Gatt L, Caggiano IA, Gaeta MC, Mollo AA, 'BCI devices and their legal compliance: A prototype tool for its evaluation and measurement' (2022) 1 EJPLT, 301-314.
DOI : https://doi.org/10.57230/EJPLT221LGIACMCGAAM

EJPLT
ISSN 2704-8012

BCI devices and their legal compliance: A prototype tool for its evaluation and measurement

Lucilla Gatt
Full professor of Private Law
Università degli Studi Suor Orsola Benincasa

Ilaria Amelia Caggiano
Full professor of Private Law
Università degli Studi Suor Orsola Benincasa

Maria Cristina Gaeta
Lecturer in Private Law
Università degli Studi Suor Orsola Benincasa

Anna Anita Mollo
Postdoctoral Research Fellow in Private Law
Scuola Superiore Meridionale

Abstract

Starting from a critical analysis of the legal issues related to BCI applications, the paper aims to provide the explanation of a prototype of an evaluation and measurement tool for legal compliance of BCI products, in order to ensure the compliance by design of the BCI products with the current legislation and the protection of human rights. Therefore, the research work will briefly illustrate the main legal issues of interest and then the related parts of the tool prototype.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: BCI regulatory perspectives; security; privacy; cybersecurity.

1. Introduction and background of the research study.[1]

In medical and educational fields, in workplaces, as well as more generally, in interpersonal relationships, the Brain Computer Interface (BCI) had an ever wider and faster development thanks to the implementation of the AI system[2]. This occurred, for example, in the case of the neural interfaces that are able to monitor the stress conditions or other negative and positive human emotions, or the technologies used in the medical rehabilitation field (therapeutic BCI), also using wearable technologies. The neurotechnology used in verifying the level of involvement and understanding of the teaching contents by the learners, or those used by individuals to express their will in relationships between private individuals, are also very relevant.

The BCI can be very useful for assisting and protecting people in different environments, but an evaluation of BCI applications appears necessary to define the legal consequences of the individual's behaviours using BCI devices.

---

[1] The paper is the result of the work of a selected team of researchers of the Research Centre of European Private Law (ReCEPL) at Università degli Studi Suor Orsola Benincasa, coordinated by the ReCEPL Director Prof. Lucilla Gatt and the ReCEPL Vice-Director Prof. Ilaria A. Caggiano.
The work was presented at the IEEE International Conference 'Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering' (MetroXRAINE), National Research Council, Rome, October 26-28, 2022, and published in the IEEE MetroXRAINE 2022 Proceedings, 551-556; awarded as 'Best paper presented by a young researcher' from MetroXRAINE scientific committee, thanks to the support of Micron.
The author of paragraphs 1, 2, 3.1, and 3.3 is Dr. Maria Cristina Gaeta, ReCEPL Senior Researcher and Scientific Secretary, Lecturer in Private Law at Università degli Studi Suor Orsola Benincasa; the author of paragraphs 3.2. and 4 is Dr. Anna Anita Mollo, ReCEPL Senior Researcher and Postdoctoral Research Fellow at Scuola Superiore Meridionale.

[2] N Liv, 'Neurolaw: Brain-Computer Interfaces' (2021) 15 (1) U. St. Thomas J.L. & Pub. Pol'y, 328-355.

This evaluation will help to verify the risk for individuals interacting with these technologies, to guarantee consequent adequate protection.

Indeed, the considerable potential of BCI is evident but, at the same time, the rapid spread of these neural technologies requires the analysis of multiple issues that can arise from the application of BCI devices or their software, to verify and measure the risks that can arise from these new technologies, and guarantee the compliance by design of the BCI application under an anthropocentric point of view. In this regard, legals have the role to verify the functioning of BCI technologies and regulate them to protect human beings in the digital environment, alias artificial, since this environment places ontologically the former in a position of vulnerability. The category of "vulnerable individuals" includes, in fact, all natural persons, who, acting in a digital environment, are exposed to the risk of damages for various reasons (minor/old age, asymmetry of contractual power or information, patients with serious diseases). This vulnerability of individuals, strictly related to the development and application of new technologies can be defined as technological vulnerability.

2. Methodology of the research.

The research activities in the field of BCI have been carried out at the Research Centre of European Private Law - ReCEPL,[3] based at Università degli Studi Suor Orsola Benincasa (Italy).

In the perspective of uniform regulation, also considering the opportunities for its effective implementation in specific sectors, ReCEPL develops research itineraries on the relationship between law and new technologies, working in close collaboration with the Living Lab Utopia, of the Interdepartmental Research Center 'Scienza Nuova',[4] also based at Università degli Studi Suor Orsola Benincasa (Italy).

The equipment of the most modern technological instruments of the 'Scienza Nuova' Center, allows ReCEPL researchers to adopt innovative research and study methodologies (empirical studies, behavioral analyses), conducted jointly with researchers (engineering, psychologists, communication sciences, statisticians), that belong to 'Scienza Nuova' Research Center and are fundamental for the application of mixed methodologies applied for the design and implementation of the tool prototype.

More in detail, starting from a critical analysis of the state of the art (legislation, case law, literature and research studeis), the research team has identified, mapped, and evaluated the possible risks related to BCI applications and their legal regulation, to then create the tool prototype that aims to verify the compliance by design.

Furthermore, the research method adopted has been hybrid (hybridization of knowledge), using not only the traditional legal methods but also the

[3] For more details on the Research Centre of European Private Law see https://www.unisob.na.it/ateneo/c008.htm?vr=1&lg=en

[4] For more details about Scienza nuova see www.centroscienzanuova.it

human-machine-interface and user experience approach (HMI&UX), as well as empirical legal studies method (ELS). Indeed, to carry out an impact assessment, it is important to really understand how new technologies work. In this light, it has been essential to resort to the behavioural sciences, and technical science, starting with practical applications of BCI.

In the 21st century, the level of an in-depth study of the new technology law is so high and complex that legal must work in synergy with experts from other sectors of science (e.g. engineers, computer scientists, psychologists and philosophers). As a matter of fact, on one side, legal science needs technical science to understand technologies and provide specific regulations based on their functioning. On the other side, technical science needs the legal and social one for putting in place the principles of techno-regulation based on current law, first of all, hard law, but also soft law, which in this context plays a fundamental role of guidance and orientation, as well as technical regulation (e.g. standards).

3. Critical analysis of the legal issues related to BCI applications and presentation of the tool prototype.

To verify and measure the possible risks related to the use of BCI technologies the research team has realised a prototype tool on the legal assessment of BCI applications, that serves as an operational tool for manufacturers to enable them to assess the level of product safety and reliability before they are put on the market. As a matter of fact, all BCI applications must be structured according to the principle of legal compliance by design, submitting BCI applications to the evaluation tool in advance, before making them available to the public and, even earlier, during the production phase.

In this light the prototype of the evaluation and measurement tool has been divided into the following parts that correspond to the main risks for the individuals using BCI application: the first part on BCI safety; the second part on BCI privacy, third part on cybersecurity, representing the main types of risks associated with the use of BCI technologies.

Figure 1 – Scheme of the prototype of evaluation and measurement tool of BCI applications

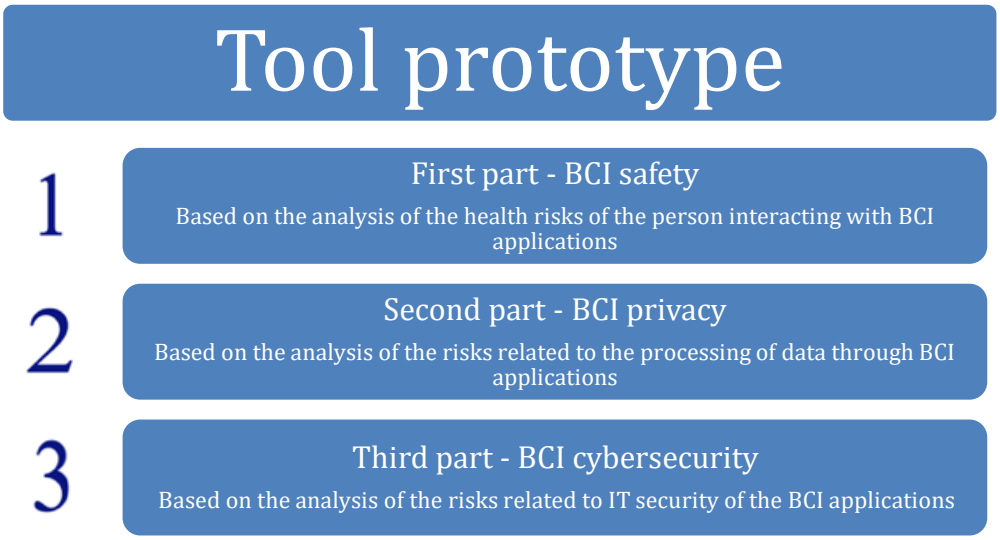

Figure 1 – Scheme of the prototype of evaluation and measurement tool of BCI applications

The paper critically analyses these risks explaining the choices made in identifying the matters of the prototype tool, that consists in an interactive questionnaire made by digital software, whose results are visible in real-time at the end of the questionnaire.

3.1. First part of the tool prototype: Liability rules and BCI, with particular regard to user's safety.

From a legal perspective, the possibility of damage (mainly of a non-pecuniary nature) for the user interacting with BCI technologies or other human beings who interact with the user using BCI, is high. Among the possible risks associated with the use of BCI, there is a high possibility of injury to the user's safety, who could suffer physical or psychological injury related to the incorrect use of neural technologies.[5] At the same time, it is also possible that damages to surrounding objects are caused. In these cases, it is foreseeable also a pecuniary damage.

Under the perspective of private law, the configurable typologies of civil liability are the following: civil liability for non-pecuniary damage and civil liability for pecuniary damage. Artt. 2043 and ff. of the Italian Civil Code, regulate the civil liability for pecuniary damage. These legal provisions also include art. 2059 of the Italian Civil Code, that governs the case of non-pecuniary civil liability, which can be compensated only in cases determined by law.

When the relationship is between the producer of the BCI application and the user (the physical person who uses these technologies) the applicable regulation is that of the Consumer Code (Italian Legislative Decree 6

[5] Q Li, D Ding, M Conti, 'Brain-Computer Interface applications: Security and privacy challenges' (2015) IEEE Conference on Communications and Network Security (CNS), 663-666.

September 2005, no. 206), which currently implement in Italy the European Directive 85/374 /EEC on liability for damage from defective products (so-called Product Liability Directive, acronym PLD), after the repealing of the previous national regulation (d.P.R. n. 224/1988).

Article 114 cons. Code (art. 1 PLD) establishes that the manufacturer is responsible for the damage caused by defects in his product, while art. 115 cons. Code (art. 2 PLD) states that by product we mean any movable property, even if incorporated into another movable or immovable property and that electricity is also a product. It is therefore evident that BCI applications can fall within the notion of product, for which the producer is responsible, in relation to the consumer. The manufacturer is the physical person or legal person who designs and manufactures BCI technologies, as well as who informs about the permitted uses of such applications (art. 2, para bis, cons. Code, in compliance with art. 3 PLD).

Unlike the general discipline of the civil code, the consumer code, as well as the PLD, provides for the strict liability of the producer.[6] This is a type of liability for which the producer is liable if the consumer proves the damage, the product defect and the causal link between defect and damage. The product is defined as defective when it does not offer the security that can be expected considering all the circumstances and in particular those indicated in art. 117 cons. Code (art. 6 PLD). To mitigate the producer's strict liability there are the causes of exclusion of liability referred to in art. 118 cons code (art. 7 PLD), but these are mandatory hypotheses subjected to the burden of proof by the manufacturer.

It is therefore evident that the producer's strict liability is directly related to the safety of the product and provides for compensation for damage under favorable conditions for the consumer, compared to the ordinary discipline of civil liability, in consideration of the weak position of the consumer. In order to avoid the producer liability, it is important to carry out an *ex ante* verification of product safety, before putting it on the market.

For this reason, the first part of the tool is focused on BCI safety. More specifically, in the section 1.1. are analysed the possible physical or psychological injury for the individuals who use BCI application (e.g. individuals who use the BCI because they have disabilities that can be overcome using BCI technologies, as well as individuals who undergo some tests such as those to check the level of knowledge and understanding or monitor the stress conditions or other negative and positive human emotions). In the section 1.2. are analysed the possible injuries caused to another human being and surrounding environment that interacts with individuals using BCI applications (e.g. relationships with a people whose cognitive and movement abilities are supported by BCI devices with particular regard to the consequences of their action).

[6] C Bublitza, A Wolkensteinb, RJ Joxc, O a Friedrichd, 'Legal liabilities of BCI-users: Responsibility gaps at the intersection of mind and machine?' (2019) 65 International Journal of Law and Psychiatry, 101-399.

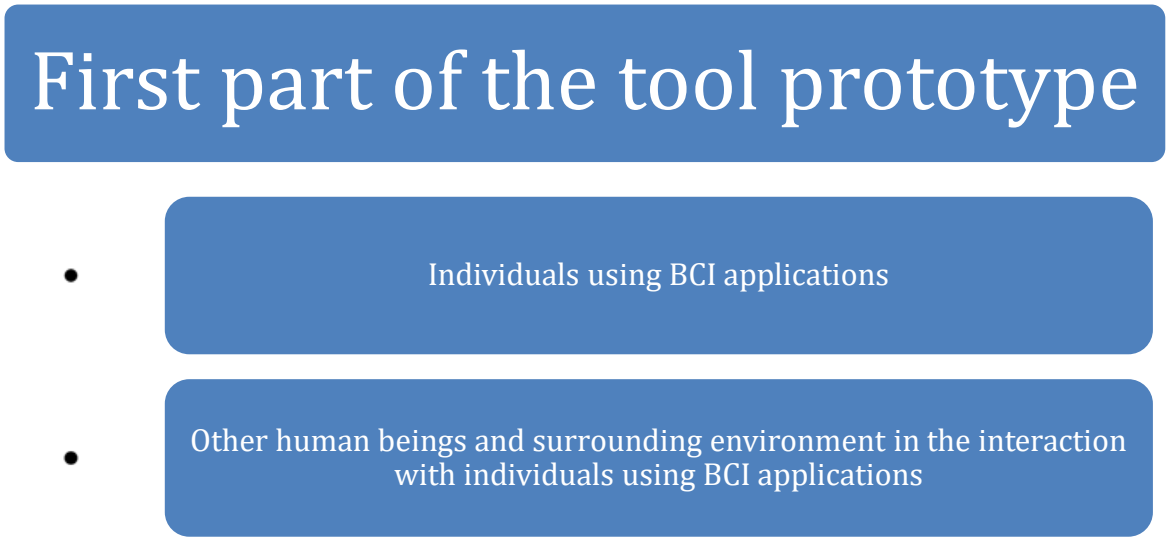

Figure 2 – Scheme of the first part of the prototype tool for the evaluation and measurement of BCI applications

In the context of the physical or psychological injury of the individuals, two possible specific risks are outlined: the first concerns the unlawful processing of personal data through brain computer interface technologies, and mainly concerns non-pecuniary damages, while the second concerns the cybersecurity breach of brain computer technologies, which can result in both pecuniary and non-pecuniary damages.

3.2. Second part of the tool prototype: the processing of neural and mental data.

A central point in the analysis of the risks that BCI systems may cause relates to the exact identification of the type of data they are able to detect by recording and decoding the user's brain activity.

In this regard, it is necessary to make a brief premise on the functioning of BCI interfaces, which is articulated in four phases: after the generation of an initial input (first phase), i.e. a brain activity by the user in response to a stimulus, this is first recorded and then decoded by the interface (second phase); in this way, the initial input is transformed by the interface into an output (third phase), i.e. in the execution of a precise function that the individual will be able to perform autonomously thanks to the BCI device (fourth phase. In the clinical field, thinks of the control of a robotic limb or of

an electronic wheelchair; expression of one's will in full autonomy thanks to the help of the interface).[7]

In this process, the third phase appears central as the data measured in the previous phase are classified and selected in order to identify the most appropriate output for the proper functioning of the BCI interface.

Such data can be distinguished into neural data and mental data. Neural data or "human brain data"[8] pertain to the structure and functioning of the brain and can reveal information on the clinical condition and, therefore, on a person's health - think of BCI used in clinical fields- understood in a broad sense, i.e. also including a condition of well-being and not pathological.

Mental data, on the other hand, are additional and distinct data from neural data, pertaining to the more intimate sphere of the subject. This category therefore includes any data that can be organized and processed to infer a person's mental states[9], including their cognitive and affective states such as inner speech,[10] memories,[11] emotions[12] and intentions.[13]

In neural interfaces, mental data are derived from the analysis of neural data by means of the so-called 'reverse inference' procedure,[14] which does not show the semantic content of a thought or memory but allows a correspondence to be established between the neural correlates of a certain brain activity and information about certain mental states.

For the purposes here, the distinction between neural data and mental data appears necessary in order to identify the legal nature of the data that BCI devices are able to detect in function of an analysis that extends to the privacy protection profile also in relation to the domain of the mind.

Neural data, referring to the functioning and structure of the brain, make it possible to identify the subject they refer to, suggesting, therefore, a first legal

---

[7] U Chaudhary, I Vlachos, JB Zimmermann, et al., 'Spelling interface using intracortical signals in a completely locked-in patient enabled via auditory neurofeedback training' (2022) 13 (1236) Nature Communications, 1-9.

[8] M Ienca, Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields, (SPDP, Council of Europe, 2021).

[9] M Ienca, G Malgieri, 'Mental data protection and the GDPR' (2022) 9 Journal of Law and the Biosciences, 1-19.

[10] DA Moses, M.K. Leonard, JG Makin, EF Chang, 'Real-time decoding of question-and-answer speech dialogue using human cortical activity' (2019) 10 (3096) Nature Communications, 1-14.

[11] J Chen, YC Leong, CJ Honey, CH Yong, KA Norman, U Hasson U, 'Shared memories reveal shared structure in neural activity across individuals' (2017) 20 Nature neuroscience, 115-125.

[12] A Tambini, U Rimmele, EA Phelp, L Davachi, 'Emotional brain states carry over and enhance future memory formation' (2017) 20 Nature Neuroscience, 271-278.

[13] M Bles, JD Haynes, 'Detecting concealed information using brain-imaging technology' (2008) 14 Neurocase, 82-92.

[14] RA Poldrack, 'Inferring mental states from neuroimaging data: from reverse inference to large-scale decoding' (2011) 72 Neuron, 692-697.

qualification of the same as personal data within the meaning of Article 4(1) of the GDPR.[15]

However, as such, neural data are also an expression of a clinical condition of the data subject, the latter not necessarily understood as a condition of a pathological nature but also expressive of a situation of physical and mental well-being.[16]

Therefore, neural data are not merely personal identification data but 'health-related data' within the meaning of Article 4(15) GDPR. From this it follows that the legal basis of the processing is to be found in Art. 9 GDPR for that 'special category of personal data' for which there is enhanced protection, which takes the form of the 'explicit consent' of the data subject.

The qualification in terms of personal data, on the other hand, is not peaceful in relation to mental data. The latter, in fact, if linked to other data allowing the certain identification of the data subject (as in the case of neural data), may qualify as personal data (neural interfaces used in the clinical field).

In this first case, the close link between the neural data and the mental data suggests a qualification of the latter as personal data, since the joint reading with the neural data is capable of allowing the identification of the data subject.

The doubt as to the qualification of mental data arises with greater force in hypotheses in which it is acquired outside the clinical sphere, as in the case of consumer neurotechnologies, which could detect mental data even though they do not directly access the functioning of the brain understood as a biological complex. In this second case, a valid normative reference seems to be found in Article 4(1) GDPR, which also considers as suitable for identifying the subject 'one or more elements characteristic of his or her psychic identity', although the same provision does not clarify what is meant by psychic identity. Therefore, only by way of interpretation can mental data be qualified as personal data at present, i.e. where it is possible to consider that an emotion or a memory is data that can unambiguously identify a subject, even without referring to his or her neural data.

As to the possible legal basis for processing mental data where these are not read in conjunction with neural data, as in the case of consumer neurotechnologies, it must be noted that in this case mental data cannot be qualified as health data since they cannot by themselves show the state of health (albeit physiological and not pathological) of the person concerned.

There would therefore remain the possibility of access to the greater protection of Article 9 GDPR only where the mental data are also capable of revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs or sexual orientation of the person with a disability.

---

[15] S Raiuney, K McGillivray, S Akintoye, T Fothergrill, C Bublitz, B Stahl, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?' (2021) 7, Journal of Law and Biosciences, 1-19.

[16] G Malgieri, G Comandé, 'Sensitive-by-Distance: Quasi-Health Data in the Algorithmic Era' (2017) Inf. Commun. Technol. Law, 229-249.

This case, i.e. mental data that is not linked to neural data and, therefore, qualifies as health data, is not envisaged in our GDPR, which is characterised by an obvious lacuna in that it does not define. In this regard, some authors believe that the lacuna is due to the failure to include in the regulatory provision of Article 9 GDPR data relating to thoughts, emotions and other mental states that are not connected with or cannot be attributed to health or other areas covered by the provision.[17] According to a different approach, on the other hand, it is necessary to start from the consideration that the special data referred to in Article 9 GDPR are such in light of the purpose of the processing; therefore, it is considered that if the purpose of the processing of mental data initially declared is not related to health, or to other purposes contemplated by the norm, the same cannot be considered sensitive data.[18]

In any case, the element that emerges is that the legal basis of the processing can currently only be found in Article 6 GDPR, which indicates in which cases non sensitive data can be the subject of lawful processing if certain conditions indicated by the norm (consent, performance of a contract, compliance with a legal obligation, protect the vital interests of the data subject or of another natural person, public interest, legitimate interests pursued by the controller or by a third party) are met.

In conclusion, the considerable implications in the protection of mental privacy[19] call for adequate ethical and legal reflection aimed at assessing the concrete functioning of such devices. This would seem to be possible on the basis of an evaluation questionnaire intended to measure not only the security and reliability of current BCI devices, but also the level of risk awareness on the part of the user.

[17] M Ienca, G Malgieri, 'Mental data protection and the GDPR' (2022) 9 Journal of Law and the Biosciences, 1-19.

[18] S Raiuney, K. McGillivray, S Akintoye, T Fothergrill, C Bublitz, B Stahl, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?' (2021) 7 Journal of Law and Biosciences,1-19

[19] M Ienca, 'Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields', 1-82.

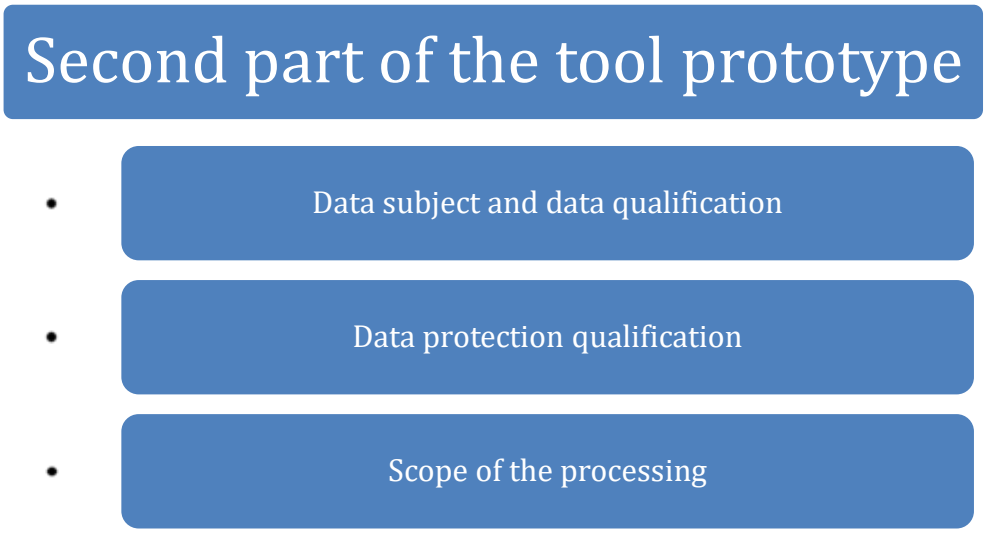

Figure 3 – Scheme of the second part of the prototype tool for the evaluation and measurement of BCI applications.

In this regard, the second part of the prototype of the evaluation tool will focus on privacy issues in relation to BCI applications. This should comprise an overview of all planned data collection and processing operations in order to develop secure data management practices and share and process data in compliance with GDPR and best security standards

Particular attention will be paid to understand if BCI system assuring effective transparency in information through suitable forms and devices; and on the verification of the level of user awareness of the possible risks of BCI systems.

In particular, the second part of the questionnaire is divided into three sections. Section 2.1. on data qualification is focused on: data subjects (vulnerable people, people who have not given their explicit consent etc.) and types of data for the legal qualification of the data processed by BCI applications, to understand whether or not data related to brain activity - neural data and mental data – are qualified as personal data.

Section 2.2. is based on data protection qualification, also trougth the application of the principles of data protection by design and by default. In this part of the questionnaire, the processing techniques of neural and mental data is identified. In this section the focus is on; identification of the type of IT tool used in the processing; any automated decision-making processes; the pseudonymization or anonymization of personal data; data minimization.

Finally, in section 2.3. is deepened the scope of the processing. The questions are structured so as to understand the purpose of the processing of the data recorded by BCI's applications in order to: identify the correct legal basis for the processing; assess whether the processing is lawful or not.

3.3. Third part of the tool prototype: BCI technologies and cybersecurity profiles.

In relation to BCI application is also very relevant to analyse the possible injuries that could result to the user in the case of a violation of the IT security of BCI technologies.[20] This case can occur for the malfunctioning of IT security systems (section 3.1.) or for the hacking of the IT security systems (section 3.2.),[21] resulting in consequent physical or psychological damage to the user, including the unlawful processing of the personal data stored or transferred for software to another software (interoperability).

Currently, there is no unitary and complete regulation on IT security but the EU Directive 2016/1148 (Directive on the Security of network and information systems, acronym NIS, implemented in Italy with the Italian Legislative Decree of May 18, 2018, n. 65), was an important landing place. The regulation aims at improving national cybersecurity capabilities and provides for cooperation at the EU level. It also envisaged the establishment of the Cyber Security Incident Response Teams (CSIRT), to deal with incidents and risks, as well as the NIS Toolkit which provides practical information to member states. Furthermore, a culture of safety and risk management in all sectors which are vital to the economy and society has been straightened. Sectors that strongly depends on Information and communication technologies (ICT) include the healthcare, digital infrastructure and cloud computing sector.

Furthermore, among the regulation recently adopted for cybersecurity, the Cybersecurity Act (Reg. 2019/881/EU) is of fundamental importance. Indeed, the Regulation aimed at creating a European framework for the certification of the cybersecurity of ICT products and digital services, and at strengthening the role of the European Union Agency for the Cybersecurity (ENISA). At the national level, in 2019, the competent NIS Authorities in the Ministries have developed the national Guidelines for risk management and accident prevention and mitigation, which have a significant impact on the continuity and provision of essential services.

Therefore, the European and national attention on cybersecurity is evident, considering the increasing possibility of risks for individuals. This is why the tool also takes into consideration aspects concerning IT Security also in the light to provide a cybersecurity certification. In this regard, the third part of the tool prototype is focused on cybersecurity and is divided into a section 3.1. on malfunctioning of IT security systems and a section 3.2. on the hacking of the IT security system.

---

[20] Ajrawi, R Rao, M Sarkar, 'Cybersecurity in Brain-Computer Interfaces: RFID-based design-theoretical framework' (2021) 22 Informatics in Medicine Unlocked, 1 - 9.

[21] S López Bernal, A Huertas Celdrá, G Martínez Pérez, M Taynnan Barros, S Balasubramaniam, 'Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges' (2020) J. ACM, 1-35.

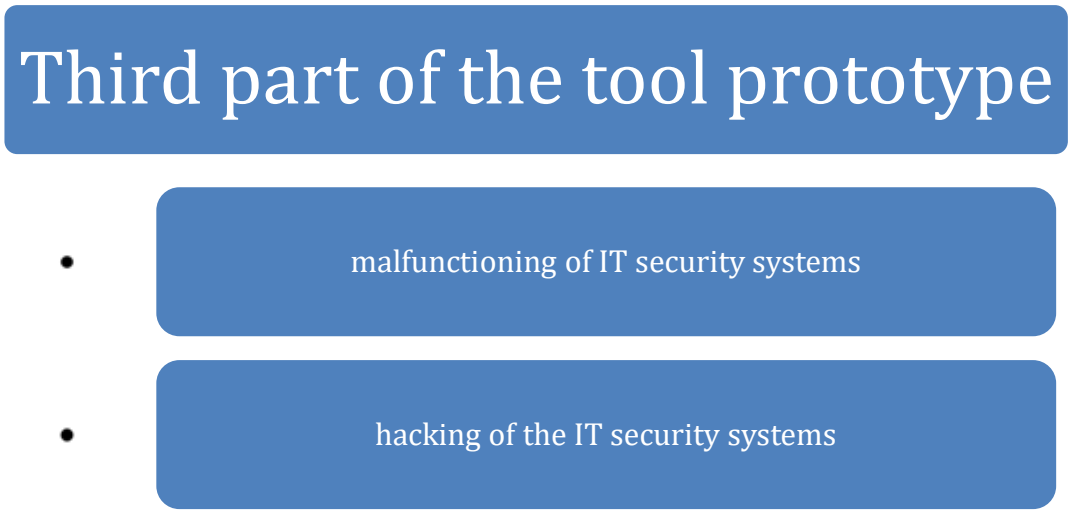

Figure 4 – Scheme of the third part of the prototype tool for the evaluation and measurement of BCI applications

4. Conclusion and future work.

The current legal framework does not provide for specific regulation of neurotechnology in relation to the distinct profiles mentioned above: security, privacy and cybersecurity.

It is clear that the preventive legal analysis of BCI devices and related risks is necessary in order to avoid situations of 'technological vulnerability' against which the legal system is unable to guarantee adequate protection for the individuals.

The creation of the tool prototype described in the paper appears, therefore, to be an innovative but necessary approach to the proper techno-regulation in order to guarantee the legal compliance of BCI products.

The production of BCI devices that is genuinely human-centred will be possible only if technical evaluations are flanked by legal ones, which must be founded on an analysis method that does not stop at theoretical reflection but opens up to a phase of integrated juridical thought in bioengineering testing, in which the design of prototypes, products, or services is inspired by a set of minimum standards (legal and ethical), so that major tech companies bring to market products according to the existing regulatory framework.

The aim is to prevent a possible 'abuse of technology' to the detriment of the progress and the benefits it can bring to vulnerable people.

Therefore, a new approach is needed to be able to offer the most appropriate protection for all interests involved: the protection of vulnerable people, especially in the clinical field, by stimulating clinical research with BCI devices for the diagnosis and treatment of severe neurodegenerative diseases, thus improving the quality of life of the patients involved; maximising the level of reliability of BCI systems, making them safe and increasing the level of confidence of users (including consumers); supporting manufacturers by providing them with precise ethical and legal standards to make products compliant with both binding European and international legislation on the protection of human rights and vulnerable consumers, and with the most appropriate soft law instruments.

All this requires a highly interdisciplinary work, in which the skills of experts from various fields of knowledge dialogue together in order to achieve the same goal: the psychophysical integrity of the human person even in the technological context.