ANALYSIS OF BRAIN COMPUTER INTERFACE INTEGRATED AUGMENTED REALITY AND PRIVACY PROTECTION APPROACHES IN THE EUROPEAN UNION

LL.M Law and Technology,

LL.M. Master in Law,

Tilburg Law School,

Tilburg University,

2017

Asli Gökçe Seven

ANR: 867503

Supervisor

mr.dr. C.M.K.C. Cuijpers

ANALYSIS OF BRAIN COMPUTER INTERFACE INTEGRATED AUGMENTED REALITY AND PRIVACY PROTECTION APPROACHES IN THE EUROPEAN UNION

1. INTRODUCTION

1.1. Background

Humans hold a tremendous wireless network in their brains. Brain Computer Interface ("BCI" hereinafter) technology is today where Fingerprint Recognition was few decades ago. These two plain yet thrilling facts have been motivating researchers who work in the realm of neuroprosthetics[1] to develop new devices and medical methodologies at an increasingly rapid rate. As neuroscience has come closer to explaining the dynamics of brain oscillations, BCI systems' success rates have been increasing. As BCI systems advances, their safety, usefulness and economic viability have been subject to careful examination by healthcare providers and commercial interests. For the first time in history, humankind has had the opportunity to explore the human mind. BCI advancements also challenge various legal concepts which makes it hard to argue that privacy is neatly tied to human persons or spatial elements.

The exciting rise of Augmented Reality (AR) in recent decades is undeniable. Most famously, Google Glass and Microsoft HoloLens have already been integrated into our daily lives.[2] Lastly, Facebook has announced its first AR Camera Effects developer platform in April 2017, as CEO, Mark Zuckerberg argued, "The first augmented reality platform that becomes mainstream isn't going to be glasses, it's going to be cameras."[3]

However, there is a problem detected in the absence of innovative and intuitive input methods. It is proposed that relying upon commands through keyboard, controllers, sensor gloves, eye-tracking and the

1 A discipline related to neuroscience and biomedical engineering concerned with developing neural prosthes, a series of devices that can substitute a motor, sensory or cognitive modality that have been damaged as a result of an injury or a disease.

2 Darly Deino, 'Microsoft's Mind-blowing HoloLens Needs Work, But Is No Google Glass' *HuffingtonPost* (5 May 2017) <http://www.huffingtonpost.com/daryl-deino/microsofts-mindblowing-ho_b_9823310.html< accessed 10 May 2017

3 Josh Constine, 'Faceook launches augmented reality Camera Effects developer platform' *Techcrunch* (18 April 2017) <https://techcrunch.com/2017/04/18/facebook-camera-effects-platform/> accessed 10 May 2017

hardness of grasping and controlling these inputs could stop AR products to be as widely prevalent as smartphones.[4]

Nevertheless, slowly but surely the AR ecosystem has been moving away from its conventional roots adhered to traditional input systems. A promising synergy between the two emerging technological fields is now underway, as BCI integrated AR is being studied in the realm of science, business and academics.

Researchers have already considered the question of whether BCIs may add value to the AR experience. A recent academic keynote speech in February 2017 touching on various aspects of *Integrating Brain-Computer Interface Technology Integration with Augmented and Virtual Reality* discusses a number of challenges such as usability of design as well as signal quality, also highlights that although we are still nowhere near understanding the brain in terms of decoding one's thoughts, we can detect how we orient our intention to things in the world.[5] This is of significance because it paves the way for the main principle behind BCI integrated AR; a recommended system in real time that erases the necessity of repeated behavioral responses. To visualize, it would not be required to even move one's eyes to command a robotic device in its physical environment, moreover, one would be able to scroll down the menu, select items or manipulate virtual objects in the physical environment. This opens the path to a scenario in which devices do not require behavioral inputs such as eye-tracking or gestures to operate, but merely the user's brain signals. Also, the integration of technology is widely anticipated to serve modalities to better understand the way the brain works, so that new therapies and applications may be developed in medicine.

4 Abhinav Lal, 'VR and AR Need Brain-Computer Interfaces to Achieve Their Full Potential' *Gadgets 360* (14 May 2015) <http://gadgets.ndtv.com/wearables/opinion/vr-and-ar-need-brain-computer-interfaces-to-achieve-their-full-potential-692413> accessed 10 May 2017

5 IEEE CESoc TV, 'Integrating Brain-Computer Interface Technology With Augmented and Virtual Reality. Paul Sajda' (12 February 2017) <https://www.youtube.com/watch?v=fn9eBJFvSuA> accessed 19 April 2017

1.2. Statement of the Problem

A piece of technology that can operate the control of robots in an AR environment by absorbing a person's thoughts and intentions, in other words, without issuing voice commands, raises intriguing questions about surveillance and other privacy intruding activities. An emerging field like BCI integrated AR technology demands an extensive privacy strategy in the light of the fundamental rights of law. The best privacy strategy, which would vary from one technology to the other, should maximize the technological advantages for users while cherishing the right to privacy. This research aims to precisely answer what regulation strategy is required to guarantee a strong privacy protection regarding BCI integrated AR in the European Union regulatory framework.

1.3. Research Question

As a result of the discussion presented above, the main research question is:

How may emerging forms of Brain Computer Interface integrated Augmented Reality Systems put privacy at risk and how can legal issues be approached within European Union Fundamental Rights Law?

In order to answer this question, several sub-questions must be addressed:

1. What is BCI integrated AR and what are its components?

2. How do BCI integrated AR systems challenge the boundaries of the European privacy framework?

3. How should the European Union regulator think about BCI integrated AR systems?

1.4. Methodology and Materials

The methodology employed in the thesis encapsulates the relevant literature review, theoretical and ethical inquiries and the legal critique.

This research's material is unavoidably influenced by its aim to provide discussions within the legal field of the European Union. ("EU" hereinafter) Therefore, the regulatory framework is built upon the legislation of the EU. With this aim, primary law, binding secondary law, case law and relevant soft-law sources will be analyzed.

Soft law does not derive an authority from the EU legislation. Article 288 of the Treaty of the Functioning of the European Union does not count soft law as a secondary law that has binding force. Although soft law is lack of legally binding effect, its potential to give birth to legal effects, remains. Soft law is seen as an important instrument within the EU precisely because it may have an informal 'soft' influence.[6] A clear definition for soft-law has not been detected during the literature review. The term is subject to contentious debates.[7] This research will acknowledge a common definition of soft-law in the literature: the flexible legal instrument which can influence Member States to consider the application and practical implications of a policy, which can motivate Member States to do so especially when a competence deficiency exists within European Union to legalize a hard-law.

This research will lean into soft-law for two paramount reasons. Primarily, in a continuously advancing technological realm, leaning towards recent opinions and recommendations may offer insight into the status quo

6 European Foundation for the Improvement of Living and Working Conditions, 'Soft Law' <https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/soft-law> accessed 16 July 2017

7 For a definition attempt within the field of EU's international relations policy, see, https://halshs.archives-ouvertes.fr/halshs-00911460/document

of ongoing discussions within the EU. In this line of thought, opinions and recommendations in a specific technological field, can be useful for the interpretation of binding Human Rights Law sources. Two unique sources of soft-law will be applied: *1. Civil Law Rules on Robotics*[8] *and 2. Dissemination and use o intrusive surveillance technologies*.[9] The selection of these sources is due to their capability to give an account of ethical considerations, legal definitions and legal ramifications concerning BCI integrated AR technology. (See Section 4.3.1.)

This research predominantly analyzes de lege lata, the regulation of robotics, that which may encompass BCI integrated AR applications, and, the regulation of the right to privacy, under which the users of said applications may be protected. To answer its main research question, this research also embodies a discussion of de lege, ferenda regarding the protection of privacy, or, how privacy issues should be approached by the EU regulator.

The selection of the secondary law sources is based on a feasibility criteria of being beneficial to this research's aims. These texts are of importance by the fact that they allude to the points on which EU authorities present a consensus.

Approaching privacy as a human right, this research will analyze two main legally binding sources. Initially, the European Charter of Fundamental Rights ("EU Charter" hereinafter) since the status of EU's founding treaties has been given to the EU Charter, through the Lisbon Treaty, on 1 December 2009.

8 European Parliament resolution of 16 February 2017 with recommendations to the Commission, 'Civil Law Rules on Robotics' (2017) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN> accessed 13 July 2017

9 European Data Protection Supervisor, 'Opinion 8/2015 Dissemination and use of intrusive surveillance technologies' (2015) <https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf> accessed 30 May 2017

Secondly, the European Convention of Human Rights, ("ECHR" hereinafter) which was amended on 1 June 2010, will also be applied. The amendment is in force since 1 June 2010. The relationship between EU and ECtHR and the ongoing debate regarding the Union's accession to the ECHR, is not relevant for this research. Even though the Court of Justice of the European Union ("CJEU" hereinafter) has recently disapproved the EU's accession to the ECHR[10], the legal interests protected in the ECHR through European Court of Human Rights ("ECtHR" hereinafter) case law is still important for the EU's law, therefore, for the purposes of this research. According to Article 6(3) of the Lisbon Treaty, "Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (…) shall constitute general principles of the Union's law".[11] The wording leaves no doubts about the CJEU judges' obligation to view ECtHR judges' issues and legal reasoning as a guidance. CJEU judges shall not ignore the issues and legal reasoning used for the interpretation of the ECHR concerning a particular fundamental right.

The literature research will be done via an analysis of the online dictionaries, online articles, published articles, published books and videos in domains of neuroscience, robotics and roboethics.

This research will use the term 'regulatory framework' to indicate the regulatory framework of the EU.

It has used materials from the English and German language.

Concerning the reference system, it has complied with Oxford University Standard for the Citation of Legal Authorities.

10 Opinion 2/13 Of The Court of Justice, pursuant to Article 218(11) TFEU, made on 4 July 2013 by the European Commission <http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=160882&occ=first&dir=&cid=240894> accessed 10 May 2017

11 The Treaty on the Functioning of the European Union (2009) 2008/C115/01 <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2008:115:TOC> accessed 12 May 2017

1.5. Approach and Outline

The aim of this research is to intertwine a scientific presentation and legal discussion of BCI integrated AR applications to offer an adequate protection of privacy, so that the prevalent use of the applications in the society is guaranteed within the regulatory framework.

The structure of this research is split to three tasks. The Chapters that are explained below will build the steps for the completeness of this study.

Determining the definitions of BCI and AR individually, their convergence, how that ideal has been linked to different applications in different fields of life, particularly health and entertainment sectors, have assumed a high degree of importance during the literature review of this dissertation. Thus, Chapter 2 will illustrate that the convergence of human and machine technology has already hurdled the barrier of conventional desktop so that our minds are the only boundaries, presenting possible effects, advantages and dangers.

Chapter 3 will provide a descriptive thought experiment about different privacy types by analyzing the complementary or exclusionary interactions among them. It will concentrate on examining how applicable the European legal framework of privacy is to the technology and whether novel privacy issues emerge, yielding the legal framework to become insufficient.

Chapter 4 will provide a comprehensive and methodical analysis of legal responses regarding different privacy protections at the EU level against the misuse of BCI integrated AR applications. By the virtue of the analysis, the Chapter will make a claim concerning whether the legal responses are well equipped and how they should be amended to guarantee a stronger privacy protection, as well as providing an efficient regulation.

Finally, the Summary and Conclusions part will provide an overview of the entire research in a nutshell and summarize the answer of the main research question.

1.6. Disclaimers

A few points regarding the context of this research should be noted clearly first and foremost.

The research is concentrating to the regulatory framework of the EU with aims to critically analyze the details about how the EU's regard to the right to privacy is put into effect and to lead a discussion on how a better governance can be succeeded. As a result, this study does not concern with rewriting the privacy conceptualizations in the legal framework, but with the scope of the current legislation, including, how it can be amended to ensure that it appropriately covers the privacy issues invoked by the use of BCI integrated AR applications. The Commission in 2001 confirmed the need for good governance, "to determine most appropriate type of legislative tool" because "the choice between legislation and less binding tools" were musts.[12] The Commission repeated its interest in the issue in 2015 through the *Better Regulation Guidelines*, so that, as the legislation should keep pace with technological developments, "the EU action must lead to a simple, clear, stable and predictable regulatory framework for businesses, workers and citizens that continue to add value as problems evolve, new solutions emerge and political priorities change".[13]

This research deliberately excludes an analysis of European Union Data Protection Law. The right to data protection and right to respect for privacy differ in content as well as in scope. However, considering the historical focus background of EU at the level of regulatory action while framing the Union's law, it must come as no surprise that privacy considerations are dominantly formulated as data protection concerns. As De Hert and Gutwirt explain: "Data protection is a catch all term for a series of ideas with regard to the processing of

12 European Commission 'White Paper On Governance' (2001) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al10109>

13 European Commission 'Better Regulation Guidelines' (2015) <http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf>, 5

personal data. Through the application of these ideas governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, governmental need for surveillance (….). [14]

This, however, is likely to cause a negligence of the user's right to privacy from several privacy types standpoint. For example, given its unique traits, neurological activity is inherently linked to and therefore presents user's bodily and behavioral characteristics. Therefore, collecting or processing of this data during an execution of BCI integrated AR application should not solely invoke data protection concerns yet also several privacy concerns.

Bearing this in mind, seeking for a regulatory framework to set of the reaction between interconnected fundamental ideas and values which construct the right to privacy, promises for a protective layer. This research will pursue the ways to constitute such a governance, which guarantees that advancements brought by BCI integrated AR applications do not lead to intrusions in private life, ensuring that they are used in a full respect of the right to privacy.

1.7. Significance of the Study

The findings of this research redound to the understanding of the challenge of placing a regulatory framework for the protection of privacy in a dynamically emerging integration of fields.

This research is important for the individual and the concerned groups of stakeholders since they have the moral right and responsibility to give their opinion on the uses of novel technologies as well as their coherence with societal orientations or ethical values. This research hopes to assist the process of encountering emerging conflicts before the BCI integrated AR technology land in the society.

14 P. De Hert and S. Gutwirth 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E. Claes, A. Duff, S. Gutwirth (eds.) *Privacy and the Criminal Law*, pp. 61–104 (Intersentia 2006), 77

Actors are also needed to operate between citizens and technology developers. For this reason, this study is of significance for the academia. Academics can contribute to the process by giving their moral and legal opinions which flows with academic analysis since this is actually "realistically bound to depend on a division of epistemic labor between ordinary citizens and experts".[15] This study provides a specialized information within a specific jurisdiction. The legal ramifications of the technology, which may trigger societal controversy regarding privacy, can be enriched by substantial researches, leaning on the information provided in this study.

Lastly, this study holds an importance for the business field in realm of the subject-matter technology since it can somehow reveal the measures, stipulations, principles and costs in the current regulatory framework, that serve as guidelines for the tech companies.

The chances are high that a technology as BCI integrated AR will put the society at the dawn of a new techno-social era, as its ancestors have done. This study differs from preceding academic literature because it questions the applicability of the EU's privacy approach, by means of landscape as well as methodology, while analyzing the privacy related normative implications, in the manner of a novel hybrid of technologies. There is an abundance of work for the components of the system[16], yet, the legal scholars are silent about the system itself. This study invites the reader to understand, envision and evaluate the socio-legal and legal implications of this interesting piece of technology.

15 Donetalla Mattie, Guglielmo Tamburrini and Fondazione Santa Lucia 'Ethical Issues in BCI Research and Systems for Motor Control' in Jens Clausen and Neil Levy (eds), *Handbook of Neuroethics* (Springer, 2015), 725-740 <https://link.springer.com/referenceworkentry/10.1007/978-94-007-4707-4_42> accessed 10 April 2017

16 See, Alzbeta Krausova 'Legal Aspects of Brain-Computer Interfaces' (2014) 8 Masaryk UJL & Tech., 199 <https://journals.muni.cz/mujlt/article/viewFile/2655/2219> accessed 16 July 2017

2. APPROACHING TO TECHNOLOGIES' STATE OF ART

This Chapter will answer the first sub-question of this research. Setting out a technical background of the components of BCI Integrated AR technology, it will ascertain the point to the technical scenarios and wider applications as near technology to convey more than just the evidence of a medical abnormality and actually interpret an individual's neural activity.

2.1. An Interaction Between Humans and Computers: Brain-Computer Interface

From ancient myths to modern science fiction novels, the intriguing history of human imagination have fantasized about interacting with the environment and communicating with other humans' mind via thoughts or human- made machines. Even these fantasies can still be considered as a fairly futuristic technology by end-users, and even if they may largely reside in the future, a part of them have already become possible after discovery of Electroencephalography (EEG), and through the advances in cognitive sciences.

Having been invented by psychiatrist Hans Berger in 1924, EEG is known for being one of the most widely used non invasive techniques for recording electrical brain activity, due to advantageous factors such as time responsiveness, harmlessness and convenience of measurement. The technique has been a useful source to seek answers to questions arising on the functioning of the brain and has served as a diagnostic tool in clinical practice.[17] Being the most used signal measurement system today, an EEG signal is determined and generated by each person's unique pattern of neural activity, which makes it impossible to replicate, fake or duplicate. Several studies have presented EEG signals as a promising bio-metric trait, which allows person identification and

17 Barbosa de Castro Lourenço 'Human Computer Interaction Via Brainwaves For Disable People' (MA thesis, University of Porto, 2013), 15

verification.[18] In other words, the information generated from EEG signals may be used to constitute the identity of a person, that is one from many other persons, and may also be used to confirm or deny the identity that is claimed by a person. Using the brain activity as a communication channel is attractive to BCI researchers, considering an elaborative and punctual analysis of brain signals has a prerequisite value.

Hundreds of steps have been taken in the direction of defining BCI technology and its operations since Vidal's groundbreaking research paper on brain- computer communication.[19] A recent research paper approaches to BCI as an interface where communications between various devices and computers are held, as a consequence of the brain activity's role.[20] In plainer words, a BCI uses brain activity as an input, in order to determine an output signal. The Merriam Webster dictionary defines *interface* as "the place at which independent and often unrelated systems meet and act on or communicate with each other."[21] Therefore, BCI is the situation in which the exchange happens between computer and brain. This fact assigns a technical specification to the technology:

18 K. Ravi and R. Palaniappan 'Leave-one-out Authentication of Persons Using 40 Hz EEG Oscillations' (EUROCON 2005 The International Conference on Computer as a Tool, Volume 2, Belgrade, Serbia and Montenegro, 21-24 November 2005)

Muhammad Kamil Abdullah, Khazaimatol S Subari, Justin Leo Cheang Loong and Nurul Nadia Ahmad, 'Analysis of the EEG Signal for a Practical Biometric System' (IEEE EMBS Conference on Biomedical Engineering and Sciences, Kuala Lumpur, November 2010)

Virgílio Bento, Luís Paula, António Ferreira, Nuno Figueiredo, Ana Tomé, Filipe Silva, João Paulo Cunha and Pétia Georgieva 'Advances in EEG-based Brain-Computer Interfaces for Control and Biometry' (7th International Conference on Image Analysis and Recognition Proceedings, Part II, Póvoa de Varzim, June 2010) <http://www.gecad.isep.ipp.pt/iscies09/Papers/19November/ISCIES09_BCI2Control&Biometry-vf.pdf> accessed 10 September 2017

19 Jacques J. Vidal 'Toward Direct Brain- Computer Communication' (1973) 2 Annual Reviews, 157-180 <http://www.annualreviews.org/doi/pdf/10.1146/annurev.bb.02.060173.001105> accessed 3 July 2016

20 Kusuke Uno and others 'Basic Investigation of Brain–Computer Interface Combined with Augmented Reality and Development of an Improvement Method Using the Nontarget Object' (2015) 98(8) Electronics and Communications in Japan, 9-15.

21 See, <https://www.merriam-webster.com/dictionary/interface> accessed 13 July 2017

being an instrument between a person and an intelligent electronic or digital device.[22] This makes it troublesome to envisage BCI without an application by which it is validated. Those applications may vary among electronic device, environmental control, navigation in virtual reality and generic cursor control applications, hosting as an integral part of BCI.[23]

Jose M. R. Delgado, whose works were famed on mind control through electrical stimulation of the brain, is viewed to be a researcher who produced the earliest publications directly related to BCIs. Having also been one of the earliest practitioners in his field, the researcher is also known for his famous experiment performance by standing in a bullring in Cordova, Spain. Back in 1963, Delgado was standing in front of an angry bull named Lucero, armed with just one weapon; a remote control. When the bull targeting him gathered speed, he flipped a switch on the unit with aim to send a signal to a chip implanted in the bull's brain. The bull immediately halted its furious charge before docilely trotted away. The outputs of the experiment were profound. The most significant was the demonstration of the special *stimoceiver*'s ability, which was developed by him, to manipulate the bull's behavior by electrically stimulating certain regions of its brain. The stimoceiver basically tracked patterns of certain regions of the brain and responded when those patterns arose. He first used the stimoceiver on a chimpanzee's amygdala. Spindle, a pattern produced by the amygdala caused the stimoceiver to automatically stimulate the central gray region of chimpanzee's brain, inducing an unpleasant nausea.[24]

22 Modern computer science studies differentiate between electronic computers and digital computers, defining computers commonly as electronic and/ or digital devices.
See, Zobair Ullah, 'Early Computer VS Modern Computer: A Comparative Study and an Approach to Advance Computer' (2012) 12(1) Global Journal of Computer Science and Technology Interdisciplinary <https://globaljournals.org/GJCST_Volume12/1-Early-Computer-VS-Modern.pdf> accessed 18 June 2017

23 Bernhard Graimann, Brendan Z. Allison, Gert Pfurtscheller (ed), *Brain-Computer Interfaces: Revolutionizing Human-Computer Interaction* (Springer 2010)

24 Henry Zheng, 'The Brain-Machine Connection: Humans and Computers in the 21st Century' *Yale Scientific* (13 February 2011) < http://www.yalescientific.org/2011/02/the-brain-machine-connection-humans-and-computers-in-the-21st-century/> accessed 12 July 2016

For several years, Delgado performed intriguing experiments on monkeys and chimpanzees by remote control and presented sophisticated inventions, which delivered measured electrical pulses to particular targets in the brain. His works, which were ahead of his time, were seminal in understanding cerebral behavior and spontaneous activities and brain dysfunctions associated with behavioral abnormalities.[25]

In 1999, a group led by a young scientist named Miguel A. L. Nicolelis, published the first demonstration of a brain controlled device. The experiment known as "reading monkey thought" was put into practice by implanting electrode arrays into a group of brains of mice and recording their brain activity. While they pressed a lever to position a robotic arm, the device detected their intent, consequently, mice controlled their movement to obtain the water. Eventually, a subgroup of the studied mice was able to conduct their movements routinely by using brain activity. This study was significant as it suggested new possibilities for paralyzed patients that may control their own muscles using electrophysical patterns.[26]

In 2008, another exciting adveancement came, which was again designed and carried out by the laboratory of Nicolelis. This time, the subjects of the study was a monkey named Idoya, in the United States, and a humanoid robot that was in Japan. Idoya was not able to talk, but her brain signals made the humanoid robot walk.[27] Basically, the set of neurons in her brain that controlled the robot's legs became attuned to the robot's legs after about an hour of practice and visual feedback. These experiments were the first steps toward a brain machine interface that might permit paralyzed people to walk by directing devices with their thoughts. Electrodes in the person's brain would send signals to a device worn on the hip, like a cell phone or pager, that would relay those signals to a pair of braces, a kind of external skeleton, worn on the legs. Nicolelis explained

25 Barbosa de Castro Lourenço (n 17), 7

26 KA Moxon, RS Markowitz, and MA Nicolelis 'Real-time control of a robot arm using simultaneously recorded neurons in the motor corte' (1999) 2(7),Nat Neurosci, 664-70.

27 Sandra Blakeslee, 'Monkey's Thoughts Propel Robot, a Step That May Help Humans' *The New York Times* (15 January 2008) <http://www.nytimes.com/2008/01/15/science/15robo.html?_r=0> accessed 10 July 2016

that this experiment was the first time that brain signals had made a robot walk, so the body was not the mere source to present the desires of the brain.[28]

2008 had also been the year when the first BCI mainstream report was announced by Columbia Broadcasting System (CBS) which was a 60 minutes segment titled "Brain Power" and consisted of interviews made by some individuals who had suffered from severe motor disabilities before their life was changed with BCI technology, presenting some of the improvements in the field. One of those improvements was the Braingate project, which has been originally developed jointly by researchers in the Department of Neuroicience at Brown University and jointly Cyberkinetics Inc, today owned by privately held Braingate, Co.[29]

Ultimately, 2014, the year when a paraplegic man who was using a mind controlled robotic ex oskeleton performed the symbolic kick-off at the FIFA World Cup in Sao Paul, is worth mentioning. According to Nicolelis, it was the first time an exoskeleton had been controlled by brain activity and offered feedback to the patients. Doing a demonstration in a stadium was something very much outside our routine in robotics and it was never been done before.[30]

If there is one mutual understanding that Neurologist scientists seem to have reached over last few years, it is that BCIs represent a trans-formative tool for improvement of human health and symbolizes a progressive tool for humans to flourish.

28 ibidem
29 Scott Pelley, 'Harnessing The Power Of The Brain *CBS News* (31 October 2008) <http://www.cbsnews.com/news/harnessing-the-power-of-the-brain> accessed 11 July 2016
30 Alejandra Martins and Paul Rincon, 'Paraplegic in robotic suit kicks off World Cup' *BBC News (*12 June 2014) <http://www.bbc.com/news/science-environment-27812218 > accessed 7 July 2017

BCI devices have not yet been properly tailored into everyday life although they have been in the realm of reality for awhile. This is argued to be due to their failure "to fulfill classification accuracy, rapid responsiveness and intentional control techniques; conditions deem to be as necessity for a BCI to become an alternative feasible interface".[31] However, one can argue that the EU market has been offering roughly satisfying solutions to these hurdles as a result of EU institutions' endeavors. European health care business has developed a variety of devices to help people with disabilities that restrict ability to move and interact with others in recent years, and constituting the third largest BCI market in the world. Consequently, European Commission has already been aware that treating brain diseases is becoming urgent for not merely health but also industrial competitiveness, and has been taking active measures in funding for brain-related Information and Communications Technology research projects. Human Brain Project is an initiative co-founded by the European Commission which "aims to put in place a cutting-edge, ICT-based scientific research infrastructure that will allow scientific and industrial researchers to advance our knowledge in the fields of neuroscience, computing and brain-related medicine." [32]

The Brainhack project is also founded by the Future and Emerging Technologies Programme of the EU and aims to "to explore and extend what is currently possible", exploring the idea that "connections can be visualized with techniques such as EEG, fMRI, and PET", by organizing a three-day creative hackathon which includes two public events, talks and discussions once a year. [33]

Some recent researches have taken a direction towards comprehension of the various aspects in the computing and neurological field. As Brent J. Lance and others envision, a more holistic approach will merge,

31 Brent J. Lance, Scott E. Kerick, Anthony J. Ries, Kelvin S. Oie and Kaleb McDowell 'Brain–Computer Interface Technologies in the Coming Decades' (2012) 100 (Special Centennial Issue) Proceedings of the IEEE, 1595 <http://ieeexplore.ieee.org/document/6162941/?reload=true> accessed 11 May 2017

32 Human Brain Project <https://www.humanbrainproject.eu/2016-overview> accessed 19 June 2016

33 Hack The Brain <http://www.hackthebrain.nl/> accessed 20 June 2016

"critical brain, behavioral, task, and environmental information obtained with advanced pervasive, multi-aspect sensing technologies, sophisticated analytical approaches, and enabled by advances in computational infrastructure such as extensions of cloud technologies"[34] which also may provoke an investigation into the synergies between human and computer, and also brain function and brain structure, due to large-scale data collection.

2.2. A Manipulation of Judgment of Reality: Augmented Reality

Overlaying the digital information onto the physical world, Augmented Reality ("AR" hereinafter) promises an enhanced or manipulated experience of the real world. AR generally takes the form of,

a) Mobile devices such as smartphones and tablets,

b) Head Mounted Displays ("HMD" hereinafter) such as gaming consoles, or,

c) Spatial Augmented Reality systems such as digital projectors.[35]

This is done by combining the physical and virtual world, enabling a real-time interaction to connect with freedom of movement in three dimensions. By the use of special worn devices, we observe the physical world in the streets and the elements produced by Virtual Reality. [36]

34 Brent J. Lance and others (n 31), 1594

35 Centre for the Promotion of Imports from developing countries (CBI) 'Virtual Reality and Augmented Reality in Europe' (6 April 2017) <https://www.cbi.eu/market-information/outsourcing-itobpo/virtual-reality-augmented-reality/> accessed 20 May 2017

36 Szczepan Paszkiel 'Augmented Reality of Technological Environment in Correlation with Brain Computer Interfaces for Control Processes' in R. Szewczyk, C. Zieliński and M. Kaliczyńska (eds), *Recent Advances in Automation, Robotics and Measuring Techniques. Advances in Intelligent Systems and Computing* (Springer 2014), 267 <https://link.springer.com/chapter/10.1007/978-3-319-05353-0_20> accessed 10 April 2017

One of the most accurate ways to define AR must be referring it as an approximate class of technologies. Despite the absence of an absolute criteria to qualify a system as AR, there are those who maintain that AR systems will display most or all of certain properties. These properties are summarized as: sensing properties of the real world, processing in real time, output information to the user (including via visual, audio, and hap-tic means, often overlaid on the user's perception of the real world), providing contextual information, recognizing and tracking real-world objects, being mobile or wearable. [37]

Various researches have already been conducted in the health sciences medical field in order to demonstrate the accuracy of AR guided operations or AR based modules.[38] A valuable amount of research has been conducted in the industrial manufacturing field as well, showing the effectiveness and efficiency of AR aided systems.[39]

37 Franziska Roesner and others 'Augmented Reality: Hard Problems of Law and Policy' (2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, September 2014)

38 See, Ashirwad Chowriappa and others 'Augmented reality–guided neurosurgery: accuracy and intraoperative application of an image projection technique' (2015) 115(2) BJUI, 336–345 <http://onlinelibrary.wiley.com/doi/10.1111/bju.12704/full> accessed 9 May 2017

L. Tabrizi Besharati and M. Mahvash 'Augmented reality-guided neurosurgery: accuracy and intraoperative application of an image projection technique' (2015) 123(1) J Neurosurg <https://www.ncbi.nlm.nih.gov/pubmed/25748303> accessed 9 May 2017

C. Moro Z. Štromberga, A. Raikos, and A. Stirling 'The effectiveness of virtual and augmented reality in health sciences and medical anatomy' (2017) doi:10.1002/ase.1696 American Association of Anatomists <http://onlinelibrary.wiley.com/doi/10.1002/ase.1696/full> accessed 8May 2017

39 See, Lorenzo Peppoloni, Filippo Brizzi, Emanuele Ruffaldi and Carlo Alberto Avizzano 'Augmented reality-aided tele-presence system for robot manipulation in industrial manufacturing' (2015 Proceedings of the 21st ACM Symposium on Virtual Reality Software and Technology, Beijing, November 2015), 237-240. <http://dl.acm.org/citation.cfm?id=2821620> accessed 8 May 2017

Susanne Stadler, Nicole Mirnig, Manurl Giulani, Manfred Tscheligi, Zdenek Materna and Michael Kapinus 'Industrial Human-Robot Interaction: Creating Personas for Augmented Reality supported Robot Control and Teaching' (Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, Vienna 2017), 291-292 <**http://dl.acm.org/citation.cfm?id=3038365**> accessed 8 May 2017

However, recent interest in the literature is being driven by the convergence of BCI and AR.[40]

Bloomberg stated it well, claiming that AR technology "has the potential to affect every aspect of how we interact with technology'' and as prudently continued, that AR industry should cope with the controversy surrounding the definition of AR, by establishing common standards people understand. "Otherwise, augmented reality will quickly meet the same fate as 'green' products: Marketers will advertise even the slightest of augments as 'augmented reality,' leaving consumers confused and bewildered."[41]

2.3. Integrating BCI and AR

The main principle behind BCI integrated AR is establishing multi-modal interactions and data flows. This establishment is to be observed by the user. The observation process is made possible by means of either BCI ready devices or combined BCI integrated AR applications, which operate through devices in a non-obtrusive way.

BCIs can eliminate the drawbacks of indirect interaction of conventional interfaces such as the mouse, keyboard, button-navigated application, and even unconventional interfaces such as touch gestures. It can also stand as a supplementary to navigate an augmented environment or a robot, along with conventional inputs such as voice or waving hand movement.

For instance, Tobias Blum et al. in their paper describe how they successfully achieved the "first steps towards a Superman-like X-ray vision where a brain-computer interface (BCI) device and a gaze tracker are used

40 See, Szczepan Paszkiel (n 36), 267

41 William Hurley, "Augmented Reality: Getting Beyond the Hype" Bloomberg (3 November 2009) <https://www.bloomberg.com/news/articles/2009-11-03/augmented-reality-getting-beyond-the-hypebusinessweek-business-news-stock-market-and-financial-advice> accessed 10 October 2016

to allow the user controlling the augmented reality (AR) visualization."[42] Practical conditions in a traditional medical AR system do not afford the opportunity to surgeons to conduct structures outside the patient and simultaneously to augment structures inside the patient's body, thus, does not lead to a total control of the visualization. The experiment overcame this common problem in medical AR which limits surgeons' perception. Having received a positive feedback from 9 medical professionals including final year medical students who participated in the questionnaire, the scientists were able to utilize participants' expertise, as well as their interest in learning how to interact using brain waves. The questionnaire revealed that participants mostly deemed BCI intuitive to use, finding the adoption of gaze-tracking as valuable element. What is more, most of them were willing to use BCI for a surgery.

Kansaku et al., on the other hand, have successfully demonstrated an AR-BMI system that enables users to control an agent robot and the home electronics in its environment, merely by commanding through their brain signals.[43] The agent robot's eyes detected the AR marker[44] for the pre-assigned infrared appliance to be controlled by the participants. For this, an ARToolKit[45] was adopted which detects the location of an AR marker. One control panel for robot and another one for the desk light was set. Thus, subjects were able to control the agent robot to move forward, backward, right and left, as well as controlling the light to be turned on and off,

42 Tobias Blum, Ralf Stauder, Ekkehard Euler and Nassir Navab, 'Superman-like X-ray Vision: Towards Brain-Computer Interfaces for Medical Augmented Reality' (IEEE International Symposium on Mixed and Augmented Reality 2012 Science and Technology Proceedings, Atlanta, November 2012)

43 Kenji Kansaku, Naoki Hata and Kouji Takano, 'My thoughts through a robot's eyes: An augmented reality-brain–machine interface' (2010) 66 Neuroscience Research <http://www.sciencedirect.com/science/article/pii/S0168010209020094> accessed 11 April 2017

44 An AR marker detects, tracks, estimates the position and orientation of an object in three-space.
See, Oliver Toole and Dave Dolben, 'Marker Detection and Tracking for Augmented Reality Applications' (2014), 1 <https://www.semanticscholar.org/paper/Marker-Detection-and-Tracking-for-Augmented-Realit-Toole-Dolben/746331b91cf29995aa613b9cf3453dd1c0d4e332> accessed 17 July 2017

45 ARToolKit is a planar marker system for Augmented Reality.
See, Martin Hirzer, 'Marker Detection For Augmented Reality Applications' (2008) Technical Report ICG–TR–08/05, 2 <http://studierstube.icg.tugraz.at/thesis/marker_detection.pdf> accessed 15 July 2017

and brighter or dimmer. At the first stage, the participants commanded the robots to move to the desk light in its environment. Subsequent to the robot's detection of the AR marker of the desk light, participants saw a flicker panel to control the appliance on the screen. Hereby, they sent commands through EEG signal to operate the robot's environment via the robot's eyes.

This Chapter has broken down BCI integrated AR into its components, clarifying which component adds what value to the system. Then, it has presented the promising amalgamation between BCI and AR, showing that BCI has payed the way for AR to move away from its conventional roots adhered to traditional inputs systems. It has defined what BCI integrated AR is, in the perspective of the Science and Technology studies. It has shown that BCI integrated AR systems make their case by constituting a communication between the brain and an external device in order to control AR. Hereby, it has depicted a hybrid technological system that emerges from the use of more than one distinct types of technologies. The normative findings of this Chapter will guide the next Chapter while classifying the BCI integrated AR system according to multiple artifacts used in its components, further building different privacy concerns evoked upon the classification of BCI integrated AR system.

3. PRIVACY CONCEPTUALIZATION

This Chapter will answer the second sub-question of this research. It intends to provide some findings, which will serve as a tool to clarify the relevance of the legal protection of privacy, assisting to answer the third sub-question in the following Chapter. By ascertaining the true privacy segments to be cherished, this Chapter will consider how the European privacy framework deals with the challenges that are brought via the BCI integrated AR applications. Beforehand, it will briefly provide some of the foremost and most recent attempts in literature, which trace privacy conceptualizations, to introduce the reader to the endeavors for the protection of privacy against the emerging technologies of the first decade of the 21st century.

3.1. Pursuing for Privacy in the Information Age

Privacy related matters provide much opportunity for legal disputes to arise. Throughout the history, privacy has been a nearly universal value although the notions that it represents have differed. There is ample anthropological studies which support that in modern societies privacy gained its meaning through legacy of race, social realities, assertive behavior, etc.[46] Because privacy has been theorized in disparate ways of thinking from society to society, it needs to be understood in terms of culture, further, in terms of sub- culture. In terms of understanding Western perception of privacy, Alan Westin, who was the most significant American scholar of privacy since Louis Brandeis, reflected a socio-cultural emphasis on the prediction for future privacy developments, elaborating a broad theory of privacy, presented the following four privacy dimensions: anonymity, intimacy, reserve, and solitude.[47]

46 See, Barrington Moore Jr, Privacy *Studies in Social and Cultural History* (United Kingdom, Routledge, 1984)
47 See, Alan Westin *Privacy and Freedom* (United States of America, Ig Publishing Incorporated, 2015)

However, the traditional Western approach to privacy has been frayed by the advent of new technologies, leading scholars to reconsider what privacy is. Helen Nissenbaum famously drew attention to the deficiency of traditional Western privacy theories. According to her, because these theories stress the governmental intrusion into one's personal and intimate space, they cannot respond to the threat of public surveillance into privacy.[48] Accounting for her analysis in terminology drawn from Westin's and Gavison's theories, she argues that the main forms of privacy these theories offer, the establishment of the conditions for a free society and one's capacity to act free and autonomously, no longer hold. Detecting that the reasons set to protect privacy in public are similar to the reasons to protect privacy of the more traditional kind, she concludes that interests to be protected from invasions of the personal and intimate realms are also threatened by public surveillance. These interests, such as autonomy, mental health, individuality, liberty, personality, are what Nissenbaum views as the essential contributions of the traditional theories.[49]

Moving forward, the next Section will show that these interests become the focal point of the newer typologies, which have been developed to serve as a punctual instrument while dealing with privacy in the Information Age.

3.2. The Technology Classifications and the Privacy Typologies Used

The Section 3.3, 3.4 and 3.5 of this Chapter will use a classification of BCI integrated ARs according to the device type they adopt. [50] Scenarios under each classification can be read as approximate problematic areas that may arise by the run of the system. As a matter of fact, these issues can also be read as the features that represent the functionalities and capabilities of an AR application.

48 Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public, Law and Philosophy' (1998) 17: 559-596 Law and Philosophy <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf> 17 Law and Philosophy accessed 19 May 2017, 1998

49 idem 586-587

50 The classification is provided in (n 35)

Such method is compatible with the fact that this research has avoided treating BCI integrated AR as a hybrid technology, as there is no consensus within global Sciences and Technology communities, but as a hybrid of technologies, which entails a unique technological system. (see Section 2.3.) Section 2.3. has showed that the system software of a device is tied to the type of device with little flexibility. On the other hand, an application software of a device, which integrates BCI with AR, is the AR itself. Thus, BCI serves as the technological instrument. In the light of these findings, this Chapter will analyze the true privacy segments to be cherished by committing to a stable framework. To build this framework, this Chapter will use two individual typologies that both serve to understand the privacy types required to protect against privacy intrusions, by applying these types to the BCI integrated AR applications.

The first typology is by Michael Fridewald, Rachel L. Finn and David Wright.[51] The reasoning is two-fold. Being a recent one, this typology serves as a punctual instrument for a research that is dealing with privacy in the Information Age. Secondly, the continent and jurisdiction the typology focused on is compatible with the subject of this research since the typology forms a European conception of privacy. Therefore, it provides an explanatory model for a privacy impact assessment within the EU.

The typology of Finn et. al acknowledges seven different types of privacy to be considered while protecting individuals against new and emerging technologies: privacy of the person, privacy of behavior and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, privacy of association. Accordingly, current decision makers should consider these types to formulate proactive privacy protections. Recognizing that these types may overlap, the authors discuss each of them separately and reason that different technologies can have an impact upon different types of privacy. This

51 Rachel L. Finn, Michael Friedewald and David Wright, 'Seven Types of Privacy' in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet (eds), *European Data Protection: Coming of Age* (Springer 2013) <https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy> accessed 30 February 2017

Chapter will refer to these types with a view of showing what segment of privacy is invoked under particular given scenarios.

Secondly, the typology presented by Koops et. al will be used.[52] Since the study examines the constitutions of European countries with the majority being the EU members, it is promising as a second typology as the typology of Finn et. al is not complete enough to cover all scenarios. The national constitutions hold a significance in the European legal tradition when it comes to privacy, since its protection in vertical relationships is primarily developed under and guaranteed in constitutions. Thus, the typology of Koops et. al is a comparative one, serving a convenient background to indicate the relevant privacy segments of the societies, which form the EU.

Privacy issues related to the BCI integrated AR systems' one of the components, will be excluded from the analysis, provided that they are already heavily addressed among scholars. The facts that do not serve any uniqueness regarding BCI integrated AR entirely as an interactive compound system, they will either briefly be mentioned to build a necessary link to the following paragraph, or will not be mentioned at all. For instance, the fact that BCI may be manipulated so that the user looses control over behavior, is sure to have impacts on the privacy associated with behavior. Or, that mobile devices can be tracked given their portable nature, is sure to have impacts on the privacy associated with one's location. Yet, such facts neither break new ground nor contribute to the aims of this research.

Before starting, it is important to repeat that the way AR provides virtual experience is by capturing input from the user's surroundings, and overlaying virtual output on the user's perception of the real world. The ahead

52 Bart- Jaap Koops and others, 'A Typology of Privacy' [2017] 38(2) University of Pennsylvania Journal of International Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043> accessed 1 February 2017

privacy analysis will be built on the issues that arise from input or output. To simplify things for the reader, this Chapter will also embed a distinction between these two functions.

3. 3. Mobile devices

Being handheld and portable computers, mobile devices' types vary; ergonomic technologies such as smartphones, tablets, e-readers.

BCI serves as an instrument for the collection and process of the user's neurological activity data in a given AR application. The data may be leaked out from the BCI, as well as the application itself. This becomes possible through the agency of a malware spread which targets the BCI or the application.

Various systems that let a mobile device know where the user is, have already been made available or are being developed. For example, AR applications which store user's location have their sources in the portability of mobile device, such as; GPS, Bluetooth, Cell ID, Wi-Fi, Terrestrial Transmitter. Having their location information stored in the device, users are already prone to privacy intrusions; from malicious parties gaining the information from location-based application vendors, to service providers delivering the information to governmental agencies. The ramifications of future investment in intelligent mobile devices, is not easy to estimate. Certainly, as more users demand to enrich their experience, more vendors aim to supply a personalized services. Constructed models specialized for users recognize the components intimately related to their users, such as location. This raises interesting questions. These models, which encompass personal information, may easily be overused, e.g., locations that the user found or finds or likely to find interesting.

However, some additional issues come into account when BCI is integrated. Since it is the BCI that provides the system's control by mirroring neurological activity, this may build grounds for relating a shift in

user's location to a shift in neurological activity. According the conceptualization of Finn et. al, the first privacy type that relates to the this scenario is privacy of location and space.[53] This concept includes a social value since there is a correlation between freedom to move in public without the fear of being tracked or identified, and the exercise of liberal democracy. Privacy of location and space may be at stake not only in public but also in spaces where we deem to be private. Finn et. al realize the "potential for detecting someone's location by comparing the DNA sample found at a specific location and people's DNA profiles."[54], arguing that this can lead to building a link between one's sensitive data and location. In the case of Finn et. al, the sort and amount of information extracted, is already determined in the borders and pace of life; the source is finite. On the other hand, under our scenario, the situation is slightly reverse. Identically, a BCI integrated AR user's location can be associated with her sensitive information (neurological activity). Since the potential information to be extracted from one's neurological activity not finite, the border here may be the technology's sophistication that is bounded up with humankind's curiosity.

One can argue that, the aforementioned statement, that the information extracted from neurological activity is infinite, is a non-testable statement, because experimenting with it would be beyond the realm of technology's current sophistication level. Indeed, the sophistication is no where near reading thoughts but measuring neurological activity, by which scientists reach different consequences regarding what one may be thinking. Having said that, the recent or under development applications can "take a glance" at one's thought, if not "read", with a high degree of preciseness. These applications are promising when one considers the systematic progressive nature of technology, serving an example of what near-term life will look alike. As a matter of fact, the statement, that the information extracted from neurological activity is infinite, should keep triggering the privacy discussion.

53 Finn and others (n 51), 6
54 idem, 13

Coming back to the AR applications that run on mobile devices, a paper by Ivan Martinovic et al., concerning security risks involved in consumer-grade BCIs, demonstrates the feasibility of extracting the user's sensitive information via EEG signals. The information includes information of credit card, PIN number, the persons known to the user, and the user's location. [55] Manipulation techniques targeting output contents also put corresponding brain activity (of outputs) in a vulnerable position, open to access of third parties, without the user's consent. Given the simplicity of this technique, authors remind the possibility of more sophisticated attacks; making the user subject to manipulation of "mind-games".[56] In this regard, Roesner et al. provide insight as to how future applications are becoming more and more threatening to make users interact with click-baits. [57] Despite our current knowledge of their likelihood of the occurrence, the sophistication level of manipulation techniques is hard to estimate.

Under the given scenario, a BCI integrated AR user's location to be associated with her neurological activity information, the impact on the "privacy of personal data and images" is obvious. Once a user loses control of her neurological activity in the form of EEG data, her sensitive information is at stake. The case here is her being unable to determine whether her sensitive data is processed or not, how long it will be kept, and to whom it will be shared. Finn et al. establishes "privacy of personal data and images" by expanding the concept of "personal data" to a point that it recognizes what Directive 95/46/EC of the European Parliament and of the Council (EU Data Protection Directive) recognizes as personal data. According to Finn et al., this privacy type concerns persons' self-determination regarding access to their data and use of it.

55 Ivan Martinonic and others, 'On the feasibility of side-channel attacks with brain-computer interfaces' (Conference: Proceedings of the 21st USENIX conference on Security symposium 2012 Washington) <https://www.researchgate.net/publication/262325698_On_the_feasibility_of_side-channel_attacks_with_brain-computer_interfaces> 12 March 2017

56 idem, 13

57 Franziska Roesner and others, 'Security and Privacy for Augmented Reality Systems' [2014] 57(4) Communications of the ACM, 88 <https://cacm.acm.org/magazines/2014/4/173222-security-and-privacy-for-augmented-reality-systems/abstract> accessed 10 March 2017, 93

However, there is more to be discussed under this scenario. There is a risk for a user to be subjected to unauthorized intrusion so that she looses control of *what* her mind creates, e.g., the choice she makes by virtue of an input; by virtue of a command towards the device.

German scholars Bublitz and Merkel offer an intriguing solution for this risk.[58] They call for the emergency to invent a right, which ascribes to have self determination of our minds, granting freedom to "self determinate one's inner realm", such as content of thoughts.[59] The authors come to this conclusion by detecting that there is a lack of a coherent framework for mind protection; such a protection that is "irrespective of bodily injury and beyond deception and fraud"[60], and is against unauthorized intrusions to mind. Above all, mental self-determination either exists or is woven into the law's structure as a tacit assumption.[61] In their definition, unauthorized interventions are "direct interventions" since they bypass the mental control, making them evidently illegitimate while mind manipulations are indirect interventions, so that "their restriction ipso facto necessitates balancing countervailing rights."[62]

Italian scholars Ienca and Adorno find Bublitz and Merkel's notion of mental self determination insufficient to encounter related legal implications.[63] They offer a reconceptualization of existing rights and establishment of new neuro-specific rights. "Right to mental privacy" is one of them. Analyzing the interaction between neuroscience and human rights, and presenting neurotechnology applications which can disperse an unprecedented degree and variety of brain information, the authors conclude that the neural privacy breaches

58 Bublitz Christoph and Merkel Reinhard, 'Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination [2014] 8 Crim Law and Philos <https://www.researchgate.net/publication/259974877_O_Crimes_Against_Minds_On_Mental_Manipulations_Harms_and_a_Human_Right_to_Mental_Self-Determination> accessed 13 March 2017

59 idem, 60
60 ibidem
61 ibidem
62 idem, 73
63 Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) 13(5) Life Sciences, Society and Policy

should be treated differently than the traditional privacy breaches. Thus, specific legal notions should be put forward. Hereby, "Right to mental privacy" may plug the gap in the regulatory framework, by granting one the right to control the extraction and dissemination of her neural information.

The legal interest that is handled by Ienca and Adorno is associated to the concept what Finn et. al identify as "privacy of thoughts and feelings".[64] The emphasis of a positive freedom is explicit in the definition of Finn et. al through cherishing persons' right to think whatever they wish. Here, one can realize that this privacy type, unlike the other ones articulated, aims to cherish what originates from a non-physical and transcendent source: the mind. Authors recognize this, stating that the concept differentiates from privacy of the person, just as mind differentiates from the body.

This Section has attempted to outline some normative consequences that derive from the question on how user's mental privacy is vulnerable to interference or intrusion by the use of BCI integrated AR on mobile devices. This leads to the next question, that will be handled in the next Chapter: *how should the right to refuse the extraction of infinite personal information from neurological activity be addressed in the regulatory framework?*

3.4. Optical Head Mounted Displays

The early signs of the use of Head Mounted Displays in AR systems are found in 1960s. HMDs are easily categorized as Optical See- Through Head Mounted Displays ("OHMD" hereinafter) and Video See- Through Head Mounted Displays. The "see- through" capability of OHMD allows users to look through their

64 Finn and others (n 51), 7

surroundings and the virtual images ("computer- generated imagery") simultaneously.[65] Thus, OHMD augments the reality of the user.

OHMDs that are used in Medical AR Applications or Game Software do not invoke as many privacy issues as their computational versions do.[66] To see the roots of this claim, one can take a look at the nature of computational OHMD devices, and the ways they have frequently been used. They serve ubiquitous monitoring, which in turn serves as a catalytic that precipitates a ubiquitous transparency of persons surrounding. It has the capacity to share intimate information to third parties via connecting Internet, or synchronizing with another device to which it connects. Herewith, user's network or social media friends may access the device's camera, so that they watch what is being monitored, from user's perspective.

Surveillance studies generally classify such monitoring practices by end-users as "participatory surveillance".[67] During the last decade, emerging technologies have indeed proved that surveillance may take various forms, in different time and space, therefore the term's context is beyond a CCTV, in which citizens are subjects.

Under the scope of wearable technologies, the monitoring capacity of a popular a OHMD device, Google Glass, has been one of the most popular products that has been discussed. Its privacy implications in society's

65 Henry Fuchs and Jeremy Ackerman, 'Displays for Augmented Reality: Historical Remarks and Future' in Ohta, Yuichi, Tamura, Hideyuki (eds), Mixed Reality (Springer-Verlag Berlin Heidelberg 1999) <http://www.cs.unc.edu/~fuchs/publications/DisplaysforAR99.pdf> accessed 10 June 2017 page 1 and 2

66 Notable computer OHMDs include Google Glass, Lumus DK-50, Microsoft HoloLens, Toshiba Glass

67 Famously, Anders Albrechtslund has introduced the term, arguing that online social networking has altered our understanding of *surveillance* to a degree that *surveillance* can be an empowering and subjectivity building.
Ander Albrechtslund, 'Online social networking as participatory surveillance' (2008) 13(3) First Monday <http://firstmonday.org/article/view/2142/1949> accessed 19 June 2017

different segments have been judged, its power to redefine the concepts of privacy have been asserted.[68] Acknowledging the already provided discussions about new technologies of participatory surveillance in the literature, this Section will avoid repeating them.[69]

What can be said about privacy when a wink is enough for OHMD to initiate monitoring?

By commanding via brain signal, the use of BCI integrated AR deviates from Google Glass. The activation and deactivation of recording of a BCI integrated AR application differs by becoming more instant while the recording process is less perceptible and evident, which eventually culminates in a difficulty to perceive, almost transparent surveillance. This may cause a perceptual shift. The doubt may turn from "This is not recording, right?" to "This is recording, right?" Furthermore, a change may occur in our understanding of the popular metaphor Big Brother Society to indicate the rhetorical effect of surveillance. This is an important point to consider since metaphors have power to shape policy commitments and to influence the analogical reasoning of courts handling new technologies.[70]

It remains hard to estimate how such ubiquitous surveillance will be responded to. It is not absurd to predict that society would head down a way for acceptance, developing a common sense etiquette to apply, as has been the case for the former intrusive surveillance technologies. However, it may be the reverse. A high-degree belief for being monitored may introduce a high- degree of chilling effect. The society may assume to be monitored by and large at any moment, except if otherwise notified. Extending the argument further, persons

68 Anisha Mehta, '"Bring Your Own Glass": The Privacy Implications of Google Glass In the Workplace' (2014) 30(3) The John Marshall Journal of Information Technology & Privacy Law <http://repository.jmls.edu/jitpl/vol30/iss3/6/> accessed 10 June 2017

69 For example, the fact that the monitored information can be aggregated with other personal data, which can yield to data mining algorithms, or, that the device can be combined facial recognition technology.

70 Ryan Calo, 'Robots as Legal Metaphors' (2016) 30(1) Harward Journal of Law & Technology <http://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech209.pdf> accessed 10 May 2017

may create a more guarded behavioral pattern, so that, acting others differently, and expecting to be acted differently. Such an internalized social norm would be primarily triggered by the inability of a casual citizen to tell; when monitoring has started; what is being monitored; with whom it will be or is being shared with; what duration it will be kept; what other data it will be combined with.

The interactive relationship between law and society leads to the question, whether additional measures to cherish privacy are necessary to refer to protect against the invasiveness of BCI or not.

To begin with, what privacy type does this shift impact?

Comes as no surprise, Privacy of Association under the illustration of Finn et al. is concerned. This privacy type protects one's right to associate with other members of the society, free from the fear of being monitored. Authors differ this privacy type from Privacy of Behavior in terms of touching to "groupings or profiles over which we have no control"[71], such as DNA testing that reveals the associations we have with a certain group or family.

Then, Privacy of Behavior and Action deserves attention. This type of privacy encompasses personal preferences, concerning "activities that happen in public space, as well as private space", the ability to "behave in public, semi-public or one's private space" without having actions monitored or controlled by others".[72] The authors attribute a positive freedom to Privacy of Behavior and Action. This can be extracted from their wording as "ability to", and their reference to Nissenbaum's linking between autonomy and privacy, that the latter one

71 Finn and others (n 51), 8
72 ibidem

"contributes to material conditions for the development and exercise of autonomy and freedom in thought and action".[73]

The increased ubiquity of surveillance demands more attention to the issue of protecting privacy of behavior and action in public. In that sense, scholars seem to largely focus on the sharp private- public dichotomy. The alteration and modification of the physical boundaries of privacy is nothing peculiar to the Information Age. The issue has been on scholars' agenda since Aristotle's sharp distinction between the public sphere, where individuals (men) were involved in politics, and the private sphere, where the province of family life was the house, which would be used as a symbol by feminists afterwards, who argued it was a shield to cover up patriarchal domination and abuse. Some of the most influential critiques of privacy have come from feminist theory in pursuit of analyzing oppression of women in the light of gendered characters of public and private.[74]

Wolfe, on the other hand, has criticized the sharp private- public dichotomy of being incapable to integrate with the empirical description of modern society's major institutions or the satisfactory normative justifications. Thus, the dichotomy must be replaced with a trichotomy, as we should accept the existence of the third realm of modern society: an "intermediate between public and private". [75]

Next, Koops has discussed the irrelevance of the physical place, which legal systems base private- public dichotomy upon, arguing that where privacy intrusion takes place is no more meaningful to ask, therefore we must find other boundary-making concepts which would "reflect what comes closest to people's private life in a

73 Helen Nissenbaum (n 48), 82
74 Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (United States of America: Cornell University Press, 1997), 88
75 Alan Wolfe, 'Public and Private in Theory and Practice: Some Implications of an Uncertain Boundary' in Krishan Kumar and Jeff Weintraub (eds), *Public and Private in Theory and Practice* (Morality and Society Series 1997)

world of (…) pervasive public-space surveillance".[76] So indeed, private and public spheres should be associated with concepts that go beyond three-dimensional locations. For centuries, they have hinged on different socioeconomic factors, and the strict ties between "private life" and "home" actually occupies just a tiny part of the relevant history.[77] Inquiring where privacy intrusion took place -whether in a public or a private physical location- is becoming less and less important, considering the portability of OHMD devices. This becomes even clearer when comparing the functionality of an OHMD device to a CCTV camera.

Forming through different premises, both authors seem to claim for a legal demarcation of private and public life, by means of an interest to draw something out of public and an interest to draw something out of private.

This Section has attempted to present some normative consequences that derive from the question concerning how one's behavioral privacy is vulnerable to interference or intrusion by the use of BCI integrated AR on OHMD. This leads to the question that will be handled in the next Chapter: *how should one's right to conduct oneself as one sees fit in public or private space without having actions monitored be addressed in the regulatory framework?*

3.5. Spatial Augmented Reality Systems

76 B.J. Koops, 'On legal boundaries, technologies, and collapsing dimensions of privacy' 3(2) Politica e Società, 264

77 According to Jürgen Habermas, one of the most influential scholars in this regard, the aforementioned part has begun with the development of the modern civil society; which has emerged in 18th century, governed by economic laws and excluded the nuclear family.

Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Thomas Burger and Frederick Lawrance tr, The MIT Press 1991) <https://pdfs.semanticscholar.org/359a/4f9e78f2efe441dce955c609db17b8295e12.pdf> accessed 1 June 2017

Through surveys and implementation examples, Oliver Bimber and Ramesh Raskar provide an extensive technical background of modern Spatial Augmented Reality ("SAR" hereinafter) systems for the reader.[78] To illustrate SAR systems, the authors draw attention to the current technological variation: the exploit of spatially-aligned optical elements, e.g., mirrors, transparent screens, holograms, by novel display paradigms, so that, the technological and ergonomic boundaries of traditional AR systems have been overcome. They are becoming increasingly popular due to the decrease in cost and availability of projection technologies' personal computers. In result, they are used in universities, digital industry, entertainment business, art community, and museums.[79]

The authors further anticipate the future of SAR systems by examining the potential of each component it is formed by. These points are intriguing for the implications they have concerning how everyday environments may look like for users, and how others may view their vision. To begin with, the ergonomic future of Displays is interesting. They promise to convert into compact, portable components, which can bring satisfactory displays into existence on different surfaces in one's daily environment. For example, a future mobile projector can fill the deficiency of a surface or an ambient light, operating as a flat panel. The authors also expect electronic papers to function as a display by virtue of movement of magnetic colored capsules within the paper. Another interesting point is of the use of photosensing tags. They can enable users to identify a physical object, and to determine the pose of a displayed image, with respect to the object.[80]

The most capturing advantage of a Spatial Augmented Reality (SAR) system must be that it provides an augmented experience to users in their daily environment without requiring wearing anything. Therefore, they convey a powerful sense of tangibility by enabling virtual elements and physical reality to co-exist, providing a highly manipulated perspective.

78 Oliver Bimber, Ramesh Raskar, *Spatial Augmented Reality: Merging Real and Virtual Worlds* (United States of America A K Peters, Ltd 2005) <http://pages.cs.wisc.edu/~dyer/cs534/papers/SAR.pdf> accessed 3 June 2017
79 Idem, 8
80 Idem, 321-331

Can such technological interoperability, the co-existence of physical and virtual elements, compel persons to control their self- imaging in the spatial environment? In other words, can one's reputation be at stake? To illustrate more vividly, one can think of an unwanted or inaccurate output overlaid onto a physical person or her physical belongings, so that, her sense of self-identity (how she is perceived by her given environment) gets disrupted.

The literature has already recognized intangible harms in digital environment, and there is an abundance of work reviewing protection of identity and reputation. Given the very new departure of SAR systems to our social discourse, the realm remains highly unexplored. This is primarily due to the literature's concentration on outputs analyzing manipulation risks, and focusing on inputs for privacy risks. For instance, there is an abundance of work pointing towards passive data collection, facial recognition, surveillance and targeted advertising. The issues are directly linked to the risk of unauthorized access to the input.[81] There is also a number of works emphasizing output risks; such as, virtual content created by malicious applications. They are demonstrated to manipulate user's physical world perception unsafely and without permission, e.g., by obscuring of oncoming vehicles to be created by an AR application.[82]

However, theoretically speaking, output-related issues may threaten persons' privacy as well, triggering them to control or determine how they are seen. These threats further may be supported by manipulation of inputs, so that threats against privacy are caused by the user unintentionally. Or, there may not be a causal link between manipulation of input and persons' claim to be free from output contents overlaid on their physical

81 Anne Hobson, 'Reality Check: The Regulatory Landscape For Virtual And Augmented Reality' (2016) No.69 R Street Policy Study <https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf> accessed 2 June 2017

82 Kiron Lebecek and others, 'Securing Augmented Reality Output' (IEEE Symposium on Security and Privacy, Oakland, 2017) <https://homes.cs.washington.edu/~kklebeck/lebeck-sp17.pdf> accessed 4 June 2017

body. In such case, the claim may be related to intention of the user; such as, an intentional wink or muscle peak to command by means of BCI.

Since SAR system, which disseminates in a spatial environment, is an offspring of AR system, it is important to mention that the discussion regarding the privacy risks of AR systems is where the discussions related to Virtual Reality systems (which consist of a mere output content) was a decade ago. More alarmingly, extensive AR systems are becoming a commercial reality, on the track of Virtual Reality systems.

Acknowledging that the SAR environment is at a stage where persons present social aspect(s) of themselves, the environment therefore serves as a place where social identity functions. Social identity is easily linked to the concept of society. Since persons hold as many social identities (therefore as many reputations) as the number of societies they function in, it seems reasonable to argue that they can also hold reputation(s) in the augmented spatial environment(s). Therefore, one's reputation in SAR systems can be of regulator's interest.

The argument above requires an examination of the validity of its conclusion.

In European tradition, reputation branches into two main different concepts: honor and dignity. Reputation as honor indicates that one's value is determined through the normative features and institutional roles assigned to her, as a result of being a member of the society. Thereby, a challenge to her honor also affects to her societal status in the social system. Hereby the concept chiefly underlines one's role in the society and her contribution or subtraction to the social good. On the other hand, reputation as dignity is about one's personal identity framed

in the society's communal identity. The concept essentially captures the membership bonds one have in the society. Hereby, one can realize that reputation concept is formed by variables beyond the individual's power.[83]

Regarding de jure recognition of reputation within conventional European law, a number of legal texts have emerged from jurisprudential developments throughout the history. Overall, an overarching legal protection is established for the concept of how a person is deemed by society and how she deems herself. Today, the EU's approach to legal interest in reputation can be read by the legacies of Roman principles natural justice (ius natural) and insult (iniuria) along with their influence on the shape of the harmonization of laws.[84]

German jurisdiction, known to be as one of the main constituents of European Union law, offers a rich explanation of one's right to personality in the intersections between reputation, identity and privacy. Allgemeines Persönlichkeitsrecht (General Personality Right) doctrine opens a gateway to understand German courts' privacy jurisprudence. The main importance of Persönlichkeitsrecht doctrine for the aims of this research lies behind the influence it had on the reasoning of the ECtHR for the interpretation of "privacy protection" in Article 8 of the ECHR, as it will be revisited in the next Chapter.

The doctrine has been developed in a manner that encapsulates a series of rights of citizens related to additional legal interests, approaching Persönlichkeitsrecht as a Quellrecht (source right), and solidifying "the notion of a right of privacy ground in the dignity of the individual."[85] Such flexible approach towards Persönlichkeitsrecht initiates the continuum of a series of rights, including reputation and privacy, which also

83 Elizabeth Anne Kirley, 'Reputational Privacy & The Internet: A Matter For Law?' (DPhil Thesis, Osgoode Hall Law School York University 2015) <https://yorkspace.library.yorku.ca/xmlui/bitstream/handle/10315/30120/Kirley_Elizabeth_A_2015_PhD.pdf?sequence=2&isAllowed=y> accessed 10 June 2017

84 idem, 34

85 Paul M. Schwartz and Karl-Nikolaus Peifer, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept' (2010) 98 Cal. L. Rev. 1925, 1950- 1952 <http://scholarship.law.berkeley.edu/facpubs/1755> accessed 8 June 2017

assigns "a single high-level concept of why privacy should be protected" to German jurisdiction.[86] Historically, German jurisdiction has been influenced and inspired by Immanuel Kant's ideas of person's flourishment through self-realization and self-determination. This can be seen through how these notions which form one's personality are linked to protection of personality, further, privacy protection.[87]

The sub-concepts derive from Persönlichkeitsrecht can be found at what Koops et al. consider as the "Protection of Identity"[88] under the Cluster of "Privacy of the Person (Body, Mind, and Identity)".[89] Contrarily, the typology of Finn et al. does not identify a legal protection of the reputation under "Privacy of the Person" although the authors admit that "Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society."[90] Hereby, the typology of Finn et. al does not suffice to cover the legal protection for one's reputation. On the other hand, by examining the national constitutions, Koops et al. detect a protection of a third-person perspective concentrating one's reputation, a legal protection of one's interest about how she thinks society perceives her. Authors further situate the protection of identity as a separate type as "ipseital privacy". The formalization of "ipseital privacy" is a contemporary and a useful one for the purposes of this research, being in line with the current legal interest protected by Article 8 of the ECHR. The ECHR cherishes the protection of identity as a collateral legal interest by underlying it under the same provision where privacy is protected. Nevertheless, it has been systematically interpreted as a personality right by the ECtHR.

Two notes should be made before closing this Section. The protection of reputation is indeed been acknowledged in the regulatory framework through interpretation of Article 8. Secondly, an augmented spatial

86 ibidem
87 James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) Faculty Scholarship Series. Paper 649, 1182 <http://digitalcommons.law.yale.edu/fss_papers/649> accessed 4 June 2017
88 Koops and others (n 53), 543
89 Idem, 528
90 Finn and others (n 51), 4

environment has potential to grow into a convenient factor in the paradigm of one's reputation. Therefore, the regulator should approach one's identity and reputation in SAR systems.

This Section has attempted to present some normative consequence that derive from the question on how one's reputation may be vulnerable to the interference or intrusion by the running of BCI integrated AR technology on a SAR system. This leads to the question that will be handled in the next Chapter: *how should one's right to ipseital privacy be addressed in the regulatory framework?*

4. SEEKING FOR PRIVACY PROTECTION IN THE REGULATORY FRAMEWORK

Consisting of four Sections, this Chapter will answer the third sub-question of this research.

The first Section will supply a functional definition to BCI integrated AR in the eyes of the EU regulator. Such definition has importance for the purposes of this study since a normative statement can strengthen the foundations of the legal analysis in the following paragraphs. It is also valuable in terms of selecting the accurate and relevant legal sources in the regulatory framework to focus on. Fundamentally, a source within the EU, *D6.2 Guidelines for Regulating Robotics*[91] ("Robolaw" hereinafter) will be resorted in terms of defining and classifying BCI integrated AR. The Robolaw is a European Commission funded project that explores the multi-dimensional interaction between robotics and regulation and provides a guidance for ethical analysis and legal methodologies that should be maintained on technological innovation. Since Robolaw elaborates on a number of regulatory principles, leaving them to the discretion of the EU policy makers, these principles are expected to be considered by the EU regulator within a relatively short time frame. Thus, Robolaw becomes more of an issue for the purposes of this research.

The following Sections will analyze whether the regulatory framework is equipped with sufficient responses for the challenges brought by the run of BCI integrated AR on the devices which are outlined in Chapter 3: Mobile devices, OHMD and SAR systems. The following Sections will make a claim regarding which regulation field (hard law regulation, soft law regulation or case law regulation) the EU regulator should focus on and what privacy protection needs to be considered. The following Sections will answer the question: which legal tools should be identified by the EU regulator, so that the content of a particular legal tool fits to the

91 Robolaw Project, 'Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics' (2014), <http://www.robolaw.eu/> accessed 21 April 205

characteristics of a particular technology? With this aim, two sources of soft-law will be applied: *1. Civil Law Rules on Robotics*[92] *and 2. Dissemination and use of intrusive surveillance technologies*.[93]

These sources are compatible with the aims of this Chapter since they are capable of giving an account of ethical considerations, legal definitions, and legal ramifications concerning BCI integrated AR technology.

4.1. Regulating Normative Definitions in an Indefinite and Dynamic Field

No common statement exists in the regulatory framework regarding what BCI integrated AR technology is. This is mainly because defining a novel hybrid technology, in the lack of any tangible consensus among the Science and Technology community, is beyond the EU regulator's interest, as well as responsibilities. Adding the fact that the technology is not advanced enough to land into societies, the EU regulator must have had no craving for attempting to settle a stance.

Nevertheless, a regulatory framework that lacks an explicit definition of a subject-matter, ipso facto, is not scarce of functional explanations. Guided by this continuity of thought, this Section will offer an explanation commonly used in social sciences and provide a functional definition. This will be done on the basis of the functions which the structure of BCI integrated AR have been construed upon. Although a functional definition can offer a great advantage for the reader to grasp the nature of the concept, by no means it is an excellent approach. This is especially the case for a technological system as hybrid as this research's subject matter. For example, the endorsement that will be provided may seem too flexible for some, so that it fails to set the authentic functions aside from the adverse impacts of the system. Or, the selection of functions may be viewed as being improper or unsuitable to be used in the definition.[94] However, encountering these criticisms exceeds

92 European Parliament (n 8)
93 European Data Protection Supervisor (n 9)

94 See more criticism on Functional Explanations, <http://www.iep.utm.edu/func-exp/> accessed 19 May 2017

the purpose of this research. This Section will solely argue that there are more reasons to favor a functional definition than there are to disfavor, for the purposes of this research.

The classes in which BCI integrated AR system are deemed to belong will be identified by investigating different sources rooted in European Union sources; from Guidelines to proposed strategies of the Commission, to detect the uniqueness of the BCI integrated AR system, and how it differentiates from other piece of technologies. Hereby, the system's functions will be revealed.

Initially, BCI requires a deep look into its components. No common definition exists in the regulatory framework although various instruments agree on its capability to enable a communication between human and computer. A consortium which is funded by the European Commission notes that the most common definitions accept that "a BCI must rely on direct measures of brain activity, provide feedback to the user, operate without delay, and rely on intentional control."[95]

BCI is mostly used through an application by which it is validated, (Section 2.1.) and the regulatory framework seems to acknowledge that BCI is theoretically meaningful and practically feasible only when it integrates with application.

The Robolaw project is interested in more sophisticated applications, such as: prosthesis, robotic arms, self-driving cars, personal care robots. The project mentions BCI during the overview of robotic prostheses, to distinguish invasive and non-invasive direct interfaces.[96] BCIs stand as a direct interface that connects with the central or peripheral nervous systems which can be invasive (implanted electrodes) as well as non-noninvasive

95 Horizon2020, 'Roadmap. The Future In Brain/Neural- Computer Interaction' (2015), 11 <http://bnci-horizon-2020.eu/images/bncih2020/Roadmap_BNCI_Horizon_2020.pdf> accessed 2 May 2017
96 Robolaw Project (n 93), 87

(EEG).[97] The project also addresses the Human Machine Interface[98], under the case of "Self- Driving Cars", while advising to address more research on the topic to discover the best paths a person and car can interact on.[99]

The Da Vinci System,[100] as depicted in the Robolaw project, can serve as an example of Human Machine Interface integrated AR. Two units form the system: A Surgeon's Console Unit and a unit composed by Human Machine Interface, Electronic Controller and Manipulator. Surgeon's Console Unit is for holding the display whereas the other unit is for telemanipulation of surgical tools.[101] The Da Vinci System provides the surgeons with hand–eye coordination and natural correspondence with manipulations. By hand motion, the surgeons control the movement of the instrument's tip inside the patient's body. However, a BCI integrated AR surgical system differentiates by means of building a connection between the surgeon's neurological brain activity and the movement of the instrument's tip inside the patient. It is deductible that such connection will require one of the techniques for evaluating and detecting the electrical brain activity, such as EEG.

Another point of the Da Vinci System is that the surgeons, by controlling the camera reference frame, get the virtual sensation of motion of the instruments inside the patient's body, to be displayed in the surgeon's unit, i.e., the patient's body is augmented on the surgeon's unit. A BCI integrated AR surgical system differentiates by means of recruiting a device (a HMD, for example) to detect the augmented object, and to display the image on more than one screen, enabling more than one surgeon to view the patient's body.

97 Idem, 109

98 This research is of the opinion that in "Self-Driving Cars" section the study uses Human Machine Interaction and BCI interchangeably. Human Machine Interface, "the interface devices between humans and machine", is one of the primarily recognized applications of BCI in practice.

99 Robolaw Project (n 93), 53

100 Idem, 81

101 This Section focuses on the da Vinci System since it is "at present the most widespread surgical telemanipulator." See an instructional video on da Vinci System, https://www.youtube.com/watch?v=EiVY-htgRUY

Under the section of "Care Robots", the Robolaw project exemplifies a framework in which robot serves as an "interface" for a disabled person to the physical world. Called as Remote-Brained Robotics, the functionality of such robots is to separate brain and body and to "connect standalone robots to a high level remote control system."[102] This system, controlling a care robot in its environment (augmenting user's reality in a degree) via brain signals, is closest to the BCI integrated AR applications detected during the source review, in terms of the functionalities they share. However, BCI integrated AR system differs by being more generous about the progress of augmenting the physical world. This requires more emphasis on the sensation of robot's environment, so that the system enables the user to control not solely robots, but also devices in its environment.

The definition attempts for AR occupy a lesser extent than the definitions attempts for BCI. The ones provided for AR seem to be a combination of physical and virtual environments. European Union's Innovation Union[103] is the most extensive source realized to identify what AR is. The Innovation Union delivers an ostensive definition through examples on how AR functions. ("...to add virtual objects into a real scene for example by superimposing them on an image of the scene captured by a camera.", "Added objects might be virtual characters in a film production or video game, simulation of a construction project, instructions for repairing a car engine, or a reconstruction of an archaeological site.")[104]

In overall, the vast majority of the meaning associated to BCI in the sources analyzed, deals with robots. On the other hand, the meaning associated to AR is more vague, realizes its two facets (physical and virtual environments) and explained through examples on how AR can be used. Apparently, the EU regulator

102 Robolaw (n 93), 169

103 "Innovation Union is a part of the European Union strategy to create an innovation-friendly environment that makes it easier for great ideas to be turned into products and services that will bring our economy growth and jobs." See, <http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=home> accessed 10 July 2017

104 See, <http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=ar-explained> accessed 16 May 2017

acknowledges BCI integrated AR as a system which relies on the user's intentional control via her brain activity, allowing her to control one or more devices in the environment.

4.2. Hard Law Findings Regarding Mental Privacy

4.2.1. Visiting the EU Charter of Fundamental Rights

The noteworthiness of the EU Charter lies in its anchorage characteristics regarding the affirmation of the central role of fundamental rights. According to Article 52(3), it reflects the fundamental rights proclaimed in the ECHR through meaning and scope.

Reiterating the question that arose in the Section 3.3, regarding *one's right to refuse the extraction of infinite personal information within her neurological activity,* Article 3 and Article 7 of the EU Charter come under consideration.

Ienca and Andorno detect a dilemma here, an "inception problem" as they name it, that arises from the fact that, information to be protected (neural activity) and the information source (the mind) may be inseparable.[105] Bearing in mind what the neurotechnological future beholds, they call for wider privacy and data protection rights to be applied at "a higher and chronologically antecedent level".[106]

This argument welcomes an amount of philosophical criticism, in terms of mind-body dualism. The authors argue that the traditional privacy rules, which concern with the privacy types other than the mental privacy, safeguard external information. Yet, the authors do not show how exactly the information source and

105 14
106 ibidem

the information to be protected may be separable when it comes to other privacy types, or whether they are as problematic as in mental privacy or not.

This contribution will argue that it is hard to conceptualize an intrusion in one's privacy that does not leak a good amount of information about her mind. As the authors note, we are approaching a neurotechnological future. Having said that, it does not require but rather remind us "to guarantee protection (...) to the source of that information."[107] Our mind is not perceived by others as electronic signals in everyday life, but conceived as thoughts and feelings, in forms of action or inaction. More mundanely, an implication of our current mood captured in a video, or a detail about our personal preferences in a family photograph. Moreover, since it is other persons that perceive our thoughts and feelings, the way we are perceived is absolutely depending on another's perception, which derives from their thoughts and feelings, exactly, from their mind. With their transcendent nature, our minds are tremendous sources of our own lives. Therefore, a coherent privacy protection should broaden its scope to recognize that, any privacy intrusion may affect one's mind, provided that a technological device is used as a means. This is indeed an objection that such protection blurs the lines; makes it unnecessary to demarcate between the legal implications in the Articles, such as an attack on BCI and a telephone interception. Nonetheless, the premise of the point is that these lines are becoming too vague and elastic to leave to the current provisions, considering we are approaching the neurotechnological advancements and will approach further. (E.g., Consider, teleportation technology)

The crucial task is to settle such ethical and philosophical framework in place in a hypothesis, which also perpetuates the organic ties in the regulatory framework to function successfully. This Section will not account for a hypothesis from which a right to mental privacy concept could be derived, but elaborates on values and tenets to guide the explanation of it.

107 ibidem

This Section will deal with the question that is raised in Section 3.3, regarding the formalization of *the right to refuse the extraction of infinite personal information from neurological activity, in the regulatory framework*. This Section will make a claim regarding how the EU Charter can assist to the formalization of a conceptualization which strongly protects one's mental privacy against intrusions.

4.2.2. What does hard law offer?

Let us begin with Article 7 *Respect for private and family life*. The provision ensures a protective tool against intrusion into one's privacy. Having ascribed a fundamental right to privacy, the explanations relating to the EU Charter recognize that the meaning and the scope of the Article 7 are equivalent to Article 8 of the ECHR, which makes "the limitations which may legitimately be imposed" on the Article 3 "the same as those allowed by Article 8".[108]

On the other hand, Article 3 *Right to integrity of the person* guarantees that "everyone has the right to respect for his or her physical and mental integrity". It can be read as another fundamental right originally coined to regulate the vertical relationship between citizen and government, assigning a *negative right* to the former, from the latter one's intrusion. When one looks into the core of the protection in the light of sanctions and key consequences of the CJEU's case law, the letter of the provision also emphasizes a *positive right* to self-determination. Such that, the Article is interpreted in a manner to enshrine persons' ability to develop physical and mental functioning to the fullest extend that they wish, whilst referring to a *negative right*, to prevent mind targeted intrusion without consent. The Article accepts personal integrity as composed of physical (body) and

108 Explanations relating to Article 7 of the EU Charter<http://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life> accessed 25 July 2017

mental (mind) integrity, further assuming that harm impacting mental integrity is comparable to the harm upon physical integrity.

Clearly, a legal interest that urges from the misuse of one's neurological activity, has not been the explicit intention of the EU Charter's drafters. The Article draws attention to the biomedical field, enumerating four provisions to be respected, namely "informed consent", "prohibition of eugenic practices", "prohibition of financial gain of body", and "prohibition of reproductive cloning". This is also in accordance with the focus of the European Union Agency for Fundamental Rights ("Agency" hereinafter) on its publications, whose latest interest driven is in mental health problems encountered within the bio-medical field.[109] However, practically speaking, one's mental integrity is subject to more than mental-health risks. The Article, its Explanation, and the Agency are silent about anything further than bio-medical practices.

The Agency's special position within the regulatory framework is notable. Having an overall duty to raise awareness of fundamental rights, it also has the duty of collecting and disseminating objective and reliable data on the current situation to advise EU institutions for the implementation of the EU Charter.[110] Herewith, the data collected enables EU institutions to benefit from evidence-based advice on the matters of discussing, amending, and reforming the scope of the EU Charter. Thereof, a shift in the Agency's perspective can be highly influential for the EU regulator, in terms of an upgrading the protection of mental privacy in its negative sense.

All in all, it is hard to argue that the EU has been totally negligent of the fact that mental integrity may be at stake in contexts other than the medical field. An interesting reference can be found in the Commission's

109 European Union Agency for Fundamental Rights, 'Involuntary placement and involuntary treatment of persons with mental health problems' (2012) Official Report <http://fra.europa.eu/en/publication/2012/involuntary-placement-and-involuntary-treatment-persons-mental-health-problems> accessed 20 May 2017

110 See, <http://ec.europa.eu/justice/fundamental-rights/agency/index_en.htm> accessed 21 May 2017

Report on the environment, security and foreign policy that was tabled in 1999.[111] The Commission urges for an international convention regarding the global ban of research and development, "which seeks to apply knowledge of the chemical, electrical, sound vibration or other functioning of the human brain to the development of weapons which may enable any form of manipulation of human being"[112], be it military or civilian.

The nature of a legal concept cannot be derived merely on the grounds of the text of a specific Article. Because the segments of privacy for legal purposes within the Union is deduced from the case law of the CJEU, the same may be expected regarding the Court's arrival at a judicial consensus regarding the context of mental privacy. A conceptual orderliness, and a harmony regarding what legal interests are encapsulated in mental integrity, and in what cases they are triggered, may quicken this process, enabling a clear framework for the judges to perform statutory interpretation.

4.2.3. Remarks

The above paragraphs have elucidated that Article 3(2) of the EU Charter keeps pace with the changes in society from the point of bio-medicine, by enumerating four particular principles to be respected, considering a biomedical research. The provision establishes a boundary regarding the freedom to research and clinical practice of bio-medicine, cherishing the individual's mental integrity. Since Article 3(2) demands that these principles be respected "in particular", the Article cannot have intended to establish an exhaustive list. The Article, however, does not focus on the emerging and pervasive detriments that may be brought forward through the abuse of the end-user computing technologies. Hereby it becomes visible that the Article lags behind the growing changes in the social conventions from the point of technological advancement, failing to ensure the

111 Committee on Foreign Affairs, Security and Defence Policy, 'Report on the environment, security and foreign policy' (1999) <http://www.envirosecurity.org/ges/TheorinReport14Jan1999.pdf> accessed 22 May 2017

112 idem, 10

protection of mental integrity in a timely fashion. In the same manner the EU regulator keeps pace with the changes in society from the point of the biomedical field, it should establish particular boundaries regarding the use of end-user computing technologies. Such emphasis on the danger of interference with mental integrity through the misuse of end-user computing technologies, can be anticipated to play a part in the interpretation of Article 7 of the EU Charter. This is because, the conclusion that the intrusion does not respect one's mental integrity, can be followed from the indication that the interference is equal to an inhuman or degrading treatment. This indication, that the interference amounts to the intrusion of mental privacy, can merely be deduced by analyzing and evaluating the principles and values that are stipulated and underscored in Article 3. In other words, for Article 7 to come into play, the interference into mental integrity should reach a particular level of gravity in terms of Article 3. That is to say, the right to privacy that is protected under Article 7, is handled with reference to the right to mental integrity, that is guaranteed under Article 3. Therefore, it is of significance for the EU regulator to take account of the technological developments regarding end-use computing technologies, by establishing an absolute minimum of warranties to cherish mental integrity against the danger of the misuse of the technology.

This Section has elaborated on the values and tenets to guide the explanation of a broader conceptualization of Article 3 which aims to offer a stronger and more efficient protection of one's mental privacy against intrusions. This Section has concluded that a non-exhaustive list of principles, which frames a particular limitation of the use of end-user computing technologies, should be explicitly stipulated in Article 3. As it has been mentioned in the beginning of this Section, to leverage the functionality of the conceptualization of Article 3, it should be ensured that the organic ties in the regulatory framework are working in harmony with the conceptualization. To show how such conceptualization can work in harmony with the related legal rights and interests, this Section also has stressed the importance of a shift in the Agency's concentration.

4.3. Soft Law Findings Regarding Behavioral Privacy

4.3.1. What does soft law offer?

Section 3.4. has noted two distinctive expectations to be emphasized. Initially, although the right to Behavioral Privacy can be formulated as a positive right, it can also be framed as a negative right, namely, the freedom to be free from unauthorized intrusions. Later, what constitutes "private life" should be determined by contemplating new boundary-making concepts, to the level that the physical place that is attached to "private life" dissolves. Finally, Section 3.4 has raised a question regarding the protection of *one's right to conduct oneself as one sees fit in public or private space without having actions monitored*.

In the wearable technology field, there is a lack of legislation concerning user privacy within the regulatory framework. This seems like a deliberate choice since the EU regulator rather prefers to adopt an existing Directive or Regulation to a rising field of technology, maximizing their compatibility.[113] Handling conflicts, the CJEU therefore cannot use the legality criterion since wearable technologies are not legislated under an umbrella legal text. Recognizing that BCI integrating AR is still at experimental stage or newly entering to the market, following guidelines by the EU institutions on the interaction between technical and societal norms, may offer an effective approach.

The legal basis for such an approach can be justified under Article 211 of the Treaty Establishing The European Community (TEC). Accordingly, the Commission shall "formulate recommendations or deliver opinions on matters dealt with in this Treaty, if it expressly so provides or if the Commission considers it

113 For instance, the EU regulator has taken the increasing rapid pace of wearable technologies into account, preparing the new legislation on medical devices, in Regulation (EU) 2017/745 and Regulation (EU) 2017/746

necessary" to "ensure the proper functioning and development of the common market".[114] This approach finds its roots in Soft Law. Soft law can be defined as rules of conduct that may have legal effects although do not impose legally binding force. They serve as an umbrella concept "for those instruments laying down rules of conduct whose legal status is unclear or uncertain."[115]

Soft law can change the behavior of jurisdictional bodies. This makes a practical purpose in the regulatory framework, because in the milestone *Grimaldi case*[116] the CJEU took a different approach by taking a quasi-legal instrument, an EU recommendation, into account. The Court held that even though a Commission Recommendation cannot "confer rights on individuals upon which the latter may rely before national courts", "national courts are bound to take those recommendations into consideration in order to decide disputes submitted to them, in particular where they are capable of casting light on the interpretation of other provisions of national or Community law."[117] All in all, a hybrid model of governance of fundamental rights which happens to blend hard law and soft law to satisfy the rising needs of novel cases in different technological fields, has already been there for awhile.[118]

To begin with, there is not a shadow of doubt that the monitoring act of a private activity should be an offense. Soft law can additionally set out the legal conditions, framing governance among the parties. For

114 Treaty Establishing The European Community (Consolidated version 2002) OJ C 325 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12002E%2FTXT> acces*sed 22 May 2017*

115 Linda AJ. Senden, 'Soft law and its implications for institutional balance in the EC' (2005) 1(2) Utrecht Law Review, 81

116 Case C-322/88 Grimaldi v Fonds des maladies professionnelles ECLI:EU:C:1989:646, (1989) <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=96317&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=379738> accessed 30 April 2017

117 idem, para 19

118 See more extensively on this, Oana Andreea Ştefan 'European Competition Soft Law in European Courts: A Matter of Hard Principles' (2008) 14(6) European Law Journal, 753. <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0386.2008.00443.x/abstract> accessed 15 June 2017

instance, legal monitoring of private activity cases in which particular circumstances are met. *A legitimate interest, legal interest* or *consent* are important exceptions that have their roots in the EU's ingrained framework.

A reference made to consent can be found in *Civil Law Rules on Robotics*[119], under the Section of *"*Protecting humanity against privacy breaches committed by a robot".[120]

Civil Law Rules on Robotics is a convenient source to understand the applicability of soft law governance in protecting particular privacy interests. Composed by the Parliament's Legal Affairs Committee, the study acknowledges that regulating hard law for the sake of an adequate legal framework turns out to be indispensable once the technological advancements call for a change. Regulating must be enacted particularly in areas where current legal response does not meet societal expectations. This should be done by means of an ethical response, which is required, because neither the EU Charter nor the ECHR has ability to fully solve the problems, that arise with the infringement of human liberties by robots.

Civil Law Rules on Robotics argues that robo-ethical principles should be considered, regarding consent from *the subject entitled to privacy*, so to ensure that *the consent derives from the subject but no one else.* Hereby, a demarcation between consensual and non-consensual actions can be read between the lines. The consent acts as a legal instrument justifying the act of monitoring by assigning persons a right to make decisions to be monitored in public or private physical places at all, or to refuse this. The consent should be freely given either implicit or explicit. All in all, a demarcation set via consent can indeed be preferable since it is announced and perceivable.

119 European Parliament (n 8)
120 idem, 22

However, the multidimensional characteristics of our everyday lives should foster the EU regulator to consider different factors in social domains come into play, and difficulties may arise in the negligence of these factors. What makes these factors suitable to be under the governance of soft law is that they can be addressed in a fashionable timely manner. One's expectation of privacy[121] in private sphere differentiates from her expectation of privacy in public sphere, so does her expectation of privacy concerning a private conversation and a non-private conversation. In this line of policy, the EU regulator can also contribute to the clarification of the matters that are beyond an explicit consent, e.g., the scope of implicit consent or the methods through which an implicit consent is sought.

Finally, such governance among parties in a surveillance network brings restriction or prohibition provisions with it. The EU regulator may consider giving its opinion on whether a particular conduct by the OHMD user should establish an offense or not. Besides, when one thinks about possible ways that an intruder may circumvent the legal restrictions, the importance of the EU regulator's contribution to an outcome between private and public course of actions, becomes even more clearer.

Another opinion of the *Civil Law on Robotics* that is relevant to our discussion is about remote monitoring. The study exemplifies a case in which personal data of users or third parties is saved in the memory of a robot which requires Internet connection to monitor its operating and functioning. Such cases, the study claims, require specific measures to construct and rule strict data access conditions and affairs. Furthermore, security design and measures should be taken into account more seriously. A security construction which enables the owner to verify or even exercise a level of control upon the robot, moreover, allows the owner as well as related third parties whose data may be stored, to update security measures such as passwords, firewalls, etc.

121 According to the Contextual Integrity Theory, as Helen Bissenbaum argues, an information is not appropriate to disclosure unless conforms with contextual information rules. These rules are related to specific individual factors.

The European Data Protection Supervisor's opinion on *Dissemination and use of intrusive surveillance technologies*[122] is another relevant point to raise because it addresses a number of crucial points that arise out of these technologies which have impacts on Behavioral Privacy. Intrusive surveillance tools basically "remotely infiltrate" Information Technology systems to "covertly monitor the activities of those IT systems and over time, send data back to the user of the surveillance tools".[123] The opportunities arise by the use of Information and Communication Technology tools come along with the downsides that may affect to the protection of privacy. Thus, EU policies should approach the strain emerged between seriously, regulating the use and dissemination of these tools appropriately, consistently, and effectively, setting the necessary safeguards.

4.3.2. Remarks

It took Uzun v. Germany for the regulatory framework to recognize that a large surveillance system which collects information about one's movement in the public sphere breaches the right to privacy.[124] The analysis on two different soft law sources above has implied that the soft law regulation can be a guidance regarding the protection of Behavioral Privacy, by providing a testing ground for the upcoming monitoring threats infiltrated from the sophistication of a technology or technologies. This contribution will explain below why soft law can guide the EU regulator for a more efficient and stronger protection of Behavioral Privacy in terms of OHMD.

Initially, soft law promises to strike a balance between the flexibility of non-binding rules and participatory norms, allowing a sufficient level of legal certainty, that might "otherwise be compromised if we were to rely solely on the judge to (re)define fundamental rights." [125] Next, enough attention should be given to the fact that technology co-exists and co-evolves among with the practice of societal rules and opinions. Soft-law

122 European Data Protection Supervisor (n 9)
123 Idem, 3
124 Case of Uzun v. Germany Application no. 35623/05 (2010) <http://hudoc.echr.coe.int/eng#{"itemid":[001-100293"]}> accessed 31 May 2017
125 Koops and others (n 53), 30

governance thus can enable a more timely solution, blending offices', agencies', bodies' and society's current values and rules. The pervasive, instant and unperceivable monitoring capacity of OHMD makes it open to a governance discussion. How should the rights and responsibilities of different stakeholders in the surveillance network be governed, if at all? Placing the users in such governance is a tricky work, because the action may go beyond the user's intention and cause the surrounding persons to form a fragment of the surveillance network although the user may not intend to initiate surveillance. However, this line of thought can become a slippery slope since it underlies pursuing a deterministic method. To divest itself out, the EU regulator can essentially concentrate into the society's responses about what they think and feel of being monitored in their intimate fields of life, by other persons, which can be measured in different time and spaces. It should be noted that the literature is largely in lack of a quantitative and explanatory research in this respect. More research and evaluation test should be executed, so that citizens may participate and engage into the process, in compliance with the EU's wide-ranging democratic principles. Societal implications of the devices, such as their severity degree, should be revealed before formulating the elements for a legal protection of privacy for the threats of OHMD monitoring.

4.4. Case Law Findings Regarding Ipseital Privacy

4.4.1. What does case law offer?

Reiterating the question that arose in the Section 3.5 regarding *how one's right to ipseital privacy should be addressed in the regulatory framework,* relevant measures and mechanisms come under the scrutiny for the CJEU to adopt in order to address the loss of ipseital privacy. Herewith, a brief presentation of ECtHR's formalization of reputation protection is needed. The relevant article is Article 8 of the ECHR.

The codified interests of the Article are *the right to respect for his private and family life, his home and his correspondence.* It retains public authorities from interfering with the right to respect for private life unless it is in accordance with law and necessary in a democratic society in the interests of national security, public safety or the economic well being of a 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, to protect the codified interests. The Court has been willing to stretch the scope of the Article, by protecting the right to self-determination. It has "extended privacy protection to horizontal relations and has gradually accepted that individual autonomy is an equally important value underlying the right to privacy", going beyond the protection of negative freedom and autonomy in vertical relations between citizen and state, as it was originally coined.[126] This can easily be read in the lines of the willing of the Court to treat right to privacy as a legal fragment which interacts with fundamental rights. Moreover, as will be outlined below, the Court has been willing to apply the self-determination rationale in the right to control one's own identity.

Preifer v Austria is the landmark case in European law for the Court to acknowledge reputation as a right for the first time and as an integral part of the right to respect for private life.[127] The Court had encountered the claim that Austrian courts had failed to protect an Austrian woman's reputation against defamatory allegations under Article 8 of the ECHR. Reiterating its previous decisions, the Court reasoned that reputation is protected since the Article aims to protect self-development. The Court held that one's reputation "forms a part of his or her *personal identity and psychological integrity* (emphasis added) and therefore also falls within the scope of his or her private life", and there was no need to scrutinize whether the defamatory allegations had taken place in

126 B. van der Sloot ' Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) 5 JIPITEC <https://www.jipitec.eu/issues/jipitec-5-3-2014/4097> accessed 2 May 2017

127 Case of Furst-Prefier v. Austria Applications nos. 33677/10 and 52340/10 (2007) <https://lovdata.no/static/EMDN/emd-2010-033677.pdf> accessed 24 May 2017

public or not.[128] Another more recent case is A. v. Norway.[129] Reiterating its Preifer verdict, the Court held that the same consideration must also apply to personal honor. It held that "the attack on *personal honor and reputation* (emphasis added) must attain a certain level of gravity and in a manner causing prejudice to personal enjoyment of the right to respect for private life."[130]

4.4.2. A comparative analysis between Right to Privacy and Right to Personality

The resemblances between the prior decisions and a given case have influenced the Court to extend the prior decisions to apply to the other one. Given the Court's tendency to widen Article 8 in a line keeping up with technological advancements and their societal implications, it is plausible to assume that, it will continue to do so.

Yet, the protection of ipseital privacy in a SAR system, will demand more than a description of thematical area to be retained from interference of public authorities. The concern remains whether the governance of ipseital privacy will refer to the protection of identity in a timely fashion.

The application of fundamental rights provisions is restricted to the point where the Court sets out an appropriate balance among them. Thus, the protection of one's ipseital privacy will inevitably touch to the countervailing fundamental rights of the Union. One of the most debated points may be whether ipseital privacy should be consolidated with right to privacy as in ECtHR standards, or rather, General Personality Right *(Allgemeines Persönlichkeitsrecht*) as the preponderant German jurisdiction approach. The right is created by the German judges, interpreting Article 1 and Article 2 of the Basic Law for the Federal Republic of Germany.

128 Case Of Karako v. Hungary Application no. 39311/05 (2009) Partly Concurring Opinion of Judge Joiene, para 64 <http://hudoc.echr.coe.int/eng#{"itemid":["001-92500"]}> accessed 10 May 2017

129 Case of A. v. Norway Application no. 28070/0 (2009) <http://hudoc.echr.coe.int/eng#{"itemid":["001-92137"]}> accessed 10 May 2017

130 Idem, para 64

(Grundgesetz)[131] To form into a question; should personality protection be covered by a general right to privacy or should privacy protection be covered by a general right to personality?

4.4.3. Remarks

This Section argues that there are reasons to favor an approach that has its roots in Right to Personality, since it can cover privacy protection regarding reputation, guaranteeing one's ipseital privacy. Assessing from both a theoretical and practical angle, personality rights are more relevant by means of "protecting people's capacity to know who they are and to become who they want to be"[132], assigning them the right to claim a positive freedom to determine the destiny of their identity; in forms of reputation, honor and dignity. Hereby, in accordance with the growing models of AR technologies, the judges can grant a protection encompassing a broad alteration of privacy related issues.

Tracing what the technological paradigm of AR brings to the information society, the CJEU hence should give attention to ECtHR judges' interpretation for a stronger and contemporary protection. Meanwhile, EU institutions can pursue this upcoming paradigm shift in the societies and its legal implications by enabling recommendations, opinions, communications and guidelines.

131 Grundgesetz für die Bundesrepublik Deutschland <https://www.bundestag.de/grundgesetz> accessed 10 April 2017
132 Koops and others (n 53), 536

5. SUMMARY AND CONCLUSIONS

This last Chapter reports the summary and conclusions culminated in this research.

The introduction of every new technology produces new advantages and dangers into our daily lives. Their adaptability into our practical use depend on a scrutiny: asking the question, *how should the regulator think about these technologies* so that a stronger and more efficient protection of fundamental rights can be ensured? This work has aimed to answer this question in terms of the privacy protection, that are anticipated to be evoked by BCI integrated AR technology and its applications.

Following the presentation of the technology in its adaptability and applicability, I have showed in Chapter 2 that even in the current state of art, the technology is highly capable to satisfy needs of disabled people, surgeons, mobile robot users, and personal robot users, which implies a promising evolution of the technology. Chapter 2 has also indicated the importance of this study for the individual and society. By virtue of the findings, it can be argued that the effects of BCI integrated AR applications shows great potential to assist with the social integration of disabled or paralyzed citizens, and those who suffer from locked-in syndrome. By advancing their autonomy and capacity in societal segments, these applications may offer a genre of social participation which exceeds the limits of mundane tasks, such as social innovation and democratic practices.

In Chapter 3, I have outlined how the execution of the technology can trigger different types of privacy protection, and discussed which approaches can be adopted to counter the privacy concerns. The arguments of the Chapter 3 made their case by adopting statements and findings from computer and science studies, cognitive science and sociology.

Inquiring the compatibility of the legal framework of privacy with the technological artifacts that are outlined in the Chapter 3, I have analyzed in Chapter 4 whether the technological artifacts require amendment or whether themselves should be regulated, through hard law, soft law or case law. This has required an analysis on whether these legal sources are sufficiently equipped to cover particular privacy concerns, that are evoked by particular privacy types, and whether they could be advanced for a contribution towards a more stronger and efficient privacy protection.

Chapter 4 has elaborated on the study of the technology regulation. Having examined the risk of different privacy intrusions (intrusion into mental privacy, intrusion into behavioral privacy, intrusion into ipseital privacy) through peculiar characteristics of the different case scenarios, I have comprehensively mapped particular types of regulations (hard law regulation, soft law regulation, case law regulation) that can potentially effectively influence the society's behavior and regulate particular types of privacy intrusions.

Returning to the main research question, this research has concluded that the EU regulator should recognize the uniqueness of different pieces of BCI integrated AR, to clearly grasp the technological space by which the society will be surrounded. Hereby, the EU regulator should introduce a number of legal responses to uphold privacy protection, guaranteed by different types of regulations. This research has argued that the most efficient tool for a stronger protection of mental privacy would be a broader conceptualization of Article 3 of the EU Charter, whereas the most efficient tool for a stronger protection of Behavioral Privacy would be the guidance of the relevant soft law sources. Finally, the most efficient tool for a stronger protection of Ipseital Privacy would be achieved by the CJEU judges' reliance on the ECtHR judges' interpretation on Right to Personality.

The scope of BCI integrated AR is broad and so are its implications on privacy protection. The area is waiting to be analyzed by further research.

TABLE OF CASES

European Cases

TABLE OF LEGISLATION

European Legislation

German Legislation

BIBLIOGRAPHY

Opinions, Recommendations and Guidelines

Committee on Foreign Affairs, Security and Defence Policy, 'Report on the environment, security and foreign policy' (1999)

Opinion 2/13 Of The Court of Justice, pursuant to Article 218(11) TFEU, made on 4 July 2013 by the European Commission

European Data Protection Supervisor, ‘Opinion 8/2015 Dissemination and use of intrusive surveillance technologies’ (2015)

European Data Protection Supervisor, ‘Opinion 8/2015 Dissemination and use of intrusive surveillance technologies’ (2015)

European Parliament resolution of 16 February 2017 with recommendations to the Commission, ‘Civil Law Rules on Robotics’ (2017)

European Union Agency for Fundamental Rights, ‘Involuntary placement and involuntary treatment of persons with mental health problems’ (2012) Official Report

Horizon2020, ‘Roadmap. The Future In Brain/Neural- Computer Interaction’ (2015)

Opinion 2/13 Of The Court of Justice, pursuant to Article 218(11) TFEU, made on 4 July 2013 by the European Commission

Other Secondary Sources

Abdullah MK, Subari K, Loong JL and Ahmad NN, 'Analysis of the EEG Signal for a Practical Biometric System' (IEEE EMBS Conference on Biomedical Engineering and Sciences, Kuala Lumpur, November 2010)

Abhinav L, 'VR and AR Need Brain-Computer Interfaces to Achieve Their Full Potential' Gadgets 360

Albrechtslund A, 'Online social networking as participatory surveillance' (2008) 13(3) First Monday

Bento V, Paula L, Ferreira A, Figueiredo N, Tomé A, Silva F, Cunha JP and Georgieva P, 'Advances in EEG-based Brain-Computer Interfaces for Control and Biometry' (7th International Conference on Image Analysis and Recognition Proceedings, Part II, Póvoa de Varzim, June 2010)

Besharati TL and Mahvash M, 'Augmented reality–guided neurosurgery: accuracy and intraoperative application of an image projection technique' (2015) 115(2) BJUI

Bimber O and Raskar R, *Spatial Augmented Reality: Merging Real and Virtual Worlds* (United States of America A K Peters, Ltd 2005)

Blakeslee S, 'Monkey's Thoughts Propel Robot, a Step That May Help Humans' The New York Times

Blum T, Stauder R, Euler E and Navab N, 'Superman-like X-ray Vision: Towards Brain-Computer Interfaces for Medical Augmented Reality' (IEEE International Symposium on Mixed and Augmented Reality 2012 Science and Technology Proceedings, Atlanta, November 2012)

Calo R, 'Robots as Legal Metaphors' (2016) 30(1) Harward Journal of Law & Technology

Christoph B and Reinhard M, 'Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination [2014] 8 Crim Law and Philos

Constine J, ‘Faceook launches augmented reality Camera Effects developer platform’ Techcrunch

De Castro Lourenço B, ‘Human Computer Interaction Via Brainwaves For Disable People’ (MA thesis, University of Porto, 2013)

De Hert P and Gutwirth S, ‘Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power’ in Claes E, Duff A, Gutwirth S (eds.) *Privacy and the Criminal Law*, pp. 61–104 (Intersentia 2006)

Deino D, ‘Microsoft’s Mind-blowing HoloLens Needs Work, But Is No Google Glass’ HuffingtonPost

Finn RL, Friedewald M and Wright D, ‘Seven Types of Privacy’ in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet (eds), *European Data Protection: Coming of Age* (Springer 2013)

Fuchs H and Ackerman J, ‘Displays for Augmented Reality: Historical Remarks and Future’ in Ohta, Yuichi, Tamura, Hideyuki (eds), *Mixed Reality* (Springer-Verlag Berlin Heidelberg 1999)

Graimann B, Allison BZ, Pfurtscheller G, (ed), *Brain-Computer Interfaces: Revolutionizing Human-Computer Interaction* (Springer 2010)

Habermas J, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Thomas Burger and Frederick Lawrance tr, The MIT Press 1991)

Hirzer M, 'Marker Detection For Augmented Reality Applications' (2008) Technical Report ICG–TR–08/05

Hobson A, 'Reality Check: The Regulatory Landscape For Virtual And Augmented Reality' (2016) No.69 R Street Policy Study

Hurley W, “Augmented Reality: Getting Beyond the Hype” Bloomberg (3 November 2009)

Ienca M and Andorno R, ‘Towards new human rights in the age of neuroscience and neurotechnology’ (2017) 13(5) Life Sciences, Society and Policy

Kansaku K, Hata N and Takano K, ‘My thoughts through a robot’s eyes: An augmented reality-brain–machine interface’ (2010) 66 Neuroscience Research

Kirley EA, 'Reputational Privacy & The Internet: A Matter For Law?' (DPhil Thesis, Osgoode Hall Law School York University 2015)

Koops BJ, ‘On legal boundaries, technologies, and collapsing dimensions of privacy’ 3(2) Politica e Società

Koops BJ, Newell BC, Timan T, Škorvánek I, Chokrevski T, Galic M, 'A Typology of Privacy' [2017] 38(2) Univesity of Pennsylvania Journal of International Law

Krausova A, 'Legal Aspects of Brain-Computer Interfaces' (2014) 8 Masaryk UJL & Tech.

Lance BJ, Kerick SE, Ries AJ, Oie KS and McDowell K, ‘Brain–Computer Interface Technologies in the Coming Decades’ (2012) 100 (Special Centennial Issue) Proceedings of the IEEE

Lebecek K, Ruth K, Kohno T and Roesner F, 'Securing Augmented Reality Output' (IEEE Symposium on Security and Privacy, Oakland, 2017)

Martins A and Rincon P, ‘Paraplegic in robotic suit kicks off World Cup’ BBC News

Mattie D, Guglielmo T and Fondazione SL, ‘Ethical Issues in BCI Research and Systems for Motor Control’ in Jens Clausen and Neil Levy (eds), *Handbook of Neuroethics* (Springer, 2015)

Mehta A, '"Bring Your Own Glass": The Privacy Implications of Google Glass In the Workplace' (2014) 30(3) The John Marshall Journal of Information Technology & Privacy Law

Moore Jr B, *Privacy Studies in Social and Cultural History* (United Kingdom, Routledge, 1984)

Moro C, Štromberga Z, Raikos A, and Stirling A,'The effectiveness of virtual and augmented reality in health sciences and medical anatomy' (2017) doi:10.1002/ase.1696 American Association of Anatomists

Moxon KA, Markowitz RS, and Nicolelis MA, 'Real-time control of a robot arm using simultaneously recorded neurons in the motor corte' (1999) 2(7),Nat Neurosci

Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public, Law and Philosophy' (1998) 17: 559-596 Law and Philosophy

Oana Andreea Ştefan 'European Competition Soft Law in European Courts: A Matter of Hard Principles' (2008) 14(6) European Law Journal

Paszkiel S, 'Augmented Reality of Technological Environment in Correlation with Brain Computer Interfaces for Control Processes' in Szewczyk R, Zieliński C and Kaliczyńska M (eds), *Recent Advances in Automation, Robotics and Measuring Techniques. Advances in Intelligent Systems and Computing* (Springer 2014)

Pelley S, 'Harnessing The Power Of The Brain CBS News

Peppoloni L, Brizzi F, Ruffaldi E and Avizzano CA, 'Augmented reality-aided tele-presence system for robot manipulation in industrial manufacturing' (2015 Proceedings of the 21st ACM Symposium on Virtual Reality Software and Technology, Beijing, November 2015)

Ravi K and Palaniappan R, 'Leave-one-out Authentication of Persons Using 40 Hz EEG Oscillations' (EUROCON 2005 The International Conference on Computer as a Tool, Volume 2, Belgrade, Serbia and Montenegro, 21-24 November 2005)

Robolaw Project, 'Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics' (2014)

Roesner F, Denning T, Newell BC, Kahno T and Calo R, 'Augmented Reality: Hard Problems of Law and Policy' (ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, September 2014)

Schwartz PM and Peifer KN, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept' (2010) 98 Cal. L. Rev. 1925

Stadler S, Mirnig N, Giulani M, Tscheligi M, Materna Z and Kapinus K, 'Industrial Human-Robot Interaction: Creating Personas for Augmented Reality supported Robot Control and Teaching' (Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, Vienna 2017)

Toole O and Dolben D, 'Marker Detection and Tracking for Augmented Reality Applications' (2014)

Ullah Z, 'Early Computer VS Modern Computer: A Comparative Study and an Approach to Advance Computer' (2012) 12(1) Global Journal of Computer Science and Technology Interdisciplinary

Uno K, Naito G, Tobisa Y and Yasuhiko J, 'Basic Investigation of Brain–Computer Interface Combined with Augmented Reality and Development of an Improvement Method Using the Nontarget Object' (2015) 98(8) Electronics and Communications in Japan

Vidal JJ, 'Toward Direct Brain- Computer Communication' (1973) 2 Annual Reviews

Wagner DeCew J, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (United States of America: Cornell University Press, 1997)

Westin A, *Privacy and Freedom* (United States of America, Ig Publishing Incorporated, 2015)

Whitman JQ, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) Faculty Scholarship Series. Paper 649

Wolfe A, 'Public and Private in Theory and Practice: Some Implications of an Uncertain Boundary' in Krishan Kumar and Jeff Weintraub (eds), *Public and Private in Theory and Practice* (Morality and Society Series 1997)

Zheng H, 'The Brain-Machine Connection: Humans and Computers in the 21st Century' Yale Scientific (13 February 2011)