


**Mind over matter:
Examining the implications of machine brain interfaces
on privacy and data protection under the GDPR.**

SABIRE SANEM YILMAZ 

LLB, LLM

Maltepe University Technology and Intellectual Property Law
Research Centre

HABIBE DENIZ SEVAL 

Ph.D. (c) University of Ottawa, Centre for Law, Technology and
Society

Abstract

Machine-brain interfaces (MBI) affect General Data Protection Regulation (GDPR), users' privacy and data protection. MBIs can transform industries and improve lives by directly connecting human brains to computers. However, these advances raise worries about personal data misuse and abuse and the need for robust regulatory frameworks to protect privacy and data. The article examines the relationship between privacy and MBIs in the context of the GDPR and closely examines surveillance risks posed by MBIs. The article also considers MBIs' ethicality and privacy as a human right. Thus, this essay examines the GDPR's current condition considering the the Brussels Effect and sustainability.



Keywords: Machine-Brain Interfaces, Privacy, Data Protection.

Summary: [Introduction.](#) – [1.1. Definition of Machine Brain Interfaces.](#) – [1.2. Overview of Privacy Rights and Data Protection.](#) – [2. Impact of MBIs on privacy rights.](#) – [2.1. Impact of MBIs on Data Protection.](#) – [2.2. Surveillance and MBIs.](#) – [3. Risks MBIs towards the right to privacy as a fundamental right.](#) – [3.1. Risks and Democracy Paradox.](#) – [3.2. Can MBIs be Ethical?](#) – [4. Brussels effect and MBIs](#) – [4.1. Outsourcing or Crowdsourcing.](#) – [4.2. Sustainability, Brussels Effect and MBIs.](#) – [Conclusion and Recommendations.](#)

Introduction.

This article will explore the implications of MBIs on data protection and privacy laws. MBIs allow for direct communication between the human brain and machines and have the potential to revolutionize many aspects of our lives. However, the development and use of MBIs also raise important questions about privacy and data protection, particularly in the context of the GDPR¹, which imposes strict rules on processing personal data.

We will begin briefly explaining what MBIs, stating that they enable direct brain-machine communication. MBI users can control and communicate via channels other than the brain's muscles and peripheral nerves. We will then delve into the impact of MBIs on data protection and privacy, including the potential for surveillance. Next, we will discuss the ethical aspects of MBIs and the Brussels effect, which refers to the phenomenon in which the regulations and standards established by the EU have a global impact. Finally, we will conclude our findings and recommendations for the responsible development and use of MBIs.

MBIs generate a large amount of data that can be used to infer sensitive information about an individual's thoughts, emotions, and behaviours. The GDPR imposes strict rules on the processing of personal data, including data generated by MBIs. Hence, this raises important questions about how companies developing and using MBIs can ensure compliance with the GDPR and protect the privacy rights of their users. For instance, one of the significant challenges regarding MBIs is the issue of legal consent. Under the GDPR, companies must obtain the explicit consent of individuals before processing their personal data. Therefore, one potential solution to this would be the implementation of robust consent mechanisms. By requiring users to consent to the collection and processing of their data actively, companies can ensure that individuals are fully aware of how their data will be used and can opt out if they do not wish to share their data. In addition to obtaining explicit consent, companies should also consider implementing other privacy-enhancing measures, such as pseudonymization and

¹ EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

encryption, to protect the security and confidentiality of MBI data. These measures can help to reduce the risk of unauthorized access to or misuse of sensitive personal data.

Besides data protection and privacy, ethical concerns need to be addressed. MBIs can be used to determine a person's willingness to accept abuse and hazardous content by acting as a warning. Also, one of the main points that will also be discussed in this article is the phenomenon of the Brussels Effect. It is a term used to explain the global impact of regulations and standards established by the EU, influencing the laws and practices of other countries worldwide. In the context of MBIs, the Brussels effect could have significant implications for how these technologies are developed and used, both within the EU and globally. By examining the legal framework governing MBIs, the types of data that may be collected through these interfaces, and the potential impacts of MBIs on the broader society, we can better understand the complex issues surrounding the development and use of MBIs and identify best practices for protecting users' privacy and data protection rights. Overall, the Brussels effect highlights the importance of considering the potential global impact of new technologies and the need for the responsible and ethical development and use of MBIs. In this article, through our analysis, we aim to understand better the complex issues surrounding the development and use of MBIs in the EU and identify best practices for protecting users' privacy and data protection rights.

1.1. Definition of Machine Brain Interfaces.

In 1973, researchers described a series of experiments meant to demonstrate that direct brain-computer communication is possible.² By using electrodes placed on the surface of the head or surgically implanted within the brain, these devices can detect and process brain signals, providing the user with a new way to interact with the world around them.

The MBIs are a type of technology that allows machines to communicate directly with the human brain.³ These interfaces have the potential to revolutionize many aspects of our lives, including healthcare, education, and entertainment. Users of MBIs can control and communication channels independent of the brain's usual output channels of muscles and peripheral nerves.⁴ By allowing direct communication between the brain and machines, MBIs could facilitate the development of new treatments for brain disorders, enhance learning and memory, and create immersive virtual reality experiences. However, the development and use of MBIs also raise important questions about privacy and data protection. However, there are still many challenges that need to be

²JJ Vidal, 'Toward Direct Brain-Computer Communication' (1973) 2 Annu. Rev. of Biophys and Bioen., pp. 157.

³T Bonaci, R Calo and HJ Chizeck, 'App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces', 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering.

⁴O Landau, R Puzis and N Nissim, 'Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space' (2021) 53 ACM Computing Surveys, pp. 1.

addressed before these technologies can be widely adopted. One major challenge is the need to improve the accuracy and reliability of MBIs.

1.2. Overview of Privacy Rights and Data Protection.

As a fundamental human right, the right to privacy is protected by various national and international laws and, therefore, an essential aspect of human life and they protect an individual's privacy. These rights are outlined in national and international laws and are intended to safeguard individuals from unreasonable intrusions into their personal lives. Furthermore, the right to privacy is undoubtedly an essential part of the modern legal system and serves as a fundamental check on government power and a source of protection for individuals. There are several essential theories on privacy to better understand, interpret it and how to embed in laws. For instance, Warren and Brandeis asserted that individuals have a right to be left alone and free from unwanted intrusions into their personal lives.⁵ According to them, privacy is a fundamental human right.⁶ On the other hand, the informational privacy theory proposed by Westin states that privacy is the ability of an individual to control the collection, use, and dissemination of their personal information.⁷ Privacy and data protection are closely related, as protecting personal data is often an important way to protect privacy. Data protection ensures that only authorized parties can access personal information, protecting an individual's privacy. The GDPR, an EU law on data protection and privacy for EU and EEA citizens, is one of the most important privacy laws. It addresses personal data exports outside the EU and EEA. It aspires to return personal data control to individuals and simplify international business regulation by harmonizing EU regulation.

2. Impact of MBIs on privacy rights.

Privacy, ethical, and human rights problems are all brought up by the close ties between individuals' data and various MBI applications. As a result, it comes as no surprise that current data protection rules are being applied in the context of MBIs, and that these laws are being amended to address specific challenges. In the case of MBIs and privacy, different perspectives must be considered. For instance, it appears necessary to distinguish between neural data and mental data to determine the extent of privacy protection in the domain of the mind.⁸ Neural data refers to the raw data collected from the brain, such as electrical activity or neural firing patterns, through various technologies like EEG, fMRI, or other neuroimaging tools. In its raw form, this data does not necessarily reveal specific

⁵SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 Harv. L. Rev., pp. 193.

⁶ibid.

⁷ A Westin, *Privacy and Freedom* (1967, New York: Atheneum).

⁸ L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance: A Prototype Tool for Its Evaluation and Measurement' (2022) 1 EJPLT, 301-314.

thoughts, emotions, or mental experiences, but it can be analyzed to infer information about a person's mental state potentially. On the other hand, mental data refers to the actual content of a person's thoughts, emotions, memories, or subjective experiences. Therefore, this data is considered more intimate and private, as it directly relates to an individual's identity, beliefs, and personal experiences. Therefore, when deciding the scope of privacy of the mind, it is essential to distinguish between neural and mental data. Since mental data may reveal more private details about a person's life than neural data, for instance, they require different sensitivity levels. Although there have been considerable breakthroughs in neuroimaging and MBIs, there is still room for improvement in humans' abilities to decipher mental content effectively and reliably from neural data. The necessity to safeguard mental data may grow as our knowledge and technology advance. Another of the potential challenges of MBIs is that they may generate a large amount of data that could be used to infer sensitive information about an individual's thoughts, emotions, and behaviors. This raises important questions about privacy and data protection, particularly in the context of the GDPR, which imposes strict rules on the processing of personal data. To ensure compliance with the GDPR, it will be important for companies developing and using MBIs to carefully consider the types of data that may be collected through these interfaces, and to implement appropriate safeguards to protect the privacy of their users. Another potential issue with MBIs is the potential for discrimination and ethical risks that has posed by this technology. While MBIs have the potential to revolutionize healthcare, education, and entertainment, there are ethical risks such as certain groups being left behind or disadvantaged if they are unable to access or afford these technologies. It will be important for policymakers and industry leaders to consider the potential impact of MBIs on the broader society and to develop strategies to ensure that the benefits of this technology are distributed fairly and equitably.

Overall, addressing the privacy and data protection challenges posed by MBIs will require a multi-faceted approach that involves both industry self-regulation and government oversight. By taking a proactive and collaborative approach, it is possible to ensure that the development and use of MBIs is responsible and ethical, and that the potential benefits of this technology are realized for all members of society.

2.1. Impact of MBIs on Data Protection.

As mentioned earlier, MBIs are a type of artificial intelligence (AI) system designed to mimic human brains' abilities, allowing computers and machines to think and reason as humans do. This technology has immense potential applications in data protection and security, as it can be used to identify patterns quickly and accurately in large amounts of data quickly and accurately. Therefore, one of the main concerns with MBIs is the potential for the devices to collect and transmit large amounts of sensitive personal information. For example, MBIs may be able to collect data on an individual's thoughts, emotions, and even memories.

This data could be used for various purposes, such as targeted advertising or medical research. At this point, data protection is an important issue as more MBIs become more common. However, with so much information stored digitally, there is always a risk that someone could gain access to personal data without consent. Therefore, organisations must have effective data protection systems in place to protect personal data and the right to privacy in specific to use cases of MBIs.

2.2. Surveillance and MBIs.

*'Nothing was your own except the few cubic centimeters inside your skull.'*⁹

One potential impact of MBIs on surveillance is that it could make it possible for governments and other organizations to monitor people's thoughts and emotions without their knowledge or consent. For instance, this could be done by placing sensors in people's homes or workplaces or using non-invasive techniques such as functional magnetic resonance imaging to read brain activity from a distance. Hence, this would allow organizations to gather vast information about individuals, including their personal beliefs, opinions, and emotional states, which could be used for various purposes, such as targeted advertising or political manipulation. It is important to refer to the fact that, if others, including the state, expose an individual to dangers that the individual has no way of knowing are present, this is unfair and will violate the individual's autonomy.¹⁰ Furthermore, MBIs can be used to create mind-reading devices that could be used by law enforcement and intelligence agencies to extract information from suspects or to monitor the activities of individuals deemed to be a threat to national security. This could be done by attaching sensors to a person's head to read their brain activity and extract information about their thoughts, memories, and intentions. Essentially, George Orwell's portrayal of a totalitarian government's constant surveillance in his novel 1984, where Big Brother watches every move of its citizens, with the goal of total control and manipulation, will be a possible scenario in this regard.¹¹ Another potential risk is hackers' ability to access MBI-enabled devices and steal sensitive personal information. As MBI devices become more prevalent, hackers will likely develop methods to access them, enabling them to steal personal information such as financial data, medical records, and other sensitive information. Moreover, MBI technology could also be used for commercial purposes, such as targeted advertising. Companies could use MBI technology to gather information about people's emotional states, preferences and interests and use that information to target them with advertising.¹² This breach of privacy allows companies to access personal thoughts and emotions, which can also be considered a violation of 'decisional privacy'.¹³

⁹G Orwell and E Fromm, 1984 (Signet Classics 2017).

¹⁰L Austin, 'Privacy and the Question of Technology' (2003) 22 Law & Philosophy, pp. 119.

¹¹Orwell and Fromm, 1984 (n 9).

¹²RJ Neuwirth, The EU Artificial Intelligence Act: Regulating Subliminal AI Systems (1st edn, Routledge 2022).

¹³L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance' (n 8), pp. 308.

On the other hand, MBI technology could also positively impact privacy by allowing people to control technology with their thoughts rather than using physical interfaces such as keyboards or touchscreens. This would make it possible for people to use devices and access information without anyone knowing.

It is important to assess the effectiveness of GDPR in protecting citizens from surveillance risks posed by MBIs. This will help ensure that personal data is collected and used responsibly and lawfully. The GDPR can be effective in addressing privacy risks associated with the use of MBIs in several ways. Firstly, the GDPR requires organizations to be transparent about their data collection and processing activities.¹⁴ This means that organizations would have to inform individuals about the collection and use of their brain data and obtain their explicit consent before collecting and processing it. Secondly, due to the principle of data minimization by the GDPR, organizations can collect and process only the data necessary for a specific purpose.¹⁵ This could be applied to MBI data by limiting the type and amount of data collected and ensuring that it is only used for specific, legitimate purposes. Thirdly, the GDPR requires organizations to implement data protection measures from the design stage of a product or service.¹⁶ This means that organizations would have to ensure that MBIs are designed with privacy in mind and include appropriate security measures to protect brain data from unauthorized access or processing. However, in this regard, the ambiguity regarding the concept of privacy by design will likely cause uncertainties and problems.

In summary, the GDPR seems like it is providing a comprehensive framework that can be applied to the use of MBIs to ensure that data is collected and processed lawfully. However, are there any flip sides of the GDPR when it comes to surveillance risks posed by the MBIs? The first weakness arises due to the GDPR's vagueness regarding non-invasive techniques. The GDPR applies to collecting and processing personal data through various means, including non-invasive procedures such as functional magnetic resonance imaging. However, neither the GDPR nor any guidelines do not address using these techniques for surveillance or gathering information about people's thoughts, emotions, and intentions without their knowledge or consent. Secondly, although MBIs use cases are widespread, there is no specific guidance on how to protect data collected through MBIs and ensure that it is only used for specific, legitimate purposes. Thirdly, while GDPR provides individuals with certain rights about their data, these rights may be limited when it comes to MBIs. For example, the right to access and delete brain data may be more difficult to exercise and may need to be more effective in protecting privacy.

MBIs collect sensitive personal data, making data protection difficult. Unfortunately, current laws like the GDPR are based on traditional privacy concepts that don't always reflect new technologies, making them insufficient for

¹⁴The GDPR (n 1).

¹⁵ Ibid.

¹⁶ Ibid.

user protection. Future-proofing privacy regulations ensures adequate protection regardless of technology. Since the GDPR was implemented in 2018, MBI technology has advanced rapidly. Thus, MBIs may not be fully addressed. For instance, neuro-marketing uses brain-computer interfaces to monitor and analyze consumers' brain activity to improve marketing strategies. GDPR restricts commercial data collection. It may not fully address neuro-ethical marketing's issues, such as consumer manipulation and lack of informed consent.

3. Risks MBIs towards the right to privacy as a fundamental right.

3.1. Risks and Democracy Paradox.

Due to their nature, MBIs constantly expose them to violating the right to privacy, which is a fundamental right. These technologies, which should be ethically audited, also act as a reminder about human rights and privacy impact assessments. Because the algorithm's unique design and MBI customization are fundamental rights issues. Ownership and exclusivity of the algorithm safeguard the end user from manipulative MBIs that could undermine her freedom of expression or personality.¹⁷ Violating the right to privacy as a fundamental right disrupts the structure of the democratic environment in the long run. For instance, reading and deciphering thoughts outside of clinical studies on analysing neuro data is unlawful processing of personal data. Hence, protecting the right to privacy in the design and innovation phases of MBIs is possible by complying with the GDPR per the principle of interoperability. Therefore, it is important to address the risk and challenges under fundamental rights and Democracy in protecting the right to privacy.¹⁸

Today, democracy requires privacy protection. GDPR's data minimisation, pseudonymisation, limitation of purpose, anonymisation, and data protection safeguard data subjects' democratic rights. MBIs' effects on democracy and self-determination cannot be disregarded. However, depending on how Democracy is perceived in the country in which MBIs are used, pluralism, democratic participation, transparency, and accountability are not yet fully validated. Hence, these technologies directly target Democracy. For example, the concern arising from using MBIS technology will be the direction of choices and manipulating groups of people who develop uniform thinking. Will their past cognitive abilities reinstate the MBI's-winning cognitive skills? However, it is even more alarming when it comes to the fact that different human brains connect to a machine and benefit from each other's abilities. Because then people will be connected to a wireless network, such as modems that provide multiple Internet, and will be able to warn each other about talent and cognitive skills. At this point, the impairment

¹⁷ B Custors, G Malgieri, 'Priceless Data: Why the EU Fundamental Right To Data Protection Is At Odds With Trade In Personal Data' (2022) 45 CLSR, pp. 5.

¹⁸A Krausová, 'Legal Aspects of Brain-Computer Interfaces' (2014) 8(2) Masaryk Univ. J. of Law and Technol., pp. 203.

of the will and the active cognitive skill may send manipulative signals.¹⁹ For instance, EMOTIV²⁰ is a device that uses the EPOC headset raised two main topics, such as transferring human brainwaves through the connection of devices and recording silent communication, beyond being a work of performance. The precision data of the neural data that provides mutually silent communication and the connection of sensitive data to specific processing conditions and explicit consent in GDPR Art. 9²¹ also prevents the destruction of Democracy and fundamental rights.²² Furthermore, using state-of-the-art technology to protect sensitive data in cyberspace, not processing data outside of its intended processing, and taking open consent based on informational results at the last point in Democracy. In MBIs, neural data is processed by AI tools and combined with large data sets. It has several tools that may cause the individual to move away from the democratic environment, such as automatic decision-making and profiling, which can result in a horizontal violation of the right to privacy. Horizontal infringement is a form of infringement that also impacts other fundamental rights.

Data protection by design and default is crucial for fundamental rights and democracy, as stated in GDPR art. 25.²³ As mentioned above, MBI sensors should be designed to limit data protection to a high level of technological methods and preserve fundamental rights and democracy by protecting device privacy.²⁴ Privacy is vital when one needs to be made aware of the right decisions. Democratic society will require these modern technologies to guarantee fundamental rights like privacy. They'll create some preferences and article 25²⁵ emphasizes that. Thus, MBIs must retain privacy by default and design without notifying the user before interacting with brain waves.²⁶

Elon Musk's Neuralink²⁷ project aims to connect everyone's brain to a machine, but how do democracy and human rights will get affected by this? The GDPR protects government data. What if the machine, schooled by the human brain, says the idea is hers? Human opinions are owned by staying naked in private. Democracies abuse fundamental rights by demanding and not intervening. Self-intervention in a democracy protects fundamental rights and legalizes action. MBI risk surveillance. All at-risk people will be victims now. For surveillance, MBI

¹⁹ M Ienca, G Malgieri, 'Mental Data protection and GDPR', (2022) 1(19) Journal of Law and the Biosciences, pp. 11.

²⁰ The EMOTIV, <<https://www.emotiv.com/about-emotiv/>> accessed 19 January 2022.

²¹ The GDPR, Article 9 (n 1).

²² Z Polina, P Chapman, M Ma, F Pollick, 'A Wireless Future: Performance Art, Interaction and Brain- Machine Interfaces' (2014) ICT, pp. 3.

²³ The GDPR, article 25 (n 1).

²⁴ B Francesca and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' (2015) 20, Law, Governance and Technology Series, pp. 12.

²⁵ The GDPR, article 25 (n 1).

²⁶ TZ Zarsky, 'Incompatible: The GDPR in the age of Big Data', (2017) 4(2) Seton Hall L. Rev., pp. 8.

²⁷ The Neuralink, <<https://neuralink.com>> accessed 19 January 2022.

creates a digital identity that compromises fundamental rights.²⁸ In a democracy, is oversight legal, appropriate, and necessary?

As we mentioned earlier, if MBIs are used to assess performance of then this application will be mandatory. The employee is given explicit consent to protect their personal data, and the application is required. It doesn't offer an alternative method to the workplace. In this case, there will be a breach of fundamental rights due to processing is unlawful and does not even fall under the scope of legitimate interest. When you think that performance assessments are used to develop a new MBI system in another employer's company and that there is no clear consent from employees, all these actions must complete the questions we asked above.²⁹ According to the High-Level Expert Group³⁰, to implement and achieve trustworthy AI, seven requirements need to be met;

- human agency and oversight,
- technical robustness and safety
- privacy, data quality, integrity
- transparency
- diversity and fairness,
- sustainability, environmental friendliness, social impact, and democracy.
- accountability

These principles should also be imported to the origin of the MBIs. The further away from these principles, the higher the risk is for Democracy and fundamental rights. In this context, the MBIs have a reverse ratio between what it wants to achieve and Democracy, fundamental rights and the right to privacy which will create a paradox.

3.2. Can MBIs be Ethical?

It is also important to consider the significant ramifications of protecting mental privacy and demand proper ethical and legal thought to evaluate the operational specifics of MBIs.³¹ Hence, the ethical issue resembles a mime artist with two different facial expressions regarding privacy and, therefore, the protection of fundamental rights. MBIs pose risks in determining willpower to accept abuse and harmful content because they process sensitive data from its first source.

Given that MBIs are used in the health sector, how can one determine the infringement of privacy rights and the extra data collection activities that will contribute to the treatment process from an ethical perspective? The right to

²⁸ The European Commission, 'High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI' (2019), pp. 12.

²⁹ V De Stefano 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection' (2018) 1 Comp. Lab. L. & Pol'y. J., pp. 10.

³⁰ High-Level Expert Group on Artificial Intelligence, 'Trustworthy AI', (n 28).

³¹ L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI Devices And Their Legal Compliance' (n 8), pp.310.

demand human ethical monitoring, self-determination without harming society, privacy, and the benefit of therapy or MBIs will maintain the balance between self-determination and society. Floridi emphasises the need to steer clear of 'ethics blue washing,' the act of making unfounded or deceptive assertions regarding the ethical merits and advantages of digital processes, products, services, or other solutions, to avert the misleading ramifications of such ethical choices.³² Thus, to tackle this issue, it is imperative to establish comprehensive ethical impact assessments, which shall regulate the field and guarantee sincere compliance with digital ethics. Therefore, ethical impact assessments will address whether this field can be regulated.³³ The ethical and human rights impact assessments should go smoothly because the rule is open to technological advances. The ethicality of a black box AI system is a crucial concern. How will shared ethical values be determined throughout societies? In 1950, the Turing Test organised only the introduction of the ethical aspect of the 1980-year Chinese Room argument with different aspects of testing and criticising the decision of machines instead of people.³⁴ In this context, we cannot go past the development of Kant's philosophy.³⁵

The requirement for the operation does not make it legal to exclude the AI systems used for MBIs from a system that can be explained and calculated. Even if you are in a position not to be able to disclose the actual consent of the user, the legal representatives of the user or the decision-making ethics board should explain how the system went to the decision-making point and the algorithm that made the decision.

4. Brussels effect and MBIs.

4.1. Outsourcing or Crowdsourcing.

Although the regulatory aspect of MBIs and the Brussels Effect³⁶ needs a more extensive study, it is beneficial to mention it to explore its more profound impacts on privacy. As with the regulation of other new technologies, the regulation of MBIs will be open to the opinions of industry representatives, NGOs, member states, and technology beneficiaries.³⁷

The recent AI Act indicates responsibilities what MBIs will have as well. Also, Ad Hoc Committee on Artificial Intelligence (CAHAI) was established in September

³² L Floridi, 'Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical' (2019) *Philosophy & Technology* pp.185–193.

³³ M Pizzi, M Romanoff, T Engelhardt, (2020) 102 'AI for Humanitarian Action: Human Rights and Ethics' *Int. Rev. The Red Cross*, pp. 154.

³⁴ The Stanford Encyclopedia of Philosophy, (2003) < <https://plato.stanford.edu/entries/turing-test/>> accessed 19 January 2023.

³⁵ O Ulgen, 'Kantian Ethics in The Age of Artificial Intelligence and Robotics' (2017) *Quest. Int. L.*, pp. 70.

³⁶ A Renda, 'Beyond the Brussel Effect' (2022) Friedrich-Ebert-Stiftung Report 17 (220301 [beyond the brussels effect.pdf](#) (feps-europe.eu) accessed 24 January 2023.

³⁷ P Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018), pp. 10.

2019 to determine human rights, the rule of law, and democratic standards in designing, developing, and implementing AI. It is an important study in Brussels, seeking digital sovereignty, benefits from Strasbourg's common sense. Representatives of non-EU countries and academics closely follow the meetings to provide opinions. The EU supports outsourcing to regulate technologies, even if it is not a member of the EU while assigning value to these views. It will be possible to use and transfer data across the border, to transfer data that is needed from the cross-border space but to exchange common views and to fulfil certain warranties by non-member states.³⁸ In particular, the cross-border flow of data and secondary uses of health care are becoming increasingly important. During the pandemic, the need for cross-border flows has increased with the development of new technologies.

Protection of the right to privacy has also been the scene of widespread debate within human rights standards.³⁹ There are also horizontal impact discussions with regulations such as data governance, digital markets act, data act, and Digital Services Act⁴⁰ (DSA).⁴¹ With Brussels focusing on legislation and supporting technological developments, human rights have been balanced by CAHAI to establish ethical principles in establishing standards of the rule of law. In its feasibility study, transparency, explainability, human oversight, the non-discrimination of AI and the human dignity need to be considered be on the axis of MBIs.⁴² In this context, Brussels will need to use various resources or externally receive services while regulating space for a more transparent, more explainable AI. Therefore, outside the EU territory, Brussels has become welcoming for innovators and developers because data must flow to the USA to benefit for Brussels to have continuous operation of technology products.

The Brussels effect is reflected in the regulation process as a risk-based approach. In CAHAI, a risk-based approach has drawn the body of AI with red lines which are also transferred to the AI Act. On the one hand, Brussels is making progress on the horizontal axis with various regulations for the growth of the digital market. The GDPR replaces the Data Protection Directive and The European Convention No. 108+⁴³ follows the DSA and Digital Marketing Act (DMA)⁴⁴ on the horizontal axis. Within these regulations, the GDPR and AI Act are the great older brother of others. On the other hand, Brussels also wants to lead the way in markets such as USA, China, and Korea to ensure that data flow is legal and compliant with human rights. Therefore, it is closely monitoring the data

³⁸ A Renda, *Beyond the Brussel Effect* (n 35), pp. 20.

³⁹ A Mantelero, *'Beyond Data'* (T.M.C. Asser Press, 2022), pp. 161.

⁴⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

⁴¹ European Commission, *'2030 Digital Compass: the European way for the Digital Decade,'* COM (2021), pp. 118.

⁴² AR Young, *'The European Union as a global regulator? Context and comparison'* (2015) 22 (9) *J. Eur. Public Policy*, pp. 1233.

⁴³ *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series - No. 108.

⁴⁴ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

protection laws and relevant laws of states to ensure that states work on the same axis as Brussels.⁴⁵ In this context, the lack of an interoperable law of states will be one of the factors directly affecting the market.⁴⁶ For example, the Data Governance Act⁴⁷, which is being worked on for the creation of common data sets platforms for data management, describes how the system will operate in concrete terms and the Brussels front.

At this point, it is a fact that Brussels cares about the creation of data sets that MBIs will use or mechanisms that can share secure data sets after anonymising the data they have obtained. They are trying to complete horizontal legal regulations in this area. However, MBIs will have a challenging position in case of the GDPR. Therefore, the Brussels front is very concerned about the data minimisation and purpose limitation stage and the control mechanisms. Privacy by design and by default phenomena also follow these principles. The signals recorded by the devices used in Brussels's MBIs are kept in the country where the device is manufactured. The possible regulations for storing signal data are also will be compliant with GDPR art. 46⁴⁸. So, keeping the data in the country in which the device is manufactured will be a method Brussels would not agree to. The country of the instrument must take the necessary measures at this point in terms of the protection of the AI Act and the GDPR. Furthermore, Brussels effect, which we can also refer to as Bradford's influence, cares about the Europeanization of data. We believe that this angle is very clear in the domain of GDPR.⁴⁹ The determination of the GDPR country in a way that includes the services that non-EU countries provide to EU citizens also led countries serving EU citizens to adopt the scope of GDPR and enforce their best practices and regulations in accordance with GDPR or try to do their best. In this context, the GDPR has spawned the concept of spreading European data.

4.2. Sustainability, Brussels Effect and MBIs.

Sustainability is an important and hidden phenomenon meaning to regulate technology and monitor it after post-regulation. Due to the high risk of computer MBIs, it is mandatory to follow the lawfulness of products allowed to operate in the market as much as the prohibition of applications that eliminate basic rights to protect the fundamental rights of data subjects.

Because of the need for neuro data, MBIs must process sensitive data. Hence, periodical privacy impact assessments, guidance on using privacy-enhancing

⁴⁵ LA Bygrave, 'The Strasbourg Effect on Data Protection in Light of The Brussels Effect: Logic, Mechanics and Prospects', (2020) 8 CLSR, pp. 10.

⁴⁶ K Sahin and T Barker 'Europe's Capacity to Act in the Global Tech Race: Charting a Path for Europe in Times of Major Technological Disruption' (DGAP Report, 6) (2021) Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V., <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73445-7> 16. accessed 24 January 2023.

⁴⁷ Proposal for a Regulation of The European Parliament And Of The Council on European Data Governance (Data Governance Act).

⁴⁸ The GDPR, Article 46 (n 1).

⁴⁹ LA Bygrave, The Strasbourg Effect on Data Protection in Light of The Brussels Effect, (n 41), 11

technologies, repeating explicit consent in each processing state, and follow-ups as objective changes are necessary. While other horizontal regulations regulate data processing processes other than GDPR⁵⁰, horizontal regulations greatly contribute to sustainability. By regulating the processes of non-personal data processing, DSA also strengthens the presence of GDPR, such as the Data Governance Act, which regulates the smooth use of data in all sectors without discrimination of personal and non-data and further details the rights of data subjects.⁵¹

There are also areas where sustainability is still problematic, such as creating secure data sets for the transfer of neuro data processed in MBIs outside the GDPR's territory. Although MBIs are more likely to show up in areas such as gaming and performance measurement, medical diagnosis and treatment processes have been used in the past and will be used more often. When EEG data is acknowledged to give the most accurate results in processing brain signals, three scales on how data subjects will impact their rights before data processing can be maintained at the heart of the right. Three scales are human rights impact assessment, ethical impact assessment, and privacy impact assessment.⁵² Another key area to ensure sustainability is ensuring that data protection authorities can interoperability and effectively use the object rights granted to the data subject. The MBI market will be partially EU-based, and services will be purchased from different locations may result in the country of conflict being other countries or the mechanisms of objection being combined with several data protection authorities. We don't want to discuss issues such as jurisdiction because this article is different from the article's subject. However, the importance of data protection authorities acting on common platforms and common law is inevitable.⁵³ The closest we have seen in the Covid 19 process is that an EU data protection field that ignores data subject rights cannot be sustained. The Brussels effect closely followed inventions, medication monitoring, continuous health data monitoring, etc. to handle the pandemic.⁵⁴

5. Conclusion and Recommendations.

As with any new technology, it is essential to carefully consider the implications and develop appropriate regulations and guidelines to protect privacy and

⁵⁰ AB Tickle and others, 'The Truth Will Come to Light: Directions and Challenges in Extracting the Knowledge Embedded Within Trained Artificial Neural Networks' (1998) 9 IEEE Transactions on Neural Networks, pp. 1057.

⁵¹ LA Bygrave The Strasbourg Effect on Data Protection in Light of The Brussels Effect (n 41), 13.

⁵² W Samek and others., 'Evaluating the Visualization of What a Deep Neural Network Has Learned, IEEE Transactions on Neural Networks and Learning Systems' (2016); MT Ribeiro and others 'Why Should I Trust You? Explaining the Predictions of Any Classifier', (2016) Proceedings of the 22nd Acm Sigkdd International Conference on Knowledge Discovery And Data Mining.

⁵³ E Palmerini, 'Algoritmi E Decisioni Automatizzate Tutele Esistenti E Linee Evolutive Della Regolazione' (2021) Editoriale Scientifica, pp. 13.

⁵⁴ L Edwards, M Veale, 'Slave to the Algorithm? Why a Right to An Explanation is Probably Not The Remedy You Are Looking For' (2017) 18, Duke L. & Tech. Rev., pp. 69.

individual rights. Mitigating risks is important to develop appropriate regulations and guidelines to protect privacy and individual rights.

New technologies like MBIs introduce new issues that, in the absence of legislative amendments, must be resolved through the interpretation and application of existing rules. These outdated rules also need to be changed to provide more clarity and to better address the challenges brought by new technologies like MBIs.⁵⁵ Additionally, to progress MBIs while preserving citizens' rights to privacy and other basic liberties, legislators will need to find a middle ground between the demands of corporations and governments. However, it won't be sufficient to enforce new regulations that apply to cutting-edge technologies like MBIs. In order to have multi-layered efficacy, it is essential to include protections and limits that are relevant to these new technologies, such as MBIs. Also, we mentioned how sustainability involves regulating and monitoring technology and how data subject rights became even more critical with the rise of MBIs. Also, the connection between MBIs and the legal side of the Brussels Effect have serious implications regarding privacy which needs to be monitored closely.

One potential solution to the privacy and data protection challenges posed by MBIs is the implementation of robust consent mechanisms. Under the GDPR, companies must obtain the explicit consent of individuals before processing their personal data. This includes data generated through MBIs. By requiring users to actively consent to the collection and processing of their data, companies can ensure that individuals are fully aware of how their data will be used and can opt-out if they do not wish to share their data. In addition to obtaining explicit consent, companies should also consider implementing other privacy-enhancing measures, such as pseudonymization and encryption, to protect the security and confidentiality of MBI data. These measures can help to reduce the risk of unauthorized access to or misuse of sensitive personal data.

MBI industry standards and guidelines are other options. These standards could address data protection, privacy, and ethics. In addition, companies and researchers may ensure that MBIs are responsibly developed and used by creating clear rules. Finally, it will be important for regulators and policymakers to closely monitor the development and use of MBIs and to act as necessary to ensure compliance with relevant laws and regulations. This may include issuing guidance or issuing enforcement actions against companies that fail to adequately protect the privacy and data protection rights of their users.

⁵⁵ F Martin-Bariteau T Scassa eds., *Artificial Intelligence, and the Law in Canada* (Toronto: LexisNexis Canada, 2021).