauthorised or unlawful processing or accidental loss, destruction or damage.

Obviously, any personal data that is processed in breach of the main principles of the processing of personal data may not be used.

Accountability

Under the GDPR, accountability is a principle that requires controllers to put in place appropriate technical and organisational measures and be able to demonstrate compliance with the main data processing principles.

Principle of proportionality (dual usage)

1. In EU law, the principle of proportionality generally has been referred together with the principle of subsidiarity in the Treaty of European Union and requires that "*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties*" .[268] It mainly regulates the exercise of power by the Union vis a vis to the Member States.

It requires the EU institutions and Member States to review the necessity of the actions taken to achieve the balance between the means utilized and the purposes aimed at. Thus, the principle of proportionality imposes boundaries to the EU Institutions' as well as Member States' actions in general terms.

[268] Article 5.4 of the Treaty on European Union (TEU)

2. Principle of proportionality in data protection.

- The processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms of individuals. As such the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[269]
- Personal data undergoing processing shall be relevant, complete and not excessive in relation to the purposes for which it is collected or subsequently processed. [270]

Legal Grounds for Processing the Data.

Lawful processing is presented in two options that must be met, one for processing data and one for lifting the ban on processing special personal data (including health data). Articles 6 and 9 of the GDPR set out the substantive criteria for the lawfulness of the processing of ordinary and sensitive personal data respectively. Data processing for personal data are carried out either with the data subject's consent or by a legal permission (to implement controller's legal obligations, to protect vital interests of the data subject or third parties, for public interest and other legitimate interests).

Member States have discretion to introduce more specific provisions to adapt the application of the GDPR's rules with regard to processing for compliance with a legal obligation; for performance of a task in the public interest (e.g. national security purposes); in the exercise of official authority; or for other specific processing situations (Article 6.2).

Where legitimate interests are relied on as a legal basis for processing (non-sensitive) data, the data subject, at the time when personal data is obtained, must be informed of the legitimate interests pursued by the controller or by a third party (Article 13.1.d) and Article 14.2.b).

To *process sensitive data*, the controller should have a specific legal basis, in addition to article 6. In principle, the processing of such data 'shall be prohibited' (9.1). The first exception for

[269] Recital 4 to the GDPR
[270] Recital 170 of the GDPR and Article 5.4 of the Treaty on European Union (TEU)

processing sensitive data is *the explicit consent of the data subject unless a specific law states that the prohibition cannot be lifted by explicit consent* (9.2.a).[271] Further relevant exemptions are:

> necessary to protect the vital interests of the data subject when data subject is incapable of giving consent (9.2.c);
>
> personal data manifestly made public (9.2 e);
>
> necessary for substantial *public interest* reasons on the basis of EU or Member State law (9.2.g);
>
> necessary for *the public interest in public health*, such as protection against serious cross-border health threats, assuring high standards of quality and safety etc. on the basis of EU or member state law when suitable safeguards for the rights and freedoms of the data subject are provided (9.2.i);[272]
>
> necessary for preventive or occupational medicine, medical diagnosis, *provision of healthcare* etc. on the basis of EU or member state law and subject to professional secrecy. It also clarifies that the activity in question must be on the basis of EU or Member State law, or pursuant to a contract with a health professional. (9.2.h and 9.3);
>
> necessary for archiving, *scientific or* historical *research* or statistical purposes in accordance with article 89.1, based on Union or member state law which must be proportionate to the aim pursued and provides suitable and specific measures to safeguard the rights and freedoms of the data subject (9.2.j) It is clearly emphasised, however, that exemptions and derogations for research purposes should not result in personal data being processed for other purposes by third parties such as employers, insurance or banking companies (Recital 54).

As seen above, the GDPR provides several exemptions and derogations for the use of health data, e.g. in the context of research or public health purposes under certain conditions. Typical procedures in this context include the application of ethical standards for scientific research as mentioned in Recital 33 and the implementation of organisational and technical safeguards as mentioned in Article 89 including anonymisation, pseudonymisation and encryption.[273]

[271] Some EU countries enacted laws to prohibit medical examinations *inter alia* for private life insurances.
[272] A new ground, including a broad definition of "public health" (Recital 54);
[273] NHS Confederation (2012) General Data Protection Regulation: NHS European Office Position Paper. http://www.nhsconfed.org/regions-and-eu/nhs-european-office/influencing-eu-policy/~/media/AF378EA1EBAF490D90F316645B65558F.ashx last accessed on 30 October 2019

Material scope of the GDPR

The GDPR applies to any data relating to a natural person. Since the definition includes "any information," one must assume that the term "personal data" should be as broadly interpreted as possible, which is also suggested in ECJ's case law. Data has to be 'personal' in order to fall within material scope of the GDPR. Data is considered personal if the information relates to an identified or identifiable individual. The definition in the GDPR is more detailed than it used to be in the Directive, extending this list of identifiers to an identification number, location data and online identifier, whilst sensitive personal data now includes genetic and biometric data (Article 4.1 and Article 9.1). So, the identification of a person is possible based on the available data. (Art. 4.1), in other words if a person can be detected, directly or indirectly, by reference to an identifier (e.g. 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). The GDPR does not apply to anonymised data. Identifiability which often used as a key benchmark for providing legal protection of privacy, is in itself problematic in a sense that advanced technical procedures can 'pseudonymise' and 'anonymise' data, thus rendering re-identification of an individual unlikely, but it is impossible to guarantee 100% anonymity.[274] The ECJ interpreted the risk of re-identification of the personal data with respect to former Data Protection Directive as below:

> "if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant"[275]

Recital 26 to the GDPR has somehow given similar explanation to identifiability:

> "[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used" and, "[t]o ascertain whether means are reasonably likely to be used to identify the natural person, 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".

Special categories of personal data:

[274] P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', UCLA Law Review Vol 57 (2010), pp. 1701-1777

[275] Case C-582/14 Breyer v Bundesrepublik Deutschland. 2016. ECLI:EU:2016:779.

Within the GDPR (Article 9), the following categories are considered sensitive data:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions, religious or other beliefs, including philosophical beliefs;
- personal data revealing trade union membership;
- genetic data and biometric data processed for the purpose of identifying a person;
- personal data concerning health, sexual life or sexual orientation.

Sensitive data remain mostly the same as the Data Protection Directive, with some additional grounds. Member states however may introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.[276] GDPR also allows Member States to derogate from the prohibition on processing sensitive categories of data if this is done by law, and subject to suitable safeguards.

Health data

Although the new GDPR aims at protecting the rights of the data subject and confidentiality of personal data as an important civil right, it is not specifically designed for health data, and interpretations for different applications can provide difficulty. Therefore, Article 40 encourages the development of sectoral codes of guidance, including code for medical research.

Nevertheless, personal data concerning the health of the data subject qualify as sensitive data under Article 9.1. Accordingly, health-related data are subject to a stricter data-processing regime than non-sensitive data. The GDPR prohibits the processing of "personal data concerning health" (understood as "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject")[277], as well as genetic data and biometric data, unless it is authorised under Article 9.2. Both types of data have been added to the list of "special categories of data".

Although genetic and biometric data have been added to the list of "special categories of data", neither in main text nor in recitals, there is not any referral either **to neuro-data or of any examples of the data derived from recent neuro-technological advancements**. Only in

[276] Article 9.4. of the GDPR
[277] Recital 35, the GDPR

Recital78 protection of personal data and privacy in a broader sense can be linked to technology: "*The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met*".

With regard to health data, controllers must either obtain explicit consent or fall under various GDPR exceptions, i.e. for medical treatment (Art 9-2.h)or , the "public interest in the area of public health," (Art.9-2.i) and scientific research (Art.9-2.j). Under Article 9-2.h and 9-2.i processing is permissible, however, only where performed by a healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.[278]

Ambiguity: The scope of the above exceptions remains uncertain, especially for research, in part because permitted conduct depends on state member-state laws which may lead to divergent requirements. As to the GDPR, it refers to exceptions for the "public interest," "public health" and "scientific research," without clearly explaining them or addressing dual-use endeavors of these overlapping terms.[279]

There are also conflicts in the guidance of the GDPR, for example, Recital 159 explains that "scientific research" should be defined broadly and include both technological development and privately funded research, Recital 54 states that public health and public interest exceptions "*should not result in personal data being processed for other purposes by third parties*...". Where the GDPR permits research exceptions, it requires "appropriate safeguards" to protect individual privacy rights—without clarifying what those safe-guards must be (for example, in Articles 89.1 and 9 and Recitals 52 and 54).[280]

There are also several scientific research exemptions in GDPR.[281]

[278] Recital 54, the GDPR

[279] For instance, see Chapter 19 in Laurie G, Harmon S, Porter G. Mason and McCall Smith's Law and Medical Ethics. Oxford University Press. 2016, "*Like privacy, the concept of the public interest is difficult to articulate across various realms of law, having attracted much attention from beyond the health sector. Whilst the notion remains 'ill-defined', public interest is perhaps more easily identifiable in the health context: the basic premise is that medical research using individual patient data can contribute to scientific knowledge that can be of benefit to the health of populations, individually and at large, now and in the future*." Powell P., and Buchan, I., Electronic Records Should Support Clinical Research, *Journal of Medical Internet Research* Vol 7 (2005).

[280] Nicholson et al, Shadow health records meet new data privacy laws; How will research respond to a changing regulatory space? Insight, 2019

[281] For general discussion see van Veen, E., Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. MLC Foundation, AL Den Haag, 2018

Purpose limitation (Art5.b) - Personal data must be processed for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes; Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (subject to the conditions in Art 89(1), concerning implementation of appropriate technical and organisational measures.)

Storage limitation (Art 5.1.e)- Personal data should not be kept in a form that permits the identification of subjects longer than is necessary for the purposes of processing except if longer storage is necessary for scientific research purposes and in accordance with article 89.1 and when subject to appropriate technical and organisational measures.[282]

Transparency principle when data have not been obtained from the data subject (14.5.b): Not if provision of such information would be a disproportionate effort, such as for scientific research but subject to the conditions and safeguards of Art. 89.1 or in so far as disclosure would render impossible or seriously impair the objectives of the processing. In such cases, appropriate measures must be taken.

[282] The CoE Medical Data Recommendation of 1997 contains similar clauses. Scientific research is explicitly acknowledged as a reason for conserving data longer than they are needed, although this will usually require anonymisation. Article 12 of the Medical Data Recommendation proposes detailed regulations for situations where researchers need personal data and anonymised data seems to be insufficient.

Right to erasure (right to be forgotten), Art 17 does not apply in the following cases:

- Art17.3.c: For reasons of public interest in the area of public health pursuant to Art 9.2.h and i.
- Art17.3.d - For research in accordance with Art 89.1 and insofar as research would be seriously impaired or rendered impossible.

Right to object, Art 21

Research per se is not one of the grounds for the right to object to data processing

However, according to Art 21.6 right to object against processing personal data for research does not apply if processing is necessary for a task carried out in the public interest

Data controller -A 'controller' is a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data, Art. 4.7 GDPR. The legal definition consists of three main components: (1) a natural or legal person, public authority, agency or other body (2) that alone or jointly with others (3) determines the purposes and means of data processing. The GDPR recognizes joint controllers in Art. 26.

In the medical context, this role is usually undertaken by the physician/healthcare organization. There is a lot of responsibility placed on the Data Controller – he/she should ensure principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality' in the processing of personal data according to Art 5. GDPR. The GDPR also mentions the accountability of controller specifically. According to Art 28 GDPR data controllers have an obligation to enter into binding agreements with the data processors. Data processors are outsourced service providers, i.e. a separate legal entity/individual with respect to the controller, which perform the processing activities on behalf and under the direction of the controller. In these agreements, data controllers must describe the obligations, control mechanisms, and security safeguards that must be applied. Meanwhile, data processors must confirm their obligation to uphold the data protection obligations including limiting their use of data as specified by the data controller and taking appropriate security measures and inform controllers of any data breaches without undue delay.

The GDPR imposes direct statutory obligations on data processors as well (Arts 28 and 29). This means processors are subject to direct enforcement by supervisory authorities, serious fines, and direct liability to data subjects for any damage caused by breaching the GDPR (Arts 82 and 83).

Data subjects have rights to their data, such as access – (to find out what the personal data relating to you data controller holds), rectification or erasure, restriction of processing, a right to object, data portability, to be notified about actions under Arts 16–18 and rights in relation with automated decision-making. Those rights are subject to various restrictions, under research exemptions or some other circumstances. For instance, the right to erasure - the newly included 'right to be forgotten' is restricted during processing for research purposes or the right to 'data portability' extends only to those data that subject has provided.

Consent in GDPR

Consent is a paramount concept in law in general and has been dominant concept in health - care and research regulation. Therefore, over the years different forms of consent have been developed such as informed, explicit/specific/narrow, broad and generic.

In privacy law too, since the German census-decision of 1983, derived from (informational) self-determination consent have become almost most prominent legal basis for processing personal data.

Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. It must be demonstrable and should be detached from other bases for which data processing is necessary, such as a contract. While being one of the more well-known legal bases for processing personal data, consent is not only legal bases mentioned in the GDPR. The five others are: previously signed contract on other subject matter, controller's legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR.

The new GDPR raises the bar for consent. Recital 32 and article 4.11 give a definition: consent means freely given, specific, informed and unambiguous - indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. In order to obtain freely given consent, it must be given on a voluntary basis. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. The Guidelines of the

former article 29 Working Party on Opinions on consent[283] and transparency[284] provides further clarification.

It is generally accepted that if a person cannot participate in a certain activity, which is not about data processing *per se*, but includes data processing, there cannot be free consent for the data processing which is constitutive element of that activity. The legal basis for data processing should then shift to the informed consent to participate in that activity. In the healthcare sector, all diagnostic and treatment procedures as a common rule is based on informed consent of the patient. In that case also, as the data processing is inherent part of the treatment, informed consent to undergo the treatment suffices for data processing. The legal basis will then be national law regulating healthcare provision.[285] Explicit consent needed for processing sensitive data (health data) as per Article 9.2 of the GDPR is not applicable here.

But for research mostly in the form of clinical trials, Clinical Trials Regulation of 2014 and research exception from consent from GDPR (Art. 9.2.h) apply. Former Article 29 Working Party Regulatory Guidance on this issue notes data minimization, anonymization, and data security as potential safeguards. It adds transparency as the research progresses as another possible safeguard to offset the absence of specific consent, such as designating a qualified person that can answer participants related questions over time, or provide them with a comprehensive research plan before they consent.[286] It should be noted that where explicit consent for participating in a single trial is applicable for the primary analysis of trial data, secondary analysis or data sharing for analysis by others should not be possible without new consent unless derogations from Article 9.2 apply.

Besides, according to Art 9.2.a Member States can enact specific laws in some circumstances to prohibit lifting the ban for processing sensitive data by mere explicit consent of the data subject.

Anonymisation:

[283]The guidelines of the article 29 working party on consent. Guidelines on consent under regulation 2016/679, 10 April 2018, WP 259/rev.01
[284] Guidelines on transparency under regulation 2016/679, 11 April 2018, WP 260/rev.01.
[285] van Veen, E., Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. MLC Foundation, AL Den Haag, 2018
[286] Article 29 Working Party 2018, p. 29

In order to facilitate the use of data in the context of medical research projects, public health or statistics, while protecting personal data, the GDPR proposes technical and organisational measures such as anonymization (de-identfication), pseudonymisation and encryption. Anonymisation is a way of modification of personal data with the result that there remains no connection to an individual. Anonymised data is either information that does not relate to an identified or identifiable individual or personal data that was rendered anonymous in such a manner that the person is not or no longer identifiable.[287] Anonymisation is achieved through a number of techniques that categorised in two types:

> 1. Randomisation: altering the accuracy of data in order to remove the strong link between the data and the individual. If the data becomes sufficiently uncertain, it can no longer refer to a specific individual.[288]
>
> 2. Generalisation: generalising attributes of data subjects by modifying the respective scale or order of the data (i.e., a region rather than a city, a month rather than a week).[289]

Pseudonymisation refers to the users replacing personally identifiable material with artificial identifiers.[290] In case of an effective anonymisation, the GDPR does not apply.

But there are three major limits to anonymisation:

First, after 25 years of the adoption of the Data Protection Directive, it is still not possible to precisely define when and under which conditions data may be seen as anonymous because the methods and degree of anonymization required to warrant fewer legal restrictions are not only inconsistent but almost unspecified,[291] causing legal uncertainty when it comes to working with health data. As mentioned above, this is partly due to an omnibus data privacy legislation approach where the specific issues of medical data privacy and contemporary biomedical research have not taken into consideration. Another factor is that de-identification (and re-identification) is a rapidly developing – and also controversial – field, which makes it challenging if not impossible to precisely put down a specific standard for anonymization in law.[292]

---

[287] Recital 26 GDPR.
[288] Art. 29 Data Protection Working Party, WP 216 (2014), p. 12. in Voigt and Bussche, EU GDPR, Practical Guide, Springer, 2017
[289] See also Art. 29 Data Protection Working Party, WP 216 (2014), p. 16.
[290] Recital 26
[291] See Art 2.a and Recital 26
[292] Dove, E., and Phillips, M., Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, Springer 2015

Second, data privacy research is now making clear that although a dataset may be anonymised according to conventional approaches, its cross-linking with data available elsewhere can make it possible to infer data subjects' identities. Therefore, although anonymisation techniques makes re-identification less likely, they do not guarantee anonymity, especially in large datasets. [293]

Third, as the context of medical confidentiality is changing with the development of precision medicine and e-health technology; our expectations about medical treatment will require greater linkages of data. Also, in nowadays international collaboration and long-term research projects, re-searchers or clinicians may want to link medical data to other data sources over time. Thus, while anonymisation may be used for achieving stronger data privacy protection, in the medical data context it offers only limited utility to both researchers and patient-participants alike.[294]

According to new-GDPR regulations clinician or research teams should undertake below steps for ensuring privacy of patient / trial participant receiving therapy with BCI.

- To obtain explicit consent from the data subject prior to processing or communication his or her data unless in situations where derogations exist. (to protect vital interests of the BCI user when he is not in capacity of giving consent, for public health interest, for treatment and research)
- To apply appropriate technical and organisational safeguards, pseudonymisation and encryption and where possible anonymisation for data use in the context of public health projects, individual research projects, or data banks.
- To provide access for the data subject (i.e. the patient) to the information collected by translating/decoding brain signals of the BCI user.
- To notify the national supervisory authority within seventy-two hours in case of breach of personal data (or record keeping in the case of derogation) and be in position to rectify any inaccurate data.

Cross-border data transfer

[293] Expert Advisory Group on Data Access: Statement for EAGDA funders on re-identification. http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtp055972.pdf (2013). Last accessed on 30 October 2019

[294] Edward S. Dove and Mark Phillips, Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, Springer 2015

EU law[295] provides for the free flow of data within the European Union. Under the GDPR, restrictions or prohibitions on the free movement of personal data between EU Member States for reasons connected with the protection of natural persons with regard to the processing of personal data are forbidden.[296] Therefore, the EU institutions came-up with special arrangements to ease the data transfer between Member States.

One of these special channels is the eHealth Network which was created in order to overcome legal, organisational, technical, and semantic interoperability challenges in the context of cross-border exchange of personal health data in the EU.[297] The eHealth Network is a voluntary network composed of national authorities responsible for eHealth that works towards interoperable applications and enhanced continuity of and access to care. The Network established the foundations for the eHealth Digital Service Infrastructure (eHDSI),[298] and adopted guidelines on Patient Summaries in November 2013[299] and on e-Prescriptions in November 2014.[300]

Under the eHDSI Infrastructure, the first wave of voluntary cross-border exchanges of patient summaries and ePrescriptions began by a few pioneering countries by the end of 2018; with around 20 Member States expected to participate by 2020. So far, 16 Member States started technical preparations for this cross-border exchange. In 2018, the Commission also adopted a Communication, which, *inter alia,* seeks to ensure appropriate governance of the eHDSI. The intention is to review the management and functioning of the eHealth network to clarify its role in the governance of the eHealth digital service infrastructure and its operational requirements.[301]

When it comes to the personal data transfers to third countries outside the EU and to international organisations EU law has some reservations. Convention 108 clearly prohibits restrictions on transfer solely for reasons of privacy between participating states, with only two exceptions, one

[295] Article 14.1 and 14.2 Convention 108 and Art 44, GDPR
[296] Art. 1.3 GDPR,
[297] 2011/890/EU: Commission Implementing Decision of 22 December 2011 providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth
[298] An IT system funded by the Connecting Europe Facility and Member States, Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, OJ L 348, 20.12.2013, p. 129.
[299] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf
[300] https://ec.europa.eu/health//sites/health/files/ehealth/docs/eprescription_guidelines_en.pdf
[301] Report from the Commission to the European Parliament and the Council on the operation of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare COM/2018/651 final

of them being related to the sensitive data, when receiving jurisdiction does not provide "*equivalent protection*". [302]

Special controls on data transfer are applied (Art. 44 GDPR) to ensure that personal data are only transferred into environments where they will continue to be subject to adequate protection; and the adequacy of data protection law in third countries is not to be assumed by controllers.[303] For this reason, transfer is permitted only if: (a) the European Commission has decided that the third country ensures an adequate level of protection;[304] (b) the controller or processor has provided adequate safeguards including enforceable rights and legal remedies for the data subject provided through standard contractual clauses, binding corporate rules, codes of conduct and certification mechanisms;[305] or (c) in the absence of either an adequacy decision or appropriate safeguards, a number of derogations are available.[306] Where a transfer cannot be based on (a) or (b), then Article 49(1) sets out eight specific situations in which (c) derogation is possible.

Adequacy approach

The adequacy approach was introduced by later developments in Europe, and in particular by the former Data Protection Directive and has been further developed with the GDPR. According to Article 45 GDPR, this approach requires that any transfer to a country outside the European Union must be made in accordance with a transfer justification that has been approved in advance by the European Commission. These prior approvals of a foreign legal framework are referred to as adequacy decisions issued by the Commission. When transferred personal data remains subject to a legal jurisdiction that has been deemed adequate, transfer requires no further justification. The CJEU explained that the term "*adequate level of protection*" requires the third country to ensure a level of protection of fundamental rights and freedoms that is "*essentially equivalent*"[307] to the safeguards provided by law in the EU. At the same time, the methods which a third country invokes with the aim of ensuring such a level of protection may be different from those used within the

[302] Convention 108, Article 12.3.a
[303] See Taylor, M.J., Wallace, S.E. & Prictor, M., United Kingdom: transfers of genomic data to third countries, *Human Genetics* Vol 137 (2018) p.637. https://doi.org/10.1007/s00439-018-1921-0
[304] Art. 45 GDPR, Recitals 103–107 and 169
[305] Art. 46 GDPR, Recitals 108–110 and 114,
[306] Art. 49 GDPR
[307] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015, para. 96.

EU, as the adequacy standard does not require the exact reflection of EU rules.[308] The European Commission assesses the level of data protection in foreign countries where data has to be transferred by looking at their national law and applicable international obligations.[309]

Although an adequacy approach is the most preferred and usually reassuring basis for international data transfer, it has three visible weaknesses:[310]

1. Very few countries have been approved by European Commission so far.[311]
2. Even when working in a country with an approved mechanism (when the adequacy decision is confined to specific sectors), the mechanisms that have been approved as adequate in countries like Canada and the United States only cover the entities which are subject to those mechanisms.
3. Those who rely on adequacy cannot hope that once approved, their adequacy decision will remain in place indefinitely. Because, first adequacy decisions are subject to monitoring on an ongoing basis as the European Commission regularly reviews such decisions to track developments that could affect their status. And if the European Commission finds that the third country or international organisation no longer meet the conditions justifying the adequacy decision, it can amend, suspend or repeal the decision.[312]

   Second, it has become clear after the Schrems case that national supervisory authorities will still have the competence to examine the claim of a person concerning the protection of their personal data which has been transferred to a third country classified by the Commission's adequacy decision as having an appropriate level of protection, where that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[313]

EU-US data transfer rules:

[308] *Ibid*. para. 74. See also, European Commission (2017), Communication from the Commission to the European Parliament and the Council "Exchanging and Protection Personal Data in a Globalised World", COM(2017)7 final of 10 January 2017, p. 6.
[309] Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p 34
[310] Philips, M., International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), *Human Genetics*, Volume 137, Vol 8, (2018) pp 575–582
[311] To date, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations falling under the scope of the Personal Information and Electronic Documents Act – PIPEDA), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection. Also, the United States of America (limited to the Privacy Shield framework) as providing adequate protection.
[312] Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p 34
[313] CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner [GC], 6 October 2015, paras. 63 and 65–66

In the 2015 Schrems case, the CJEU declared the European Commission's 2000 decision on the 'adequacy' of the EU-US Safe Harbour regime, which previously formed the legal basis for data transfers from the EU to the USA, invalid.[314] The reasoning of the Court relied on the equivalence conception which is for measuring the level of similarity of data protection between a third country in question, and the EU. The Court invalidated the Commission's Safe Harbour adequacy decision as it had several shortcomings, which compromised EU citizens' fundamental rights to the protection of privacy, the protection of personal data and the right to an effective legal remedy. More specifically, it did not contain any explanation/provision regarding the existence in the USA laws and practices limiting interference on the right to privacy and data protection (e.g. interference by public authorities for security purposes), nor effective judicial remedies for individuals. According to the judgement, laws which establish exceptions (e.g. measurers to be undertaken for security purposes) which can interfere with fundamental rights should set forth clear and precise rules regarding the scope and application of the measure, and minimum safeguards against the risk of abuse, including unlawful access and further use of such data.[315]

Thus in 2016, the European Commission and the USA adopted a new framework for transatlantic exchange of personal data, known as the Privacy Shield, to replace the Safe Harbour regime.[316] Like the Safe Harbour regime, the EU-US Privacy Shield framework aims to protect personal data that are transferred from the EU to the US for commercial purposes. US companies can voluntarily self-certify their adherence to the Privacy Shield list by committing to meet the framework's data protection standards. The competent US authorities monitor and verify the compliance of the certified companies with these standards.

As of September 2018 (the timing of the second annual review of the Privacy Shield framework) 4200 companies had subscribed to the new framework, and the US Federal Trade Commission triggered more than 50 cases of non-compliance with the Privacy Shield. In the second joint annual review of the Privacy Shield regime the Commission concluded that:

> "T]he United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States.

[314] The Privacy Shield, In-depth Analysis, European Parliamentary Research Service, 2018
[315] The Privacy Shield, In-depth Analysis, European Parliamentary Research Service, 2018
[316] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207. The Article 29 Working Party commended the improvements brought by the Privacy Shield mechanism compared to the Safe Harbour decision. See Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 16/EN WP 238.

> In particular, the steps taken to implement the Commission's recommendations following the first annual review have improved several aspects of the practical functioning of the framework in order to ensure that the level of protection of natural persons guaranteed by the adequacy decision is not undermined"

To sum-up data protection is strongly regulated area in Europe. Both on a fundamental rights level and on a lower regulatory level, it is now treated as an independent doctrine from the right to privacy. As such there are strict regulations in place for collecting, storing and sharing the personal data. However, there is a gap between legal language and technological development.

4.3 Constitutional, statutory and tort law (common law) protection of privacy in the U.S.

In the U.S. information privacy law concerns constitutional law at state and federal level, federal and state statutory laws, common law as emerged in tort law, evidentiary privileges, property law, contract law and criminal law. A landmark article written by Supreme Court Justice Brandeis at Harvard Law Review in 1890 is widely credited as establishing the right to privacy, i.e. "the right to be let alone" as a tradition of common law in the U.S.

The term "privacy" does not appear in the U.S. Constitution or the Bill of Rights. Nevertheless, the US Constitution, particularly the Fourth Amendment, is often invoked as a foundational source of the "right to privacy." And the U.S. Supreme Court has ruled in favor of various privacy interests-deducting the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution.[317] However, any constitutional protection of privacy afforded to individuals is restricted to state action and does not apply to private industry, where information is collected and stored. The Constitution in general only applies to governmental actors and not to private individuals or entities which was the view of the Supreme Court in *Whalen v. Roe case* when first time the Supreme Court mentioned the right to information privacy in 1977. It noted that the Constitution protected two kinds of individual interests: "*One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions*". After that decision, a number of decisions pursued which

[317] In Griswold v. Connecticut, (381 U.S. 479 1965) the Court reasoned that such a right is found in the "penumbras" as many as the ten amendments of the Bill of Rights.

ruled to interpret certain aspects of the rights to privacy, for creating precedence at state level courts. As such a lot of the law protecting confidentiality is not set out in statute but has evolved through legal judgments. However, albeit some lower courts have recognized a constitutional right to keep personal facts private,[318] other courts noted the Supreme Court's failure to explicitly acknowledge that the Constitution protects the right to privacy of medical information.[319]

The Warren and Bandies privacy *torts* (mostly *public disclosure of private fact* and *intrusion upon seclusion*, and *appropriation of name or likeness*) protect medical information in tort law.

As defined by the Restatement of Torts, intrusion upon seclusion provides: [320]

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The tort of public disclosure of private facts provides: [321]

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

Appropriation torts is explained as below in the Restatement:

> One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.[322]

Besides the Warren and Brandeis privacy torts, the tort of *breach of confidentiality* has been developed to protect disclosures of information in violation of trust within professional relationships. In particular the concept of breach of confidentiality is used in medical ethics and law. For example, in 1920, in *Simonsen v. Swenson*, the court hold that

[318] Wyatt v. Fletcher, 718 F.3d 496, 505 (5th Cir. 2013).
[319] Nunes v. Mass. Dep't of Corr., 766 F.3d 136, 144 (1st Cir.)
[320] Restatement (Second) of Torts § 652b.
[321] Restatement (Second) of Torts § 652d.
[322] Restatement (Second) of Torts § 652c

> [t]he relation of physician and patient is necessarily a highly confidential one. It is often necessary for the patient to give information about himself which would be most embarrassing or harmful to him if given general circulation. This information the physician is bound, not only upon his own professional honor and the ethics of his high profession, to keep secret. ... A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong.[323]

In the Simonsen v Swenson case court concluded that *the breach of confidentiality tort* is not absolute, and it does not apply when disclosure is mandated by statutory law or when disclosure is for safeguarding the health and safety of others. In some other cases, courts ruled that because *the breach of confidentiality* tort emerges from the patient-physician relationship, similar to a fiduciary one, the tort extends to a third party who "*induces a breach of a trustee's duty of loyalty, or participates in such a breach, or knowingly accepts any benefit from such a breach, becomes directly liable to the aggrieved party.*"[324]Also, *intentional infliction of emotional distress* and *negligence torts* can be invoked in US courts when medical information is disclosed unlawfully.

Thus, tort law has been well developed to protect confidential health information in medical law.

At state level almost all states recognize tort liability for instances where physicians disclose a patient's medical information.[325]

When it comes to statutory law, the US mostly takes a sectoral approach to privacy legislation. There are only few statutory acts which can be considered having more or less overarching effect, which are described below.

In mid XX century, the growing number of government agencies at federal as well as state level and the expanding regulatory scope of the administrative state formed an opinion that government records should be open to the public. Therefore, in 1966, the Freedom of Information Act (FOIA) was adopted to grant American people the right to access the records kept about them by any government agency. Thus, under the FOIA, "any person" may request "records" maintained by an executive agency without showing the reason for requesting the records.[326]

[323] Simonsen v. Swenson, 177 N.W. Neb. 1920, at 832
[324] Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793 (D. Ohio 1965).
[325] Schwartz and Solove, Information Privacy Law, Aspen Publishing Co. 2018
[326] United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 771 (1989)

The increasing electronation of information and collection of voluminous personal data in the depositories of federal government agencies again raised some concern. To address this concern in 1973, the United States Department of Health Education and Welfare (HEW) prepared the Report on "Records, Computers, and the Rights of Citizens." The HEW report's finding was, *inter alia*:

> [A]n individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often, he may not know it, much less contest its accuracy, control its dissemination, or challenge its use by others.[327]

The report recommended the passage of a code of Fair Information Practices:

> • There must be no personal data record-keeping systems whose very existence is secret.
>
> • There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> • There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> •There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> •Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent mis- use of the data.[328]

As also mentioned by Prof. Solove and Prof. Rotenberg, the Fair Information Practices Principles (FIPPs) which "*played a significant role in framing privacy laws in the United States*" influenced the formation of privacy laws around the world.[329] For example, the OECD Privacy Guidelines were adopted based on these Fair Information Practices. The recent EU law- the GDPR also significantly benefited from the Fair Information Practices Principles.

---

[327] U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems 29 (1973)

[328] U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems 29 (1973), 41-42

[329] Rotenberg, M., Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), *Stanford Technical Law Review*. Vol 1 No44 2001; Solove, D., A Brief History of Information Privacy Law, *George Washington University Law School*, 2006.

The Privacy Act is one of the oldest federal privacy laws. Despite its rather broad name, it applies only to collection, maintenance, use, and dissemination of personal data by federal agencies. Nevertheless, it can be considered the most comprehensive document to structure data processing in the public sector in the US.[330] The Privacy Act is underpinned by FIPPs,[331] which is similar to the conditions for legitimate data processing set out in EU legislation.[332]

Although the Privacy Act made important efforts in bringing government information systems under unified control, the Act has a number of shortcomings. As mentioned above it does not apply to the private sector. But it does not even apply to State or local agencies. Another weakness of the Privacy Act is the "routine use" exception where information may be disclosed for any "routine use" if disclosure is "compatible" with the purpose for which the agency collected the information. Many privacy scholars have criticized the "routine use" exception as a biggest shortcoming.[333]

The Privacy Act also attempted to restrict the use of Social Service Numbers as the preceding HEW report noted that there was "an increasing tendency" for the SSN to be used as a standard universal identifier.[334] The Privacy Act tried to "*curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers*."[335] The Privacy Act did not restrict the use of SSNs by the private sector as it did not apply to private sector. As a result, the use of SSNs continued to be used frequently. Nowadays, SSNs are even used as a password to access different public accounts (such as banks, hospitals, universities, etc.).

The Privacy Act along with FOIA also provide some protection for *health care records* maintained by the federal government. Health data cannot be disclosed unless the individual has provided consent, or one of the twelve statutory exceptions apply. Some of the exceptions applicable in health sector can be "*statistical research*". Another is "*routine uses"* which has been mentioned above. If a data was collected with research in mind, it may fall under a "routine uses" exception, being equal to "*the use of such record for a purpose which is compatible with the purpose for*

[330] Schwartz, K., and Solove D., Information Privacy Law, Aspen Publishing Co. 2018
[331] These principles are set out in 5 USC § 552a(e).
[332] Article 5 GDPR.
[333] Solove A Brief History of Information Privacy Law, George Washington University Law School, 2006.
[334] U.S. Dep't of Health, Education, and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers, and the Rights of Citizens, 1973
[335] Doyle v. Wilson, 529 F. Supp. 1343, 1348 D. Del. 1982.

which it was collected." On the other hand, the Privacy Act requires a federal agency to maintain data only to the level "relevant and necessary" to accomplish an agency purpose.

Several federal statutes and regulations provide additional protection of privacy to the specific field of data they control, such as COPPA, HIPAA, GLBA. Privacy provisions can also appear as incidental parts within a broader statute whose main purpose is unrelated to privacy. For instance, within the chapter of the federal US Code that authorises the creation of the Public Health Service, there is a provision on privacy. A section in the chapter on "General provisions respecting effectiveness, efficiency, and quality of health services" contains a special subsection regulating the protection of personal information obtained for research purposes by the National Centers for Health Services and for Health Statistics.[336]

Until the Health Insurance Portability and Accountability Act (HIPAA) of 1996 adopted regulation of privacy in health sector was a concern of the States. It was the first comprehensive US federal Department of Health and Human Services guideline for the protection of the privacy of "*protected health information*" (PHI). The HIPAA privacy regulations[337]- known collectively as the "Privacy Rule" which came into force in 2003, are based on FIPPs and set forth rules governing the access, use, and disclosure of personal health information (or PHI), by "covered entities",[338] which include healthcare providers[339] (e.g. hospitals, laboratories, pharmacies,), health plans[340] and healthcare clearinghouses.[341] The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH Act) expanded HIPAA's scope to include the "business associates" additional to covered entities. A business associate is a person or an organization, other than a workforce member of a covered entity, that performs certain functions on behalf of, or provides certain

[336] United States: Code of federal regulations. title 45: public welfare. part 164: security and privacy. http://www.ecfr.gov/cgi- bin/text- idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl (2014).
[337] *The Privacy Rule*, which sets national standards for when protected health information (PHI) may be used and disclosed; *The Security Rule*, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) and *the Enforcement Rule* contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules.
[338] Code of Federal Regulations (CFR) Title 45, Section 160.103.
[339] *Covered Health Care Provider*: Any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard, such as: Chiropractors, Clinics, Dentists, Doctors, Nursing homes, Pharmacies, Psychologists
[340] *Health Plan:* Any individual or group plan that provides or pays the cost of health care, such as: Company health plans Health insurance companies; Government programs that pay Health maintenance organizations (HMOs) for health care, such as Medicare, Medicaid, and the military and veterans' health care programs.
[341] *Health Care Clearinghouse:* A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa, in other word processes health information into various formats, such as: billing services, repricing company's community health management, value-added networks information systems

services to, a covered entity that involve access to PHI.[342] The business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate. Business associates provide services to covered entities that include accreditation, billing, claims processing, legal or business consulting, data analysis, cloud services, other administration, etc. Subcontractors are also covered meaning a covered entity can be a business associate of another covered entity. If a covered entity enlists service of a business associate, then a contract or other written arrangement between them shall be made. [343] The contract must establish the permitted and required uses and disclosures of protected health information by the business associate and provide appropriate safeguards with regard to electronic protected health information.[344]

HIPAA provides that a covered entity may not use or disclose PHI except either (1) as permitted by the Privacy Rule, or (2) as authorised in writing by the individual who is the subject of the information (or the individual's personal representative). The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes: For example: when required by law, public health activities reporting abuse or domestic violence; health oversight activities; judicial and administrative proceedings, etc.

It should be noted that HIPAA does not create a broad exception for research, rather uses exception of "research, under certain conditions". More specific provision about the use of research data is in the Regulations written by the Department of Health and Human Services (DHHS) for federally funded research with human subjects (the "Common Rule"). According to the Common Rule researchers must generally get consent from subjects or obtain an Institutional Review Board waiver to use identifiable data.

The Privacy Rule applies to identifiable health information in paper or electronic form.[345] HIPAA defines information as identifiable when "*there is a reasonable basis to believe the information can be used to identify* [an] *individual*". HIPAA is one of very few data privacy laws in the world

[342] Code of Federal Regulations (CFR) Title 45, Section 160.103.
[343] HHS.gov, Health Information Privacy https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html, last accessed on 19 September 2019
[344] 45 CFR 164.504(e)
[345] The HIPAA Security Rule establishes national standards to protect individuals' *electronic* personal health information that is created, received, used, or maintained by a covered entity.

that address data de-identification in technical detail. It defines, on the one hand, individually identifiable health information and, on the other hand, provides a list of 18 precisely named identifiers that shall be removed in order to achieve de-identified data. There are no restrictions on the use of de-identified (in other words, anonymous) data.

With 2009 HITECH Act, a breach notification requirement was added to HIPAA. The Breach Notification Rule requires covered entities to notify affected individuals; HHS and, in some cases, the media of a breach of unsecured PHI. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.[346]

Most notifications must be provided without unreasonable delay and no later than 60 days following the breach discovery. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.[347]

There are three exceptions to the definition of "breach." The first exception applies to the unintentional access or use of protected health information by an employee of a covered entity or business associate, if such access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at covered entities or business associates. In both cases, the information cannot be further used or disclosed in a manner not

[346] HHS.gov Health Information Privacy https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, last accessed on 22 September 2019
[347] HIPAA Basics for Providers: Privacy, Security, And Breach Notification Rules, MLN Factsheet 2018

permitted by the Privacy Rule. Third, if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.[348]

HIPAA is oversighted by the Office for Civil Rights (OCR) in HHS. Also, state attorneys general may enforce HIPAA, when there is a violation of its provisions.

It should be deducted from review of US federal law applicable to medical data that while it protects medical information and generally guards against unfair or deceptive practices, neither clinical nor research health information protection structures contain specific rules or standards to limit access to BCI-generated data.

Privacy protection at the State level

At the state level, Georgia Supreme Court's Decision in Pavesich represented the first time any high instance court recognized an independent constitutional right to privacy.

In Pavesich v. New England Life Ins. Co., the Supreme Court ruled the State's residents to have a "liberty of privacy" guaranteed by the Georgia State's constitutional provision: "no person shall be deprived of liberty except by due process of law." The court grounded the right to privacy in the doctrine of natural law as below:
"*The right of privacy has its foundations in the instincts of nature. It is recognized intuitively, consciousness being witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private and there are matters public so far as the individual is concerned. Each individual as instinctively resents any encroachment by the public upon his rights which are of a private nature as he does the withdrawal of those rights which are of a public nature. A right of privacy in matters purely private is therefore derived from natural law*."[349]

Over the next five decades after the decision, the majority of American states adopted the principle of an individual right to privacy, either by express constitutional provisions or by interpretation of

[348]HHS.gov Health Information Privacy, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, last accessed on 24 September 2019

[349] Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905) para69

existing constitutional language. Currently, at least 10 States' constitutions include an explicit right of privacy which also have data protection implications. In addition, almost all states have laws that address the individual's interest in knowing when the security of his/her data has been breached. Some state privacy laws apply to all industry sectors and all types of personal data, others fill gaps in federal protection. Some states have gone further than the federal government in creating an area of data protection.[350] With regard to health data, some states have passed laws requiring encryption or other security measures for medical data. For example, Kentucky requires security procedures and practices to maintain the confidentiality of personal information and have breach notification law that was adopted even before HITECH.[351] The State of Maine also has a law declaring the confidentiality of health information including genetic information.

State laws also provide more comprehensive protection for research subjects, than at federal level. California, Maryland, New York, and Virginia have laws that apply the Federal Common Rule to all research with human subjects in the state, regardless of funding.[352] Illinois and New Jersey require hospitals patients to be informed whether they are enrolled as research subjects.[353] Some other states adopted laws allowing genetic research on human specimens after the deidentification of samples have been carried out.[354]

In January 2013, the US Federal Register published omnibus amendments made by the DHHS to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules to establish uniform minimum standards[355] by covering holders of health information as broadly as possible[356] and consequently to avoid divergences at the level of health information protection afforded by different States. Nevertheless, the terrain of State health privacy law remains uneven.

---

[350] For example, California has passed a new Consumer Privacy Act which is at some parts similar to the GDPR. What lacks in it is a deadline for notifying consumers of a data breach, also hefty fines for data breaches foreseen in the GDPR

[351] Ky. Rev. Stat. § 61.932(1)(a)./ 933

[352] California. Health & Safety Code § 24175, Maryland. Code Ann., Health-Gen. § 13-2002, N.Y. Pub. Health §§ 2442, 2444, Virginia Code Ann. §§ 32.1-162.16 to 32.1-162.2 cited in Biobanking Research and Privacy Laws in the United States Heather, L. Harrell and Mark A. Rothstein, The Journal of Law, Medicine & Ethics, 44 (2016)

[353] Illinois Comp. Stat. § 50/3.1(a) and New Jersey Stat. Ann. § 26:14-4.

[354] Arkansas Code § 20-35-103; Colorado. Rev. Stat. §10-3-1104.6(4); Georgia. Rev. Code §§ 33-54-3; Georgia. Rev. Code §§ 33-54-6; Maine. Rev. State. Ann. tit. 22, § 1711-C; New Mexico Stat. Ann. § 24-21-3.

[355] HIPAA provides that its regulations "*shall not supersede a contrary provision of a State Law, if a provision of the State Law imposes requirements, standards or implementation specifications that are more stringent than the requirements, standards or implementation specifications imposed under the regulation.* A standard is more "*stringent*" if it "*provides greater privacy protection for the individual who is the subject of individually identifiable health information"* than the standard in the regulation.

[356] It should be noted that the use of patient data outside of the healthcare context by private entities, is not covered under HIPAA.

Conclusion

From a comparative perspective, European regulations are quite advanced, setting a unified, high level of data protection. In the United States the emphasis is more on sectoral based self-regulatory approaches. EU data protections laws require a sound legal basis to process personal data, while US health privacy law or research acts typically doesn't have any such limitations, but they require authorization by relevant State bodies. Based on adequacy approach, EU law have restrictions on cross-border transfer. Additionally, the EU legislative framework has higher level of threshold of ensuring valid consent in data sharing.

As such, at first glance, data protection seems to be highly regulated area in Europe. Both on a fundamental rights level and on a lower regulatory level, and with the adoption of the GDPR it is now treated as an independent doctrine from the right to privacy. There are stricter regulations in place for collecting, storing and sharing the personal data than it used to be before.

However, as in the U.S., the EU also applies distinct rules to processing of data in some sectors, naturally for purposes of national security within Common Foreign and Security Policy and Police and Judicial Cooperation. Besides, the public sector benefits from significant exceptions to EU data protection regulation too. Also, there is a visible gap between legal language and technological development, and fragmentation among national standards of data protection in the EU region.

The CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) to date is the only legally binding international instrument in the data protection field applied in whole European continent. Although the ECHR with its Article 8 and the precedent creating jurisprudence of the European Court of Human Rights provides protection for the right to privacy by also evolving its coverage over the decades to encompass not only the right to private and family life, but also privacy of many other values such as freedom of holding opinions, privacy of thought, autonomy, even data protection which also include the protection of health data, the scope of the ECHR is mainly limited to State actors.

The newly adopted GDPR does not fully harmonise the law on data protection in Europe as it grants the member states a wide margin of manoeuvre with regard to providing exceptions to data protection. Besides, in the EU, the legislation covering healthcare remains in the competence of each member state and is thus falls outside the scope of EU law- that means health data protection during the clinical treatment are too regulated at the national level and these legislative differences between member states may be detrimental to the patient data protection during provision of cross-border health-care and formulation of the unified approach to the protection of brain data.

When it comes to the GDPR, it raises the bar for consent. Recital 32 and article 4.11 give a definition: consent means freely given, specific, informed and unambiguous - indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. In order to obtain freely given consent, it must be given on a voluntary basis. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR.

The GDPR brings new safeguards to the data protection such as to data portability and the right to erasure, specific provisions on the processing of data relating to children; obligations of data protection by design and default, etc.

However, in structure, the GDPR is similar to the Data Protection Directive, laws remain basically the same, but the technologies that it aims to regulate are changed prominently. For instance, the GDPR does not apply to anonymous data. But with the development of new technologies, there are three major limits to anonymisation:

First, With the development of new technologies, de-identification (and re-identification) techniques is rapidly changing which makes it challenging to precisely put down a specific standard for anonymization in law.[357]

Second, data privacy research is now making clear that although a dataset may be anonymised according to conventional approaches, its cross-linking with data available elsewhere using modern technologies can make it possible to infer data subjects' identities. Therefore, although

[357] Dove, E., and Phillips, M., Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, Springer 2015

anonymisation techniques makes re-identification less likely, they do not guarantee anonymity, especially in large datasets. [358]

Third, as the context of medical confidentiality is changing with the development of precision medicine and e-health technology; our expectations about medical treatment will require greater linkages of data. Also, in nowadays international collaboration and long-term research projects, re-searchers or clinicians may want to link medical data to other data sources over time. Thus, while anonymisation may be used for achieving stronger data privacy protection, in the medical data context it offers only limited utility to both researchers and patient-participants alike.[359]

With regard to neuro-data collected during BCI treatment, GDPR remains silent. Although genetic and biometric data have been added to the list of "special categories of data", neither in main text nor in recitals, there is not any referral either **to neuro-data or of any examples of the data derived from recent neuro-technological advancements**. Only in Recital 78 protection of personal data and privacy in a broader sense can be linked to technology: "*The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met*".

Additionally, in BCI application, where data collection is automated and clinical care or research teams are large consisting of neuroscientists, neurotechnologists, computer scientists, clinicians, bioethicists there is an additional challenge in identifying the data controller - who holds responsibility for ensuring the lawful processing of data under the GDPR, and ensuring everyone involved in experimental research or therapy understand the extent of their legal responsibilities.

[358] Expert Advisory Group on Data Access: Statement for EAGDA funders on re-identification. http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtp055972.pdf (2013).
[359] Dove, E., and Phillips, M., Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, 2015

Chapter V Medical Law and Ethics applicable to BCI

5.1 Regulating the development of therapeutic BCI

The regulatory framework on medical devices govern the entry of the technologies into the market, including the clinical investigations preceding this and post-market surveillance. By providing an analysis of the relevant legislative framework in Europe and the United States, I look at whether current regulatory provisions are effective and proportionate to the requirements of protecting patients' safety, autonomy and in particular privacy while also facilitating technological and scientific innovation in medicine. Through this review, the current regulatory gap or deficiency in the present system of device regulation (covering pre-clinical and clinical testing, marketing approval and post-market surveillance) are identified.

The medical device industry is a complex with abundant definitions for the expression of 'medical device' and several tired regulations and standards at international, regional and national levels applicable to devices along with the existence of a number of different agencies designed for evaluating devices before commercialization. An implantable neural computer interface, a type of novice medical devices, constitutes a complex set of applications since its use involves interacting with the most important and vulnerable human faculties, thus raising a number of ethical, legal and social concerns.

Before, in Europe, each country had its own legislation, and a device's registration was different in Member States. After 90th, three main pieces of legislation were adopted to regulate medical devices: the Medical Devices Directive 93/42/EEC (*hereinafter*, MDD), Active Implantable Device Directive 90/385/EEC (*hereinafter*, AIMDD), and *In vitro* Diagnostic Devices Directive 98/79/EC. These directives were transposed to each member state's legislation to bring them into line with the objectives of the Directives. Further to ensure the uniform application of the directives, EC has issued legally nonbinding documents - the form of guidance documents. As such the EU regime applying to medical devices[360] pursues a historical objective of securing a harmonised European market to remove technical barriers and safeguard public health.

[360] EU also adopted several additional documents either to provide further guidance on a specific topic or to regulate certain types of devices. See e.g. Directive 2001/95/EC of 3 December 2001 on General Product Safety, EU Commission Regulation No 207/2012 of 9 March 2012 on Electronic Instructions for Use of Medical Devices,

However, related regulations are too broad and wide-ranging to adequately address the particular technical characteristics and potential for harm or abuse that the devices might exhibit. For instance, having been adopted in 1990, the AIMDD, which is *lex specialis* for BCIs using implanted electrodes, is even older than the general MDD. Therefore, it cannot take into account the latest therapeutic tools developed in implantable neuro-modulation.[361] In fact, the AIMDD itself does not even include a classification of medical devices into three categories according to the level of risks they pose, mentioned in the general MDD and thus there is no stricter requirements for class III devices in the AIMDD, which is the highest class of risk.[362]

The regulatory obligations put upon manufacturers differ between EU countries in a number of aspects, for instance pre-market oversight of medical devices in Europe is decentralised. Concerns regarding effective oversight of medical devices apply especially to invasive neurodevices such as DBS and BCI, as there is uncertainty about long-term and unintended effects of these devices which might pose greater risks to patients' safety and autonomy.[363]

Pre-market scrutiny of neuro-devices is light - touch, in terms of what the evidence manufacturers must supply to demonstrate that their products conform to statutory safety and performance requirements. Due to the nature of BCI, there is uncertainty about the benefits, risks and mechanisms for achieving desired effects, yet the regulation of medical devices does not itself encourage collection of extensive clinical evidence.[364] The clinical testing needed to set up such devices cannot easily be accommodated within the current legislation as Clinical Trial Directive 2001/20/EC[365] applies only to trials involving medicinal products, i.e. to drugs, not to clinical investigations involving medical devices. Currently, clinical investigations, which differ from standard clinical trials, are poorly defined in the Medical Device and Active Implantable Medical Device Directives. Due to under-regulation, not only patients' or research participants' interests in

Directive 93/42/EEC as Regards Medical Devices Incorporating Stable Derivatives of Human Blood or Human Plasma.

[361] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015

[362] But in Annex IX of the MDD implantable devices are classified as III category- the category with the highest risk.

[363] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013,

[364] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013

[365] Although the EU Clinical Trials Regulation No 536 entered into force in 2014, its application depends on confirmation of full functionality of the Clinical Trials Information System (CTIS) through an independent audit. The Regulation becomes applicable only after six months the European Commission publishes notice of this confirmation, which is yet to happen.

having safe and effective treatment are not meet appropriately, but also the therapeutic potential of novel types of devices cannot be fully exploited, and accordingly their clinical availability may be delayed.

However, the EU has revised the medical device regulatory scheme with the adoption of the Medical Device Regulations[366] which will be fully applicable in a year. After the full enforcement the Regulations will increase patient's safety by introducing a number of measures such as enhancing requirements for clinical investigations, at the same time introducing provisions to promote innovation and device development such as harmonisation of the works carried out by notified bodies all over Europe through reinforcement of the criteria for the designation of and control over notified bodies.

In the USA, the first regulatory system for medical devices was created in 1976 when the Medical Device Amendments assigned the Food and Drug Administration (FDA) with the responsibility to oversight the field.[367] Currently, most of the regulations are found in Title 21: Code of Federal Regulations Part 800 to Part 1299 and are enforced by the FDA.

More specifically, within the FDA, the Center for Devices and Radiological Health (CDRH) was created to control the approval and manufacture of all medical devices marketed in the USA and set the relevant regulatory standards for investigation of new devices.

The mission of the CDRH is to achieve a balance between stimulation of medical device innovation and protection of public health and promotion of ethical standards (such as respect for privacy and autonomy).

Unlike FDA drug regulation, which is mostly about the actual drug approval process,[368] CDRH regulations also extend beyond the regulatory approval process to cover the post-market period - after the devices have been sold and are actually being used.[369] Continuing regulation is a key

[366] Medical Devices Regulation (EU) 2017/745 (MDR) and In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR)
[367] Medical Device Act Amendments of 1976, Pub. L. 94-295, 90 Stat. 539 (May 28, 1976)
[368]FDCA, 21 U.S.C. § 355 (2006) (describing approval requirements for New Drug Applications)
[369] Such as postmarket surveillance and medical device reporting ("MDR").

feature of the US law which makes it especially appropriate for the uncertainty characteristic to the developments of novel neuro-technologies including brain-computer interfaces. [370]

In Europe, the responsibility for the regulatory cycle is assigned to competent authorities (CAs) and third-party certification organizations (private entities) – notified bodies (NBs).

A CA is a body with the authority to act on behalf of the government to ensure that the requirements of the EU medical device provisions are met. The jurisdiction of each CA is limited to the country in which it was created,[371] however they liaise with European agencies, share information among themselves and reach common ground on important issues. CAs are responsible for appointing and supervising Notified Bodies and monitoring the safety of medical devices after they are placed on the market and evaluating adverse incidents.

A notified body is an organisation designated by an EU country to assess the conformity of medical devices before being placed on the market. Notified bodies are authorised to ensure that manufacturers of medical devices have the required technical documentation and perform quality control for processes and products that may pose a significant risk. The CE mark is awarded by a Notified Body. Each Notified Body has specific areas of expertise and is permitted to carry out assessment of medical devices based on their competency. Device manufacturers can choose which competent notified body they want to approach for the certification process throughout Europe.

All notified bodies are listed on the EU Commission's New Approach Notified and Designated Organizations website. Notified bodies listed on this website along with passing a national assessment are evaluated by independent assessment experts from the EU Commission. There are currently more than 80 notified bodies in the EU member states.

Until the expected date of full application of the new Regulations - 26 May 2020, medical devices can continue to be certified and placed on the market according to the current Directives.

[370] Chan, E., The Food and Drug Administration and the Future of Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement, *John Marshall Journal of Computer & Information Law*, Vol 25, 2007

[371] In Italy, the CA is the Ministry of Labour, Health and Social Affairs – Department of Innovation Directorate General of Medicine and Medical Devices

Alternatively manufactures can, on a voluntary basis, certify their devices to the new Regulations ahead of the date of full application.

The requirements which must be fulfilled before being designated as a notified body under the new Regulations have been increased. These new requirements that set out in Annex VII of the Medical Devices Regulation are divided into four categories:

- organisational and general requirements,
- quality management requirements,
- resource requirements;
- process requirements.

Notified Bodies are accountable for assessing medium-risk and high-risk medical devices before the products are placed on the market in the EU. With the implementation of the new Medical Devices Regulation, the notified bodies will additionally get a right as well as duty to perform unannounced on-site audits of medical device manufacturers.

The designation process of notified bodies under the new Regulations should take up to 18 months. Only after that notified bodies are themselves designated, they can begin to certify devices according to the new Regulations.

The medical devices regulations not only confirm the device's safety and/or effectiveness for the intended treatment but also guarantee that they meet established quality standards. Those standards are created by international organisations- the International Organization for Standardization (ISO) and the Association for the Advancement of Medical Instrumentation (AAMI).

In the USA, the quality systems for FDA-regulated products are known as Current Good Manufacturing Practices (CGMPs). Medical devices must abide by the Quality System Regulations– QSR CFR Part 820 – which is based on ISO 9001 and ISO 13485.

In the European Union, a medical device is awarded a CE mark for being able to be marketed in EU. For obtaining EC mark, the quality management systems are described in the Annexes II and V of the Medical Device Directives. These annexes do not refer to the type of quality insurance

system as such, but it generally agreed that Annex II is equivalent to ISO 9001 plus ISO 13485, and Annex V is equivalent to ISO 9001 plus ISO 13485 without any design control.[372]

5.1.1 Definition of "medical device"

The Global Harmonization Task Force (GHTF) was formed in 1993 with the goal to achieve uniformity in standards and national regulatory practices related to the safety, performance and quality of medical devices. The Global Harmonization Task Force has proposed the following harmonized definition for medical devices:[373]

"Medical device" means any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purposes of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury
- investigation, replacement, modification, or support of the anatomy or of a physiological process
- supporting or sustaining life and …
- providing information for medical purposes by means of in vitro examination of specimens derived from the human body and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.

Although some countries (such as Japan, Australia) use definitions similar to the GHTF one, a unique definition of medical device has not been agreed yet and currently various definitions for the expression of 'medical device' coexist. For instance, in the USA, pursuant to section 201(h) of the Food Drug and Cosmetic Act the device is:

"an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,

[372] Santos et al, Medical device specificities: opportunities for a dedicated product development methodology, *Expert Review Medical Devices*, Vol 9, 2012
[373] See GHTF document SG1/N029R11

- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or

- intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and

which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o).

BCI definitely falls within the general definition of "device" which is "an instrument, apparatus, implement, machine, *implant*" intended for use either in "the diagnosis ... treatment, or prevention of disease" or "to affect the structure or any function of the body".

In Europe, the current definition differs from GHTF which is defined in Article 1.2 of the Medical Devices Directive (93/42/EEC) as "*...any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation or compensation of an injury or handicap,*
- *investigation, replacement or monitoring of the anatomy or a physiological process,*
- *control of conception."*

BCI is however, covered with the specific legislation, the Active Implantable Device Directive which uses similar definition for general medical device, but goes further to specify the active implantable device as:

> any active medical device which is intended to be totally or partially introduced, surgically or medically, into the human body or by medical intervention into a natural orifice, and which is intended to remain after the procedure;

As implantable medical devices are considered to be 'high risk' due to their invasive nature, the pre-market regulatory oversight of this type of medical devices is relatively more demanding than the ones not listed in high risk category, for instance the pathways for assessing conformity with the legislation is more nuanced. But the existing legislation still have huge shortcomings (e.g.

demonstration of equivalence with existing devices should not be considered as sufficient justification" for relying on existing clinical data)[374], some of which will be rectified with the application of the new Medical Devices Regulations.

Although there are differences among the GHTF, European and U.S definitions, they all cover a wide range of products and have many common points in that they regulate the device's full lifecycle.

For example, in the US definition, despite the fact that the word software is omitted, the US FDA is responsible for regulating these products too.[375]

According to the GHTF and the European definitions, manufacturers define the device's intended use. The European Court of Justice confirmed that the intended purpose of the device, has to be specifically defined by the manufacturer as being for medical use in order to fall within the field of application of the Medical Devices Directive 93/42/EEC.[376] This also means that raw materials are not considered medical devices, and legislation is only valid when the devices are supplied to the public for medical purposes. Furthermore, the principal intended action declared by the manufacturer defines the field under which the device will be included, as such also defining the legislation to be complied with. Such a narrow interpretation seems to serve the double-edged objective of this legislation, which is to protect the health of patients through a system of certification, but also to ensure the free movement of goods without posing any unjustified restrictions. BCI aimed at human enhancement therefore do not fall within the current MDD regime.

The new Medical Device Regulations, [377] which merges two existing Medical Devices Directives (MDD and AIMDD) into one, brings in conformity the definition with the GHTF one. The definition of medical devices includes any "*implantable"* devices. It also adds "*reagent"* into the list of identifications for medical devices. The intended use is also extended to cover "*prediction*" and *"prognosis".*

[374] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[375] Davey S, Anderson J, Meenan B. An overview of current classification systems for healthcare devices and their limitations, (Multidisciplinary Assessment of Technology Centre for Healthcare (MATCH) Deliverable 2, P1 D2 V2.0 051025, www.match.ac.uk
[376] Case C-219/11, Brain Products GmbH v BioSemi VOF and Others, 22 November 2012
[377] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

Additionally, the new Medical Device Regulations also applies to the groups of products developed without an intended medical purpose but taking into account the state of the art, and in particular existing harmonised standards for analogous devices with a medical purpose, based on similar technology. In Annex XVI it provides the List of Groups of Products Without an Intended Medical Purpose covered by the Regulations. The Regulations requires for certain group of non-medical products enlisted in Annex XVI the application of risk management and, where necessary, clinical evaluation of safety. Paragraph 6 of Annex XVI [378] specifically mentions equipment used for BCI as one of products developed for non-medical use falling into the scope of the Medical Devices Regulation. This provision ensures the same level of safety controls are applied for implantable BCIs used for enhancement purposes.

5.1.2 Classification of medical devices

The nomenclature created by the Global Medical Devices Nomenclature Agency are used by the regulators in the European Economic Area (EEA) to support the conformity assessment process required for CE marking. [379] It divides the medical device product market into different level groups based on device application, technology, or other common characteristics. The standard (ISO 15225) allocates codes for 20 categories (of which 16 are presently allocated) 01 designates Active Implantable Device.

It should be noted there are differences in the classes allocated by Europe and the U.S. – e.g. products considered Class II or III in the USA might carry a different classification in Europe. The risk categorization is associated with the approval process- the higher is the class of the product, the more demanding becomes the process.

The European rules governing device classification are listed in Annex IX of the Medical Device Directive. There are a further 18 rules outlined in Annex IX which lay down the basic principles of classification. These rules are subdivided into four categories: Rules 1-4 (non-invasive devices); Rules 5-8 (invasive devices); Rules 9-12 (active devices); and Rules 13-18 (special rules – devices containing tissue of animal origin, drug-device combinations). The European rules correspond, to a large extent, to the classification rules established by the GMDN User Guide Version 2010.

[378] Equipment intended for brain stimulation that apply electrical currents or magnetic or electromagnetic fields that penetrate the cranium to modify neuronal activity in the brain. Para 6, Annex XVI, The Medical Devices Regulation
[379] Anand K, Saini S, Singh B, Veermaram C. Global medical device nomenclature: the concept for reducing device-related medical errors. Young Pharmaceuticals. 2(4), (2010). pp403–409

The new Medical Device Regulations sets out 22 classification rules which are used to classify devices based on mentioned risk criteria of degree and type of invasiveness, duration of contact with body, site of contact with device, specific characteristics- active/non-active, single use/reusable; combined with medicinal substance; incorporating animal tissues, etc.[380] The application of these rules will depend on the intended purpose of the device and will replace the 18 rules currently used under the MDD. The new rules primarily relate to software, nanomaterials, ingested products, non-viable human tissues, cells and derivatives

Medical devices are classified, on the basis of risks they pose, into four classes i.e. class I, class IIa, class IIb and class III. Risk increases from class I to class III and as mentioned above classification is proposed on the basis of duration and intended use of device, the degree of invasiveness, anatomical part and the patient experience from the use of similar devices. It is the classification of a device which influences pre-market requirements, the conformity assessment route, clinical data requirements as well as post-market obligations.

The manufacturer is responsible for confirming the classification with an established notified body, which will ensure that the conformity assessment procedures are rigorously followed by the manufacturer.

It should also be mentioned that if the product is a "Device Combination", the notified body assess the product to ensure compliance with the Medical Devices Legislation. If the product is a "Drug Combination", the regulatory pathway is determined by medicinal product legislation such as the Community Code relating to medicinal products for human use (Directive 2001/83/EC).

According to an explicit rule, invasive BCI is included in class III, which is the highest class of risk, to which distinct provisions are applied in order to deal with the particular aspects of III class devices and the increased safety challenges they present:[381]

> All implantable devices and long-term surgically invasive devices are in Class IIb unless they are intended:
>
> - — to be placed in the teeth, in which case they are in Class IIa,

[380] Article 51 and Annex VIII, Medical Device Regulation (EU) 2017/745, See also New EU Device Legislation Information Pack, Health Products Regulatory Authority.
[381] Rule 8, Annex IX of the MDD

- — to be used in direct contact with the heart, the central circulatory system or *the central nervous system,* in which case they are in Class III

However, neither the current legislation nor new Medical Devices Regulations does directly address the lack of specific rules for different types of implanted *neural interfaces*, which differ significantly from those related to other types of implants, *inter alia,* require surgery and pose intraoperative risks. As such, implanted neural interfaces, not only carry specific risks associated with the need to perform neurosurgery, but there is a need to monitor the electrodes placed during the operation event after surgery as the follow-up phase, in order to ensure their functioning. They therefore entail both perioperative and postoperative complex management with constant monitoring compared to other treatments.[382] Second, neuro-modulation devices directly and permanently interfaced with the central nervous system may also interfere with the patient's personality and raise issues of responsibility for the actions taken by the patient after the treatment.[383] Third the live-time monitoring and automotive collection, storage and transmission of neuro data from brain presents difficulties for ensuring patient privacy.[384] Further specialty is that, due to its concept of treatment BCIs are operated by research teams consisting of large and diverse professions (e.g. doctors, neuro-engineers, IT specialists, etc.), it is therefore important to employ additional safeguards to limits access to the BCI data.

In the revision process of medical devices legislation the option of introducing a separate model to regulate the most dangerous devices was examined, for example a systematic assessment of conformity, which would take place before launching the device onto the market, instead of a pre-market evaluation. This would have meant that new or high-risk devices as a rule would have been assessed before they were brought to market. However, the option was rejected, because it would have slowed down the access to the market of highly valuable and innovative products.[385] A standard, albeit somehow strengthened pre-market approval along with specific requirements for a post market surveillance and vigilance system have been adopted.

[382] Erica Palmerini, A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015
[383] Experimental tests from deep brain stimulation (DBS) have shown the potential for modifying mood, personality, and cognitive abilities. Synofzik, M., Vosgerau, G., & Voss, M. The experience of agency: An interplay between prediction and postdiction. Frontiers in Psychology, Vol 4, 2013
[384] Chapter 5, Patients and participants: governing the relationships, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[385] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015

In the U.S., FDA has established classifications for approximately 1700 different generic types of devices and grouped them into 16 medical specialties referred to as panels. Each of these generic types of devices is assigned to one of three regulatory classes based on the level of control necessary to assure the safety and effectiveness of the device.[386] It classifies each device into one of three categories based on the amount of risk involved in use of the device, and the level of regulation the FDA will require to ensure the device's safety and effectiveness. This classification depends on both the intended use as well as indications for use of the device.

Devices classified as "Class I" pose the least risk and are subject to the least regulation, while "Class III" devices are the most dangerous and require the highest scrutiny.[387] The FDA relies upon the advice of classification panels comprised of experts from relevant fields in making its classifying decisions.[388]

Class I devices are low-risk, low-complexity devices. The FDA primarily regulates Class I devices through the use of "general controls" very basic provisions governing misbranding, device registration, records and reports, and good manufacturing practices. [389]

Class II devices consist of general controls and special controls. It means they are devices for which general controls are insufficient to ensure safety and effectiveness, but for which available methods exist providing such assurances.[390]

Lastly, Class III contains the most dangerous and complex devices, for which general controls and special controls alone cannot ensure safety and effectiveness. They include devices "represented to be for a use in supporting or sustaining human life" or that present a "potential unreasonable risk of illness or injury. ' [391] For this reason, Class III devices are subject to the FDA's most stringent form of review, Premarket Approval ("PMA"). In addition, the general and special controls regulating the design, labeling, and post-market performance of Class I and II devices apply to

[386] FDCA §513(a), 21 U.S.C. § 360c(a) (2006)
[387] FDCA §513(a), 21 U.S.C. § 360c(a) (2006), Each successive device class is also subject to the regulations for the classes below, such as general controls, special controls, and performance standards.
[388] FDCA § 513(b), 21 U.S.C. § 360c(b) (2006) (directing FDA to assemble classification panels to assist FDA in classifying devices in interstate commerce before May 28, 1976);
[389] Chan, E., The Food and Drug Administration and the Future of Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement, John Marshall Journal of Computer & Information Law, Vol 25, (2007)
[390] Eric Chan, The Food and Drug Administration and the Future of Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement, John Marshall Journal of Computer & Information Law, Vol25 (2007)
[391] FDCA §513 (a)(1)(C), 21 U.S.C. §360c(a)(1)(C) (2006).

Class III devices as well. Examples of Class III devices are replacement heart valves, silicone gel-filled breast implants, and implanted cerebella stimulators. Invasive BCIs are considered to belong to Class III.

The classification of a device will determine the burden of proof the FDA will require to demonstrate its safety and effectiveness for a given indication of use. [392] For this a device must pass one of two regulatory routes: the 510(k) process (simple notification) or the PreMarket Approval (PMA) process, additional to Humanitarian Device Exemption (HDE) and Evaluation of Automatic Class III Designation (De Novo Classification Process) all of which will be discussed below.

The FDA's Product Classification Database contains medical device names and associated information developed by the CDRH in support of its mission to enhance transparency in management of medical device approval and monitoring. It is possible to look up for a device's class and any exemption provided for it and incident reports on this website.[393]

In May 2011, European Commission launched a similar databank – European Database on Medical Devices – but, for now, it is not functioning. The new Medical Devices Regulation and In Vitro Diagnostic Medical Devices Regulation (IVDR) establish a much wider EUDAMED2 database[394] than the existing one under the current Medical Devices Directives.

Currently, the EC database on medical devices, EUDAMED, is a secure web-based portal. It is a central repository for information on market surveillance exchanged between national competent authorities and the European Commission. Its use is restricted to national competent authorities, it is not open for consultation and is not publicly accessible. EUDAMED contains information on registration of manufacturers, authorised representatives and devices, and clinical investigations, also relating to certificates issued, modified, supplemented, suspended, withdrawn or refused, and obtained in accordance with the Medical Device Vigilance System.

However, the new medical devices regulations possess significant improvements including a much larger EUDAMED database. The new rules will only apply after a transitional period of 3 years and 5 years for the regulation on medical devices and for the regulation on in vitro diagnostic

[392] *See* FDCA §513 (f)(1)(A), 21 U.S.C. § 360c(f(1)(A) (2006) (stating 510(k) standard); 21 U.S.C. §360c(a)(C) (2006) (noting that Class III devices are subject to the PMA process of 21 U.S.C. §360e)
[393] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPCD/classification.cfm, last accessed on 12 October 2019
[394] Eudamed2 - European Databank on Medical Devices

medical devices respectively. Thus, EUDAMED2 database will be in production and available to the public after mid-2020. It will include different modules on actors, medical devices, notified bodies and certificates, clinical investigations and performance studies and market surveillance. It will function as a registration system, a collaborative system, a notification system, a dissemination system (open to the public), and will be interoperable.[395]

It should be mentioned that currently, the disparities in the classification of medical devices' classification among countries pose considerable difficulties applying their implementation globally and thus limiting technological innovation and harmonized governance.

Therefore, it is the hope that centralised collection and sharing of important information about medical devices can form part of a valuable web of networked evidence that improves understanding of the risks of neurodevices and permits regulatory oversight to be proportionate to the imperative to protect the safety and autonomy of patients using invasive neurodevices.[396]

U.K. Nuffield Council on Bioethics proposes that in order to further strengthen market surveillance and transparency in the field of medical devices in Europe, EUDAMED2 should aspire to a similar degree of transparency as that in the US, mentioning the Product Classification Database which is a publicly accessible database through where information on, for example, approved medical devices and incident reports, can be searched and accessed.[397]

5.1.3 Pathway to the Market/ Market approval

As far as medical devices are concerned, the differences between Europe and the USA are not limited to the risk classification system, which is four tired in Europe and three level in the USA. The route manufacturers should follow to launch their devices (for instance, obtaining market approval or exceptions) is also noticeably different. For instance, the FDA operates a highly centralised system, whereas in EU medical device regulations has not yet been completely harmonized. Also, unlike the European system, before medical devices can be marketed under the U.S. system, it is usually necessary to demonstrate that they are not only safe, but also effective

[395] Eudamed2, https://ec.europa.eu/growth/sectors/medical-devices/new-regulations/eudamed_en last accessed on 12 October, 2019
[396] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[397] *Ibid.*

(Under humanitarian device exemption the demonstration of effectiveness is not needed). In Europe, however, manufacturers must only demonstrate that the device is safe and performs according to its intended use.

Pathway to Market in Europe

EU law is governed by the principles of subsidiarity and proportionality, and shared competences between Union and Member States. This is also true in the field of public health as the principal objective of the law is to protect human health, ensure safety and prevent the fragmentation in medical device development. The current medical device legislation consisting of mainly the MDD and AIMDD due to the legal nature of Directives is decentralised and also light-touch with respect to pre-market oversight of medical devices. New adopted Medical Device Regulations which is about to be applied fully in less than a year improves the harmonisation of relevant national laws and provides for stricter pre-market regulations on high-risk devices and adds additional mechanisms for post-market-surveillance and other issues. I will briefly give an overview of the current legal framework applied to market approval or otherwise use of medical devices. After that, I will analyse new provisions introduced with the Medical Device Regulations to improve existing regulatory regime.

Medical devices must be CE (abbreviation of the French term '*Conformité Européenne*' meaning 'European Conformity) marked before they can be placed on the market. CE marking shows that the device complies with EU legislation and can be used. The essential requirements in the Medical Device Directive 93/42/EEC are divided in two groups: set of general requirements for safety and performance that applies to all devices, and a list of specific and technical requirements regarding design and manufacturing that apply to certain devices.[398]

In order to obtain a CE mark for Class I medical devices and general category IVDs, the manufacturer have to demonstrate and document compliance with the regulations and issue (self-declaration of compliance).

For Active Implantable Medical Devices, and class IIa, IIb and III medical devices, in order to be CE marked, a manufacturer must submit an application together with technical documentation to

[398] Santos et al, Medical device specificities: opportunities for a dedicated product development methodology, *Expert Review Medical Devices*, 9, 2012

a Notified Body who assesses if the documentation for the product's safety and performance is sufficient for the product to be CE marked. Once this declaration has been signed, the manufacturer may affix the CE marking to its device and begin marketing the product.

It should be mentioned that when devices are needed for clinical investigation or custom made, the CE mark is not mandatory. The manufacturer has to follow the requirement of Annex VIII on the Statement concerning devices for special purposes and only declare that their products conform to the essential requirements.

As a general rule, for implantable devices and devices in Class III confirmation of conformity with the requirements concerning the safety, technical characteristics and performances determined with Annex I of the MDD under the normal conditions of use of the device and the evaluation of the undesirable side-effects must be based on clinical data. The adequacy of the clinical data must be based on: [399]

> either a compilation of the relevant scientific literature currently available on the intended purpose of the device and the techniques employed as well as, if appropriate, a written report containing a critical evaluation of this compilation…
>
> …or the results of the clinical investigations undertaken according to Annex X of the MDD.

With regard to device-related research, instead of clinical trial, the term of 'clinical investigation' is generally used and as such EU Clinical Trials Directive does not apply to clinical investigation.[400] It is because, medical device clinical investigations differ from standard clinical trials, such as they involve fewer human subjects and also due to a short lifetime of medical devices which need frequent modifications clinical investigations have a shorter follow-up period than clinical trials of medicinal products, etc.

However, clinical device investigations on CE marked devices, conducted for post-market registry studies, may involve larger patient numbers and longer follow up periods and are considered to gather comparative performance and safety data for a marketed device. As such data collected

[399] Annex X (Clinical Evaluation), the Medical Devices Directive 93/42/EEC

[400] There are a number of other guidelines applicable to clinical investigations: the Medical Device Directive 93/42/EEC (e.g. Article 15, Annexes I, VIII, Annex X) or Active Implantable Medical Device Directive 90/385/EEC (e.g. Article 10, Annexes 1, 6, 7); ISO 14155 Parts 1 & 2 – Clinical Investigations involving medical devices in human subjects, MEDDEV 2.7-1 Clinical evaluation: Guide for manufacturers and notified bodies (including Appendix 1 Clinical Evaluation of Coronary Stents), MEDDEV 2.7-2 Guide for Competent Authorities in making an assessment of clinical investigation notification; GHTF SG5(PD)N3R7 Clinical Investigations (draft)

from post-market clinical investigations studies becomes an essential part of a device's long-term safety and performance profile.

Clinical investigation is defined in ISO 14155, 'Clinical Investigations of Medical Devices for Human Subjects', as "*...any designed and planned systematic study in human subjects undertaken to verify the safety and/or performance of a specific device.*"

There is a distinction between device investigations that are conducted purely for obtaining market approval and device investigations that are conducted as part of academic or clinical research. Device investigations that are proposed, designed and sponsored by clinical investigators rather than device manufacturers solely for the purposes of clinical or academic research without manufactures financial support, with no commercial intent, are not regulated as strictly as the ones which seek market approval. In such instances, investigational devices are used within acceptable professional and ethical boundaries and for the purposes of research only.[401]

'Off-label' device investigations are about devices used outside its existing intended purpose or indications for use for investigational purposes. Use of the device in this manner may, since the market release of the device, have become an established or standard clinical practice. This type of clinical investigation is often led directly by clinicians and has no commercial basis and therefore do not require prior approval by a Notified Body as in case with device investigation for research described above.[402]

When manufacturers directly or indirectly sponsor these off-label studies with a view to extending their devices current indications for use, a full review, including all relevant data, will be required.

In on all other instances, when the manufacturer is proposing to conduct an investigation to gather the necessary clinical data to demonstrate the basic safety and performance of their device provisions of clinical investigations defined in Medical Device Directive 93/42/EEC (Articles 15 along with Annex X) and Active Implantable Medical Devices Directive 90/385/EEC (Article10, and Annex VII) apply.

[401] HPRA Guide for Ethics Committees on Clinical Investigation of Medical Devices, 2010
[402] HPRA Guide for Ethics Committees on Clinical Investigation of Medical Devices, 2010

It should be mentioned that very little specific guidance for ethical rules in relation to investigations[403] that involve medical devices exist in Annex X of the Medical Devices Directive, (93/42/EEC). It also also very broadly defines methodological criteria according to which the investigation needs to be carried out. Similar provisions are to be found in Annex VII, sec. 2, of the AIMDD. Some further generic informative guidance can be found in Annex B of the relevant international standard 'Clinical Investigations of Medical Devices for Human Subjects – Part 1: General Requirements' (ISO 14155-1:2003).

There are no specific provisions under the Medical Device Directives relating to the processing of personal data by manufacturers/distributors/healthcare units. Such data either will be protected by national health laws of each country or would be classified as sensitive personal data under the GDPR (as health data), and thus normally would require standard precautions of the explicit informed consent or the anonymisation of shared data.

New Medical Devices Regulation

The Medical Devices Regulation 2017/745 has enhanced requirements for the designation of Notified Bodies, with increased control and monitoring by the national competent authorities and the Commission. Compared to the Medical Device Directives, the Medical Devices Regulation also places more emphasis on a continuous control of safety, to be proved by clinical data and also increases co-ordination with improved European database on medical devices (EUDAMED 2). A new Unique Device Identification system used in EUDAMED will enhance the transparency and the effectiveness of post-market safety-related activities.[404]

As in the case with the Medical Device Directives, pre-market approval process differs according to the class of the device. However, now there are more stringent assessment procedure for the conformity of a device for CE marking. Article 52 foresees the intervention of a Notified Body for some specific Class I devices, and for all Class IIa, IIb and III devices.[405]

Article 54 of the Medical Devices Regulation introduces additional pre-market scrutiny of the highest risk medical devices (certain Class IIb devices and for implantable Class III devices) in

[403] Other than already given in the WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects
[404] Article 27, the Medical Devices Regulation (EU) 2017/745
[405] Article 52, 7a, b, and c, the Medical Devices Regulation (EU) 2017/745

the form of a clinical evaluation consultation procedure by an independent expert panel operating on behalf of the European regulatory system.

For Class III and implantable devices, manufacturers have to describe the summary of safety and clinical performance of devices, in addition to existing technical standards when making application. The summary of safety and clinical performance shall be written in a way that is clear to the intended user and, if relevant, to the patient and should be publicly available via EUDAMED. [406]

The scope of the Quality Management System for conformity assessment procedure includes clinical evaluation and post-marketing clinical follow-up (PMCF).[407] The most important change is the introduction of stricter requirements for clinical evaluation.[408] For clinical evaluation there are two options as previously:

a) collection of clinical data already available in the literature

b) undertaking clinical investigations

But, increased clarity and more tighter requirements about how clinical data from predicate or equivalent devices can be used as part of clinical dossiers make it harder to obtain the degree of equivalence needed for clinical evaluation in terms of the new Medical Devices Regulation. Therefore, in order to comply with the requirement of clinical evaluation, almost in all circumstances implantable and Class III medical devices must go through clinical investigations.[409]

[406] Preamble, para 46 and Article 32, the Medical Devices Regulation (EU) 2017/745
[407] Article 10.9, the Medical Devices Regulation (EU) 2017/745
[408] Article 61, the Medical Devices Regulation (EU) 2017/745

[409] Article 61.4, the Medical Devices Regulation (EU) 2017/745 provide few exceptions to this rule:
In the case of implantable devices and class III devices, clinical investigations shall be performed, except if:
— the device has been designed by modifications of a device already marketed by the same manufacturer,
— the modified device has been demonstrated by the manufacturer to be equivalent to the marketed device, in accordance with Section 3 of Annex XIV and this demonstration has been endorsed by the notified body, and
— the clinical evaluation of the marketed device is sufficient to demonstrate conformity of the modified device with the relevant safety and performance requirements.
In this case, the notified body shall check that the PMCF plan is appropriate and includes post market studies to demonstrate the safety and performance of the device.
In addition, clinical investigations need not be performed in the cases referred to in paragraph 6:
(a) which have been lawfully placed on the market or put into service in accordance with Directive 90/385/EEC or Directive 93/42/EEC and for which the clinical evaluation:
— is based on sufficient clinical data, and

It should be mentioned that *common specifications* (CS) defining additional requirements in respect of the general safety and performance (the technical documentation set out in Annexes II and III, the clinical evaluation and post-market clinical follow-up set out in Annex XIV or the requirements regarding clinical investigation set out in Annex XV of the Regulations)may be put in place for certain devices.[410]

In the case of BCI, common specifications can be defined by the legislators, however, that has not been directly indicated in the Medical Devices Regulation. Further, BCI manufacturers may not need to undertake a device clinical investigation if there are only some modifications are made to the device, or when the Notified Body is satisfied with equivalence test of the device with already existing one, or when the manufacturer intends to conduct post-market studies.

Also, BCI devices which have been already placed on the market or put into service in accordance with the current Medical Device Directives for which the clinical evaluation is based on sufficient clinical data there is no need for undertaking clinical investigations when new the MDR enters into force.

BCI devise when they are custom-made, used off-label or developed only to be used for research purposes in health-care settings will still be regulated with less strict regulations.

Mainly, Article 62 and Annex XV set out the new and more precise requirements for clinical investigations to include many specific provisions for protecting people enrolled in clinical studies. Among the provisions safeguarding patient rights Article 63 (*informed consent)* and Article 72 (*Conduct of Clinical Investigation*) worth mentioning. Article 63 provides for baseline requirements for obtaining informed consent and national laws can consider higher degree of autonomy protection.

Unlike the current Medical Device Directives, the upcoming Medical Device Regulation included certain guidelines to safeguard patient's privacy. Data protection considerations have been taken into account with regard to clinical investigations as well as in all other cases when personal (health) data are collected, processed and shared for the purposes of the Regulation. Article 72.3 and Annex XV requires that all clinical investigation information to be recorded, processed,

— is in compliance with the relevant product-specific CS for the clinical evaluation of that kind of device, where such a CS is available;

[410] Article 9, the Medical Devices Regulation (EU) 2017/745

handled and stored in a way to ensure the confidentiality of the personal data. Appropriate technical and organisational measures are needed to be undertaken to protect information and personal data from unauthorised or unlawful access, disclosure, dissemination, or destruction, in particular where the processing involves transmission over a network.

Article 109 (*Confidentiality*) and 110 (*Data Protection*) are general provisions to ensure privacy in processing personal data, which, by referring to the EU data protection legislation, require all parties involved in the application of the MDR to respect the confidentiality of information and data obtained in carrying out the tasks derived from their obligation under this Regulation.

Although the scope of the new MDR has been extended to include all economic operators and their roles and obligations have been increased and elaborated in detail to ensure better compliance and increased protection of safety and public health, there are still some shortcomings with regard to regulation of BCIs.

Pathway to Market in the USA

In the USA, medical devices for human use are regulated by the Center for Devices and Radiological Health. The CDRH's objective is to assure that patients in the U.S. have access to high-quality, safe, and effective medical devices. Although the CDRH allows third parties – accredited persons – to conduct the primary review of some devices, it retains final authority over all devices' approval.[411]

In order to market a medical device in the USA, there are four options: premarket notification 510(k), premarket approval (PMA), the Humanitarian Device Exemption, and Evaluation of Automatic Class III Designation (*De Novo Classification Process*).

Additionally, there is an Investigational Device Exemption (IDE)- a simplified procedure for allowing a manufacturer to conduct clinical trials for a newly developing device.

a) The Humanitarian Device Exemption[412]

[411] Santos et al, Medical device specificities: opportunities for a dedicated product development methodology, Expert Review Medical Devices, 9, 2012

[412] FDA (2010) Humanitarian device exemption, available at: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/HumanitarianDeviceExemption/default.htm. (last accessed on 14 October 2019)

The U.S. operates a Humanitarian Device Exemption (HDE) addressing conditions affecting fewer than 8,000 people in the USA per year.[413] Humanitarian Use Device (HUD) is a Class III medical device intended to benefit patients in the treatment or diagnosis of a disease or condition that affects or is manifested in not more than 8,000 individuals in the United States per year.[414] An HDE is a marketing application for an HUD.[415] The HDE is exempt from the effectiveness requirements of Sections 514 and 515 of the FD&C Act and is subject to certain profit and use restrictions. This path aims to be an incentive for the development of devices for use in the treatment or diagnosis of diseases affecting small populations without having a need to seek the lengthy pre-market approval process. (although evidence of safety is a requirement in obtaining an HDE).

It must however be mentioned that in the USA, the HDE has been subject to criticism. One group of commentators raised their concern about HDA -a simpler, cheaper, and faster approval process – which used to approve DBS for the suppression of symptoms of severe OCD – means that devices are not subject to sufficiently rigorous clinical investigation, potentially risking patient safety.[416] Additional concerns are about the potential commercial motivations for manufacturers to pursue the HDE, and that "*the humanitarian device exemption is being used to give the device manufacturer access to patients, rather than giving researchers access to subjects, or patients access to sound scientific evidence*."[417]

b) Evaluation of Automatic Class III Designation (De Novo Classification Process)

Since 2010, the FDA has begun releasing summary documents for devices classified through the *De Novo process*. *The De Novo* summary is intended to present an objective and balanced summary of the scientific evidence that served as the basis for the decision to grant a *De Novo* request. The *De Novo* summary also serves as a resource regarding the types of information necessary to support substantial equivalence for device manufacturers that may wish to use the device as a predicate for future 510(k) submissions.

[413] Section 3052 of the 21st Century Cures Act (Pub. L. No. 114-255
[414] Section 3052 of the 21st Century Cures Act (Pub. L. No. 114-255
[415] Section 520(m) of the Federal Food, Drug, and Cosmetic Act (FD&C Act)
[416] Fins JJ, Mayberg HS, Nuttin B et al. (2011) Misuse of the FDA Humanitarian Device Exemption in deep brain stimulation for obsessive-compulsive disorder Health Affairs 30(2): 302-11, at p 305.
[417] *Ibid.*

Prior to the Food and Drug Administration Modernization Act of 1997, if an innovative device was found 'not substantially equivalent,' it was classified as Class III, and a PMA was required, resulting in a conflict between the need to be innovative and a more complex commercialization process.[418] Currently, there are two options for de novo process of reclassification of the devices to Class I or II providing a simpler route to market for novel low-risk devices.

First option the process which has to start within 30 days after receiving 'not substantially equivalent' (NSA) letter to a 510(k) submission. It has a review period of 60 days and if the device is classified into Class I or II, the applicant receives an approval order to market the device. But, if it is determined that the device must remain in the Class III category, it cannot be marketed until the applicant has obtained an approved PMA.

The second option was brought with the amendments of 2012. [419] Any person (a medical device sponsor) is now free to submit a De Novo classification request to the FDA for market approval without first being required to submit a 510(k).

c) Pre-Market Notification: The 510(k)152

The most common method of FDA device approval for the low or medium risk devices is the "traditional" 510(k) Premarket Notification. The 510(k) process is a 90-day review procedure which requires proof that a given device is "substantially equivalent" to a device that has been previously classified and approved. Under the substantial equivalence standard, a new device does not need to be identical to the predicate device; it just needs to have the same intended use and technological characteristics. [420]

In 2007, Neuronetics Inc. applied for 510(k) clearance of its NeuroStar rTMS device to treat drug resistant depression claiming that the TMS device was equivalent to electroconvulsive therapy (ECT). The FDA had initially required not only that Neuronetics demonstrate that rTMS treatment was favourable and comparable to ECT, but that any reduction in effectiveness of the former was

[418] The Food and Drug Administration Modernization Act of 1997 (FDAMA) added the De Novo classification option as an alternate pathway to classify novel medical devices that had automatically been placed in Class III after receiving a "not substantially equivalent" (NSE) determination in response to a premarket notification -510(k) submission.

[419] Section 513(f)(2) of the Food, Drug and Cosmetic Act was amended by section 607 of the Food and Drug Administration Safety and Innovation Act (FDASIA), on July 9, 2012

[420] Ethicon, Inc., v. Food and Drug Admin., 762 F. Supp. 382 (D. D.C. 1991) (discussing the substantial equivalence standard).

counter-balanced by a reduction of the risk involved. After thorough evaluation however, the FDA Advisory Panel found that the risk-benefit profile of the rTMS device was not comparable to that of ECT and declined to pass the device on the basis of substantial equivalence. It did, however, grant approval to NeuroStar for marketing its device on the evidence of the rTMS device's its own efficacy and safety.[421] Subsequent transcranial brain stimulation devices may now follow the 510(k) pathway with less controversy, as more closely comparable devices are on the market.[422] For instance, in 2013 the Brainsway Deep rTMS System received clearance on grounds of substantial equivalence to be marked in the US for the treatment of major depression.[423]

d) Pre-Market Approval

Pre-Market Approval is similar with the procedure that is needed to market European Class III devices. Pre-Market Approval ("PMA") is FDA's most stringent form of premarket review, reserved for Class III devices, due to the level of risk associated with these devices. In contrast to the streamlined 510(k) process, the FDA typically requires the submission of significant additional documentation in evaluating a PMA to ensure *safety* and *effectiveness*, and annual reports even after the PMA.

The regulation governing premarket approval is located in Title 21 Code of Federal Regulations (CFR) Part 814, Premarket Approval of Medical Devices. A Class III device that fails to meet PMA requirements is considered to be adulterated under section 501(f) of the FD&C Act and may not be marketed. Although FDA regulations provide 180 days to review the PMA and make a determination, depending on the device type the process can take between 6 months and 2 years, depending on some factors such as the final reports of clinical studies, time given to manufactures collecting necessary documents, etc.

Evidence Required for safety and effectiveness: Typically, a PMA will require clinical studies and other scientific data on the device's safety and effectiveness. [424] The valid scientific evidence used to determine the *effectiveness* of a device shall consist principally of well-controlled

[421] FDA(2008)Repetitive transcranial magnetic stimulator for treatment of major depressive disorder, available at: http://www.accessdata.fda.gov/cdrh_docs/pdf6/K061053.pdf
[422] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[423] FDA(2013) Brains way deep TMS system, available at: http://www.accessdata.fda.gov/cdrh_docs/pdf12/K122288.pdf
[424] FDA PMA Approval, https://www.fda.gov/medical-devices/premarket-submissions/premarket-approval-pma (last visited Oct. 14, 2019)

investigations.[425] The valid scientific evidence used to determine the *safety* of a device must demonstrate the absence of unreasonable risk of illness or injury associated with the use of the device for its intended uses and conditions of use. In addition to clinical investigations, the FDA may also require significant non-clinical laboratory studies related to toxicology, immunology, biocompatibility, stress, wear, etc.[426]

Since much of this data, especially clinical data, cannot be gathered until the device has been tested in humans and also non-approved FDA device cannot be transported cross-state borders, a special exemption had been made by the U.S. Congress to allow distribution of medical devices for the purpose of conducting clinical trials. Thus, the FDA is entitled to provide an *Investigational Device Exemption* (IDE) to promote clinical trials on new devices. Section 520(g) of the Federal Food, Drug, and Cosmetic Act[427] establishes a framework for FDA to study medical devices for investigational use. This provides an exemption from certain requirements so that scientific experts qualified by special training and experience can investigate their devices' safety and effectiveness. This exemption is known as an Investigational Device Exemption (IDE). An IDE is granted based on information about the scope and duration of the testing, the number of human subjects involved in the study, explanations of possible changes to be made to the device to accommodate the study and the methods for data collection and whether or not that the collected data will be used to obtain FDA approval for the device. It is usually is not visible to obtain an IDE for a device that will not be looking for FDA approval in the future. Also, the sponsor of the new device[428] must provide all information gathered from previous testing, a protocol for testing, assurance that every study participant will provide informed consent and that a local Institutional Review Board (IRB) has approved the testing. Under 21 CFR Part 56, an IRB is an appropriately constituted group that has been formally designated to review and monitor biomedical research involving human subjects. In accordance with FDA regulations, an IRB has the authority to approve, require modifications in (to secure approval), or disapprove research. This group review serves an important role of ensuring that tests of 'significant risk devices'[429] are completed in a manner that will minimize the

[425] 21 U.S.C. § 360c(a)(C)(3) (2006)
[426] FDA PMA Clinical Studies, https://www.fda.gov/medical-devices/premarket-approval-pma/pma-clinical-studies, last accessed on 14 October, 2019
[427] 21 U.S.C. § 360j(g)
[428] The person responsible for initiating the investigation
[429] U.S. Food and Drug Administration, the Guidance for Institutional Review Boards (IRBs), Clinical Investigators, and Sponsors Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/institutional-review-boards-frequently-asked-questions , last accessed on 14 October

risks to the study subjects and that these risks are minimal in comparison with the knowledge to be gained and also with the benefits to the study subjects themselves. The IRB is also responsible for ensuring that the selection of test subjects is equitable and that the informed consents received are adequate, and *patient information is protected appropriately*. The IRB must evaluate the usefulness of the investigation and weigh the "knowledge to be gained" against the "benefits to the subjects", both of which = must be substantial. Although there may be no direct benefits for the participants during the study, IRB should nevertheless look into whether there are potential benefits for the participants with the future developments of Health Care which are based on the research results.[430]

The FDA considers implanted BCI devices to be "significant risk devices" because they are "intended as an implant and present a potential for serious risk to the health, safety, or welfare of a subject."[431] In order to study a significant risk device in human subjects, a sponsor must receive approval of an investigational device exemption (IDE) application prior to beginning the investigation.[432] Investigational BCI devices are generally evaluated by the Division of Neurological and Physical Medicine Devices (DNPMD), one of seven divisions in CDRH's Office of Device Evaluation (ODE).

A number of pathways exist to study BCIs including: [433]

- Early Feasibility Study (EFS): a limited clinical investigation of a device early in development, typically before the device design has been finalized (e.g., innovative device for a new or established intended use, marketed device for a novel clinical application).[434]
- First in Human (FIH) Study: a type of study in which a device for a specific indication is evaluated for the first time in human subjects.
- Traditional Feasibility Study: a clinical investigation that is commonly used to capture preliminary safety and effectiveness information on a near-final or final device design to adequately plan an appropriate pivotal study.

---

[430] Allison, Legal and Ethical Issues in the Regulation and Development of Engineering Achievements in Medical Technology: A 2006 Perspective, *Proceedings of the 28th IEEE EMBS Annual International Conference New York City*, USA, Aug 30-Sept 3, 2006

[431] 21 CFR 812.3(m)

[432] 21 CFR 812.20

[433] FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.

[434] Investigational Device Exemptions (IDEs) for Early Feasibility Medical Device Clinical Studies, Including Certain First in Human (FIH) Studies Guidance for Industry and Food and Drug Administration Staff http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm279103.pdf

- Pivotal Study: a clinical investigation designed to collect definitive evidence of the safety and effectiveness of a device for a specified intended use, typically in a statistically justified number of subjects. It may or may not be preceded by an early and/or a traditional feasibility study.

Clinical Study Considerations for Human Investigations with BCI Devices[435]

- BCI devices also present additional risks compared to conventional devices (e.g. prostheses) due to technology, such as the use of implanted components. Implantation carries potential risks such as neural tissue damage that can result in additional functional or sensory deterioration. Therefore, development of adequate clinical study designs for BCI devices that are intended to support marketing authorization in the U.S. is essential to the successful translation of BCIs from concept to patient access.
- Also, clinical metrics or endpoints are important for defining the benefits and risks of medical devices. Metrics should be clinically meaningful, measure how a patient functions or feels or both, and ideally be validated for the indicated patient population. Unfortunately, there are few clinically meaningful endpoints that have been validated for assessing BCI devices and there is a need for defining and developing such metrics. Under these circumstances, feasibility studies can be used to help develop metrics and determine clinically relevant changes in performance.
- Home use: It is important to study BCI devices in realistic home-use environments since lab conditions may not adequately reflect where a patient will actually use the device.

One of the most prominent examples of neural interface systems, BrainGate has been studied through a pilot clinical trial under an Investigational Device Exemption ("IDE") from the FDA.

Device Approval Process

After the submission of required data on safety, effectiveness, and completed clinical investigations, the CDRH evaluates the pre-market application and decide upon granting approval. It should be mentioned that often a sponsor submitting a premarket submission (i.e., an applicant) needs to use another party's product (e.g., ingredient, subassembly, or accessory) or facility in the

[435] FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.

manufacture of the device. In order that a sound scientific evaluation may be made of the premarket medical device submission, the review of data and other information related to the other party's product, facility, or manufacturing procedures is required.[436]

In making decisions regarding premarket submissions, the FDA weighs benefits and risks. There are a multitude of factors to consider for assessing benefits and risks, such as type, magnitude, probability of patient experiencing one or more benefit, duration of favourable effect, type, number and rates of harmful events associated with the device, stage of device development, uncertainty, characterization of disease, patient tolerance for risk and perspective on benefit, availability of alternative treatments, risk mitigation, etc.[437]

The FDA often uses outside expertise to make device approval decisions that involve cutting-edge technology or controversial issues. The FDA maintains a system comprised of 50 committees and panels to provide the agency with independent scientific, technical and policy advice in specialized areas, such as antiviral drugs, anesthesiology, allergenic products, or medical devices.[438] The committees have as members representatives from industry and consumer groups also from medical sector and general academia. Although the final regulatory decision is with the FDA, great weight is placed on committee discussions and recommendations. Committees not only provide the FDA with technical advice, but they may raise issues of safety or efficacy, or suggest additional studies. Members can also raise relevant policy issues, and public comment is invited at committee meetings.[439]

Additional Considerations for Evaluating BCI Devices [440]

In addition to standard device testing such as biocompatibility, sterility, and electrical safety, BCI technologies may have unique testing considerations, for example:

[436] FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.
[437] "Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval and De Novo Classifications" http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM296379.pdf last accessed on 14 October 2019
[438] FDA Advisory Committees, http://www.fda.gov/oc/advisory/default.htm (last visited Oct. 14, 2019)
[439] Carol Lewis, Advisory Committees: FDA's Primary Stakeholders Have a Say, FDA Consumer Magazine, Sept.-Oct. 2000, available at http://www.fda.gov/fdac/features/2000/500_adv.html (discussing issues surrounding an advisory committee's approval of an AIDS drug).
[440] FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.

- BCI technologies may measure signals from the brain or peripheral nerves; so important factors to consider include electrode reliability, signal-to-noise ratio, artifact removal (e.g., eye or muscle movement), and battery longevity.
- The signal of interest may vary among and within subjects over time, making the quality of BCI input signal for a specific individual at a specific time very difficult to predict. As a result, most BCI systems require training or adjustment to each subject individually.
- If the device provides stimulation to the nervous system, determining maximum safe levels of stimulation that can be applied to brain tissue or peripheral nerves is important.
- In "real world" use, BCI systems may need to perform reliably in complex and unstable environments that often contain sources of electronic noise.

5.1.4 Post-Approval / Post-market surveillance

In the case of medical devices, as they involve human safety, manufacturers have two obligations when they deliver a device to market: to conduct postmarket surveillance and provide adverse event reporting.[441] As such the manufacturer is required to first conduct active monitoring of medical devices during their use and detect rare but serious adverse events and long-term failures that are unable to be detected during the premarket surveillance owing to the short duration of the clinical studies and/or the limited number of participants and then submit periodic reports to the FDA, in the form of annual reports that summarize any unpublished clinical or laboratory data, and any published literature, related to the device.[442] It allows the identification of complications related to inexperience and improper use of a device and make necessary adjustments to it. It also helps to identify 'off-label uses' of the devices and problems related to the manufacturing process. Manufactures are responsible to report, "PMA supplements" whenever changes are made to the device that affect its safety or effectiveness. Such changes may include new indications for use, labeling, technological characteristics, or manufacturing processes. [443]

Regulators can be informed of adverse cases not only by manufacturers themselves, but also from users and other third parties who report the malfunction of a medical device, and competitors who

[441] Tice JA, Helfand M, Feldman MD, Clinical evidence for medical devices: regulatory processes focusing on Europe and the United States of America (Background Paper 3). WHO, Geneva, Switzerland (2010)
[442] 21 C.F.R. §814.84.
[443] 21 C.F.R. §814.39

complain about noncompliance by another manufacturer. The FDA maintains a database, called Manufacturer and User Facility Device Experience Database (MAUDE), to collect such data.[444]

It is seen from the overview of the U.S. medical devices regulatory framework that, device regulations are mostly designed to cover approval of medical devices, which are restorative in nature, whereas implantable neural devices have in addition to restoration and rehabilitation feature, human enhancement capacity. The implantable neural devices deserve specialized regulation rather than being dealt within general Class III high-risk device category, because they have potential for integration with the nervous system, and can provide both input and output capabilities, intended to be used life-time and operated remotely through network.[445]

Implantable neural devices present different challenges with regard to effectiveness as well. As a threshold matter, it is unclear how effectiveness itself should be defined in relation to restorative and enhancement devices. If it can be nevertheless defined, then the effectiveness of BCI devices would need to be ensured over a greatly extended time frame - ideally, the life of the device user. Additionally, effectiveness must also take into account the way different patients adapt to the learning curve of their implanted devices.[446]

The U.S. FDA's one objective is also to provide neuroelectronic developers with favourable regulatory procedures in order to avoid the situation when device developers and those seeking to use neuroelectronic devices shift their activities, whether it is the development, testing, or surgical installation, overseas. It is also acknowledged that a transnational device regulation regime may be required for effective regulation of the development and use of BCI devices. For this purposes, the FDA conducts transnational regulation pilot programs with its counterparts, such as Japan.[447] It also was one of the initiators for the establishment of the International Medical Device

[444] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM, last accessed on 14 October 2019
[445] With regard to the informational security of active implantable medical devices, the US Government Accountability Office also acknowledged that the threat is sufficiently plausible and serious and therefor the U.S. FDA should develop a plan for "*enhancing its review and surveillance of medical devices as technology evolves [to] incorporate the multiple aspects of information security*".
[446] Chan, E., The Food and Drug Administration and the Future of Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement, *John Marshall Journal of Computer & Information Law*, Vol 25, 2007
[447] U.S. - Japan Medical Device Harmonization by Doing (HBD), http://www.pmda.go.jp/int-activities/int-harmony/hbd/0015.html (last visited 19 October 2019)

Regulators Forum, which is a group of countries that works towards acceleration of international medical device regulatory harmonization and convergence.

5.2 Governance of medical data (neuro-data) in clinical practice

5.2.a) Breach of confidentiality in common law and medical ethics

Both legally and ethically, information that doctors learn about a patient in the course of their professional duties is confidential.[448] The Hippocratic Oath stipulations of doctor's professional confidentiality coming from ancient times are still firmly endorsed: "*Whatever, in connection with my professional service or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."* The Declaration of Geneva imposes the same obligation on the doctor, requiring him to *"respect the secrets which are confided in me, even after the patient has died"*[449]

Critics, however, see the concept being problematic in modern society where information technology facilitate wider and faster dissemination of patient information and heighten concerns about the risk of unauthorised disclosure.[450] Health data are indeed circulated widely and among not only medical professionals but also others who are less deeply indoctrinated to confidentiality than their medical colleagues. As such law of confidence cover a broader complex of responsibilities but earlier proposals that institutions should take over custodianship of confidences and impose an overall standard of duty on everyone who work in health institutes have now been recognised both at common law[451] and by statute.[452]

In the United Kingdom, guidance on legal responsibilities associated with handling of confidential patient data has been summarised in the 2003 NHS Code of Practice:

[448] The British Medical Association's handbook of ethics and law: Medical Ethics Today, 2012
[449] The 2nd General Assembly of the World Medical Association, Geneva, Switzerland, Sept 1948, last amended at the WMA General Assembly, Chicago, United States, Oct 2017
[450] See Nuffield Council on Bioethics, The collection, linking and use of data in biomedical research and health care: ethical issues (2015); G Laurie et al., A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data (2015)
[451] *A-G* v *Guardian Newspapers Ltd (No 2);* para 6.1 imposes a duty on all those who receive confidential information in circumstances which objectively (and reasonably) import a duty of confidence.(e.g. communications in a hospital *W*, X, *Y and Z* v *Secretary of State for Health et al* [2015] EWCA Civ 1034.)
[452] The Data Protection Act 1998, the Human Rights Act 1998, the National Health Service Act 2006, including Regulations laid under s 251, the Health and Social Care Act 2012, GMC, Confidentiality: Protecting and Providing Information (2009), as updated by Good Medical Practice (2013), the common law of confidentiality, and the tort of misuse of private information

> information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so.[453]

The healthcare mentioned in this guidance is the patient's own. Identifiable patient data may be shared to support the patient's treatment based on an implied consent.[454] A secondary use of identifiable patient data however requires an explicit consent or other legal grounds. This obligation to seek explicit consent, or other legal basis, is attributed to the common law duty of confidentiality.[455] The Guidance issued by the General Medical Council which has statutory, regulatory powers, imposes a strict duty on registered medical practitioners to refrain from disclosing voluntarily to any third-party information about a patient which he has learnt directly or indirectly in his professional capacity. A breach of this duty which has binding effect over doctors will be a serious matter, exposing the doctor to a wide range of potential professional penalties.[456] As such principally a common law duty, interpreted in the context of the Human Rights Act 1998,[457] is imposed on a doctor to respect the confidences of his patients.

---

[453] Department of Health Confidentiality: NHS Code of Practice (November 2003) 7. See also GMC Confidentiality (2009) p.6

[454] See Department of Health (n 2) paras 33 and 41.

[455] The U.K. Data Protection Act 1998 (DPA) itself imposes no such requirement. Paragraph 8 of Schedule 3 of the DPA provides an alternative legal basis to consent for a data controller when processing for medical purposes. There is an argument that a proper understanding of Schedules 2 and 3 of the DPA would prioritise consent as 'first among equals' and, as per the Human Rights Act 1998, any failure to process on the basis of consent would require justification as necessary and proportionate, in accordance with law, and in pursuit of a legitimate aim. See, for example, D Beyleveld, Data Protection and Genetics: Medical Research and the Public Good (2007) 18 King's Law Journal 275, 284–85. However, that does not appear to be the current advice of the Information Commissioner's Office (ICO). See, for example, the ICO response to GMC Consultation on Confidentiality Guidance. In particular, in regards to paragraph 8: '*If it is anticipated that the disclosure has a legal basis to take place anyway, regardless of consent, then for the purposes of the DPA another schedule condition should be applied and consent not sought - patients should simply be clearly informed that the disclosure will take place, to whom and why*'. https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1043273/ico-response-to-gmc-confidentiality-guidance-consultation.pdf

[456]GMC, Confidentiality: Protecting and Providing Information (2009), as updated by Good Medical Practice (2013)

[457] A right to 'respect for private and family life', under Article 8 of the ECHR, is guaranteed by the Human Rights Act 1998. This right is not unqualified right, but can be derogated from where the law allows and where '*necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*'. The effect is similar to that of the common law duty of confidentiality: privacy is an important principle that must be respected, *but confidentiality may be breached where other significant interests prevail*. The British Medical Association's handbook of ethics and law: Medical Ethics Today, 2012

The nature of this obligation[458]-which applies to all confidential information and not only to medical material[459]-was dealt with by the House of Lords in *A-G* v *Guardian Newspapers Ltd (No 2),*[460]in which it was reiterated that there is a public interest in the protection of confidences received under notice of confidentiality or in circumstances where the reasonable person ought to know that the information was confidential:

> a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.[461]

Protection similar to that originally offered by Lord Goff's broad principle can be found in the concept of 'reasonable expectation'. Thus, a duty will arise whenever a person knows or should know that another person can reasonably expect his or her privacy to be protected[462] or, as Supreme Court Justice Hale explained it in Campbell v Mirror Group Newspapers:

> [W]hen the person publishing the information knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential.[463]

Further, in *Hunter* v *Mann,* the court stated that: "*the doctor is under a duty not to disclose, without the consent of the patient, information which he, the doctor, has gained in his professional capacity*" [464]

In the UK, much of the law protecting confidentiality is not set out in statues but has evolved trough common law. Society has an interest in maintaining a confidential health service and

---

[458] The doctor-patient and priest-penitent relationships were cited as classic examples in *Stephens* v *A very* [1988] Ch 449 at 455; [1988]2 All ER 477 at 482, per Browne-Wilkinson V-C.

[459] The duty to respect confidences is to be distinguished from the (broader) notion of respecting individual privacy although the two are obviously related. Indeed, the House of Lords has confirmed that there is no common law right of privacy in the United Kingdom (UK): see *Wainwrightv Home Office* [2003] 4 All ER 969; [2003]3 WLR 1137, HL; this is not at all the same as saying that privacy interests are not protected.

[460] [1990] AC 109;

[461] [1990] AC 109, 281.

[462] Campbell v Mirror Group Newspapers [2004] UKHL 22 Lord Nicholls of Birkenhead 21, Lord Hope of Craighead 84 and Baroness Hale 137. In Campbell, the common law duty of confidence was interpreted so as to give effect to Art 8 of the European Convention on Human Rights, affirming that the common law can address *the misuse of private information.* In the context of the facts in Campbell, Lord Nicholls stated that the more natural description was that the information was private, and the essence of the tort was better encapsulated as misuse of private information, rather than breach of confidence. There are cases when information may be described as private as well as confidential and could therefore qualify for protection by both torts. In some other situations, information may be only private but not confidential.

[463] [2004] UKHL 22 Baroness Hale 134

[464] [1974] QB 767 at 772; [1974]2 All ER 414 at 417, per Boreham J,

common law imposes a duty on health professionals to respect the confidences of patients. Duty to protect patient information arises when it is given by patients in situations where an obligation of confidence is implied (such as the doctor–patient relationship), or when it is, by its nature, confidential (such as health information). This duty also arises when there is a public interest that confidentiality should be protected, or when the confider may suffer from revelation of the information.

The common law provides for when information may be disclosed with consent or where the law requires or permits it. As a general rule, uses of data unconnected with the direct provision of patient care require express consent unless the data are anonymised. Explicit consent is generally needed in order for information to be shared outside the healthcare team providing care, unless the data are anonymised prior to disclosure. The alternative routes for sharing health information, in the absence of patient consent, are when the *law authorises its disclosure* or *when it is justifiable in the public interest*. Legal judgments have also established that confidentiality may be breached, but only when there is a public interest that overrides the patient's right to confidentiality (and also the public interest in maintaining a confidential health service). [465]

Though England has recognized a similar breach of confidence doctrine as the basis of privacy protection, in America judges and scholars thought an approach would be redundant with the existence of invasion of privacy tort,[466] it would present a number of practical[467] and constitutional difficulties,[468] and it would be under-protective of privacy interests.[469] But it was acknowledged also by the courts that unlike statutory Fourth Amendment law, tort law recognizes breach of confidentiality as a distinct harm and the breach of confidentiality differs from other torts, in particular from the invasion of privacy tort in a way it violate the trust in a specific relationship.

[465] See, Ashworth Security Hospital v MGN [2002] UKHL 29.
[466] Alan B. Vickery, Comment, Breach of Confidence: An Emerging Tort, Columbia Law Review Vol 8, No 1426, (1982) pp1460-61 "The law of confidence should not intrude in the realm of family and personal relationships, even though damaging information is often revealed in the course of such relationships.... Privacy law with its 'highly offensive' threshold provides ample protection for personal relations."
[467] Katz, Comment, Unauthorized Biographies and Other "Books of Revelations": A Celebrity's Legal Recourse to A Truthful Public Disclosure, Vol 36 UCLA Law Review (1989) p 819, "A breach of confidence may take many forms, only some of which are legally actionable.... [G]ossip in its simplest form, between individuals, cannot practically speaking be the basis of a cause of action by the person whose activities are the subject of the conversation."
[468] Alan B. Vickery, Comment, Breach of Confidence: An Emerging Tort, Columbia Law Review Vol 8, (1982) p1426 ("Attaching a legal duty to every confidentiality received with knowledge of its confidential nature demands too much.... It would not be consistent with the notion of a free society for the state to intrude so deeply into individual decision making with respect to one's casual relationships absent a compelling reason . . .."
[469] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review, Vol (1890) (developing other tors of privacy by rejecting the "narrower doctrine" of breach of confidence because "modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party")

In this way, the tort emerges from the concept of a fiduciary relationship, which is "*founded on trust or confidence reposed by one person in the integrity and fidelity of another*." [470]

The harm from a breach of confidence, is not only that information has been disclosed, but that the victim has been betrayed: "*the physician is bound, . . . upon his own professional honor and the ethics of his high profession, to keep secret [*a patient's information*]. . . . A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong*."[471]

In the U.S. as well, there are exceptional cases when disclosure of information by the doctor is not considered as breach of confidentiality "*majority of the jurisdictions faced with the issue have recognized a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest.*"[472]

The summary of the ethical and legal rules about confidentiality in common law is that health professionals are liable to keep patients' health information confidential and secure. It is well established that there should be no disclosure of any confidential information obtained during the fulfillment of professional duty by doctor for any purpose other than for clinical care of the patient (or direct support of healthcare of the patient) to whom it relates. Three broad exceptions to this conception have been developed over time:

- consent
- provision of law
- overriding public interest.

Overall, it can be concluded that duty of confidence which is an agency-based approach provides a better framework for developing an account of informational obligations in the protection of health data.

[470] MobilOilCorp.v.Rubenfeld,339N.Y.S.2d623,632(Civ.Ct.1972)
[471] Simonsen v. Swenson, 177 N.W. Neb. 1920, at 832
[472] McCormickv.England,494S.E.2d431,432(S.C.Ct.App.1997)

5.2.b) Health-care provisions of European countries applicable to the patient's privacy

With the development of information technology, shift happening in the delivery of health services and patients' increased access to health care through a range of methods, makes it particularly important to elevate the protection of personal data in the health sector, by paying special attention to basic requirements of confidentiality for diagnostic and therapeutic information. Achieving a reasonable balance between protecting patient data and ensuring their appropriate use for the vital interests of the data subject or other persons, but also for research and public healthcare purposes presents a challenge.

In general, national legislations apply to all processing of personal health data[473] and therefore cover all personal health data in the country. There are, however, gaps in some national legislative frameworks that create inconsistencies in privacy protection or result in some personal health data falling through the cracks and having no legislative protection.[474] In the EU, both health law and tort and contract law are not harmonised, as such the legislation on healthcare remains in the competence of member states and is outside the scope of EU law. The newly adopted GDPR applies to the processing of health data, however in most cases it refers to national legislations of Member States either for more specific provisions to adapt the application of the GDPR's rules such as defining the term of *public interest* or *public health* for applying exceptions (Arts 6.2 and 9 GDPR), including limitations, with regard to the processing of genetic data, and health data[475] or regulating the whole branch of law such as governance of health data during provision of healthcare.

Because, the healthcare systems across the EU are broadly diverse, patients, healthcare professionals and service providers operate in a very complex legal landscape, especially when transnational services are offered.

As provision of healthcare are regulated at national level of each EU member state, governance of medical records (health data) dramatically differ one from another (e.g. professional

[473]Whereas common law duty of confidentiality arises with regard to personal health information disclosed in the context of a confidential relationship, such as that between a patient and his or her doctor, statutory protection extends such duties to holders of information who does not necessarily have a confidential relationship to a patient but where the data kept is detailed enough to identify the data subject.
[474] See e.g. Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en
[475] Article 9.4. of the GDPR

confidentiality requirements for healthcare professionals remain regulated on the national level and are often subject to different standards of liability).[476]

For example, the Italian context is characterized by many levels of authorities and rules which protect citizens privacy rights: starting from the EU level legislations transposed in Italy with the Data Protection Code,[477] to the Guidelines and recommendations provided by the Italian Data Protection Authority - Garante della Privacy in collaboration with the Ministry of Health on Electronic Health Records.[478] Moreover each region has its own competences on applying healthcare legislation, which is done by many local healthcare providers called "ASL: Azienda Sanitaria Locale" that deliver assistance services to patients.[479] This context shows clearly that in Italy, like in other countries, there exist many bodies having different competences that define privacy legislations on different aspects of health-care.[480]

Finland provides a broad framework for governance of health data that is realised through a number of legal acts. First, most health data are in the custody of public institutions, including national institutions such as the National Institute for Health and Welfare (THL) and regional governments and public clinics. The Act on the Openness of Government Activities which applies to government bodies has also provisions regarding the use of classified and sensitive public data, such as personal health data. The Act on the Status and Rights of Patients in detail covers clinical research including research involving personal health data. Further, the Act on Social Registers mandates legislative authority for the development of health data registries within THL. Finland has also adopted an Act for governing the national electronic health record system including e-prescriptions which contains, *inter alia,* provisions governing the development and use of a national data archive of electronic health records. In 2013, a new Biobank Act came into effect which, among other things, allowed previously collected samples to be transferred to biobanks and made available to researchers. The act covers all with provisions related to data collection, use and access and allows using some samples contained in the data bank for research purposes based on

[476] Bächle, T., and Wernick, A., The futures of eHealth – introducing the social, legal and ethical challenges, 2019
[477] Legislative decree no. 101 of August 10, 2018 (Decree), amending and adapting the Italian Data Protection Code (Legislative decree no. 196/2003, Data Protection Code or DPC) to the GDPR, has been issued on September 4, 2018 in the Official Journal and entered into force on September 19, 2018.
[478] Italian Data Protection Authority, *Guidelines on the Electronic Health Record*; Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012)
[479] Armellin, G., et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB workshop* (2010): 6368; Municipality of Trento. *Regulations for the protection of personal data of the municipality of Trento*. http://www.comune.trento.it/, 2007;
[480] Stevovic, J., et al, Enabling Privacy by Design in Medical Records Sharing, Chapter 16 in *Reforming European Data Protection Law*, Gutwirth, S., et al, Springer 2015

the ‘broad consent’ of data subjects. There is however a separate Medical Research Act which safeguards patient’s health data with explicit consent.

The Data Protection Act 1998 governs the processing of data that identify living individuals – personal data – in the UK. Section 1 of Part 1 of the Act lists eight principles requiring the data:

- fairly and lawfully processed
- processed for limited purposes and not in any manner incompatible with those purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than necessary
- processed in line with the data subject’s rights
- secure
- not transferred to countries without adequate protection.

Further protection of health data is provided in Human Rights Act 1998 which is based on Article 8 of the ECHR.

The National Health Service Act 2006 determines that explicit consent is generally needed in order for information to be shared outside the healthcare team providing care, unless the data are anonymised prior to disclosure. But section 251 of it allows to make regulations permitting the disclosure of identifiable information without consent, in certain circumstances, where it is needed to support essential NHS activity and medical research. Thus, institutions can apply to the Health Research Authority's Confidentiality Advisory Group to seek support for disclosure under the Health Service (Control of Patient Information) Regulations 2002 issued by the Secretary of State for Health.

The NHS Care Record Guarantee summarises the legal and policy position for patients on how their information will be used and safeguarded by the NHS. It established 12 commitments of the NHS in England to the confidentiality and security of patient information and highlights patients’ rights regarding use of their health information. There is also the Health and Social Care Act of 2012 which reformed the health management in the U.K.

In Western Europe, the legal framework for the protection of personal data recognises health data as sensitive data and therefore require a high level of protection. There are particular variables

within national health datasets, that may be considered to be of even higher sensitivity than general health data. Variables that lead to the direct identification of individuals are highly sensitive, such as DNA. Also, particular health conditions that may carry additional social stigma are considered highly sensitive in some national laws. They include mental health conditions, sexually transmitted infections including HIV, substance use, etc.[481]

In certain countries there have been legislations or practices introduced for the protection of certain topics of personal health data that have been deemed as more sensitive. For example, in some countries such as Germany,[482] Portugal,[483] Sweden[484], Italy,[485] there are specific pieces of legislation for particular types of health/medical information that have been determined to be more sensitive than other personal medical information such as Genetic Information Laws.

In processing particular categories of data, with reference to genetic and health data, the Garante-Italian Data Protection Authority establishes, on a two-yearly basis, provisions aimed at identifying "*the security measures, such as …pseudonymization procedures, minimization measures, specific methods of selective data access and [*provides] *information to data subjects, as well as other necessary measures to guarantee the data subjects' rights*."[486] The general authorizations for the processing of sensitive data according to the Privacy Code, shall be updated by the DPA after holding public consultation.

Secondary uses of patient information:

The secondary analysis of personal health data is typically permitted in countries with the implied or express consent of the data subject or when the analysis has been legally authorised.[487] When disclosure is justified by a legal authority, it can be according to a legal requirement to report

[481] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en
[482] The German Human Genetic Examination Act of 2010 determine the requirements for genetic examinations and genetic analyses to prevent discrimination and harm on the basis of genetic characteristics and for the protection of human dignity and right to self-determination.
[483] Portugal's Personal Genetic Information and Health Information Act in 2005 (Lei No 12/2005 de Janeiro) governs performance of the genetic tests, use of genetic information and conduction of research.
[484] The Act on genetic integrity prohibits the use of or demanding genetic information without a support of legal provision as a precondition for any agreement.
[485] Genetic Authorization for the Processing of Genetic Data (Italian Data Protection Authority 2011)
[486] Article 2, para 2, the Italian Data Protection Code (DPC), as amended by Legislative Decree no. 101/2018
[487] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en

certain diseases or a court order to disclose information, or the public interest, such as where failure to disclose would result in death or serious harm.[488]

It should be mentioned that important difference among countries depends on whether or not the national legislation governing data privacy protection allows statistics and research as potential areas where an exemption to patient consent requirements could be granted. In these countries, an exemption can be granted for a proposed secondary use of personal health data that are in the public interest. For instance, all Nordic countries and the United Kingdom (England) are regularly linking most of their national health care datasets for statistics and research.[489]

In other countries where such exemptions are not legally permitted under the general data protection legislation, health-sector specific legislation might or might not be introduced to clarify permitted uses of personal health datasets for statistics and research in the public interest.[490] Additionally, the EU law mentions that States can provide that the data subject's express consent is not enough to allow others to use his/her " *sensitive data* " – concerning *inter alia*, health,– without an *ad hoc* authorisation issued, by a designated supervisory authority. Section 26 of the Italian Data Protection Code provides that processing of health data is only allowed with the data subject's consent and additionally the Garante's authorisation if the data controller is a private body. In general, for secondary use of data for research purposes collected during treatment are allowed with the consent of data subject. Article 110-bis of the DPC titled "Third party data reuse for purposes of scientific research or for statistical purposes", applies different requirements when a third party carries out the further processing of data rather than such further processing is carried out by a scientific institute for research, hospitalisation and healthcare which actually undertakes treatment. In the first case, consent is required except when informing data subjects are not possible. In the second case, the data use falls under Article 89 of the GDPR, which is processing of health data during research. Besides two-yearly guidance on safeguarding measures to be issued by the Garante, Article 106 of the DPC furhter stipulates the adoption of deontological rules

[488] BMA Handbook 2012
[489] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en
[490] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019

relating to the processing of personal data for statistical and scientific purposes - which controllers/ processors must respect to ensure the lawfulness of the processing.[491]

Security of health data

Proven data security practices are important to meet legal requirements for the protection of the health information when they held at national datasets, transferred or shared with others. Main features of good governance within data processors include physical security, IT security, and secure channels for data transmission. Other important aspects are separation of duties, where only employees that need to see identifiable data to process it do so; signed obligations binding employees to protect data confidentiality; and regular staff training about their responsibilities for data security and confidentiality protection.[492]

There are international guidelines such as the International Committee on Harmonization Guideline for Good Clinical Practice,[493] and several standards adopted by the International Standards Organisation regarding privacy and security requirements of Electronic Health Record systems (ISO/TS 14441:2013); security of electronic health records communications (ISO/TS 13606-4:2009); and data protection to facilitate transborder flows of personal health data (ISO 22857:2011); ISO 22221: 2006—Good Principles and Practices for a Clinical Data Ware-house to harmonise national data security and privacy protection practices.

In general, all health facilities should have security policies in place to protect patient information both electronic and paper-based health information.[494] Besides this, all health professionals, and everybody else working in healthcare establishment, have legal and contractual obligations of maintaining patient confidentiality. In addition, doctors have particular obligations relating to the storage and use of health information and may be held to civil or criminal responsibility for any breaches of confidentiality resulting from insecure handling. For instance, the UK General Medical Council states that doctors must:

[491] Aurucci, P., Secondary use of clinical trial data in the Italian legal framework in the futures of eHealth – introducing the social, legal and ethical challenges, Thomas Christian Bächle and Alina Wernick, 2019

[492] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019
[493] The International Committee on Harmonization Topic E 6 (R1) Guideline for Good Clinical Practice (Step 2, 2015)
[494] The general principles about record keeping apply to all types of records, including visual and audio recordings of patients.

- make sure that any personal information is effectively protected at all times against improper disclosure
- ensure that any staff they manage are trained and understand their responsibilities towards protecting personal information.

Several countries, such as Denmark, Finland, New Zealand, Norway and the United Kingdom. have made their data security processes transparent to the public by publishing policy statements or guidelines at national level.[495] For instance, in the United Kingdom, the Information Governance Toolkit draws together the legal rules and guidance on how organisations should handle personal information. A good example can be seen in Switzerland and the United Kingdom and the United States, where external experts are used to test the security of the datasets.

5.3. Human research and experimentation in Neuroscience: departure from "consent or anonymise" approach to proportionality and principle based one

Research conducted with human beings is devoted to a row of legally binding research principles to achieve a balance between the protection of the patient wellbeing and the necessity of research involving human beings in order to find cures for diseases. The use of healthcare data in medical research is an evolving area of research practice which raises a number of ethical dilemmas deserving a special focus. Debate over this particular use of health data has taken place in the context of significant advancements in computer technology, changes in the way information shared within healthcare settings, competing commercial interests and political pressures. [496]

In order to identify the applicable rules to research, it should first be distinguished from an experimental therapy on the basis of the intent of the physician.[497] The U.K. Royal College of Physicians defines that:

> The distinction between medical research and innovative medical practice derives from the intent. In medical practice the sole intention is to benefit the individual patient consulting the clinician,

[495] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019

[496] BMA Handbook, 2012

[497] Stauch, Wheat and Tingle (2002, p. 552) distinguish 'foresight' that new knowledge (from innovative therapy) will be generated from the intention to generate knowledge which is the essential aim of a research procedure.

> not to gain knowledge of general benefit, though such knowledge may emerge from the clinical experience gained. In medical research the primary intention is to advance knowledge so that patients in general may benefit: the individual patient may or may not benefit directly.[498]

With regard to research it can be divided into clinical trials (or device investigations) to test newly developing medicinal products or devices for human use or to check their performance at a later stage and to observational researches consisting of cohort and case control studies where the researchers observe the natural course of the treatment.

At international level, several regulatory frameworks applicable to biomedical research exist such as the Nuremberg Code of Medical Ethics 1947, The World Medical Association's Declaration of Geneva of 1948, with its revised mention of 2017, The International Code of Medical Ethics of 1949, the World Medical Association's Declaration of Helsinki of 1964, with its latest revision of 2013, the UNESCO's Universal Declaration on the Human Genome and Human Rights of 1997 and Universal Declaration on Bioethics and Human Rights of 2005, WHO International Guidelines for Biomedical Research involving Human Subjects" (CIOMS-Guidelines) of 2016, the EMA Guideline for Good Clinical Practice of 2015, the International Declaration on Human Genetic Data of 1995 and last but not least, the Council of Europe's Convention on Human Rights and Biomedicine of 1997 and the its Additional Protocol to the Convention on Human Rights and Biomedicine, relating to biomedical research of 2005.

But with the exception of the Council of Europe's Convention, they do not have any legally binding force and thus do not result in legally enforceable commitments for states. Article 2 of the Convention on Human Rights and Biomedicine stipulates that the protection of dignity, personality and health of the human being is higher than the sole interest of the society in research and progress. According to Art. 13 Para. 2 of the Additional Protocol on Biomedical Research the researcher has to inform precisely about the envisaged arrangements to ensure the confidentiality of personal data. The Biomedicine Convention has been accessed by 29 CoE States, whereas the Protocol was ratified by 11 States.

Non-binding instruments, however, (documents / declarations) in international law provide an example of international reflection on these subjects, making them useful texts for development of

[498] Royal College of Physicians (1996, para. 6.4).

national laws, and more specific international guidelines. Furthermore, these instruments set out legal standards such as the informed consent and other biomedical principles.

The Declaration of Helsinki was developed by the World Medical Association as a set of ethical principles for the medical community regarding human experimentation in 1964. It has constantly been modified ever since, with the last revision of 2013. The new version has more detailed provisions concerning informed consent. The Declaration of Helsinki is based on three basic principles: respect for all persons, beneficence in the maximization of benefits over harms, and justice for all those who could benefit from the research. The Declaration of Helsinki is about biomedical research on human subjects, while the European Convention provides a framework for all biomedical practice.

On the whole, these non-binding standards are quite substantive (for example, they require approval by an ethics committee of the research protocol, on the basis of a complete description of the study, including detailed information on the risks and burdens that it may entail for research participants and on the ways participants will be selected and requested to participate).

However, in the case of a drug trial the applicable regulations are much more extensive and elaborate, since clinical trials must meet all the requirements laid down under the new Regulation (EU) No 536/2014 on Clinical trials on medicinal products for human use.[499] The Regulation articulates the general principle that a clinical trial may be held only if: (1) the rights, safety, dignity and well-being of participants are protected and prevail over all other interests; and (2) it is designed to generate reliable and robust data.

It should however be mentioned that Clinical Trials Regulation of 2014 does not apply to BCI experimental studies. Currently the Medical Device Directives regulates BMI device investigations and from May 2020 the Medical Device Regulations will replace the Directives.

Generally, Article 89, of the GDPR relates to the processing of (health) data for research purposes. Article 89.1 provides exemption for processing health data, which is in principle forbidden by the GDPR:

[499] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical trials on medicinal products for human use

> necessary for archiving, *scientific or* historical *research* or statistical purposes in accordance with article 89.1, based on Union or member state law which must be proportionate to the aim pursued and provides suitable and specific measures to safeguard the rights and freedoms of the data subject (9.2.j) It is clearly emphasised, however, that exemptions and derogations for research purposes should not result in personal data being processed for other purposes by third parties such as employers, insurance or banking companies (Recital 54).

However, this article leaves too much room for different legislation in the EU's member states. In general many of the research exemptions for using data considered in the GDPR have been left to the member states national laws.

Neuroscientific research often combines elements from many different disciplines ranging from technological sciences to humanities.[500] Although neuroscientific research often involves elements from, for example, behavioural sciences, it is likely that any studies conducted on implantable neural devices that use medical equipment falls under the scope of application of the Medical Device Regulations or national health laws.

Neuroscientific research in BCIs implies the obtainment, collection, classification, and analysis of a high number of data records. They can be saved in databases, which enable their use for different purposes for an indefinite time and their transfer even across national borders. The number of cross-national research projects is growing and adequate data sharing systems shall be established to enable the exchange more efficient, so that contribute to the development of medical innovation in the field.[501]

European Commission has an objective to connect national research data with European networks of scientific and clinical expertise, such as the International Consortium for Personalised Medicine, the European Reference Networks, the European Research Infrastructures, the EU Human Brain Project and other relevant initiatives. [502]

The neuroscientific research has its specifics, not applicable in other researches. Such as the researcher has to provide information about the wide range of temporal and spatial application

[500] Salla Silvola, Legal Landscape of Neuroscientific Research and Its Applications in Finland in International Neurolaw: a comparative analysis, Springer, 2012
[501] *Ibid*
[502] European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, (25 April 2018)

possibilities. Brain data have the potential to give very important and sensitive information about the personality of the participant. If third parties become unintentionally aware of the personal information, this knowledge may lead from stigma to fatal consequences for the participant.[503]

Furthermore, data protection is an important issue with a view to insurance and employment applications. Therefore, the researcher has to inform participants and other interested parties precisely about the envisaged arrangements to ensure the confidentiality of personal data. The creation of a pseudonym could guarantee data protection, on the one hand, but on the other hand would increase the risk of reidentification of the volunteer/participant by third parties, as research participants in implantable neuro devices are few compared to other medical researches. Current legislation regulating the research field dictates that if the participant wishes to remain completely anonymous she or he has to be excluded from the research study.

According to the literature reviewed in medical research[504] as well as deducting from findings of international organizations' relevant reports,[505] there is not yet a single country which provides for specific regulations concerning neuroscientific research on human beings. Accordingly, general legal framework on research with human beings is commonly applied to the field of neuroscientific research in countries all over the world. However, the state of regulation on scientific research differs from country to country. France is one of the few countries with a specific national regulation on biomedical research, Law on Bioethics. Being a part of the French Public Health Code, the Law on Bioethics covers the basic legal conditions for biomedical research with human beings in France.[506] French legislator has come up with a unique structure- rotational revision of the Law on Bioethics to respond to the fast-growing knowledge in biomedical research. Within rotational revision, specific provisions on neurosciences has been suggested.[507]

German Basic Law, which is formed by the first 19 articles of the German constitution, plays a special part in regulating not only neuroscientific research, but also general new technical developments. Among the most important provisions, which become relevant in the context of neurosciences, a number of human rights, such as the general *right of the personality*, deriving

[503] Ulmer S, et al, Impact of Incidental Findings on Neuroimaging Research Using Functional MR Imaging. American Journal Neuroradiology Vol 30 No 55, 2009
[504] E.g, T. Spranger, International, Neurolaw: a comparative analysis, Springer, 2012,
[505] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019
[506] H. Wegmann, Summary: Neurolaw in an International Comparison in *International Neurolaw: a comparative analysis*, ed. Spranger, Springer, 2012
[507] *Ibid.*

from Art. 2 para. 1 in connection with Art. 1 para 1, *the equality before the law* of article 3, the *freedom of faith, and conscience* of article 4, Basic Law can be mentioned.[508] These articles create basis for German conception of privacy which is self-determination or self-reservation. Applying by analogy of the German court interpretation where it determined that "*DNA-samples of identification have to be protected according to the individual's right to determine the usage of his own personal data, and the coding part is part of the absolutely protected core of personality*",[509] we can deduct that individual brain data is protected by German constitution.

Along with above mentioned countries, Italy also does not have any specific legal act dedicated to neuroscientific research. The legal and ethical foundations of research derive from the same article covering medical activity: protection of the fundamental right to health contained by Article 32 of the Constitution. The actual national general legal framework relies mostly on Law 211/ 2003 and 200/2007 implementing EU directives on pharmaceuticals, Law 219/2006 implementing Directive 2001/83/EC and Directive 2003/94/EC. In addition, M.D. of 12 May 2006 on basic requirements for Ethical Committees for medical drugs trials must be mentioned.[510]

Protection of health data when used for research purposes is covered by the Data Protection Code. As mentioned above Article 2 of the DPC provides that sensitive health data can be processed if specific safeguarding measures (including security measures, such as encryption and pseudonymisation) are implemented. The Italian legislation provides stronger protection to the health data and relies on consent as the proper legal basis to justify the primary use of sensitive data for research purposes. There are some exceptions though.[511]

Article 110-bis(4) specifies that the secondary use for research purposes of personal data originally collected for clinical activity – by either public or private scientific institute for research, hospitalisation and healthcare – does not fall under "third party data reuse" due to the instrumental nature of the activity of healthcare provided by the aforementioned institutions with respect to research. In this case, in fact, the further processing for research purposes is not carried out by a third party but by the same controller who collected the data in the first place.[512] In this case, legal

[508] H. Wegmann, Summary: Neurolaw in an International Comparison in *International Neurolaw: a comparative analysis*, ed. Spranger, Springer, 2012
[509] Decision of the Federal Constitutional Court, cited in Germany as: BVerfGE 103, 21 (32 et seq.).
[510] Comandé, G., Medical Law in Italy, Wolters Kluwer Law & Business, 2014
[511] Aurucci, P., Secondary use of clinical trial data in the Italian legal framework in the futures of eHealth – introducing the social, legal and ethical challenges, Thomas Christian Bächle and Alina Wernick, 2019
[512] *Ibid.*

basis set out in Article 5(1)(b) – used in accordance with Article 89[513] - should apply and, therefore, the reuse of data for scientific research does not require a new legal basis such as consent. On 19 December 2018, the Garante issued the Deontological Rules Relating to the Processing of Personal Data for Statistical and Scientific Purposes to further clarify the processing health data by research institutes.

As mentioned above, the GDPR provides several exemptions and derogations for the use of health data, e.g. in the context of research or public health purposes under certain conditions. Typical procedures in this context include the application of ethical standards for scientific research as mentioned in Recital 33 and the implementation of organisational and technical safeguards as mentioned in Article 89 including anonymisation, pseudonymisation and encryption.[514]

There are also conflicts in the guidance of GDPR, for example, Recital 159 explains that "scientific research" should be defined broadly and include both technological development and privately funded research, Recital 54 states that public health and public interest exceptions "*should not result in personal data being processed for other purposes by third parties*...". Where the GDPR permits research exceptions, it requires "appropriate safeguards" to protect individual privacy rights—without clarifying what those safe-guards must be (for example, in Articles 89.1 and 9 and Recitals 52 and 54).[515]

There are also several scientific research exemptions in GDPR.[516]

Consent or anonymise approach

Data protection legislation has two major goals of protecting individual autonomy and promoting the public interest. It is often hard to find optimal mechanisms for achieving this aim, without establishing prevalence of one over another. Out of this necessity, in the health data context the consent or anonymise approach emerged. But recent, technological advancement and big data made this approach obsolete. As a recent Nuffield Council on Bioethics reports notes, "*Faced with*

[513] GDPR, Article 5.1b) "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')"
[514] NHS Confederation (2012) General Data Protection Regulation: NHS European Office Position Paper. http://www.nhsconfed.org/ regions-and-eu/nhs-european-office/influencing-eu-policy/ ~/media/AF378EA1EBAF490D90F316645B65558F.ashx
[515] Nicholson et al, Shadow health records meet new data privacy laws; How will research respond to a changing regulatory space? Insight, 2019
[516] See above p. 95

contemporary data science and the richness of the data environment, protection of privacy cannot reliably be secured merely by anonymisation of data or by using data in accordance with the consent from data subjects."[517] Therefore, effective governance of the use of data through proportionality and principle-based approach is indispensable. As it seen above the new GDPR has taken this approach, by providing a number of exceptions to processing personal health data without data subject's explicit consent.

A governance model for research data access based on defined data protection principles, with also pragmatic review of legality of use proportionate to the level of risk, can provide the needed solid foundation and flexible and transparent environment to address current and future challenges in the field of research with emerging technologies.[518] The core issue here is both defining how conventional privacy principles can be incorporated into a research data access framework and how the principle of proportionality developed first in human rights context can be used to create a fair, trustworthy and efficient data access review process.

Proportionality is a general principle of law developed within the context of European Convention on Human Rights. According to the jurisprudence of the European Court of Human Rights certain qualified rights, such as freedom of expression, respect for private and family life, political liberties can be limited under certain conditions to protect public interest or fundamental rights of others. But such limitations should be based on certain safeguards, such be defined in law, was necessary in a democratic society and be proportionate to the aim pursued. Proportionality acts as a criterion for fairness and reasonableness when applied to complex decision-making contexts where interpretative discretion must be used [519]and serves to "*...regulate the spaces between hard laws*".[520]

The Principle of proportionality in data protection.

- The processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms of individuals. As such the right to the protection of personal data is not an absolute right; it must

[517] Nuffield Council on Bioethics: The collection, linking and use of data in biomedical research and health care: ethical issues. http://nuffieldbioethics.org/wp-content/uploads/Biological_ and_health_data_web.pdf (2015) last accessed on 30 October 2019

[518] McGrail, K., et al, Chapter 28 Building on Principles: The Case for Comprehensive, Proportionate Governance of Data Access in *Medical Data Privacy Handbook*, ed. Aris Gkoulalas-Divanis, Grigorios Loukides, Springer 2015.

[519] Engle, E.: The history of the general principle of proportionality: an overview. Dartmouth Law Journal 1, 11 (2012)

[520] Lin, Z., Owen, A., Altman, R.: Genomic research and human subject privacy. *Science* Vol 305, No5681, (2004)p 183

be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[521]

- Personal data undergoing processing shall be relevant, complete and not excessive in relation to the purposes for which it is collected or subsequently processed. [522]

In practice when the principle of proportionality is applied to research data access it ensures that the review process for approving access to research data takes into consideration the perceived risk for data subjects, and the disciplinary measures for non-compliance are proportionate to the damages that may arise. A proportionate approach would adjust the extent and stringency of review according to the potential risk posed by the data request, so that higher risk requests receive more scrutiny.[523] The U.K. Academy of Medical Sciences report on the governance and regulation of human health research recommended the adoption of regulation that is symmetrical and proportionate: "*approving an inappropriate study is clearly unacceptable but delaying or prohibiting an appropriate study harms future patients as well as society as a whole*". [524] The idea of proportionality is also considered as one of main principles in the ethics review process that is a standard requirement for accessing research data:

> Given that research involving humans spans the full spectrum of risk, from minimal to significant, a crucial element of [research ethics board] review is to ensure that the level of scrutiny of a research project is determined by the level of risk it poses to participants …A reduced level of scrutiny applied to a research project assessed as minimal risk does not imply a lower level of adherence to the core principles. Rather, the intention is to ensure adequate protection of participants is maintained while reducing unnecessary impediments to, and facilitating the progress of, ethical research.[525]

The GDPR has incorporated in its text most of the data protection principles developed within the framework of international organizations such the UN and OECD.

According to article 5 of the GDPR, processing of personal data shall be carried out complying with the principles of "*lawfulness, fairness and transparency*", "*purpose limitation", "data*

[521] Recital 4 to GDPR
[522] Recital 170 of GDPR and Article 5.4 of the Treaty on European Union (TEU)
[523] McGrail K., et al, Chapter 28 Building on Principles: The Case for Comprehensive, Proportionate Governance of Data Access in *Medical Data Privacy Handbook*, ed. Aris Gkoulalas-Divanis, Grigorios Loukides, Springer 2015.
[524] The Academy of Medical Sciences.: A new pathway for the regulation and governance
of health research. URL https://www.gov.uk/government/news/a- new- pathway- for- the- regulation-and-governance-of-health-research (2011). Accessed on 26 October 2019
[525] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada.: Tri-council policy statement: ethical conduct for research involving humans.
http:// www.ncehr-cnerh.org/english/code_2/ (2010). Accessed on 26 October 2019

minimization", "accuracy", "storage limitation", "integrity and confidentiality", and the data controller's "accountability".

Lawfulness, fairness and transparency

This first means the data should be processed fairly, having a clear legal basis, and in a transparent manner. Also, the principles of fairness and transparency about data processing require that the data subject shall be informed of the existence of the data processing and its purposes (Articles 13 and 14).

Data minimization[526] stipulates that collected personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. IT systems should be configured by minimising the use of personal data or its identification, in such a way as to rule out their processing should the purposes sought in data processing are achieved by using either anonymous data or by making suitable arrangements to limit identification of data subjects only in cases of necessity.

Accuracy:

Personal data shall also be processed accurate and, when necessary, kept up to date; and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased. Also, any mistakes on the stored or processed data should be rectified without delay. This principle is also linked to fair and transparent processing.

Integrity and confidentiality

The data should be processed and stored in a secure way using appropriate technical or organisational measures to avoid unauthorised or unlawful processing or accidental loss, destruction or damage.

Accountability

Under the GDPR, accountability is a principle that requires controllers to put in place appropriate technical and organisational measures and be able to demonstrate compliance with the main data

[526] The data "minimisation" principle has been established in national privacy laws, such as Section 3(a) of the German Bundesdatenschutzgesetz and Section 3 of the Italian data protection code.

processing principles. This principle has been further elaborated in the GDPR, compared to its previous version in the DPD.

Data protection by design and by default

A new principle of general application has been enlisted in Article 25. This new principle aims to create sustainable data protection system through incorporating data protection procedures into the scheme of technology during its development.

Chapter VI Neuro-data as the content of mind transcending the conceptions of privacy and data protection

6.1 Mind of a human as the centre of his/her existence and the protection of thought as a distinct legal right

Every human being is by default entitled to not share or share whenever s/he wishes it his/her thoughts, hopes, feelings, and plans, along with the well-established right to control information dissemination about his/her life, family, and friends. Advocates of cognitive liberty demand that the individual should enjoy a wide range of autonomy over what is on – and in – his/her mind, as such creative freedom not only good for well-being of human, but it benefits society: "*The right to control one's own consciousness is the quintessence of freedom.*"[527] Thus, cognitive liberty activities of XX century, posit that "*if freedom is to mean anything, it must mean that each person has an inviolable right to think for him or herself. It must mean, at a minimum, that each person is free to direct one's own consciousness; one's own underlying mental processes, and one's beliefs, opinions, and worldview. This is self- evident and axiomatic*". [528]

Freedom of thought stands behind other well-accepted human rights and freedoms which could be severely undermined without its firm protection. [529]

In general thoughts are free because of their private character. Except the thinker, no other person else could know the exact content of thoughts in the same way as the thinker does. Thoughts are not in general directly observable for others; they can be assumed from verbal and/or behavioral expressions of the person. "*In addition to this privileged epistemic access that confers authority over the knowledge of one's thoughts, privacy of thoughts can also mean that others cannot control our thoughts because they are inaccessible from the outside*". [530] In ordinary circumstances it

[527] Boire, R. G., On cognitive liberty I. *Journal of Cognitive Liberties* Vol 1 (1999) pp7-13, Boire R.G. Searching the brain: The fourth amendment implications of brain-based deception detection devices, *American Journal of Bioethics*, (2005);
[528] Boire, R. G., On cognitive liberty I. *Journal of Cognitive Liberties*, Vol 1, (1999) pp7-13
[529] Blitz, Freedom of thought for the extended mind: Cognitive enhancement and the constitution. *Wisconsin Law Review*, 2010.
[530] Bublitz, C., Cognitive Liberty or the International Human Right to Freedom of Thought in *Handbook of Neuroethics*, edited by Clausen J. and Levy N., 2015

should be impossible to compel another person to contemplate a particular thought or to induce idea or form opinion.

Famous Privacy Law Scholar Gavison also highlighted the importance of privacy of thought in her famous Privacy and the Limits of Law treatise that intrusion into our thoughts is tantamount to total lack of privacy:

> In such a state, there would be no private thoughts, … and no private parts. Everything an individual thought and planned would immediately become known to others.
> …We would probably try hard to suppress our daydreams and fantasies once others had access to them. We would try to erase from our minds everything we would not be willing to publish, and we would try not to do anything that would make us likely to be feared, ridiculed, or harmed...[531]

In ethics brain privacy is considered having both physical and informational aspects. In a locational sense, brain privacy would afford individuals the right to control access to their brains by any technology stimulating or monitoring a specific location of brain. The right to control access to and use of this specific brain location would be a form of physical privacy right. On the other hand, thoughts, feelings, or preferences that can be inferred from monitoring brain are informational in nature. Brain privacy, understood as a subset of a more general right to privacy, would thus include (1) rights over access to and uses of the brain itself, and (2) over the information that may be deducted from scanning.[532]

In scientific literature thought is referred as 'mental state'. It is rather broadly encompasses "*every aspect of an individual's psychology, including, but not limited to, personality traits and dispositions (e.g. sexual preferences, personal tastes and habits...), qualitative states (e.g. perceptions, emotions, feelings...), propositional states (e.g. knowledge, beliefs), intentions and goals, plans, memories etc*."[533] Privacy of the information decoded from a human brain has been

[531] Gavison, R., Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, 1980
[532] Moore, Privacy, Neuroscience, and Neuro-Surveillance, Springer Science+Business Media Dordrecht 2016
[533] Giulio M., and Haselager, P., Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, Science Engeniering Ethics, 2017

defined with different terms including "brain privacy",[534] "neural privacy", [535] "cognitive privacy",[536] "thought privacy", [537] and "cognitive liberty".[538]

Advocates of cognitive liberty suggest considering it a "fundamental human right". [539]The reason of its fundamental function stems from the fact that "*the right and freedom to control one's own consciousness and electrochemical thought processes is the necessary substrate for just about every other freedom*"[540] It was further stated that "*it is hard to conceive any conception of a legal subject in which the mind and mental capacities (e.g. acting from reasons, deliberation) are not among its necessary constitutive conditions*."[541] Freedom of thought or as it was coined by the scholars in late XX century, cognitive liberty, is a necessary condition to all other liberties, because it is their neuro-cognitive substrate.[542] Cognitive liberty or classic freedom of thought is a basis of all other freedoms such as freedom of expression, freedom of religion, freedom of holding opinions, political freedom, etc. As a current technological advancement allows to measure brain activity and manipulate cognitive function, freedom of thought has been reconceptualized as cognitive liberty.[543]

[534] Räikkä, J. Brain imaging and privacy. *Neuroethics* Vol 3 (2010) pp5–12

[535] Schneider J., Fins J., and Wolpaw, J., Ethical issues in BCI research Brain–Computer Interfaces: Principles and Practice, ed Wolpaw, J., and Wolpaw, E., Oxford: Oxford University Press (2012); Trimper J, Root Wolpe P., and Rommelfanter, K., When 'I' becomes 'we': ethical implications of emerging brain-to-brain interfacing technologies, *Frontiers* Neuroengineering. Vol 7, (2014)

[536]Klein E, Chapter 7 Neuromodulation ethics: Preparing for brain–computer interface medicine in *Neuroethics Anticipating the Future*, ed. Illes J, Oxford University Press, 2017

[537] Illes, J. and Racine, E. Imaging or imagining? A neuroethics challenge informed by genetics. American Journal of Bioethics, Vol 5, (2005) pp.5–1

[538]Boire, R. G., On cognitive liberty, *Journal of Cognitive Liberties*, Vol 1, 1999/2000 pp7–13.

[539] It should be mentioned that freedom of thought articulated in Article 18 UDHR, as "everyone has the right to freedom of thought, conscience and religion", and replicated in almost every human rights treaty (e.g. Article 18 ICCPR and Art 9 ECHR) does not prima facie protect the privacy of thought, rather create negative obligations for States not to interfere with people's political, religious and ideological and other convictions/determinations.

[540] Sententia, W., Neuroethical Considerations: Cognitive Liberty and Converging Technologies for Improving Human Cognition, *Annals of New-York Academy of Sciences*, 2004 p.1013

[541] Bublitz C., My Mind Is Mine!? Cognitive Liberty as a Legal Concept in Cognitive Enhancement: An Interdisciplinary Perspective, ed. Hildt E, Franke A, 2013

[542] Marcello, I., and Andorno, R., Towards new human rights in the age of neuroscience and neurotechnology, *Life Sciences, Society and Policy*, 2017

[543] Sententia presents cognitive liberty as a conceptual update of freedom of thought that "*takes into account the power we now have, and increasingly will have to monitor and manipulate cognitive function*".

Also, as cognitive life is inherent to all human beings, cognitive liberty is consistent with a definition of human rights as inalienable fundamentals rights to which a person is inherently entitled from birth because she or he is just a human being.[544]

Based on these considerations and in the light of neuro-engineering advancements where a degree of access into and manipulation of neural processes significantly higher than other techniques, a reconceptualization of traditional human rights and the creation of a new neuro-specific right is suggested.[545]

6.2 Intentional and/or unintentional breach of the patient's neuro-privacy and the risks of mental, emotional and physical harms

Personal information in the form of brain data might, not only be collected from neurodevices for legitimate reasons, there is a possibility that this sensitive information may be vulnerable to unauthorised interception through hacking or wireless transmission.[546] This is related to a potential parallel problem of accidental or malicious interference with the functioning of neurodevices.

Privacy by design would suggest that one of ways of preventing these kinds of infringements of privacy would be for manufacturers to respond by designing technical protections (such as user-authorisation checks) into implantable neural devices.[547] However, the principle also requires weighing up the risks and benefits of technical solutions for users of these technologies. Obligations to improve the protection against unauthorised interference should be proportionate to how critical a device's safe functioning is to patients' well-being.[548]

With regard to the informational security of active implantable medical devices, the US Government Accountability Office also acknowledged that the threat is sufficiently plausible and serious and therefore the U.S. FDA should develop a plan for "*enhancing its review and*

[544] Sepuldeva, M., Van Banning, T., van Genugten, W., Human Rights Reference Handbook, Tilburg Law School, 2004;
[545] Boire RG. Mind matters. Journal of Cognitive Liberties. 2003; Marcello, I., and Andorno, R., Towards new human rights in the age of neuroscience and neurotechnology, *Life Sciences, Society and Policy*, 2017
[546] Chapter 5, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[547] W. Maisel, Improving the security and privacy of implantable medical devices, *New England Journal of Medicine* Vol 362 No13, 2010 pp1164-6,
[548] *Ibid.*

surveillance of medical devices as technology evolves [to] *incorporate the multiple aspects of information security*".[549]

Information security is "*the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability*".[550] It can raise even higher security concerns, when applied to intracortically implanted neuroprosthetics, in that the neuroprosthetic might at some point compromise the implanted person's neural environment and allow what might be termed biohacking, where physiological cognitive information may be not only accessed but modified.[551]

As BCI technology develops further, scientific literature envisages the possibility of creation more sophisticated "spying" applications for different malicious purposes.[552] Based on recent neuroscience results,[553], it is not impossible anymore to extract private information about users' memories, prejudices, religious and political beliefs, as well as about their possible neurophysiological disorders. The extracted information can be used to manipulate BCI users or coerce them to certain activities, or otherwise harm them.

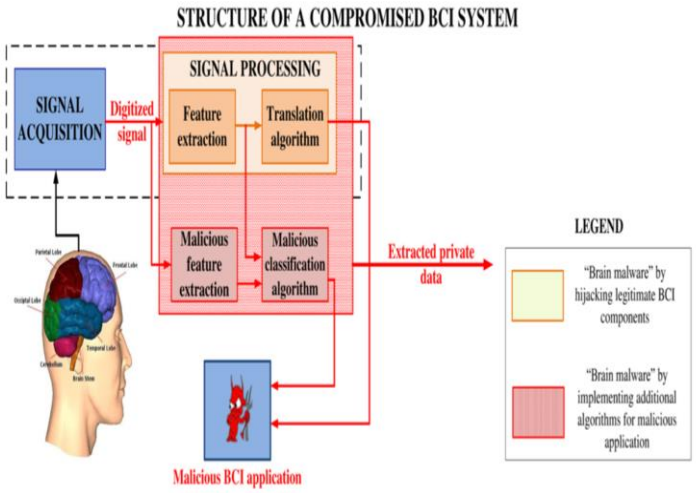
BCI users that are victims of this sort of brain-hacking typically lose the ability to seclude confidential or inherently sensitive information about themselves, thus experience along with an intrusion of their private sphere, emotional distress.[554] As experimentally shown by Martinovic et al.[555], brain-hacking via input manipulation exposes BCI users to physical and psychological insecurity. The reason for that stems from the fact that the sort of information potentially extractable from a user's mind is not limited to ordinary personal or financial information but may be extended to information about the health condition of the users, their location, psychological

[549] United States Government Accountability Office: Report to Congressional Requesters Information security of active medical devices, 2012, available at: http://www.gao.gov/assets/650/647767.pdf, last accessed on 27 October.
[550] NIST SP 800-53 Rev. 4, 2013
[551] Gladden, M.E. The Handbook of Information Security for Advanced Neuroprosthetics. Indianapolis: Synthypnion Academic. 2015
[552] E.g. the US Medical Device Security Center in Massachusetts has shown how hacker can easily attack BCIs.
[553] J.P. Rosenfeld et al, P300-based Detection of Concealed Autobiographical Versus Incidentally Acquired Information in Target and Non-target Paradigms. *International Journal of Psychophysiology*, Vol 60 No 3 2006 pp251–259; Chiu, Y., Mind Reading to Predict the Success of Online Games, February 2013
[554] Bonaci et al, Application of BCI, 2014; Prescient report; BMI Privacy Australia, 2017
[555] Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. On the feasibility of side-channel attacks with brain– computer interfaces. *In USENIX security symposium*, 2012

capacities, religious beliefs, routine activities etc. It is also possible to extract equally complex information in a similar manner.[556]

Brain-hacking via measurement-manipulation, decoding-manipulation, and feedback-manipulation pose a problem for physical and psychological safety.[557] Hacking in these forms may result in severe physical and psychological harm to patients using BCI. For example, patients using BCIs to control wheelchairs may suddenly lose their reacquired spatial mobility, and in case of robotic limb users and patients a hacker could try to hijack these signals to take control of the robotic limb or give erroneous movement feedback to the patient.[558]

Bonaci et. al in a simplified diagram of a compromised BCI system has shown how the malware involved in brain-hacking can extract information directly from brain signaling and also manipulate.



App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces, Bonaci T, et. al

Apart from malicious data hacking, the brain data can be suspectable to privacy breaches processed by legitimate data holders. First, BCI data can be shared informally between researchers, laboratories or through formal laboratory data-sharing agreements. At one hand sharing of raw neural data between BCI laboratories can enhance co-operation and development in this field and open opportunities for working out new analytic methods and reduce financial costs and

[556] Bonaci et al, Application of BCI, 2014; Prescient report; BMI Privacy Australia, 2017
[557] Marcello, I., Haselager, P., Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity, *Ethics of Information Security*, 2016
[558] Chapin JK: Using multi-neuron population recordings for neural prosthetics. Neuroscience Vol 7, (2004) pp 452–455

organizational burden. However, sharing of de-identified neural data sets can raise security concerns if not encrypted or procedures are not in place to prevent reassociation with identity-compromising data.[559]

Also, BCI data can be shared through large data repositories of big projects such as BRAIN initiative, FP7-BRAIN project, the Human Connectome Project. Particular relevance to BCI, efforts have been made to collect EEG data and make these available to researchers.[560] Privacy concerns raised about data repositories more generally will arise with respect to BCI to.[561]

BCI big data challenge appropriateness of deidentification. In general research regulations require removing identifiers from BCI data. But, many scientists as well as privacy scholars voice their concern about the technical adequacy of deidentification, particularly when one form of data (e.g., BCI neural data) can be combined with other data—genetic or microbiomic sequencing data, biological specimens, electronic medical records, administrative hospital data, or other forms of neural data (e.g., MRI for localizing lead placement).[562] A more specific concern in BCI research is risk of reidentification of research participants because of the small size of BCI research studies and publicity around such studies.[563] Publications listing different information about research participant such as gender, age, or type of medical condition add to this risk of reidentification.

To sum up, data privacy breaches happening in medical application of BCIs can be divided into three category:

Table 1.Privacy breaches in BCI

Risks with automated collection, storage or transmission of data by the data holders (clinicians/ operating technicians/ device manufactures, BCI platform providers)	Intentional- breaching operation guidelines of data minimization (e.g. obtaining information not necessarily required for treatment or health care of the patient)

[559] Chapter 34 by Klein, E., and Rubel, A., "Privacy and Ethics in Brain–Computer Interface Research" in *Brain-Computer Interfaces Handbook*, 2018
[560] Available at https://www.nedcdata.org/drupal/ , last accessed on 30 October 2019
[561] Sorani, M., John K., Sharma, S., Manley, G., Ferguson, A., Cooper, S., O'Connor, K., et al. Genetic data sharing and privacy. *Neuro-informatics* Vol 13 No1 (2015) pp1–6
[562] Chapter 34 by Klein E., and Rubel, A., "Privacy and Ethics in Brain–Computer Interface Research" in *Brain-Computer Interfaces Handbook*, 2018
[563] Neergaard, L., Obama shakes mind-controlled robot hand wired to sense touch. US News & World Report, 2016. http://www.usnews.com/news/news/articles/2016-10-13/paralyzed-man-feels-touch -through-mind-controlled-robot-hand; Poldrack, Russell A., and Gorgolewski, K., Making big data open: Data sharing in neuroimaging. *Nature Neuroscience*, Vol 17 No 11. 2014 pp. 1510–1517

	Intentional- unauthorized data sharing without patient's permission or proper pseudonymization (e.g. sharing data with other actors in health or research sector, or with commercial entities for their private benefit)
	Un-intentional data leakage through inappropriate storage and transfer of data, technical malfunction
	mixing brain data with another person's data in data pools
Accidental signal interference or malware problems occurring during patients use of the device	Problems occurring in communication or stimulation. (e.g. DBS, or using of assistive devices)
Spyware or Hacking BCI data by third parties	Extracting information from patient's brain
	Feedback Manipulation, Decoding Manipulation

Chapter VII Prospects in ensuring adequate protection of the patient's neuro-data

7.1 Strengths and weaknesses of a unified privacy data protection or sectoral approach in protecting the patient's neuro-data during BCI use– the European law and national practices

7.1.1 Unified approach - the GDPR clauses applicable to processing of neuro-data

For comparison, European regulations look advanced, setting a unified, high level of data protection. In the United States the emphasis is more on sectoral based self-regulatory approaches. EU data protections laws require a sound legal basis firmly embedded in regulations to process personal data, while US health privacy law or research acts typically doesn't have any such limitations, but they require authorization by relevant State bodies. Based on well-established adequacy approach, EU puts restrictions on cross-border data transfer. Additionally, the EU legislative framework envisages higher level of threshold for ensuring valid consent in data sharing.

Data protection seems to be highly regulated area in Europe. Both on a fundamental rights level and on a lower regulatory level, and with the adoption of the GDPR it is now treated as an independent doctrine from the right to privacy. There are stricter regulations in place for collecting, storing and sharing the personal data than it used to be before. However, as in the U.S., the EU also applies distinct rules to processing of data in some sectors, for instance, for purposes of national security within Common Foreign and Security Policy and Police and Judicial Cooperation. Besides, the public sector benefits from significant exceptions to EU data protection regulation as well. Another weak point is that despite numerous reforms there stays a visible gap between legal language and technological development, and fragmentation among national standards of data protection in the EU region.

It should be mentioned that Convention 108 adopted within the auspices of the CoE to date is the only legally binding international instrument in the data protection field applied in whole European continent. Despite the fact that Art 8 ECHR and its dynamic interpretation at the ECtHR have

provided protection for the right to privacy which entailed not only the right to have private and family life, but also privacy of many other values such as freedom of holding opinions, privacy of thought, autonomy, even data protection which also include the protection of health data, the scope of the ECHR is mainly limited to State actors.

The newly adopted EU data protection regulations- GDPR with its 99 articles and 173 interpretative recitals a complex piece of legislation which aims to achieve regulating privacy in a technologically developing world. While the ECHR and the EU Charter provide basis for the principles concerning the protection of privacy, personal life and personal data, the GDPR covers the procedures of specific protection of personal data in the EU region. The main purpose of the GDPR is to define and update a number of basic rights of data subjects regarding control of and access to their personal data, and to implement common rules for data protection in all member states. However, it does not fully harmonise the law on data protection in the EU region, because it grants the member states a wide margin of manoeuvre with regard to providing exceptions to data protection.

Nevertheless, the GDPR is considered a big step towards unifying and increasing personal data protection in the EU region. It for instance raises the bar for consent of the data subject for processing his/her personal data. Recital 32 and article 4.11 give a definition: consent means freely given, specific, informed and unambiguous - indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. In order to obtain freely given consent, it must be given on a voluntary basis. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR.

Also, the GDPR brings new safeguards to the data protection such as to data portability and the right to erasure, specific provisions on the processing of data relating to children; obligations of data protection by design and default, etc. A new principle of *data protection by design and by default* has been enlisted in Article 25. This new principle aims to create sustainable data protection system through incorporating data protection procedures into the scheme of technology during its development, once its implanted it can provide needed protection for the data used in BCIs applications.

Under the GDPR, accountability is a principle that requires controllers to put in place appropriate technical and organisational measures and be able to demonstrate compliance with the main data processing principles, another principle can be used for ensuring heightened protection of neuro-data. This principle has been further elaborated in the GDPR, compared to its previous version in the DPD.

However, in structure, the GDPR is somehow similar to the Data Protection Directive, it has mainly remained the same, despite the fact the technologies that it aims to regulate have changed prominently. To give an example, as DPD the GDPR also does not apply to anonymous data. But with the development of new technologies, there are three major limits to anonymisation. A)With the development of new technologies, de-identification (and re-identification) techniques are rapidly changing which makes it challenging to precisely put down a specific standard for anonymization in law.[564] B) data privacy research is now making clear that although a dataset may be anonymised according to conventional approaches, its cross-linking with data available elsewhere using modern technologies can make it possible to infer data subjects' identities. Therefore, although anonymisation techniques makes re-identification less likely, they do not guarantee anonymity, especially in large datasets. [565] C) as the context of medical confidentiality is changing with the development of precision medicine and e-health technology; our expectations about medical treatment will require greater linkages of data. Also, in nowadays international collaboration and long-term research projects, re-searchers or clinicians may want to link medical data to other data sources over time. Thus, while anonymisation may be used for achieving stronger data privacy protection, in the medical data context it offers only limited utility to both researchers and patient-participants alike.[566]

With regard to neuro-data collected during BCI treatment, GDPR remains silent. Although genetic and biometric data have been added to the list of "special categories of data", neither in the main text nor in recitals, there is not any referral either **to neuro-data or of any examples of the data derived from recent neuro-technological advancements**. Only in Recital 78 protection of personal data and privacy in a broader sense can be linked to technology: "*The protection of the*

[564] Edward S. Dove and Mark Phillips, Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, Springer 2015

[565] Expert Advisory Group on Data Access: Statement for EAGDA funders on re-identification. http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtp055972.pdf (2013).

[566] Edward S. Dove and Mark Phillips, Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, Springer 2015

rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met".

Additionally, in BCI application, where data collection is automated and clinical care or research teams are large consisting of neuroscientists, neurotechnologists, computer scientists, clinicians, bioethicists there can be a challenge in identifying the data controller - who holds responsibility for ensuring the lawful processing of data under the GDPR, and ensuring everyone involved in experimental research or therapy understand the extent of their legal responsibilities.

Generally, Article 89, of the GDPR relates to the processing of (health) data for observational research purposes in BCI application. Article 89.1 provides exemption for processing health data, which is in general forbidden by the GDPR, and no consent is needed for procession the data. Here the GDPR applies the principle of proportionality developed previously in human rights context, rather than classic consent or anonymise approach of bioethics. It has been clearly emphasized, however, that exemptions and derogations for research purposes should not result in personal data being processed for other purposes by third parties such as employers, insurance or banking companies.

It should be mentioned that in the EU region, the legislation covering healthcare remains in the competence of each member state and is thus falls outside the scope of EU law- that means health data protection during the clinical treatment are regulated at the national level and these legislative differences between member states may be detrimental to the patient data protection during provision of cross-border health-care and formulation of the unified approach to the protection of brain data.

7.1.2 Sectoral approach – improved medical devices regulations' provisions applicable to data protection in BCI

Neuroscientific research in BCIs implies the obtainment, collection, classification, and analysis of a high number of sensitive brain data. They can be saved in databases, which enable their use for different purposes for an indefinite time and even their transfer over national borders. The number

of cross-national research projects is growing[567] and adequate unified data sharing systems shall be set up not only for enabling exchange of data more efficient but also provide heightened protection to patient's privacy. It is also important taking into consideration that EU Clinical Trials Regulation of 2014 does not apply to BCI experimental studies. Currently the EU Medical Devices Directives regulates BMI device investigations and from May 2020 an improved new EU legislation- Medical Device Regulations will replace the Directives which has rather few clauses on clinical investigations compared to the EU Clinical Trials Regulations.

Nevertheless, compared to the former Medical Devices Directives, the new EU Medical Devices Regulation places more emphasis on a continuous control of safety, to be proved by clinical data and also increases co-ordination with improved European database on medical devices (EUDAMED 2). A new Unique Device Identification system used in EUDAMED enhances the transparency and the effectiveness of post-market safety-related activities.[568]

As in the case with the Medical Devices Directives, pre-market approval process differs according to the class of the device. However, now there are more stringent assessment procedure for the conformity of a device for CE marking. Article 52 foresees the intervention of a Notified Body for some specific Class I devices, and for all Class IIa, IIb and III devices.[569]

Article 54 of the Medical Devices Regulation introduces additional pre-market scrutiny of the highest risk medical devices (certain Class IIb devices and for implantable Class III devices) in the form of a clinical evaluation consultation procedure by an independent expert panel operating on behalf of the European regulatory system.

For Class III and implantable devices, manufacturers have to describe the summary of safety and clinical performance of devices, in addition to existing technical standards when making application. The summary of safety and clinical performance shall be written in a way that is clear to the intended user and, if relevant, to the patient and should be publicly available via EUDAMED. [570]

[567]The EU Human Brain Project and other relevant initiatives, the European Reference Networks, the European Research Infrastructures
[568] Article 27, the Medical Devices Regulation (EU) 2017/745
[569] Article 52, 7a, b, and c, the Medical Devices Regulation (EU) 2017/745
[570] Preamble, para 46 and Article 32, the Medical Devices Regulation (EU) 2017/745

The scope of the Quality Management System for conformity assessment procedure includes clinical evaluation and post-marketing clinical follow-up (PMCF).[571]

The most important change is the introduction of stricter requirements for clinical evaluation.[572] Although for clinical evaluation there are two options as previously, collection of clinical data already available in the literature for showing equivalence with existing device or undertaking clinical investigations, the degree of equivalence required have higher threshold.

As such, increased clarity and more tighter requirements about how clinical data from predicate or equivalent devices can be used as part of clinical dossiers makes it harder to obtain the degree of equivalence needed for clinical evaluation in terms of the new Medical Devices Regulation. Therefore, in order comply with the requirement of clinical evaluation, almost in all circumstances implantable and Class III medical devices must go through clinical investigations.[573]

BCI manufacturers may not need to undertake the device clinical investigation if there are only some modifications are made to the device, or when the Notified Body is satisfied with the equivalence test of the device with already existing one, or when the manufacturer intends to conduct post-market studies.

Also, for BCI devices, which have already been placed on the market or put into service in accordance with the current Medical Device Directives where the clinical evaluation is based on sufficient clinical data, there is no need to conduct clinical investigations after the new MDR enters into force.

---

[571] Article 10.9, the Medical Devices Regulation (EU) 2017/745

[572] Article 61, the Medical Devices Regulation (EU) 2017/745

[573] Article 61.4, the Medical Devices Regulation (EU) 2017/745 provide few exceptions to this rule:
In the case of implantable devices and class III devices, clinical investigations shall be performed, except if:
— the device has been designed by modifications of a device already marketed by the same manufacturer,
— the modified device has been demonstrated by the manufacturer to be equivalent to the marketed device, in accordance with Section 3 of Annex XIV and this demonstration has been endorsed by the notified body, and
— the clinical evaluation of the marketed device is sufficient to demonstrate conformity of the modified device with the relevant safety and performance requirements.
In this case, the notified body shall check that the PMCF plan is appropriate and includes post market studies to demonstrate the safety and performance of the device.
In addition, clinical investigations need not be performed in the cases referred to in paragraph 6:
(a) which have been lawfully placed on the market or put into service in accordance with Directive 90/385/EEC or Directive 93/42/EEC and for which the clinical evaluation:
— is based on sufficient clinical data, and
— is in compliance with the relevant product-specific CS for the clinical evaluation of that kind of device, where such a CS is available;

Mainly Article 62 and Annex XV set out the new and more precise requirements for clinical investigations to include many specific provisions to ensure that people enrolled in clinical studies are appropriately protected. Among the provisions safeguarding patient rights Article 63 (*informed consent)* and Article 72 (*Conduct of Clinical Investigation*) worth mentioning. Article 63 provides for baseline requirements for obtaining informed consent and national laws can consider higher degree of autonomy protection.

Unlike the current Medical Device Directives, the upcoming Medical Device Regulation included certain guidelines to safeguard patient's privacy. Data protection considerations have been taken into account with regard to clinical investigations as well as in all other cases when personal (health) data are collected, processed and shared for the purposes of the Regulation. Article 72.3 and Annex XV requires that all clinical investigation information to be recorded, processed, handled and stored in a way to ensure the confidentiality of the personal data. Appropriate technical and organisational measures are needed to be undertaken to protect information and personal data from unauthorised or unlawful access, disclosure, dissemination, or destruction, in particular where the processing involves transmission over a network.

Article 109 (Confidentiality) and 110 (Data Protection) are general provisions to ensure privacy in processing personal data, which require all parties involved in the application of the Regulation to respect the confidentiality of information and data obtained in carrying out the tasks derived from their obligation under this Regulation by referring to the EU data protection legislation.

Although the scope of the new MDR has been expanded to include all economic operators and their roles and obligations have been increased and elaborated in detail to ensure better compliance and increased protection of safety and public health, there are still some shortcomings with regard to regulation of BCIs.

First, analysis of the regime applicable the regulatory framework for medical devices is too general and broad in scope to adequately address specificities of implantable neural interfaces. Although Article 9 envisages possibility of the adoption of the *common specifications* (CS) for defining additional safety and technical requirements in respect of certain devices, it does not, *per se,* mentions BCIs. It is surprising that a narrowly tailored legislation has not been drawn up for BCIs, because besides being one of promising field of health sector, application of brain and neural interfaces constitute a very controversial ethical, legal and social issues due its specificity. BCIs

use involves interacting with the most important organ of human in a completely novel way and there is still a lack of knowledge on long-term effects of these devices and the risks they can have are extremely uncertain at this stage.

As mentioned above, due to specific and novel nature of BCIs there is a need for a special designed regime applicable to clinical investigation for evaluating safety and conformity. Implanted neural interfaces, not only carry specific risks associated with the need to perform neurosurgery, but there is a need to monitor the electrodes placed during the operation event after surgery as a follow-up phase, in order to ensure their functioning. These therefore entail both perioperative and postoperative complex management with constant monitoring compared to other treatments.[574]

Second, neuro-modulation devices directly and permanently interfaced with the central nervous system may also interfere with the patient's personality and raise issues of responsibility for the actions taken by the patient after the treatment.[575]

Third the live-time monitoring and automotive collection, storage and transmission of neuro data from brain presents difficulties for ensuring patient privacy.[576] Further related specialty is that, due to its concept of treatment BCIs are operated by research teams consisting of large and diverse professions (e.g. doctors, neuro-engineers, IT specialists, etc.), it is therefore important to employ additional safeguards to limit access to the BCI data.

However, neither the current legislation nor new Medical Devices Regulations does directly address the lack of specific rules for different types of implanted *neural interfaces*, which differ significantly from those related to other types of implants, who also require surgery and pose intraoperative risks.

As such the new regulatory framework for medical devices is still too general and broad in scope to adequately cover the experimentation phase of neural interfaces.

---

[574] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015

[575] Experimental tests from deep brain stimulation (DBS) have shown the potential for modifying mood, personality, and cognitive abilities. Synofzik, M., Vosgerau, G., & Voss, M. The experience of agency: An interplay between prediction and postdiction. *Frontiers in Psychology*, Vol 4, 2013

[576] Chapter 5, Patients and participants: governing the relationships, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013

The new MDR strengthened the requirements for Clinical Investigations and added many specific provisions to ensure that clinical study participants are appropriately protected, including a provision on transparency of the study results concerning Class III devices.

However, in respect to implantable neural devices, no additional measures have been considered that take into account scientific and technological advancements specific to this field and the features that clinical investigations with these kinds of devices present.[577]

Clinical studies involving body implants and neural interfaces consist of small sample sizes[578] or even singular case studies, due to the fact that a prerequisite to enrolment in an experimental protocol is availability of other treatments.[579] Therefore there is a need to apply accustomed procedures to this type of experimental studies.

There are also particular issues with obtaining valid informed consent in trials with BCIs. First, participants usually have reduced capacity to consent, due to communication impairments such as in the locked-in syndrome. Then in investigations regarding devices that alter brain functions, the uncertainty of the benefits and the nature of the potential risks (such as mood or personality changes) create challenges in the acquisition of informed consent. [580]

It should be mentioned that the Clinical Trials Regulations is applicable only for clinical trials on pharmaceutical products, it leaves the domain of clinical investigations on medical devices rather under-regulated (with only few Articles of the Medical Devices Regulation and Annex XV thereof) Mentioned flaws and the lack of special law in the regulatory scheme may hinder the availability of volunteers, the experimentation process, and the subsequent rapid adoption of advanced implantable devices in clinical practice.[581]

Further, despite the fact that new legislation narrowed the circumstances in which manufacturers can rely on evidence concerning similar devices (rather than conducting new clinical investigations) to demonstrate conformity, it left possibility, by invoking general exception clause,

[577] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015
[578] Here it should be mentioned that although the research participants number can be few, the data generated from brain during BCI use, can be enormous, as BCI can monitor and store patient brain signals on live mode for a long time (depending on the type of BCI used it can be even for life-time)
[579] Raspopovic et al. 2014 in Palmerini, 2015
[580] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015
[581] *Ibid*

to use pre-existing evidence for conformity assessment even in case of BCIs. It is however recommended that since neurodevices intervene in the brain, the case for relying on pre-existing evidence must be particularly sound and tailored to the needs of these devices. [582]

Also, unlike the U.S. system which envisages demonstration of not only safety of the device, but also its effectiveness as a step to market approval, even the modernized regime of medical device regulation in Europe, requires manufacturers to only demonstrate that the device is safe and performs according to its intended use. Improved evidence on the efficacy of neurodevices is a particular priority, as there is uncertainty about the benefits, risks and mechanisms by which novel neurotechnologies achieve their effects.[583] In other words, there is a need for in-depth assessment of their inherent qualities, and sensitive functions they are intended to affect including adequacy of enhancement, and their actual acceptability by a user.[584]

Medical devises when they are custom-made, used off-label or developed only to be used for research purposes in health-care settings will still be regulated with less strict regulations. This creates problems, because experimental treatments or ad-hoc investigations undertaken with custom-made devices in health-care setting are common feature of neurotechnology development. BCI's advanced prosthetics and exoskeletons, DBS and other neuro-engineering technologies are not common clinical products - they remain largely at a research stage or as experimental treatment, only recently being developed towards introduction into general clinical practice. As such, as mentioned above not having proper regulations for early stage development of neuro-devices forces the manufacturers as well as clinicians to operate in a legal vacuum, which hinders the innovative development of emerging technologies,[585] at the same time puts users, research participants and/or patients vulnerable to the abuse.

It is also recommended to have greater transparency about the basis of all decisions on the conformity of devices with regulatory requirements similar to the U.S. where the Product Classification Database operates in a publicly accessible way and provide for free-exchange of information on, for example, approved medical devices and incident reports. Currently, the EUDAMED, European equivalent of the US Product Classification Database is not open for

[582] Chapter 7 of Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[583] Chapter 7 of Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[584] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015
[585] *Ibid*

consultation and is not publicly accessible. [586] Although, the Medical Devices Regulation requires manufactures of Class III devices to make publicly available safety and clinical performance of their product via EUDAMED. [587]

It should be mentioned that the amended regulation of medical devices still mainly deals with safety and adequacy in terms of the treatment of diseases and injuries. If not to take into consideration Article 17 of Annex I discussed below, the MDR does not separately address other kinds of threats that neural implants with data processing capabilities, real-time communication with external sources and direct connection to the web can create.[588] BCI's vulnerabilities to cyber-criminality in the form of hacking attempts in this software controlled network connected device have been highlighted in a number of scientific literature.[589]An attack to the device implanted into the human body or directly interfacing with the nervous system (such as a deep brain stimulator or the controller of a prosthetic limb) could have major consequences for the health and privacy of its user.

The new MDR included new provisions to secure patient's data in general,[590] no prior assessment of privacy measures or security, however, is required before neural implantable products are marketed, even though the potential risk in the form of third-party cyber-attacks on implantable neural technologies is high.

There is a standard requirement of data protection during clinical investigations detailed in Article 72.3-4[591] and Annex XV[592] of the Medical Devices Regulation. The MDR further touches upon

[586] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[587] Preamble, para 46 and Article 32, the Medical Devices Regulation (EU) 2017/745
[588] Palmerini, E., A legal perspective on body implants for therapy and enhancement, *International Review of Law, Computers & Technology*, 2015
[589] Ienca, M., and Haselager, P., Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity, Ethics, Information, Technology, 2016; Bonaci et al, App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces, 2014 IEEE Int'l Symp. on Ethics in Sci., Tech. & Eng'rg at 1-7, reprinted in IEEE Tech. & Soc'y Mag., June 2015
[590] Article 109 (Confidentiality) and 110 (Data Protection) are core provisions to ensure privacy in processing personal data, which require parties involved in the application of the Regulation to respect the confidentiality of information and data obtained in carrying out the tasks derived from their obligation under this Regulation by referring to the EU data protection legislation.
[591] Article 72.3 All clinical investigation information to be recorded, processed, handled and stored in a way to ensure the confidentiality of the personal data.
Article 72.4 Appropriate technical and organisational measures are needed to be undertaken to protect information and personal data from unauthorised or unlawful access, disclosure, dissemination, or destruction, in particular where the processing involves transmission over a network.
[592] According to Article 4.5 of Annex XV of the MDR, Sponsor shall submit in the application form for clinical investigation among other documents, the description of the arrangements to comply with the applicable rules on the protection and confidentiality of personal data, in particular:

the risks of malicious hacking or of unauthorised data interception during the development process of the device in Annex 1 General Safety and Performance Requirements:

> Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended. [593]

> Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorized access that could hamper the device from functioning as intended.[594]

Data flowing from a BCI may include different type of information starting from treatment regimens, physiological and psychological information, to very private cognitive information about memories, prejudices, religious and other beliefs of the patient as well as metadata about the patient and the device. These devices have the potential to create a closed loop system in which devices provide a continuous data feed and can be controlled remotely and/or automatically.[595]

It is therefore recommended to conduct pre-market assessment to monitor the vulnerability of neurodevices to accidental, unauthorised or malicious interference and anonymized records of any such incidents should be made publicly accessible as it is in the U.S.[596]

In general elaborating detailed guidelines for improving joint efforts in better information governance and data linkage by manufacturers, hospitals, clinicians, and other practitioners are needed. The adoption of new rules or an adjustment to the present legislation is necessary to tackle novel forms of intrusion into the integrity of the human body which could impair health, undermine patients' confidence in their devices, or lead to the interception of sensitive personal data about health or neural activity.

- organisational and technical arrangements that will be implemented to avoid unauthorised access, disclosure,
- dissemination, alteration or loss of information and personal data processed;
- a description of measures that will be implemented to ensure confidentiality of records and personal data of subjects; and
- a description of measures that will be implemented in case of a data security breach in order to mitigate the possible adverse effects.

[593] Article 17.4 of Annex I, MDR
[594] Article 17.5 of Annex I, MDR
[595] Medical Data Privacy Handbook, 2015
[596] Chapter 7, Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013

7.1.3 EU member states' national laws applicable to the protection of sensitive health data/ neuro-data

In general, national legislations apply to all processing of personal health data and therefore cover all personal health data in the country. There are, however, gaps in some national legislative frameworks that create inconsistencies in privacy protection or result in some personal health data falling through the cracks and having no legislative protection.[597] In the EU, both health law and tort and contract law are not harmonised, as such the legislation on healthcare remains in the competence of member states and is outside the scope of EU law. The newly adopted GDPR applies to the processing of health data, however in most cases it refers to national legislations of Member States either for establishing more specific provisions to adapt the application of the GDPR's rules such as defining the term of *public interest* or *public health* for applying certain exceptions (Arts 6.2 and 9), including applying limitations, with regard to the processing of genetic data and health data,[598] and processing health data for research purposes,[599] or for regulating a whole branch of law such as governance of health data during provision of healthcare.

Because, the healthcare systems across the EU are broadly diverse, patients, healthcare professionals and service providers operate in a very complex legal landscape, especially when transnational services are offered.

As provision of healthcare are regulated at national level of each EU member state, governance of medical records (health data) dramatically differ one from another (e.g. professional confidentiality requirements for healthcare professionals remain regulated on the national level and therefore have different standards of liability).[600]

It should be mentioned however that in most EU member satates, the legal framework for the protection of personal data recognises health data as sensitive data and therefore require a high level of protection.

[597] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en
[598] Article 9.4. of GDPR
[599] Article 89, In general many of the research exemptions for using health data considered in the GDPR have been left to the member states' national laws.
[600] Bächle, T., and Wernick, A., The futures of eHealth – introducing the social, legal and ethical challenges, 2019

There are particular variables within national health datasets, that may be considered to be of even higher sensitivity than general health data. Variables that lead to the direct identification of individuals are highly sensitive, such as DNA. Also, particular health conditions that may carry additional social stigma are considered highly sensitive in some national laws. They include mental health conditions, sexually transmitted infections including HIV, substance use, etc.[601]

In certain countries there have been legislations or practices introduced for the protection of certain topics of personal health data that have been deemed as more sensitive. For example, in some countries such as Germany,[602] Portugal,[603] Sweden[604], Italy[605], there are either specific pieces of legislation or legal provision in general law for safeguarding particular types of health/medical information that have been determined to be more sensitive than other personal medical information such as Genetic Information Laws. No such legal provisions however were found with regard to brain data collected at health sector. According to the literature reviewed in medical research[606] as well as deducting from findings of international organizations' relevant reports,[607] there cannot be determined a single country providing specific regulations concerning neuroscientific research either. As a consequence, the general legal framework on research with human beings is commonly applied to the field of neuroscientific research in countries all over the world. However, the state of regulation on scientific research differs from country to country. France is one of the few countries with a specific national regulation on biomedical research. In Germany, scholars applying by analogy of the German court interpretation where it determined that "*DNA-samples of identification have to be protected according to the individual's right to determine the usage of his own personal data, and the coding part is part of the absolutely*

[601] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en
[602] The German Human Genetic Examination Act of 2010 determine the requirements for genetic examinations and genetic analyses and was adopted to prevent discrimination and harm on the basis of genetic characteristics and for the protection of human dignity and right to self-determination.
[603] Portugal's Personal Genetic Information and Health Information Act in 2005 (Lei No 12/2005 de Janeiro) governs performance of the genetic tests, use of genetic information and research.
[604] The Act on genetic integrity prohibits the use of or demanding genetic information without a support of legal provision as a precondition for any agreement.
[605] In the field of the processing of particular categories of data, with reference to genetic and health data, Article 2 of the Data Protection Code require the Garante to establish, on a two-yearly basis, provisions aimed at identifying "*the security measures, such as …pseudonymization procedures, minimization measures, specific methods of selective data access and to provide information to data subjects, as well as other necessary measures to guarantee the data subjects' rights*."
[606] E.g, T. Spranger, International, Neurolaw: a comparative analysis, Springer, 2012
[607] Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019

protected core of personality",[608] conclude that individual brain data is protected by the German constitutional guarantee for self-determination or self-reservation. Along with the above mentioned countries, Italy also does not have any specific legal act dedicated to neuroscientific research.

7.2 The key elements of legal framework applicable to BCI and processing of neuro-data in the U.S.

When it comes to statutory law, the US mostly takes a sectoral approach to privacy legislation. There are only few statutory acts which can be considered having more or less overarching effect. It should however be mentioned that the Fair Information Practices Principle (FIPP)currently applied as the basis of universal data protection principles worldwide, also recognized in the GDPR, were developed by the United States Department of Health Education and Welfare in 1973 for protecting citizens' rights in the context of increased electronation of information and collection of voluminous personal data by the development of computer technology. Moreover, after brief review of the U.S. law, it is clear that although as in Europe there is no specific legislation provision dedicated to BCI, more general provisions covering health sector data together with device regulations are better equipped to deal with peculiarities of BCI application.

The HIPAA privacy regulations[609]- known collectively as the "Privacy Rule" which came into force in 2003, are based on FIPP and set forth rules governing the access, use, and disclosure of personal health information (or PHI), by "covered entities", which include healthcare providers (e.g. hospitals, laboratories, pharmacies,), health plans and healthcare clearinghouses. The 2009 HITECH Act expanded HIPAA's scope to include the "business associates" additional to covered entities.

HIPAA provides that a covered entity may not use or disclose PHI except either (1) as permitted by the Privacy Rule, or (2) as authorised in writing by the individual who is the subject of the

[608] Decision of the Federal Constitutional Court, cited in Germany as: BVerfGE 103, 21 (32 et seq.).
[609] *The Privacy Rule*, which sets national standards for when protected health information (PHI) may be used and disclosed; *The Security Rule*, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) and *the Enforcement Rule* contains provisions relating to compliance and investigations, and the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules.

information (or the individual's personal representative). The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes: For example: when required by law, public health activities reporting abuse or domestic violence; health oversight activities; judicial and administrative proceedings, etc.

It should be noted that HIPAA does not create a broad exception for research, rather uses exception of "research, under certain conditions". More specific provision about the use of research data is in the Regulations written by the Department of Health and Human Services (DHHS) for federally funded research with human subjects (the "Common Rule"). According to the Common Rule researchers must generally get consent from subjects or obtain an Institutional Review Board waiver to use identifiable data.

HIPAA is one of very few data privacy laws in the world that address data de-identification in technical detail. It defines, on the one hand, individually identifiable health information and, on the other hand, provides a list of 18 precisely named identifiers that shall be removed in order to achieve de-identified data. There are no restrictions on the use of de-identified (in other words, anonymous) data.

To sum up, with regard to health data, the U.S. federal regulations differentiate three categories data: identified patient data sets, limited data sets, and anonymized (de-identified) data sets. Identified data sets (that is, fully original data sets containing patients' identifiers) may only be released for research if broad informed consent from all patients has been obtained, whereas de-identified, or limited data sets can be shared without the consent.

Although the U.S. federal law applicable to medical data protects medical information and generally guards against unfair or deceptive practices, neither clinical nor research health information privacy structures contain specific rules or standards to limit access to BCI-generated data in ordinary cases.

In the U.S. also, medical information is protected through tort and contract law with breach of confidence cases. Some scholars claim that that duty of confidence which is *an agency-based approach* provides a better framework for developing an account of informational obligations in the protection of health data.

With regard to device regulations, unlike the European system, before medical devices can be marketed under the U.S. system, it is usually necessary to demonstrate that they are not only safe, but also *effective* (Under humanitarian Device exemption the demonstration of effectiveness is not needed). In Europe, however, manufacturers must only demonstrate that the device is safe and performs according to its intended use. This bring to a big difference between American and European legal systems, where in the former the number of tests the high-risk devices must pass are proportionate to the protection of patients interests and in the latter the speed of introduction of the devices into the market are disproportionate to the risks they pose.

It should be highlighted that improved evidence on the efficacy of neurodevices, (their inherent qualities, and sensitive functions including adequacy of enhancement, and acceptability by a user) is a particular priority, as there is uncertainty about the benefits, risks and mechanisms by which novel neurotechnologies achieve their effects.[610]

The U.S has *greater transparency* about the basis of all decisions on the conformity of devices with regulatory requirements where the Product Classification Database operates in a publicly accessible way and provide for free exchange of information on, for example, approved medical devices and incident reports. Currently, the EUDAMED, European equivalent of the US Product Classification Database is not open for consultation and is not publicly accessible. [611]

The U.S. also operates a Humanitarian Device Exemption (HDE) addressing conditions affecting fewer than 8,000 people in the USA per year.[612] It must however be mentioned that in the USA, the HDE has been subject to criticism. One group of commentators raised their concern about HDA -a simpler, cheaper, and faster approval process (which was used to approve DBS for the suppression of symptoms of severe OCD) – means that devices are not subject to sufficiently rigorous clinical investigation, potentially risking patient safety.[613] Additional concerns are about the potential commercial motivations of manufacturers to pursue the HDE, and that "*the humanitarian device exemption is being used to give the device manufacturer access to patients,*

[610] Chapter 7 of Novel neurotechnologies: intervening in the brain, Nuffield Council of Bioethics, 2013
[611] *Ibid*
[612] Section 3052 of the 21st Century Cures Act (Pub. L. No. 114-255
[613] Fins JJ, Mayberg HS, Nuttin B et al. Misuse of the FDA Humanitarian Device Exemption in deep brain stimulation for obsessive-compulsive disorder, *Health Affairs* Vol 30 No2 (2011) p 305.

rather than giving researchers access to subjects, or patients access to sound scientific evidence."[614]

The FDA considers implanted BCI devices to be "significant risk devices" because they are "intended as an implant and present a potential for serious risk to the health, safety, or welfare of a subject."[615] In order to study a significant risk, device can have in human subjects, a sponsor must receive approval of an investigational device exemption (IDE) application prior to beginning the investigation.[616] Investigational BCI devices are generally evaluated by the Division of Neurological and Physical Medicine Devices (DNPMD), one of seven divisions in CDRH's Office of Device Evaluation (ODE).

A number of pathways exist to study BCIs including: [617]

- Early Feasibility Study (EFS) through IDE: a limited clinical investigation of a device early in development, typically before the device design has been finalized (e.g., innovative device for a new or established intended use, marketed device for a novel clinical application).[618]
- First in Human (FIH) Study: a type of study in which a device for a specific indication is evaluated for the first time in human subjects.
- Traditional Feasibility Study: a clinical investigation that is commonly used to capture preliminary safety and effectiveness information on a near-final or final device design to adequately plan an appropriate pivotal study.
- Pivotal Study: a clinical investigation designed to collect definitive evidence of the safety and effectiveness of a device for a specified intended use, typically in a statistically justified number of subjects. It may or may not be preceded by an early and/or a traditional feasibility study.

Also, the U.S. like EU does not have BCI specific legislation. However, FDA's objective along with ensuring public safety is to provide neuroelectronic developers with sound device regulation

[614] *Ibid.*
[615] 21 CFR 812.3(m)
[616] 21 CFR 812.20
[617] FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.
[618] Investigational Device Exemptions (IDEs) for Early Feasibility Medical Device Clinical Studies, Including Certain First in Human (FIH) Studies Guidance for Industry and Food and Drug Administration Staff http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm279103.pdf

procedures in order avoid the situation when device developers and those seeking to use neuroelectronic devices shift their development, testing and surgical installation activities overseas. At the federal level, it has also been acknowledged that a transnational device regulation regime may be required for effective regulation of the development and use of BCI devices. For this purposes, the FDA conducts transnational regulation pilot programs with its counterparts, such as Japan.[619] The U.S. also was one of the initiators for the establishment of the International Medical Device Regulators Forum, which is a group of countries that works towards acceleration of international medical device regulatory harmonization and convergence.

Lastly, it should be mentioned that the U.S. government and professional legal bodies have recognized the emergence of new ethical and legal challenges with recent development of the neuroscience. For instance, in 2013, US President Obama brought into the attention the potential impact of neuroscience on human rights, raising the need to address questions such as those "*…relating to privacy, personal agency, and moral responsibility for one's actions; questions about stigmatization and discrimination based on neurological measures of intelligence or other traits; and questions about the appropriate use of neuroscience in the criminal-justice system*"[620]

With regard to the informational security of active implantable medical devices, the US Government Accountability Office also acknowledged that threat is sufficiently plausible and serious and therefore the U.S. FDA should develop a plan for "*enhancing its review and surveillance of medical devices as technology evolves* [to] *incorporate the multiple aspects of information security*".[621]

The Association of the Bar of the City of New York, among all others, observed that although genetic data and neuro data have a few similarity, unlike genetic data which is considered as specific category of sensitive data,[622] neuro-data have not been recognized as one and therefore stricter control over security of data sharing platforms are not yet in place.

[619] U.S. - Japan Medical Device Harmonization by Doing (HBD), http://www.pmda.go.jp/int-activities/int-harmony/hbd/0015.html (last visited 19 October 2019)
[620] Presidential Commission for the Study of Bioethical Issues, 2014.
[621] United States Government Accountability Office: Report to Congressional Requesters Information security of active medical devices, 2012, available at: http://www.gao.gov/assets/650/647767.pdf, last accessed on 27 October.
[622] See the US DNA Genetic Information Non-discrimination. Act of 2008

Chapter VIII Conclusion

Advances in scientific fields such as neuroscience, engineering and information technology has opened vast prospects for understanding brain function and treating neurological and mental disorders. Those promising new approaches are based on the ability to record and stimulate neural activity with ever-increasing precision. This precision has resulted to the rapid expansion of neural interface devices which is one of the most promising areas of research in the diagnosis and treatment of disorders of the nervous system. A distinguishing aspect of a neural interface is its function as a stimulation or brain signal monitoring and translation device. The term brain-machine interface (BMI) or brain-computer interface (BCI)-is used to describe this artificial intelligence system that can recognize a certain set of patterns in brain signals following five consecutive stages: signal acquisition, signal enhancement, feature extraction, classification, and translation of the signal into command. Different thinking activities in humans result in different patterns of brain signals. BCI's artificial intelligence system can recognize a certain set of those patterns. As shown in Chapter II, in doing so BCI extracts some features from brain signals that reflect similarities to a certain class as well as differences from the rest of the classes. BCI relies on the recording process that measures electrophysiological activity generated by electro-chemical transmitters exchanging information between neurons which are monitored by electroencephalography, electrocorticography, and/or intracortical electrical signal acquisition in single neurons. Conventional neuroimaging methods, however, are only able to measure the hemodynamic response (a process in which the blood releases glucose to active neurons at a greater rate than in the area of inactive neurons), that is in contrast to electrophysiological activity, is not directly related to neuronal activity.

Since BCI applications potentially represent a powerful tool for revealing hidden information in the user's brain without it being expressed, the issues of data integrity, data security, and privacy are important issues to consider. It is not disputable that better recording of brain activity and the corresponding data processing provide more help in alleviating the consequences of a disease or disability and restoring patient's quality of life. However, these neuro-data derived from the patient's brain also become more "sensitive" the more precisely it is interpreted.

While drugs and genetic modifications can also interfere with our identities and affect us in certain ways, no biotechnology can have the same power to penetrate and alter our personality in real time as does BCI.

As mentioned in Chapter III of this thesis, due to its novel nature, there is not yet a unified concept explaining moral value of privacy in the context of BCI. Some describe a number of scenarios where BCI may affect different types of privacy. For instance, according to Finn et al, BCI "*carry the potential to impact upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of thoughts and feelings*." [623]

Also, first in Finn et al, it was recognized that the previously identified privacy typology of *freedom of thought and feelings* are coming under threat as a direct result of new and emerging technology-BCI. Because, it has now been clear that "*information from brain computer interfaces may be able to recognise and identify patterns that shed light on certain thoughts and feelings of the carrier*."

Dening et al identified potential security threats against implanted neural devices and introduced the term "neurosecurity" for the protection of the confidentiality, and integrity of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will.

Very recently, in 2018, Klein and Rubbel identified three privacy typologies affected by BCI, physical privacy, informational privacy and decisional privacy. While, physical privacy is an important topic in itself, the focus of current research has been mainly on informational and decisional privacy affected with the collection of neuro-data by the BCI.

Apart from being used as communication device for paraplegic patients as an experiment or licensed for treating diseases such as epilepsy, implantable neural interfaces are currently studied within a number of ongoing national and transnational research programmes such as the U.S. Brain Research through Advancing Innovative Neurotechnologies (BRAIN) initiative, the European Union's Human Brain Project, the Strategic Research Program for Brain Sciences, etc. Brain data is the main resource for any BCI research, and experimental or standard treatments in the process of which large amounts of neuro-data are generated from research participants' or patients' intracortical, subdural, and extracranial sources. Data flowing from a BCI may include different

[623] Finn et al, Seven types of privacy, 2013

types of information starting from treatment regimens, physiological and psychological information, to very private cognitive information about memories, feelings, preferences, religious and other beliefs of the patient as well as metadata about the patient and the device. As such, concerns have been raised about the collection and use of these data that generate risk to privacy.

Novel and unique characteristics of neuro-data collected with BCI are categorized as below:

1. Brainwaves can be recorded on real-time for over prolonged period without individual's awareness, and therefore can undermine informed and explicit consent to the collection and use of that information.
2. Brain signals similar to DNA are individual to every human and can be used as a unique identifier. Also, the inherence of neuro-data to the human it belongs makes it almost impossible to disassociate from that data subject (i.e. to de-identify or pseudonymize). Certain forms of neuro-data are the reflection of the individual's unique brain function.
3. Neuro-data may reveal such unique information that might even not known to the person himself/herself.
4. Neurodata collected through BCI may allow to have insight into 'real time' brain processes, allowing the direct recording of processes associated with personality, mood, behaviours, preferences, thoughts or emotional state and feelings.
5. Data monitoring and recording techniques as well as translation algorithms for its interpretation are not at that advanced level yet to allow exact comprehension of all collected data. Information can be gathered more than required or not all the gathered information can be interpreted or interpreted accurately. However, it also worth mentioning that the field of neurotechnology and abilities of artificial intelligence is evolving constantly.

Although neuroscientific developments have started to be approached from a legal point of view in different countries all over the world, there has not yet been a single country where significant legislative initiatives have been undertaken. This holds true for regulating the BCI as distinct device or recognising neuro-data as a new type of data in the legal context. I examined privacy and data protection regimes and medical device regulations in the EU law and the U.S along with concisely reviewing national legal frameworks of EU member states applicable to health care and medical research in Chapters IV-VII. Even though in the U.S. transparent device regulatory regime provides for stronger protection of effective device development, its sensitive/health data

protection regime has too many exceptions when it comes to data sharing and neither clinical nor research information guidance structures contain specific rules or standards to limit access to BCI-generated data under ordinary circumstances.

In the EU, even improved data device regulation is light touch to the level that in some cases BCI can receive market or use approval without showing the safety and adequacy of the device with proper clinical evaluation/investigation. Although the GDPR, has adopted a number of novel principle and requirements such as privacy by design or stronger data controller accountability and improved data subject rights, if looked in detail it is not constructed to deal with the unique demands of neuro-data protection. In structure, the GDPR somehow stays similar to the Data Protection Directive, despite the fact the technologies that it aims to regulate have changed prominently. To give an example, as the DPD the GDPR also does not apply to anonymous data. But anonymisation cannot be considered enough for preserving privacy where re-identification remains a persistent risk in light of emerging neuro-technologies. Further, it does not fully harmonise the law on data protection in the EU region, because it grants the member states a wide margin of manoeuvre with regard to providing exceptions to data protection, for instance in research or for public interest purposes.

In the EU region, the legislation covering healthcare remains in the competence of each member state and is thus also falls outside the scope of EU law- that means health data protection during the clinical treatment are regulated at the national level differently. As mentioned above, I have briefly reviewed relevant laws of few selected EU members countries to reveal that none of them possesses any *lex specialis* provision in their legislation to address neuro-data, although some countries have specific laws on DNA.

Based on these specific challenges, I observe that current EU regional privacy legal framework and medical device regulations, as well as health data protection safeguards of national laws are not sufficient to adequately address the emerging neurotechnological issues.

Law can protect what is “tangible” (actual), which can be understood and observed. Until now, thoughts have been an abstract notion, with the development of neuroscience and brain recording techniques however, it has become clear that thinking makes physiological changes through electro-chemical activity in human brain which can be traced. The latest developments in neuroengineering (the emergence of brain-computer interfaces) call for alterations in the classic

conception of privacy/freedom of thought and analogous human right which once was designated to protect one's right to holding opinions, practicing religion or having political determination. This idea that has already found its justification in the treatises of advocates of "cognitive liberty" from the late XX century. However, with the development of BCI, numerous other scholars- Dening et al, Adorno et al, Hallinan et al, narrowed it down to the recognition of neuro-specific rights or development of neuro-data protection provisions specifically tailored to characteristics of brain information to address new challenges brought with advancements of neurotechnology. It is recommended that such normative response should have foundations at human rights law, if not then at least a new legal conception in data protection framework for neuro privacy should be developed. Suggested *lex specialis* approach is aimed at protecting patients against unqualified access to their brain information and prevent the unauthorized sharing of brain data.

References

Table of Cases

European Court of Human Rights

Folgerø and Others v. Norway, ((2008) 46 EHRR 47

Friedl v Austria (1996) 21 EHRR 83

Goodwin v United Kingdom (2002) 35 EHRR 18

KH v Slovakia (2009) 49 EHRR 34

Malone v United Kingdom (1985) 7 EHRR 14

Mockutė v. Lithuania, [2018] ECHR 200

Niemietz v Germany (1992) 16 EHRR 97

Peck v United Kingdom (2003) 36 EHRR 41

Perry v United Kingdom (2004) 39 EHRR 3

PG and JH v United Kingdom (2008) 46 EHRR 51

Rotaru v Romania (App No 28341/95) (unreported) 4 May 2000

Vgt Verein Gegen Tierfabriken v Switzerland (2001) 34 EHRR 159

Von Hannover v Germany (No. 1) (2005) 40 EHRR 1.

X and Y v Netherlands (1985) 8 EHRR 235

Z v Finland (1998) 25 EHRR 371

European Union

Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Hartmut Eifert [2010] ECR I-1106

Case C-582/14 Breyer v Bundesrepublik Deutschland. 2016. ECLI:EU:2016:779.

Case C-139/01 Österreichischer Rundfunk and Others [2003] ECRI-4989

Case C-288/12 European Commission v Hungary [2014] OJ C175/6

Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Grand Chamber, 6 October 2015)

Case C-461/10 Bonnier Audio AB et al v Perfect Communication Sweden AB [2010] OJ C317/24

Case C-219/11, Brain Products GmbH v BioSemi VOF and Others, 22 November 2012

Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 9 March 2017

National- United Kingdom

Campbell v Mirror Group Newspapers [2004] UKHL 22

Ashworth Security Hospital v MGN [2002] UKHL 29

Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109

Fairstar v Adkins [2012] EWHC 2952 (TCC)

W, X, Y and Z v Secretary of State for Health et al [2015] EWCA Civ 1034

National- United States

Griswald v. Connecticut, 381 U.S. 479 (1965)

Roe v. Wade, 410 U.S. 113 (1973)

Lawrence v. Texas, 539 U.S. 558 (2003)

Whalen v. Roe, 429 U.S. 589 (1977)

MobilOilCorp.v.Rubenfeld,339N.Y.S.2d623,632(Civ.Ct.1972)

Simonsen v. Swenson, 177 N.W. Neb. 1920, at 832

McCormickv.England,494S.E.2d431,432(S.C.Ct.App.1997)

Griswold v. Connecticut, (381 U.S. 479 1965)

Wyatt v. Fletcher, 718 F.3d 496, 505 (5th Cir. 2013).

Nunes v. Mass. Dep't of Corr., 766 F.3d 136, 144 (1st Cir.)

Simonsen v. Swenson, 177 N.W. Neb. 1920, at 832

Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793 (D. Ohio 1965).

Doyle v. Wilson, 529 F. Supp. 1343, 1348 D. Del. 1982

Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905) para69

Stephens v A very [1988] Ch 449 at 455; [1988]2 All ER 477

Germany

Constitutional Court, Dec. 15, 1983, *EuGRZ*, 1983

International documents

United Nations documents

International Covenant on Civil and Political Rights G.A. Res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6313 (1966) 999 UNTS 171

International Covenant on Economic, Social and Cultural Rights G.A. Res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 49, UN Doc. A/6316 (1966) 993 UNTS 3

Universal Declaration on Human Rights (1948) G.A. Res. 217 (111) of 10 December 1948, UN Doc. A/810 (1948)

General Comment No. 16: Article 17 (Right to Privacy, Family, Home and Correspondence and Protection of Honour and Reputation) 8 April 1988, Adopted at 32nd Session of the Human Rights Committee

Universal Declaration on the Human Genome and Human Rights G.A. Res. 152, UN GAOR, 53rd Sess., UN. Doc A/53/625/Add.2 (1998)

Universal Declaration on Bioethics and Human Rights adopted by UNESCO's General Conference on 19 October 2005

General Assembly, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18 December 2013;

General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19 November 2014

WHO International Guidelines for Biomedical Research involving Human Subjects" (CIOMS-Guidelines) of 2016,

Council of Europe Conventions

Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5; 213 UNTS 221

First Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms CETS No. 009

Convention for the Protection of individuals with regard to Automatic Processing of Personal Data (1981, ETS No. 108)

Council of Europe, Convention for the Protection of Human Rights and the Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, ETS. No. 164 (1997)

Additional Protocol to the Convention on Human Rights and Biomedicine concerning genetic testing for health purposes (2008)

Council of Europe Recommendations

Recommendation No. R (90) 13 of the Committee of Ministers to Member States on Prenatal Genetic Screening, Prenatal Genetic Diagnosis and Associated Genetic Counselling (21 June 1990)

Recommendation No. R (92) 3 of the Committee of Ministers to Member States on Genetic Testing and Screening for Health Care Purposes (10 February 1992)

Recommendation No. R (97) 5 on the Protection of Medical Data (13 February 1997)

Recommendation CM (Rec 2010) 11 of the Committee of Ministers to Member States on impact of genetics and training of health organisation of health care services and training of health professionals (29 September 2010)

Documents of European Union

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.

Consolidated Version of the Treaty on the Functioning of the European Union (2012) OJ C 326

EU, Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389 and [2012] OJ/C 326/02

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119

Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Regulation (EU) no 536/2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, amending Directive 2001/83/EC

Regulation (EU) 2017/746 (IVDR)on In Vitro Diagnostic Medical Devices

Regulation No 207/2012 of 9 March 2012 on Electronic Instructions for Use of Medical Devices,

Directive 2001/95/EC of 3 December 2001 on General Product Safety,

Directive 93/42/EEC as Regards Medical Devices Incorporating Stable Derivatives of Human Blood or Human Plasma.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)

Other international documents

Nuremberg Code of Medical Ethics 1947,

The World Medical Association’s Declaration of Geneva of 1948, with its revised mention of 2017,

The International Code of Medical Ethics of 1949,

The World Medical Association’s Declaration of Helsinki of 1964, with its latest revision of 2013,

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

The EMA Guideline for Good Clinical Practice of 2015

Bibliography

1. Alan B. V., Comment, Breach of Confidence: An Emerging Tort, Columbia Law Review Vol 8, No 1426, (1982) pp1460-61.
2. Alan, W., Privacy and Freedom, 25 Wash. & Lee L. Rev. 166 (1968).
3. Allison et al, Toward Smarter BCIs: Extending BCIs through Hybridization and Intelligent Control, Journal of Neural Engineering, Vol 9 No1, (2012).
4. Allison, B. Z., & Neuper, C. Could anyone use a BCI? In Applying our Minds to Human-Computer Interaction (pp. 35-54). London: Springer Verlag. (2010).
5. Allison B.Z., Legal and Ethical Issues in the Regulation and Development of Engineering Achievements in Medical Technology: A 2006 Perspective, Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, Aug 30-Sept 3, 2006.
6. Anand K, Saini S, Singh B, Veermaram C. Global medical device nomenclature: the concept for reducing device-related medical errors. Young Pharmaceuticals. 2(4), (2010). pp403–409.
7. Angelakis, E.; Stathopoulou, S.; Frymiare, J.; Green, D.; Lubar, J.; Kounios, J. EEG neurofeedback: A brief overview and an example of peak alpha frequency training for cognitive enhancement in the elderly. Clinical. Neuropsychology. Vol 21, 2007, pp. 110–129.
8. Arendt, H., The Human Condition, The University of Chicago Press (1958).
9. Armellin, G., et al., "Privacy preserving event driven integration for interoperating social and health systems," Secure Data Management 7th VLDB workshop (2010): 6368.
10. Aurucci, P., Secondary use of clinical trial data in the Italian legal framework in the futures of eHealth – introducing the social, legal and ethical challenges, Thomas Christian Bächle and Alina Wernick, 2019.
11. Bächle, T., and Wernick, A., The futures of eHealth – introducing the social, legal and ethical challenges, 2019.
12. Bai, O.; Rathi, V.; Lin, P.; Huang, D.; Battapady, H.; Fei, D.; Schneider, L.; Houdayer, E.; Chen, X.; Hallett, M. Prediction of human voluntary movement before it occurs. Clinical Neurophysiology. Vol 122 (2011) pp364–372.
13. Baillet, S.; Mosher, J.C.; Leahy, R.M. Electromagnetic brain mapping. IEEE Signal Processing Magazine. Vol 18, (2001) 14–30.
14. Bashashati A, Fatourechi M, Ward RK, Birch GE., A survey of signal processing algorithms in brain–computer interfaces based on electrical brain signals, Neural Engineering, Vol 4. (2007).
15. Bazelon, Probing Privacy, 12 Gonzaga Law Review. Vol 587, No 592 (1977).
16. Beaney, W., The Right to Privacy and American Law, Law & Contemporary. Problems.1966.
17. Benabid, A. L., P. Pollak, C. Gervason, D. Hoffmann, D. M. Gao, M. Hommel, J. E. Perret, and J. de Rougemont. Long-term suppression of tremor by chronic stimulation of the ventral intermediate thalamic nucleus. Lancet 337 (1991) pp.403–406.
18. Bennett C., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, 1992.

19. Beyleveld D., Data Protection and Genetics: Medical Research and the Public Good (2007) 18 King's Law Journal 275, 284–85.
20. Birbaumer, N., Murguialday, A. R., and Cohen, L., Brain–computer interface in paralysis. Current. Opinion. Neurology. Vol 21, (2008) pp 634–638.
21. Birbaumer, N.; Elbert, T.; Canavan, A.G.; Rockstroh, B. Slow potentials of the cerebral cortex and behavior. Physiological Reviews. Vol 70 (1990) pp 1–41.
22. Blitz, Freedom of thought for the extended mind: Cognitive enhancement and the constitution. Wisconsin Law Review, 2010.
23. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, The New York University Law Review Vol 962 No 971 (1964).
24. Boire R.G., Searching the brain: The fourth amendment implications of brain-based deception detection devices, American Journal of Bioethics, (2005).
25. Boire, R.G., Mind matters. Journal of Cognitive Liberties. 2003.
26. Boire, R. G., On cognitive liberty I. Journal of Cognitive Liberties, 1, 7–13. 1999/2000.
27. Bonaci et al, App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces, 2014 IEEE Int'l Symp. on Ethics in Sci., Tech. & Eng'rg at 1-7, reprinted in IEEE Tech. & Soc'y Mag., June 2015.
28. Bonaci et al, Application of BCI, 2014; Prescient report; BMI Privacy Australia, 2017.
29. Bonaci T, et. al, App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces. 2014.
30. Bouchard, K. E., Conant, D. F., Anumanchipalli, G. K., Dichter, B., Chaisanguanthum, K. S., Johnson, K., and Chang, E. F. High-resolution, non-invasive imaging of upper vocal tract articulators compatible with human brain recordings. PloS One, Vol 11 No 3: (2016).
31. Bouton C. E. et al., "Restoring cortical control of functional movement in a human with quadriplegia," Nature, 2016.
32. Brumberg, J. S., Krusienski, D. J., Chakrabarti, S., Gunduz, A., Brunner, P., Ritaccio, A. L., and Schalk, G., Spatio-temporal progression of cortical activity related to continuous overt and covert speech production in a reading task. PloS One, Vol 11 No11(2016).
33. Brunner, P., Ritaccio, A. L., Emrich, J. F., Bischof, H., and Schalk, G. Rapid communication with a "P300" matrix speller using electrocorticographic signals (ECoG). Front Neuroprosthestics, Vol 5 No 5, (2011), pp1–9.
34. Bublitz C., My Mind Is Mine!? Cognitive Liberty as a Legal Concept in Cognitive Enhancement: An Interdisciplinary Perspective, ed. Hildt E, Franke A, 2013.
35. Bublitz, C., Cognitive Liberty or the International Human Right to Freedom of Thought in Handbook of Neuroethics, edited by Clausen J. and Levy N., 2015.
36. Burkert H., 'Dualities of Privacy – An Introduction to 'Personal Data Protection and Fundamental Rights", in Privacy- New visions, ed. Perez M., Palazzi A., Poullet, Y., Cahier du Crid, (2008).
37. Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada.: Tri-council policy statement: ethical conduct for research involving humans. http:// www.ncehr-cnerh.org/english/code_2/ (2010). Accessed on 26 October 2019.

38. Chan, E., The Food and Drug Administration and the Future of Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement, John Marshall Journal of Computer & Information Law, Vol 25, 2007.
39. Chapin J.K., Using multi-neuron population recordings for neural prosthetics. Neuroscience Vol 7, (2004) pp 452–455.
40. Chi, Y.M., Jung T., Cauwenberghs G., Dry-contact and noncontact biopotential electrodes: methodological review, Biomedical Engineering, IEEE Vol 3 No 1(2010) pp06-119.
41. Chiu, Y., Mind Reading to Predict the Success of Online Games, February 2013.
42. Clarke R., "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, 2016.
43. Comandé, G., Medical Law in Italy, Wolters Kluwer Law & Business, 2014.
44. Cossu M., et al., "Stereoelectroencephalography in the presurgical evaluation of focal epilepsy: A retrospective analysis of 215 procedures," Neurosurgery, vol. 57, pp. 706–18, (2005), pp 706–718.
45. Curran, E.A., and Maria J. S., 2003. Learning to control brain activity: A review of the production and control of EEG components for driving brain–computer interface (BCI) systems. Brain Cogn 51 (3).
46. Davey S., Anderson J., Meenan B., An overview of current classification systems for healthcare devices and their limitations, (Multidisciplinary Assessment of Technology Centre for Healthcare (MATCH) Deliverable 2, P1 D2 V2.0 051025, www.match.ac.uk.
47. Debbie, K., The Evolution (or Devolution) of Privacy, Sociological Forum Vol 20, (2005).
48. DeCew, J., In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Cornell University Press, Ithaca (1997).
49. deCharms, et. al, Control over brain activation and pain learned by using real-time functional MRI. Proceedings of the National Academy of Sciences, USA Vol 102 (2005)pp 18626–18631.
50. Denning T., Matsuoka Y., Kohno T., Neurosecurity: Security and Privacy for Neural Devices, Neurosurgical Focus, Vol 27 No1, 2009, pp1-4.
51. Donchin, E., et al., "The mental prosthesis: Assessing the speed of a P300- based brain–computer interface," IEEE Trans. Rehab. Eng., vol. 8, (2000) pp. 174–179.
52. Donoghue, J.P., Bridging the brain to the world: A perspective on neural interface systems. Neuron Vol 60 (2008) pp 511–521.
53. Dornhage et al., Toward Brain-Computer Interfacing, MIT press, 2007.
54. Dove, E., and Phillips, M., Privacy Law, Data Sharing Policies, and Medical Data: A Comparative Perspective, in Medical Data Privacy Handbook, ed. Aris Gkoulalas-Divanis, Grigorios Loukides, Springer 2015.
55. Eckmiller, R., System identification of leaming retina encoders for a retina implant, Investigative. Ophthalmology. & Visual Science. No 38 (1997).
56. Engle, E., The history of the general principle of proportionality: an overview. Dartmouth Law Journal 1, 11 (2012).
57. European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, (25 April 2018).

58. Evarts E., Pyramidal tract activity associated with a conditioned hand movement in the monkey. Neurophysiology, Vol 29 No 6 (1966) pp1011-27.
59. Farah, M., "Neuroethics: The practical and the philosophical", Trends in Cognitive Sciences, Vol. 9, No. 1, 2005, pp. 34-40.
60. Farwell L. A, Donchin E., Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials. Electroencephalography Clinical Neurophysiology. Vol 70 No 6 (1988) pp510-523.
61. FDA Discussion paper for the "Brain-Computer Interface (BCI) Devices for Patients with Paralysis and Amputation" Public workshop, Maryland, November 21, 2014.
62. Fenton, A., and Alpert, Extending our view on using BCIs for locked-in syndrome. Neuroethics Vol 2 No1 (2008) pp119– 132.
63. Fetz, E., Finocchio, D., Operant conditioning of specific patterns of neural and muscular activity. Science No 174 (1971) pp 431–435.
64. Fetz, E., Operant conditioning of cortical unit activity. Science No163 (1969) pp 955–958.
65. Finn, R., Wright D., and Friedewald, M., "Seven Types of Privacy." In European Data Protection: Coming of Age?, edited by Gutwirth, S., Leenes, R., Hert P., et al. Dordrecht: 2013.
66. Fins J.J., Mayberg H.S., Nuttin B. et al. (2011) Misuse of the FDA Humanitarian Device Exemption in deep brain stimulation for obsessive-compulsive disorder Health Affairs 30(2): 302-11, at p 305.
67. Floridi, L., The ontological interpretation of informational privacy, Ethics and Information Technology, 2006.
68. Fried, C., Privacy, Yale Law Journal, Vol 77 No 475, (1968).
69. Friedevald et al, Privacy, data protection and emerging sciences and technologies: towards a common framework, The European Journal of Social Science Research, 2010.
70. Gavison, R., Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, 1980.
71. Georgopoulos A., et al., Neuronal Population Coding of Movement Direction, Science, Vol 233 1986 pp 1416-19.
72. Georgopoulos et al. Synchronous neural interactions assessed by magnetoencephalography: A functional biomarker for brain disorders. J. Neural Engineering. 2007, doi: 10.1088/1741-2560/4/4/001.
73. Giulio M., and Haselager, P., Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, Science Engineering Ethics, 2017.
74. Gladden, M.E. The Handbook of Information Security for Advanced Neuroprosthetics. Indianapolis: Synthypnion Academic. 2015.
75. GMC, Confidentiality: Protecting and Providing Information (2009), as updated by Good Medical Practice. 2013.
76. Graimann, B., Allison, B., Pfurtscheller, G., Brain-computer interfaces: a gentle introduction. In Brain-computer interfaces, ed. Graimann B, Berlin: Springer, 2010, pp 1–27.
77. Gross, H., The concept of Privacy, The New York University Law Review, Vol 42, 1967.
78. Gutwirth, S., Privacy and the information age, Rowman & Littlefield, 2002.
79. Hallinan, D., et. al, Neurodata and Neuroprivacy: Data Protection Outdated? Surveillance & Society Vol 12 No1: 2014, pp 55-72.

80. Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p 34.
81. Hanslmayr, S.; Sauseng, P.; Doppelmayr, M.; Schabus, M.; Klimesch, W. Increasing individual upper alpha power by neurofeedback improves cognitive performance in human subjects. Applied Psychophysiology Biofeedback, Vol 30, 2005, pp1–10.
82. Haselager, P., et al., A note on ethical aspects of BCI, Neural Networks 22 (2009) 1352–1357;
83. He, B., Gao, S., Yuan, H., & Wolpaw, J. R. Brain–computer interfaces. In Neural Engineering: Second Edition. Springer US. (2013). https://doi.org/10.1007/9781461452270, pp. 87-151.
84. Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, OECD Publishing, Paris, 2015 http://dx.doi.org/10.1787/9789264244566-en Last accessed on 24 October 2019.
85. Heersmink R., Embodied Tools, Cognitive Tools and Brain-Computer Interfaces, Neuroethics, 2013.
86. Herff, C., Heger, D., De Pesters, A., Telaar, D., Brunner, P., Schalk, G., and Schultz, T. Brain-to-text: Decoding spoken phrases from phone representations in the brain. Frontiers in Neuroscience, 9:217, 2015.
87. Hinterberger, T., Widman, G., Lal, T., Hill, J., Tangermann, M., Rosenstiel, W., Schölkopf, B., Elger, C., and Birbaumer, N. Voluntary brain regulation and communication with electrocorticogram signals. Epilepsy Behav, Vol 13 No2 (2008) pp300–306.
88. Hinterberger, T.; Schmidt, S.; Neumann, N.; Mellinger, J.; Blankertz, B.; Curio, G.; Birbaumer, N. Brain-computer communication and slow cortical potentials. IEEE Transactions on Biomedical Engineering, Vol 51, (2004) pp1011–1018.
89. Hochberg L.R., et al., "Reach and grasp by people with tetraplegia using a neurally controlled robotic arm," Nature, vol. 485, 2012, pp. 372–375.
90. Hochberg L.R., Serruya M.D., Friehs G.M., et al. Neuronal ensemble control of prosthetic devices by a human with tetra-plegia. Nature. Vol 442 No 7099, 2006, pp.164-171.
91. Hochmair I., et al., "Deep electrode insertion and sound coding in cochlear implants," Hearing Research., vol. 322, (2015) pp. 14–23.
92. HPRA Guide for Ethics Committees on Clinical Investigation of Medical Devices, 2010.
93. Hubel D., Tungsten Microelectrode for Recording from Single Units, Science. 22;125 (1957) pp549-50.
94. Humayun M. S., et al., "Interim results from the international trial of Second Sight's visual prosthesis," Ophthalmology, vol. 119, 2012, pp. 779– 788.
95. Ienca, M., Andorno, R.: 'Towards new human rights in the age of neuroscience and neurotechnology', Life Sciences, Society and Policy, 2017, 13, (1), pp. 5.
96. Ienca, M., Haselager, P., Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity, Ethics, Information, Technology, Vol 18, 2016, pp117–129.
97. Illes, J. and Racine, E. Imaging or imagining? A neuroethics challenge informed by genetics. American Journal of Bioethics, Vol 5, 2005, pp.5–1.
98. Inness J., Privacy, intimacy, and isolation, Oxford University Press, 1996.
99. Italian Data Protection Authority, Guidelines on the Electronic Health Record; Italian Ministry of Innovation and Technology, InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2., 2012.

100. James Q. W., The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Journal, Vol 113 (2004), pp 1153-54.
101. Kant I., Political Writings, 2nd edition, Cambridge texts in the history of political thought, 1991.
102. Kasper, D., "The Evolution (or Devolution) of Privacy", Sociological Forum, Vol. 20, No. 1, 2005, pp.69-92.
103. Katz, Comment, Unauthorized Biographies and Other "Books of Revelations": A Celebrity's Legal Recourse to A Truthful Public Disclosure, Vol 36 UCLA Law Review, 1989, p 819.
104. Kim T. I., et al., Injectable, cellular-scale optoelectronics with applications for wireless optogenetics, Science, vol. 340, pp. 211–216, 2013.
105. Klein E, Chapter 7 Neuromodulation ethics: Preparing for brain–computer interface medicine in Neuroethics Anticipating the Future, ed. Illes J, Oxford University Press, 2017.
106. Klein, E., et al., Engineering the Brain: Ethical Issues and the Introduction of Neural Devices, Hastings Center Report Vol 45 No 6, 2015; pp26-35.
107. Klein, E., Nam, C., Neuroethics and brain-computer interfaces (BCIs), Brain-Computer Interfaces, Vol3No3, 2016, pp123-125.
108. Klein E., Rubel A., Privacy and Ethics in Brain– Computer Interface Research in Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Nam et al., Taylor&Francis Group, 2018.
109. Kokott J., and Sobotta C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law Vol 3, 2013.
110. Koops et al, A Typology of Privacy, University of Pennsylvania Journal of International Law, 2017.
111. Kotov N.A., Winter J.O., Clements I.P., Jan E, Timko B.P. et al. Nanomaterials for neural interfaces, Advanced Materials Vol 21 (2009) pp3970-4004.
112. Kranenborg, Herke, Access to documents and data protection in the European Union: on the public nature of personal data, Common Market Law Review, vol. 45, 2008, 1079–1114, at 1093.
113. Krusienski D.J., Shih J. J. Control of a brain–computer interface using stereotactic depth electrodes in and adjacent to the hippocampus. J Neural Engineering, Vol 8 No 2, 2011.
114. Krusienski D.J., Shih J.J. Control of a visual keyboard using an electrocorticographic brain-computer interface. Neurorehabilitation Neural Repair. Vol 25 No4, (2011) pp323-331.
115. Krusienski D.J., Wentrup MG, Galán F, Coyle D, Miller KJ et al. Critical issues in state-of-the-art brain–computer interface signal processing, Neural Engineering Vol 8, 2011.
116. Kübler A, Neumann N, Kaiser J, Kotchoubey B, Hinterberger T, Birbaumer NP. Brain-computer communication: self-regulation of slow cortical potentials for verbal communication. Arch Phys Med Rehabil. Vol 82 No 11 (2001). pp 1533-1539.
117. Kutas et al., Augmenting mental chronometry: the P300 as a measure of stimulus evaluation time. Science, 1977.
118. Kyselo M., Locked-in syndrome and BCI: Towards an enactive approach to the self. Neuroethics. (2011) doi:10.1007/ s12152-011-9104-x.
119. Laureys S., Boly M., Tononi, G., Functional Neuroimaging. In The Neurology of Consciousness; Steven, L., Giulio, T., Eds.; Academic Press: New York, NY, USA, 2009; pp. 31–42.

120. Laurie G., et al., A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data. 2015.
121. Laurie G., Harmon S., Porter G. Mason and McCall Smith's Law and Medical Ethics. Oxford University Press. 2016,
122. Lebedev M., Nicolelis, M., Brain–machine interfaces: past, present and future, TRENDS in Neurosciences Vol.29 No.9, 2006.
123. Lebedev M., Nicolelis M.., "Toward a whole-body neuroprosthetic," Progress in Brain Research, vol. 194, 2011 pp. 47–60.
124. Leeb et al, A Hybrid Brain-Computer Interface Based on the Fusion of Electroencephalographic and Electromyographic Activities. Journal of Neural Engineering, Vol 8 No2, 2011.
125. Leuthardt E.C., Gaona, C., Sharma, M., Szrama, N., Roland, J., Freudenberg, Z., Solis, J., Breshears, J., and Schalk, G. Using the electrocorticographic speech network to control a brain–computer interface in humans. J Neural Eng, 8(3):036004, 2011.
126. Leuthardt E.C., Schalk, G., Roland, J., Rouse, A., Moran D., Evolution of brain-computer interfaces: going beyond classic motor physiology, Neurosurgery Focus, Vol 21 No1, 2009.
127. Li Z., O'Doherty J. E., Lebedev M. A., Nicolelis M. A., Adaptive decoding for brain-machine interfaces through Bayesian parameter updates. Neural computation, Vol 23, 2011, pp 3162–3204.
128. Lin Z., Owen A., Altman R.: Genomic research and human subject privacy. Science Vol 305, No5681, 2004, p 183.
129. Linksy O., The foundations of EU data protection law, Oxford University Press, 2015.
130. Maisel W., Improving the security and privacy of implantable medical devices, New England Journal of Medicine Vol 362 No13, 2010, pp1164-6.
131. Marcello, I., Andorno, R., Towards new human rights in the age of neuroscience and neurotechnology, Life Sciences, Society and Policy, 2017.
132. Marcello, I., Haselager, P., Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity, Ethics of Information Security, 2016.
133. Martin S., Brunner P., Iturrate I., Millán J. d. R., Schalk G., Knight R. T., and Pasley B. N., Word pair classification during imagined speech using direct brain recordings. Sci Rep, 6, 2016.
134. Martinovic I., Davies, D., Frank, M., Perito, D., Ros, T., Song, D. On the feasibility of side-channel attacks with brain– computer interfaces. In USENIX security symposium, 2012.
135. Maureen C., Laurent B., Fabien L., Brain–Computer Interfaces, Foundations and Methods, 2016.
136. Maynard, E., et al., Neuronal interactions improve cortical population coding of movement direction. Neuroscience. Vol 19, 1999, pp. 8083–8093.
137. Mazzone P., Lozano A., Stanzione P., Galati S., Scarnati E., Peppe A., Stefani A., Implantation of human pedunculopontine nucleus: a safe and clinically relevant target in Parkinson's disease. Neuro-reporting No 16 Vol17, 2005, pp 1877–1881.
138. McFarland, Wolpaw, Brain-Computer Interfaces for Communication and Control, Communications of the ASM, 2011, p. 63.

139. McGrail K., et al, Chapter 28 Building on Principles: The Case for Comprehensive, Proportionate Governance of Data Access in Medical Data Privacy Handbook, ed. Aris Gkoulalas-Divanis, Grigorios Loukides, Springer 2015.
140. Mecacci G., Haselager P., Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy, Science Engineering Ethics, 2017.
141. Michelfelder D., The moral value of informational privacy in cyberspace. Ethics and Information Technology, Vol3, 2001, pp129–135.
142. Middendorf M., McMillan G., Calhoun G., Jones K., Brain-computer interfaces based on steady-state visual evoked response. IEEE Transaction on Neural Systems and Rehabilitation Engineering Vol 8 No2, 2000, pp211–214.
143. Middlebrooks, et al., A panoramic code for sound location by cortical neurons. Science. Vol 264, 1994, pp842–844,
144. Millán J., Rupp R., Müller-Putz G., Murray-Smith R., Giugliemma C., Tangermann M., Vidaurre C., Cincotti F., Kübler A., Leeb R., Neuper C., Müller R., and Mattia D., Combining brain–computer interfaces and assistive technologies: state-of-the-art and challenges, Front Neuroscience, 2010.
145. Miller A.R., The Assault on Privacy: Computers, Data Banks, and Dossiers, 1971.
146. Moore, Privacy, Neuroscience, and Neuro-Surveillance, Springer Science+Business Media Dordrecht, 2016.
147. Moritz C. et. al, New Perspectives on Neuro-engineering and Neurotechnologies: NSF-DFG Workshop Report, IEEE Transactions on Biomedical Engineering, Vol. 63, no. 7, 2016.
148. Morshed, et al., A Brief Review of Brain Signal Monitoring Technologies for BCI Applications: Challenges and Prospects, Bioengineering Biomedical Sciences, Vol 4 No1, 2014.
149. Müller O., Rotter, S. Neurotechnology: Current Developments and Ethical Issues, Front System Neuroscience.; Vol 11 No 93, 2017.
150. Municipality of Trento. Regulations for the protection of personal data of the municipality of Trento. http://www.comune.trento.it/, 2007.
151. Nam et al, "Brain-Computer Interfaces Handbook - Technological and Theoretical Advances", Taylor&Francis Group, 2018;
152. Neergaard L., Obama shakes mind-controlled robot hand wired to sense touch. US News & World Report, 2016.
153. Newell, et al., Privacy in the family. In The social dimensions of privacy, ed Edited by Roessler, B., et al, Cambridge University Press. 2015.
154. Nicholson, et al, Shadow health records meet new data privacy laws; How will research respond to a changing regulatory space? Insight, 2019.
155. Nicolas-Alonso L., Gomez-Gil J., Brain Computer Interfaces, a Review, Sensors Vol 12, 2012, pp 1211-1279.
156. Nicolelis M.A., Actions from thoughts. Nature Vol 409, 2001, pp 403–407.
157. Nijholt, et al, Brain-Computer Interfacing for Intelligent Systems, Intelligent Systems, Vol 23 No3, 2008, pp72-79.
158. Nissenbaum H., “How computer systems embody values”, IEEE Computer, Vol. 34, No. 3, 2001.

159. Nissenbaum H., Privacy in Context: Technology, Policy and the Integrity of Social Life, Stanford University Press, 2010.
160. Nuffield Council on Bioethics: The collection, linking and use of data in biomedical research and health care: ethical issues. 2015. http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf (2015) last accessed on 30 October 2019.
161. Ohm P., 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', UCLA Law Review Vol 57, 2010, pp. 1701-1777.
162. Ortner R., Allison B., Korisek G., Gaggl H., Pfurtscheller G., An SSVEP BCI to control a hand orthosis for persons with tetraplegia, IEEE Transaction on Neural Systems and Rehabilitation Engineering, Vol 19 No1, 2011, pp1–5.
163. Palmerini E., A legal perspective on body implants for therapy and enhancement, International Review of Law, Computers & Technology, 2015.
164. Pacareu C.S., Morshed B.I., Power Optimization of NeuroMonitor EEG Device: Hardware/Software Co-Designed Interrupt Driven Clocking Approach, 6th Intl IEEE EMBS Neural Engineering Conf: 25-28. 2013.
165. Penfield W., Rasmussen T. editors. The Cerebral Cortex of Man. MacMillan, New York, 1950.
166. Philips M., International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), Human Genetics, Volume 137, Vol 8, 2018, pp 575–582.
167. Poldrack, Russell A., Gorgolewski K., Making big data open: Data sharing in neuroimaging. Nature Neuroscience, Vol 17 No 11. 2014, pp. 1510–1517.
168. Powell P., Buchan I., Electronic Records Should Support Clinical Research, Journal of Medical Internet Research Vol 7, 2005.
169. Räikkä J., Brain imaging and privacy. Neuroethics Vol 3, 2010, pp5–12.
170. Regan D., Human Brain Electrophysiology: Evoked Potentials and Evoked Magnetic Fields in Science and Medicine; Elsevier: New York, NY, USA, 1989.
171. Reiman J.H, Privacy, Intimacy, and Personhood, in Philosophical Dimensions of Privacy: An Anthology, Ferdinand, David Schoeman ed., 1984.
172. Robert G., Does Privacy Work? in Technology and Privacy: The New Landscape, edited by Agre P., and Rotengberg M., 1997.
173. Ronald G., Neural Technologies: The Ethics of Intimate Access to the Mind, Hasting Centre Report, 2015.
174. Rosenfeld J.P., et al, P300-based Detection of Concealed Autobiographical Versus Incidentally Acquired Information in Target and Non-target Paradigms. International Journal of Psychophysiology, Vol 60 No 3, 2006, pp251–259.
175. Rota, et al., Self-regulation of regional cortical activity using real-time fMRI: The right inferior frontal gyrus and linguistic processing. Human Brain Mapping. Vol 30, 2009, pp1605–1614.
176. Rotenberg M., Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), Stanford Technical Law Review. Vol 1 No44, 2001.
177. Sanei S., Chambers JA EEG Signal Processing, John Wiley & Sons, West Sussex, 2007.
178. Santos, et al, Medical device specificities: opportunities for a dedicated product development methodology, Expert Review Medical Devices, Vol 9, 2012.

179. Schalk G., Can electrocorticography (ECoG) support robust and powerful brain–computer interfaces? Front Neuroengineering ,Vol 3, 2010.
180. Schmitz-Luhn B., et al., Law and ethics of deep brain stimulation, International Journal of Law and Psychiatry 35, 2012, pp130–136.
181. Schneider F., et al, Self-regulation of slow cortical potentials in psychiatric patients: Alcohol dependency. Applied Psychophysiology Biofeedback, Vol 18, 1993, pp23–32.
182. Schneider F., et al., Self-regulation of slow cortical potentials in psychiatric patients: Depression. Applied Psychophysiology Biofeedback Vol 17, 1992, pp203–214.
183. Schneider J., Fins J., Wolpaw J., Ethical issues in BCI research Brain–Computer Interfaces: Principles and Practice, ed Wolpaw, J., and Wolpaw, E., Oxford: Oxford University Press, 2012.
184. Schwartz K., Solove D., Information Privacy Law, Aspen Publishing Co. 2018.
185. Sententia W., Neuroethical Considerations: Cognitive Liberty and Converging Technologies for Improving Human Cognition, Annals of New-York Academy of Sciences, 2004, p.1013.
186. Sepuldeva M., Van Banning T., van Genugten W., Human Rights Reference Handbook, Tilburg Law School, 2004.
187. Shih J.J., Krusienski D.J., and Wolpaw J., Brain-Computer Interfaces in Medicine, Mayo Clinic Proceedings, Vol 87 No 3 (2012); pp268-279.
188. Silvola S., Legal Landscape of Neuroscientific Research and Its Applications in Finland in International Neurolaw: a comparative analysis, Springer, 2012.
189. Smith R., Shao J.: Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research Vol7, 2007, pp 89–116.
190. Solove D., Conceptualizing Privacy, California Law Review Vol 90, 2001, pp. 1041–1043.
191. Solove D., A Brief History of Information Privacy Law, George Washington University Law School, 2006.
192. Solove D., A taxonomy of privacy, University of Pennsylvania Law Review, 2006.
193. Sorani M., John K., Sharma S., Manley G., Ferguson A., Cooper S., O'Connor K., et al. Genetic data sharing and privacy. Neuro-informatics Vol 13 No1, 2015, pp1–6.
194. Spencer K.M., Dien J., Donchin E., Spatiotemporal analysis of the late ERP responses to deviant stimuli. Psychophysiology Vol 38 No2, 2001, pp343–358.
195. Spranger T., International Neurolaw: a comparative analysis, Springer, 2012.
196. Stevovic J., et al, Enabling Privacy by Design in Medical Records Sharing, Chapter 16 in Reforming European Data Protection Law, Gutwirth, S., et al, Springer 2015.
197. Strehl, et al., Self-regulation of slow cortical potentials: A new treatment for children with attention-deficit/hyperactivity disorder. Pediatrics Vol 118, 2006, pp1530–1540.
198. Sturm I., Blankertz B., Potes C., Schalk G., Curio G., ECoG high gamma activity reveals distinct cortical representations of lyrics passages, harmonic and timbre-related changes in a rock song. Frontiers in Human Neuroscience, Vol 8 No798, 2014.
199. Suzana H., The human brain in numbers: a linearly scaled-up primate brain, Frontiers Human Neuroscience, Vol3, 2009, pp1-11.
200. Synofzik M., Vosgerau G., Voss M., The experience of agency: An interplay between prediction and postdiction. Frontiers in Psychology, Vol 4, 2013.

201. Szekely I., Regulating the future? Law, ethics, and emerging technologies, Journal of Information, Communication & Ethics in Society, Vol 9, 2011, pp180-194.
202. Taylor D.M., Tillery S.I., Schwartz A.B., Direct cortical control of 3D neuroprosthetic devices. Science. Vol 296, 2002, pp1829–1832.
203. The Academy of Medical Sciences.: A new pathway for the regulation and governance of health research. URL https://www.gov.uk/government/news/a- new- pathway- for- the- regulation-and-governance-of-health-research (2011). Accessed on 26 October 2019.
204. The British Medical Association's handbook of ethics and law, Medical Ethics Today, 2012.
205. The Privacy Shield, In-depth Analysis, European Parliamentary Research Service, 2018.
206. Thomas M., The Rights of Publicity and Privacy, Thomas and Reuters, 2019.
207. Thomson J. J., The right to privacy. Philosophy and Public Affairs, 1975.
208. Tice J.A., Helfand M., Feldman M.D., Clinical evidence for medical devices: regulatory processes focusing on Europe and the United States of America (Background Paper 3). WHO, Geneva, Switzerland, 2010.
209. Trimper J., Root Wolpe P., Rommelfanter K., When 'I' becomes 'we': ethical implications of emerging brain-to-brain interfacing technologies, Frontiers Neuroengineering. Vol 7, 2014.
210. Tzanou M., Data protection as a fundamental right next to privacy? 'reconstructing' a not so new right. International Data Privacy Law Vol 3, 2013, pp. 88–99.
211. U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems 29, 1973.
212. Ulmer S., et al, Impact of Incidental Findings on Neuroimaging Research Using Functional MR Imaging. American Journal Neuroradiology Vol 30 No 55, 2009.
213. Van der Sloot B., Legal Fundamentalism: Is Data Protection Really a Fundamental Right? in Data Protection and Privacy: (In)visibilities and Infrastructures, edited by Leenes, R., Springer, 2017.
214. Vansteensel M., Pels E., Bleichner M., Branco M., Denison T., Freudenberg Z., Gosselaar P., Leinders S., Ottens T., VandenEboom M., van Rijen P., Aarnoutse E., Ramsey N., Fully implanted brain– computer interface in a locked-in patient with ALS. The New England Journal of Medicine, Vol 375 No 21, 2016, pp2060–2066.
215. Veen E., Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. MLC Foundation, AL Den Haag, 2018.
216. Voigt P., Von dem Bussche A., The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.
217. Wahlstrom K., et al, Privacy and Brain-computer Interfaces: Identifying Potential Privacy Disruptions. SIGCAS Computer Society, Vol 46 No 1, 2016, pp.41-53.
218. Wahlstrom K., Fairweather B., Ashman H., 'Privacy and brain-computer interfaces: method and interim findings', Ethicomp/CEPE, 2017, pp. 1-26.
219. Wahlstrom K., Fairweather B., Ashman H., Privacy and Brain-Computer Interfaces: Identifying potential privacy disruptions, ACM Computers & Society, Vol 46, 2016, pp41-5.
220. Waldert S., Pistohl T., Braun C., Ball T., Aertsen A., Mehring C., A review on directional information in neural signals for brain-machine interfaces. J. Physiology. Vol 103 Paris, 2009, pp 244–254.

221. Walker J.E., Kozlowski G.P., Neurofeedback treatment of epilepsy. Child and Adolescent Psychiatric Clinics of North America, Vol 14, 2005, pp163–176.
222. Wang W., Collinger J. L., Degenhart A. D., Tyler-Kabara E. C., Schwartz A. B., Moran D. W., Weber D. J., Wodlinger B., Vinjamuri R. K., Ashmore R. C., et al. An electrocorticographic brain interface in an individual with tetraplegia. PloS One, Vol 8 No2, 2013.
223. Warren S.D., Brandeis L.D., The Right to Privacy, Harvard Law Review, Vol 4 No 5, 1890.
224. Wegmann H., Summary: Neurolaw in an International Comparison in International Neurolaw: a comparative analysis, ed. Spranger, Springer, 2012.
225. Westin A., Privacy and Freedom New York: Atheneum, 1967.
226. Wolpaw J.R., Birbaumer N., et al. Brain-computer interfaces for communication and control. Clinical Neurophysiology. Vol 113 No 6, 2002, pp767–791.
227. Wolpaw J.R., Brain-computer interfaces for communication and control. 'Clinical. Neurophysioogy. Vol 113, 2002, pp 767-791.
228. Wolpaw, J.R., Brain–Computer Interface Technology: A Review of the First International Meeting, IEEE Transactions on Rehabilitation Engineering, Vol. 8, No. 2, 2000.
229. Wolpaw J., Wolpaw E.W., editors. Brain-Computer Interfaces: Principles and Practice. Oxford University Press; Oxford: 2012.
230. Yijun W., Ruiping W., Xiaorong G., Bo H., Shangkai G., A practical VEP-based brain-computer interface. IEEE Transaction on Neural Systems and Rehabilitation Engineering., Vol 14, 2006, pp234–240.
231. Yuan H., Hee B., Brain-Computer Interfaces Using Sensorimotor Rhythms: Current State and Future Perspectives, IEEE Transactions on Biomedical Engineering. Vol 61 No5, 2014, pp1425–1435.
232. Zander, et al, Enhancing Human-Computer Interaction with input from Active and Passive Brain-Computer Interfaces. In Brain-Computer Interfaces, Desney Tan and Anton Nijholt editors, Springer, 2010, pp181-199.