EMOTIONS RECOGNITION SYSTEMS AND DATA ECONOMY

Claudia Confortini
Tor Vergata University of Rome
Department of Law and Management

(claudia.confortini@uniroma2.it)

Abstract

Should the European Union recognise a set of neuro-rights? How could privacy and autonomy be adequately protected in the face of the advancement of mind-reading technologies in the data-driven economy? This work sets the stage for a discussion through an analysis of the European legal framework, suggesting how to close some loopholes in order to shape an effective governance of emotional AI.

1. *Introductory remarks.*

In the context of the data-driven economy, the widespread deployment of computing and artificial intelligence techniques to sense, learn about, and interact with human emotional life (so-called 'emphatic media') raises serious legal issues. Both fundamental rights and civil liberties are threatened (Simoncini and Longo, 2021).

Contemporary machine learning techniques can gain accurate information about affective states from neural data or digital footprints, predicting the course of action, sometimes subliminally. Privacy and autonomy are jeopardized. Some of the most serious threats to individuals' rights and democratic values are related to the possible exploitation of such technological tools for *psycho-psychological profiling* (Bakir and McStay, 2022). Big concerns are related to the use of emotional AI by companies, governments, and political candidates to manipulate and control economic choices, and social and political behaviours.

In the first instance, this work points to analysing the major risks connected with the deployment of emotion recognition systems (*breviter*, ERSs): *i.e.*, Artificial Intelligence systems able to detect, interpret, process, and simulate human emotions. Secondly, it aims to outline the latest developments in the regulation of emotional AI within the context of the European Union, especially in light of the Artificial Intelligence Act.

Some scholars suggested we should resist to exploit emotional AI because it is based on a "reductivist approach" to 'reading' – and exerting authority over – human emotions and intentions. According to the AI Now Institute, regulators should indeed heavily restrict the deployment of emotional AI: governments should prohibit the use of affect recognition in high-stakes decision-making processes and until then, AI companies

should stop employing it[1]. In the view of some civil society organizations, emotional AI represents one of the greatest threats to the European Union's desire to create an ecosystem of trust and excellence for AI and should therefore be forbidden[2]. The AI Act only partially banned emotional AI. The analysis, therefore, turns into a discussion on the extent to which the current EU legislative framework is apt to offer adequate protection to the fundamental rights enshrined in the CFREU and in the ECHR in the face of the challenges posed by emotional AI. Is there a call for the introduction of new constitutional rights or an actual need for further advancements in the EU regulation, especially concerning the protection of mental data? The work questions whether the European Union missed a chance in regulating emotional AI and investigates what could be done in the future *de lege lata* or *de lege ferenda* to strengthen the protection of the rights of European citizens from privacy and data protection to agency and non-discrimination. Efforts will focus on identifying potential loopholes. The paper will also try to suggest how to fill them in order to safeguard individuals' rights and freedoms in front of the rapid progress of mind-reading technologies in the context of a data-driven economy.

2. *Emotion recognition in the data-driven economy.*

Emotion recognition is being widely used in many fields and has become a research milestone in several scientific areas: not only cognitive science, neuroscience, computer science, and psychology but also law. Our emotions are being detected in real-time and tracked, both in private and public spaces. Quantifying, tracking, and manipulating emotions constitute a significant part of the social media business model (Stark and Crawford, 2015).

It is well known that communication is a multimodal process and that emotions can be inferred based on different signals: using both non-physiological signals such as facial expressions, speech, body movements, or eye tracking (Sposini, 2023) as well as physiological signals and images like electrical skin resistance (GSR) or heart rate (HR), electrocardiogram (ECG), functional magnetic resonance imaging (fMRI), electroencephalogram (EEG) and magnetoencephalogram (MEG). Magnetoencephalography and electroencephalography measurements of neural activity, for example, combined with generative AI models can decode human thoughts and emotions with high percentages of accuracy. However, emotion recognition does not concern uniquely neurotechnologies. The *spectrum* of applications able to infer human emotions is wider. If neurotechnologies such as brain-to-computer interfaces (BCIs) provide large sets of data to make inferences about emotional states, also non-neural contextual information like a written test can be the basis for such inferences (Ienca and Malgieri, 2022). Recent research has demonstrated that algorithms, for instance, are highly accurate in recognizing emotions from speech signals (Singla et al, 2024).

In our online interactions we all reveal information that could be used by intelligent systems to 'read our minds' (Burr and Cristianini, 2019).

---

[1] AI Now Institute 2019 Report, NYU University, December 2019, p. 6.

[2] See Prohibit emotion recognition in the Artificial Intelligence Act, p. 2: paper drafted by Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 and IT-Pol, further supported by AlgorithmWatch, Fair Trials, the European Centre for non-profit Law (ECNL) and Panoptykon Foundation, following the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

The analysis of content shared through blogs or social media can disclose significant information about the emotional state of a person[3]: the use of certain keywords, typing patterns, likes, user tags, or emoji can provide important cues as to the emotions and intentions of an individual, being of enormous interest to businesses in the digital economy. Studies show that individuals with depression seem more likely to use an increased number of first-person singular (Rude et al, 2004). Such information could be employed to deliver targeted messages at particular times when the person is likely to be more receptive, thereby subtly shaping (or even distorting) the thought process, emotions, and behaviours.

Technological developments allow for the grasp of emotions from various types of data: not only neural data but also behavioural and phenotypic data (Ienca and Malgieri, 2022). Privacy is threatened by various technologies which allow for mental incursion. Data protection is at risk. Neural data could illuminate and help predict personality traits[4], addictions, mental health, and various disorders and it does not take an enormous leap of imagination to consider how this data could be misused by corporations and specific groups of interests. Information revealing personality or psychological traits could lead to discrimination; individuals with mental illnesses or psychological weakness could receive differential treatment by companies; companies might disclose information that consumers wanted (or needed) to keep private. Mental data leaks can cause harmful effects on the consumer's dignity, opportunities, and social life.

3. *Potential uses of emotional AI: contexts, purposes, challenges.*

Before examining more in detail the major risks associated with emotional AI – *e.g.*, privacy invasion, manipulation, unjust discrimination, etc. – and the law tools apt at mitigating them within the European Union legislative framework, is important to put in evidence that the potential uses of ERSs cover a wide range of applications: provision of personalised services; advertising and microtargeting; customer behaviour analysis; detection of diseases such as autism or prediction of psychotic disorders and depression (healthcare). In the employment sector, ERSs can help the decision-making of recruiters; can be used to identify uninterested candidates in a job interview; and monitor the moods and attention of employees. In education, ERSs can be deployed to monitor students' attention; detect emotional reactions to educative programs in order to adapt the learning path, etc. Emotional AI is being widely used in border protection and law enforcement to identify dissimulating and otherwise suspect individuals (regardless of potential harm to people and society as a whole and of substantial evidence or proof about their efficacy and accuracy). Other possible uses include the detection of political attitudes.

It is almost self-evident that ongoing advances in mind-reading technologies present both great promises and potential risks. In particular, the findings of AI in combination with neurotechnology may significantly improve the quality of life of individuals but can also seriously threaten human rights and democratic values. Devices that are capable of

[3] See EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021, p. 35.

[4] Recently, a machine learning model has successfully inferred personality from the texts that readers consume. See Simchon A, Sutton A, Edwards M, Lewandowsky S (2023) Online reading habits can reveal personality traits: towards detecting psychological microtargeting. PNAS Nexus. 2(6):gad191.

recording or altering the activity of the brain and the wider nervous systems have wide applications not only in settings of research and medicine, ranging from studying Alzheimer's to treating Parkinson's, but also in other contexts.

As a consequence of the progress in the field of non-invasive brain-computer interfaces (BCIs), devices that can collect relevant amounts of brain data once confined to hospitals, universities, and laboratories are now increasingly user friendly, affordable, and easily available to consumers all over the world. Such products are sold mainly for entertainment and *neurogaming* or wellness and *neuroenhancement*: to deepen meditative and sleep states, reduce stress or anxiety, sharpen focus, enhance productivity, and improve cognitive states…Current wellness neurotechnology products include, for example, a headset that promises to provide home treatment for depression and anxiety using transcranial Direct Current Stimulation: the brain runs on electricity; the device sends gentle electrical impulses into the area that has slowed down. This is supposed to get cells firing again and reduce the symptoms of depression.

It is also interesting to report that in 2022, the world's largest cosmetics company, L'Oréal, launched a partnership with neurotechnology company EMOTIV to deploy EEG technology in its stores as part of personalized fragrance consultations that identify fragrance preferences through neural activity.

This is only some evidence of the growing mass commercialization of neurotechnology and of the spread use of mind-reading technologies for the purpose of *neuromarketing*. Sources report an increase of 62% in global neurotechnology investment between 2019 and 2020[5].

There is clear evidence of the fact that neurotechnologies are proliferating far beyond medical settings into the public marketplace.

A growing number of neuro-technologies are not regulated as medical devices and can be purchased without the involvement of clinicians, researchers, or other intermediaries (without prescription). However, especially the advancement of BCIs raises profound ethical and legal issues (Krausová, 2014). The long-term effects of BCIs on cognitive functions and overall health are yet to be fully understood[6]. Moreover, these affordable devices, which are marketed for public consumption, allow for the collection of neural data beyond laboratory settings. The range of companies that can collect neural data from consumers today is already wide. As consumers increasingly use neurotechnology devices, companies can build bigger and bigger databases of brain scans and other neural data.

In the field of *medical research* and *health care*, the use of neural data could aid the *diagnosis* of a wide range of mental and neurological diseases, from schizophrenia to depression, bipolar disorder, anxiety, post-traumatic stress disorder, panic attacks, Alzheimer's, and Parkinson's disease.

In the area of *emotional marketing* (Galli, 2022) though, mental data collected through wearable neurotechnology devices could be processed for the purpose of *prediction*, (manipulative) *persuasion*, and (subliminal) *control* over human emotional states.

---

[5] Global Neurotech Industry Investment Digest (2021), Deep Knowledge Group for EIN News, July 14, 2021, available at https://www.einnews.com/pr_news/546252348/global-neurotech-industry-investment-digest-2021.

[6] See the Research Paper of the Council of the European Union From vision to reality. Promises and risks of Brain-Computer Interfaces, September 2024, p 14 ff.

Due to the fast advancements in neurotechnology and artificial intelligence-driven software, especially deep learning (LeCun et al, 2015), but also because of the commodification of brain data (Farahany, 2023), humans are exposed to unparalleled threats (Ruffolo and Amidei, 2024).

Neural activity is the core of self and the foundation of personal identity. Manipulation of brain activity might have unprecedented consequences as regards individual identity, autonomy, and personal liability[7]. The deployment of certain types of BCIs can potentially result in manipulation or influence of decisions, undermining the very essence of free will. The use of BCIs and intelligent systems can affect a user's sense of agency (Haselager, 2013). Data leaks and brain hacking (of brain-computer interfaces or deep brain stimulation devices) may be a source of additional harm (Ienca, 2015). BCIs are potentially exposed to cybercriminality (Ienca and Haselager, 2016).

The storage and transmission of neural data seriously challenges data security. Manipulation or theft of neural data can potentially result in identity theft. Both privacy and security breaches must be prevented (Ienca et al, 2018).

Even if it is hard to predict the pace of neurotechnology development, there is ground for arguing that the pace will be very rapid and that technologies like BCIs will be soon integrated into everyday life. It is a common view that over the coming decades, neurotechnologies will become mainstream and can potentially alter what it means to be human (Yuste et al, 2021).

In the occidental tradition, it is widely recognized that human identity is linked to consciousness, freedom of thought (Alegre, 2021), and the ability to self-present. Cartesio *docet*: «*cogito ergo sum*». Potential risks for humans are unrivaled.

Aside from the obvious privacy and data protection concerns, at stake are individual autonomy, equality, and human dignity.

It is well known that advertising and marketing seek to capitalize on emotions to drive financial profit (Clifford, 2019). Emotional AI, though, allows for the further, granular personalization of both commercial and political communications, facilitating marketing campaigns in real-time (Burr et al, 2019).

Machine learning algorithms allow for the automated detection even from people's digital footprints of information related to emotional states, personality traits, and intents which can be used to tailor persuasive messages capable of increasing the chance of a person clicking on an online advertisement and buying a product (Matz et al, 2017). An increasingly personalised environment allows for more "nudging" potentially resulting in undue influence over (and exploitation of) individual choices, in a loop that augments the knowledge power of few actors or groups of interests. Big Data driven nudges are extremely potent due to their continuously updated, dynamic, and pervasive nature. For this reason, they have been referred to as 'hypernudges' (Yeung, 2017).

Emotion recognition, especially if extensively used for psychological targeting and mass persuasion, can have serious implications for democracy.

It can endanger the soundness of personal opinion formation and independent decision-making, having an impact on public opinion and altering electoral outcomes.

---

[7] For a critical summery of the legal implications and the main legal issues raised by modern neuroscientific acquisitions see D'Aloia A (2020) Law Challenged. Reasoning about Neuroscience and Law. In D'Aloia and Errigo MC (eds) (2020) Neurosciences and Law: complicated crossings and new perspectives, Springer, p. 1 ff.

Through, for example, Facial Emotion Recognition technology, it is possible to infer political attitudes by looking at facial expressions and reactions of the audience during political events.
In contexts other than business-to-consumer relationships (*e.g.*, political campaigning), fine-grained, subconscious, and personalized levels of algorithmic persuasion may negatively affect the cognitive autonomy of individuals and their right to form independent opinions and make free and conscious decisions. Both democracy and the rule of law are endangered since they suppose that individuals act like independent moral agents[8].
On social media platforms and in political campaigns, human vulnerabilities may be exploited, for example by disseminating advertisements at specific moments or in places when/where the receiver would be more sensitive to a certain kind of message.
Profiling by ERSs is highly invasive. In political communication, it could negatively affect individuals' fundamental rights and freedoms like as not being manipulated or being treated equally. It may lead to the manipulation of the electorate, producing harmful consequences on the democratic process.
The potential risks of the deployment of AI and microtargeting to craft political messages delivered to individuals based on their emotional states and personality traits are grave and probably underestimated. Recent technological advancements, involving generative AI and sentiment analysis (even personality inference from consumed text) may originate a highly scalable "manipulation machine" that targets individuals based on their vulnerabilities. This should be an area of special concern to academics and policymakers (Simchon et al, 2024).
Legal issues also concern accountability for illegal actions. Mind-reading technologies like BCIs can alter a user's mental state to the extent that a person can be no longer the same after their use, showing behavioural changes like impulsivity or intemperance. In such a case, it would be difficult to determine who should be held accountable for certain actions[9].
Questions arise also about social justice and non-discrimination. The use on a large scale of neurotechnologies devices for the purpose, for example, of mental augmentation could widen social disparities and marginalise groups that do not have equal access to them[10].
In the following pages, attention will be focused, firstly, on the main risks linked with the deployment of emotional AI in various fields; secondly, on the legal safeguards within the EU legal framework and on the shortcomings of the legislation of the European Union.

4. Main issues arising by ERSs: opacity, inaccuracy, inconsistency, unjust discrimination.

[8] See "Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes", adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies, p. 2.

[9] From vision to reality. Promises and risks of Brain-Computer Interfaces, cit., p. 17.

[10] Whether and how to regulate neuroenhancement is an open question. A study of the European Parliament outlined possible strategies, identifying a reasoned pro-enhancement approach, a reasoned restrictive approach and a case-by-case approach as viable options for the EU (see European Science and Technology Options Assessment. Human Enhancement Study, 2009). For an in-depth analysis see Errigo MC (2020) Neuroenhancement and Law. In D'Aloia A and Errigo MC (eds) (2020) Neurosciences and Law: complicated crossings and new perspectives, Springer, p 208 ff. (the Author is against a total ban and in favour of a reasoned narrow approach).

Some of the biggest concerns related to the deployment of ERSs are based on the fact that emotional AI, like most artificial intelligence, is often invisible to the people most affected by its decisions (*hiddenness*).

Worldwide, a growing number of AI systems (*e.g.*, vibraimage) algorithmically classify suspects/non-suspects, yet are accused of being themselves deeply suspect (Wright, 2021). Data used by the system may be collected and analysed in a hidden or covert manner (for example, via CCTV at an event or in a public place) and the exact method of analysing this data is also opaque – it is not clear to its subjects how the system works or what exactly it is quantifying. The corporate value of a technology often seems to be generated through its very *opacity.*

Generally, transparency gaps are a source of vulnerability. Without knowing what Google does when it ranks sites, for instance, we cannot assess when it is acting in good faith to help users, and when it is biasing results to favour its commercial interests. The same goes for status updates on Facebook or trending topics on Twitter (Pasquale, 2015).

Transparency alone, though, is not a sufficient condition for holding algorithmic assemblages accountable. I agree with those who criticise the idea 'that knowing is possible by seeing' (Ananny and Crawford, 2018). Does it matter whether we can see exactly how algorithms work in this field to hold the outputs accountable? Indeed, even if we had full visibility of them, how would we know whether they actually 'work' properly in interpreting emotional states?

Especially in this field, leaving algorithms without appropriate safeguards would mean opening the way towards techno-determinism, which appears to be a much more serious threat when it comes to the inner sphere of emotions and cognitive liberty (McStay, 2018).

Additionally, emotional AI is likely to have algorithmic failures that lead to unfair and/or biased outcomes. There might be inference inconsistencies, *e.g.*, when the emotional AI identifies a particular facial expression but does not infer the concomitant emotion (there is undoubtedly a significant facial expression uncertainty, linked with demographic-based differences in the emotions recognized by humans and by affective AI models) (Rhue, 2019).

Indeed, it must be noted that facial expressions and their meaning are highly dependent on social and cultural context.

When it comes to facial coding (Ekman and Friesen, 1978), the most basic critique is that one does not necessarily smile when one is happy; common sense suggests that facial expressions do not always, or even often, map to inner feelings, that emotions are often fleeting or momentary, and that facial expressions and their meaning are highly dependent on social and cultural context (Crivelli et al, 2015).

Emotion recognition systems reduce emotion to a highly reductive and simplistic model that is digitally scalable. As Barrett argues (Barrett et al, 2019), emotion isn't a simple reflex or a bodily state that's hard-wired into our DNA, and it's certainly not universally expressed (Russell, 1994). Culture to culture, person to person even, it's never quite the same.

Emotion detection as well as categorising based on inferred emotions are culturally mediated processes.

There's also evidence of the fact that emotion recognition can amplify both race and gender disparities (Dibeklioglu et al, 2015). The use of machine-learning methods

involved in emotion recognition systems has been harshly criticised for racial biases based on the data sets on which the algorithms are trained.
Recent studies have found that emotional analysis technology assigns more negative emotions to black men's faces than white men's faces: facial recognition programs are often biased. On average, Face++ rates black faces as twice as angry as white faces. Face API scores black faces as three times more contemptuous than white faces (Rhue, 2019). Black men's facial expressions are scored with emotions associated with threatening behaviours more often than white men, even when they are smiling.
These studies suggest that facial recognition may perpetrate the same biases that people have, formalizing preexisting stereotypes into algorithms and automatically embedding them into everyday life.
Some argue that if emotional AI had to be evaluated in human terms, it would be judged as psychopathic (McStay, 2022). ERSs are not emphatic. They do not understand our emotions: they simply process data such as biometrics and generate outputs called emotional states (Bakir and McStay, 2022).
It has even been argued that ER is pseudoscience. Emotions recognition systems mainly rely on the six basic emotions indicated by Ekman: *i.e.*, happiness, sadness, surprise, fear, anger, and disgust (Ekman and Keltner, 1997). However, this classification is harshly criticized as not accurately reflecting the complex nature of an affective state[11]. It has been remarked that many more facial expressions of emotion exist and are regularly used by humans (Du et al, 2014).
The AI Now Institute at New York University alerts that facial recognition reactivates 'a long tradition of physiognomy and is pseudoscience since it claims facial features can reveal innate aspects of our character and personality' and emphasizes that contextual, social and cultural factors play a larger role in emotional expression than was believed by Ekman and his peers[12].
Some argue that physiognomic AI is unjust and deceptive. Therefore, it should be banned (Stark and Hutson, 2021).
Leaving to one side the point that emotion detection in particular through facial expressions is a pseudoscience, it must be put in evidence that improving the accuracy of emotion detection may arguably require more invasive surveillance to gather more contextual insights and signals, paradoxically adding difficulties from a privacy perspective (Valcke, Clifford and Dessers, 2021).

5. *ERSs threaten privacy, individual autonomy, agency, and dignity. Emotions monitoring produces chilling effects encroaching on the ability and the freedom to "self-present".*

In addition to technical issues about 'accuracy', these technologies pose several concerns related to the protection of fundamental rights of consumers, voters and people in general: if the scientific validity of these technologies is questionable, the potential harm from misuse is significant.
The use of emotional AI (*i.e.*, systems characterized by complexity, opacity, dependency on data, and autonomous behaviour) can adversely affect several fundamental rights

[11] According to Barret such categories fail to capture the richness of emotional experiences. Patterns, for example, for anger or sadness are not stable among people. Barrett L (2006) Are Emotions Natural Kinds? Perspectives on Psychological Science 1 (1): 34.
[12] AI Now Report 2018 (n. 63) 14. See also A. McStay (2016) Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (the Case for Intimacy) BD&S 3(1): 3–6.

enshrined in the EU Charter of Fundamental Rights as the right to respect for private and family life, and protection of personal data (Article 8 ECHR; Articles 7–8 CFREU); equality and non-discrimination (Article 14 ECHR; Articles 20–21 CFREU); freedom of thought and conscience (Art. 9 ECHR; Art. 10 CFREU).

The most serious issues raised by ERSs concern privacy (Valcke, Clifford and Steponenaite, 2021), which is central to this analysis, but also self-determination, individual autonomy, and human dignity (Bakir and McStay, 2020).

ERSs pretend to have the algorithmic authority to empower the operator to know subjects better than subjects know themselves by directly accessing and revealing their unconscious. Emotional information is often conveyed by the body through unconscious reactions to an external stimulus . Emotional AI can hence undermine the agency of the subject and his capacity to consciously and autonomously determine and communicate their own mental emotional state.

By means of ER, the right to the future tense (Zuboff, 2018) is profoundly infringed.

ERSs represent a source of power imbalance and power imbalance allows for limitless exploitation, which is a distinctive feature of digital capitalism (Cofone, 2023) and the core of human digital vulnerability.

If consumers' vulnerability mostly depends on the imbalance in the level of knowledge between the two bargaining parties (Galli, 2022), detection and exploitation of mental data can generate a new form of 'universal' vulnerability. This new shape of human digital vulnerability rests in (consciously and unconsciously) exposing sensitive parts of the self to AI technologies and to digital architectures that reside in the hands of just a few powerful actors.

It should be noted, that the inference of emotions through the collection of neural data or non-physiological signals involves involuntary disclosure of information. Even if individuals consent to the collection and processing of their personal data for a narrow use, they are unlikely to be fully aware of the content or quantity of information they are sharing.

A recent study suggests that neural data holds the potential for diverse personal insights possibly beyond the current public understanding (Huang et al, 2024).

People are not in a position to properly foresee the consequences of their inferred data.

Neurotechnology users cannot decide what specific neural information they would like to disclose and they are unlikely to understand the extent to which their neural data can be decoded, currently or in the future[13]. Neurotechnologies can collect information about an individual that the individual did not even know existed.

In the digital environment, even if there is not a brute force coercing us, still individuals are under the undue influence of powerful counterparts who can nudge us to act the way that is more profitable to them (Malgieri, 2023).

Advancements in neuroscience, combined with the use of AI in the digital realm are giving rise to a new form of 'universal' rather than 'situational' vulnerability connected to the exploitation of human emotions (De Mari Casareto dal Verme, 2023).

[13] House bill 24-1058 an act concerning protecting the privacy of individuals' biological data, and in connection there with, protecting the privacy of neural data and expanding the scope of the "Colorado Privacy Act" accordingly.

Presumably, we all agree that we need to prevent and deter emotional manipulation, considering the 'ontological' vulnerability of human beings in the digital environment (Gatt and Caggiano, 2022)[14].

The point is, as noted by Sunstein (Thaler and Sunstein, 2008), that manipulation has 'many shades' and is extremely difficult to define.

Distinguishing between (unacceptable) manipulation and (acceptable) persuasion may be problematic[15].

Probably, we should link the concept of manipulation to the one of self-determination and individual autonomy. Therefore, we should consider a statement or action as manipulative to the extent that it does not sufficiently engage or appeal to people's capacity for reflective and deliberative choice.

Moreover, emotional surveillance may cause chilling effects on behaviour. The pervasive deployment of AI models that allow individuals and companies to take advantage of "*feeling-into*" the inner world of people, as well as the online and offline behaviour of the *civic body*, raise the spectre of perpetual surveillance (Bakir and McStay, 2022).

ERSs, in this way, encroach on our rights to freedom of expression (Art. 10 ECHR; Art. 10 CFREU), freedom of assembly and association (Art. 11 ECRH; Art. 12 CFREU), and – to the extent that our moral integrity is at stake – our right to private life and personal identity (Art. 8 ECHR; Art. 7 CFREU) (Valcke, Clifford and Dessers, 2021).

There is a serious risk of chilling effects as people are becoming aware that our actions are being scrutinized and evaluated on a second-by-second basis. Such emotional monitoring can have an impact on the ability to 'self-present' individuals (Warner and Sloan, 2014).

We have previously referred to biases and profiling errors. Emotional AI, though, can have an impact on an individual's autonomy and capacity to self-present irrespective of its accuracy: the lack of accuracy of emotional AI, resulting in profiling errors and incorrect inferences, poses additional risks of harm.

Emotion recognition technologies add a layer of intimacy-invasion because they are capable of detecting not only expressed emotions but also underlying emotions deliberately disguised. This would constitute not merely a breach of privacy but a violation of autonomy (Brown, 2024).

While privacy and autonomy are not the same, it can reasonably be argued that the right to privacy serves as a means of safeguarding autonomy (Clifford, 2019).

The intimate knowledge of a person is the basis of many forms of manipulation. Privacy law plays a crucial role since it helps to prevent other entities from eroding the individual autonomy of the data subject (Pasquale, 2024).

---

[14] In the digital environment the concept of vulnerability «is not linked to specific physical or psychological disabilities but is identified in the relationship between the physical person and the technological environment in which he/she operates'». We can therefore speak of «ontological vulnerability of human beings – in general – with respect to digital technology structures». See L. Gatt and I.A. Caggiano (2022) Consumers and Digital Environments as a Structural Vulnerability Relationship. European Journal of Privacy Law & Technologies 2:12. On this topic, see also A.A. Mollo (2023) Vulnerabilità e sostenibilità: primi spunti per uno studio dell'impatto sulle persone con disabilità e sulle future generazioni dei dispositivi [neuro]tecnologici. European Journal of Privacy Law & Technologies:28-49.

[15] «From a policy perspective, understanding the exact point where *acceptable persuasion* becomes *unacceptable manipulation* is one of the crucial issues for the regulation of marketing and commercial practices, especially in the digital environment». See European Commission, *State of the art of neuromarketing and its ethical implications*, 2023:27 https://op.europa.eu/en/publication-detail/-/publication/43754ac8-26aa-11eea2d3-01aa75ed71a1/language-en.

Emotional AI challenges both (*i*) privacy as seclusion or intimacy: ER puts at risk the freedom to think without being monitored by others (*forum internum*) and (*ii*) privacy as freedom of action and self-determination (Ziegler, 2007).
Certain rights, including the right to privacy, the right to freedom of conscience and belief, and the right to be free from discrimination are crucial for preserving human dignity (Feldman, 1999). Since the employment of emotional AI threatens these rights (*e.g.*, the right to respect for private and family life and the right to be free of discriminatory treatment), it poses threats to human dignity as well (Valcke, Clifford and Dessers, 2021).
It has been noted that individual autonomy and human dignity are not sufficiently protected by articles 8, 9, and 10 of the ECHR[16]. We could argue about the need for a type of 'Oviedo Convention' about (emotional) AI. However, it might be not necessary to introduce novel rights such as the right to the future tense; the right to cognitive liberty, the right to self-determination over our brains and mental experiences (Farahany, 2023); the right to not be measured, analysed, or coached; the right to cognitive sovereignty; the right not to be manipulated as far as we refer to them in interpreting art. 8 of the ECHR. The introduction of novel constitutional rights may indeed have a negative effect, diluting the significance of the existing constitutional rights. Nevertheless, it is important to shape appropriate remedies, reinterpreting the existing human rights and redefining the content of art. 8 and 9 ECHR.

6. *The European legal framework: a multilayered protection.*

Having a look at the global picture of the EU rules and principles is possible to find various positive tools to limit abusive exploitation of cognitive liberty and mental integrity[17].
As above noted, Emotional AI challenges some of the very basic principles for a trustworthy and human-centric AI: privacy, personal autonomy, non-discrimination, human dignity, agency, and transparency. For this reason, the *Artificial Intelligence Act* of 13th of June 2024 (Reg. Eu 2024/1689) lays down several harmonised rules on ERSs. These provisions, which will be examined separately[18], shall apply across sectors without affecting the application of existing Union law. The regulation is complementary to the existing Union law, in particular on data protection[19], fundamental rights, and consumer protection. The text of the AI Act is clear in this respect[20].

---

[16] Council of Europe, Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (2019) Responsibility and AI. A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework. Rapporteur: Karen Yeung. https://rm. coe.int/responsability-and-ai-en/168097d9c5.

[17] The right to 'mental integrity' is protected in Article 3 of the Charter of Fundamental Rights of the European Union.

[18] See § 7 and § 7.1.

[19] The right to the protection of personal data is safeguarded by Reg. Eu 2016/67911, Reg. Eu 2018/172512 and by Dir. Eu 2016/680. Dir. 2002/58/EC additionally protects private life and the confidentiality of communications.

[20] According to *Recital* 9 of the AI Act: «The harmonised rules laid down in this Regulation should apply across sectors and, in line with the New Legislative Framework, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, protection of workers, and product safety, to which this Regulation is complementary». As envisioned in *Recital* 45 of the AI Act: «data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation». Under art. 2(7-9) «This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725 […] This Regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety».

On the basis of the dir. 2005/29/EC, for example, unfair commercial practices leading to economic or financial harm to consumers are forbidden under all circumstances, irrespective of whether they are put in place through AI systems or otherwise (see *Recital* 29 AIA).
Since AI is a data-dependent enterprise, privacy law is paramount in addressing the key emotional AI governance issues.
The intersections between the AI Act and the GDPR will be delved into further on[21], with special regard to art. 9, 22, and art. 35 of GDPR[22].
It is worth noting that the European legal framework counts several sets of rules that aim to protect individuals from the risk of manipulation, particularly in the digital realm (Parenzo, 2024).
Art. 26 (3) of the *Digital Services Act*, for instance, is crucial in this respect. It prohibits to exploit people's vulnerability through advertisements based on profiling using the particular categories of personal data referred to in ART. 9 of the Reg. EU 2016/679 (*breviter*: GDPR)[23]. Other existing provisions refer to 'dark patterns' (Kollmer and Eckhardt, 2023) and price personalization. Art. 25 of the DSA states that: «Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions». The main issue with this prohibition is that, according to paragraph 2, it shall not apply to practices covered by dir. 2005/29/EC or by reg. Eu 2016/679. Since is not clear whether exploiting emotions through AI emotional marketing techniques is to be considered an unfair commercial practice, is uncertain accordingly whether art. 25 DSA applies to it (De Mari Casareto dal Verme, 2023).
In addition, dir. 2019/2161/EU introduced in dir. 2011/83/EU the letter e-*bis*) to art. 6 whereby the consumer must be informed that the price is personalised based on an automated decision-making process (one could remark that consumers should be aware of why and how the price is personalised as well as of the extent of personalization).
Like the Data Protection Impact Assessment under art. 35 of the GDPR, according to art. 34 of the DSA, very large online platforms are under a duty to assess the systemic risks arising from the design (including algorithmic systems), operation, and use of services, taking into consideration «[…]any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in

[21] Especially in the last paragraph.

[22] According to art. 9 GDPR «Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited». Art. 22 GDPR provides for the data subject's right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. Art. 35 GDPR states that: «where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data» (DPIA).

[23] Moreover, art. 26 (1) of the DSA requires providers of online platforms that present advertisements on their interfaces to take steps to ensure that the recipients of the service can understand that the information constitutes an advertisement, identify the natural or legal person on whose behalf the advertisement is presented, and the parameters used to determine the recipient of the advertisement. Under art. 26(3) of Reg. Eu 2022/2065 «Online platform providers may not present advertisements to service recipients based on profiling, as defined in Article 4(4) of Regulation (EU) 2016/679, using the special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679)».

Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter […]». Once systemic risks have been identified «Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights» (art. 35.1 DSA).

Furthermore, in the context of online political advertising, art. 18 of the regulation EU 2024/900 prohibits targeting techniques and ad-delivery techniques involving profiling using special categories of personal data referred to in Reg. Eu 2016/679 and Reg. Eu 2018/1725. It is not possible to rely on the exceptions laid down in art. 9(2) of Regulation (EU) 2016/679 and art. 10(2) of Regulation (EU) 2018/1725 for using those techniques in the context of online political advertising. The use of targeting techniques and ad-delivery techniques involving the processing of personal data, other than special categories of personal data, is allowed only when it is based on personal data collected from the data subjects and with their explicit consent, provided separately for political advertising.

In summary, within the European legislative framework: data protection regulations impose stringent conditions on the collection and processing of personal data. European and national regulations offer robust protection to consumers, curbing manipulative practices in business-to-consumer transactions: consumer protection legislation safeguards against aggressive, unfair, and deceptive trade practices. Media and advertising laws establish clear prohibitions against false, misleading, deceptive, and covert advertising, including a specific ban on subliminal advertising (*see*, especially, the above-mentioned art. 26(3) of the DSA). Under contract law, coercion, misrepresentation, or fraud commonly constitute grounds for a contract to be annulled.

Within the European Union, the existing legislation addresses several aspects pertinent to the development and application of neurotechnologies, including regulations not only on data protection and artificial intelligence but also on medical device safety (Steindl E, 2024) and cybersecurity.

Overall, the legislation of the EU offers multilayered protection against the potential harms of emotional AI. Still, there are shortcomings. These loopholes will be further discussed below.

7. *The AI Act provisions regarding emotional AI: a brief review.*

Before reviewing the substantive provisions of the AI Act concerning emotional AI is interesting to consider that the EU legislator is aware that: «There are serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems are the limited reliability, the lack of specificity, and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons based on their biometric

data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons […]» (*Recital* 44).
Art. 2(6) clarifies that AI systems or AI models specifically developed and put into service for the sole purpose of scientific research and development are excluded from the scope of the AI Act (see also *Recital* 25).
The following article contains the definition of an emotion recognition system: «an AI system to identify or infer emotions or intentions of natural persons based on their biometric data» (art. 3 AIA). To properly interpret this provision, it is necessary to refer to *Recital* 18, according to which: «The notion of 'emotion recognition system' referred to in this Regulation should be defined as an AI system inferring to identify emotions or intentions of natural persons based on their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction, and amusement. It does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers to prevent accidents. This does also not include the mere detection of readily apparent expressions, gestures, or movements unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering».
As evident, the EU legislator only refers to emotion recognition techniques that are based on biometric data even if, as highlighted above, there are emotion scanning tools that are not based on the processing of biometric data. Not all systems capable of inferring emotions use physiological data that meet the high bar for identification required to be classified as biometric data. In such cases, providers could argue that their system is not subject to obligations under the AIA[24]. For this reason, it is open to debate whether, in the future, it would be useful to enlarge the definition of ERSs so as to comprise those systems that make inferences about emotions or states of mind based on physiological data or other data (*e.g.*, written tests or voice records) which are not biometric, provided that the definition (does not and) should not cover systems that detect purely physiological traits or behaviours, such as whether a bus driver is falling asleep or a man on an emergency services line is having a heart attack.
However, at the core of the regulation stands art. 5 (f), which expressly prohibits the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons.
Alongside this prohibition, the AI act introduces, in relation to any emotion recognition system, duties to inform.
As said before, the process of monitoring and coding emotions is part of a more general paradigm of personalization of advertisements, digital services, and products offered to users. The profiling, though, this time is based on human emotions and the user does not fully know the functions and purposes of the automated process.

[24] See Prohibit emotion recognition in the Artificial Intelligence Act, p. 2 ff.: paper drafted by Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 and IT-Pol, further supported by AlgorithmWatch, Fair Trials, the European Centre for non-profit Law (ECNL) and Panoptykon Foundation, following the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.

In this respect, art. 50, par. 3 of the AI Act plays a crucial role since it establishes «Transparency obligations for providers and deployers of certain AI systems» stating that: «Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data per Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in compliance with Union law».
The transparency obligation only concerns the operation of the IA whereas it is not extended to its specific purposes or manner of use. This choice is open to doubt.
Besides, is essential to highlight that based on ANNEX III, par. 1, lett. c) AI systems intended to be used for emotion recognition are among those high-risk AI systems referred to in art. 6(2): emotion recognition systems that are not expressly prohibited under the AI Act should be classified as high-risk (*Recital* 54).
A general picture of the provisions of the AI Act related to emotional AI wouldn't be complete without mentioning Art. 27, according to which: «Prior to deploying a high-risk AI system referred to in Article 6(2) into use, with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce…».
This crucial article, which provides for a fundamental rights impact assessment for high-risk AI systems (FRIA) must be coordinated with art. 35 of GDPR, which requires a data protection impact assessment (DPIA). This AI governance solution provided for by the AI Act foresees the overlap with preexisting provisions. FRIAs, though, do not need to be conducted for aspects covered under existing legislation. As such, if a DPIA and FRIA have an overlapping aspect, that aspect arguably needs only to be covered under DPIA[25].

7.1. *A critical analysis of emotional AI current regulation. Proposals.*

Among civil organizations there is a widespread view that European Union missed a chance in regulating emotional AI. A critical opinion asserts that "human-centric" risks becoming a buzzword when speaking of Emotional AI. Whether the AI Act is a gold standard and not primarily a concession to industry, serving police and private companies more than people is a matter of debate[26].
Despite the criticisms, this legislative act seems to contain useful elements as it introduces some substantive prohibitions. It clearly represents a compromise, trying to establish a delicate balance that does not excessively obstruct innovation and investment.
Overall, it is important to note that art. 5 (1) lett. a) prohibits the placing on the market, the putting into service, or the use of an AI system that deploys subliminal techniques

[25] See AI Governance in Practice Report 2024 of IAPP AI Governance Centre, June 2024, p. 31.

[26] EU's AI Act fails to set gold standard for human rights, Wednesday 3 April 2024, ARTICLE 19, Access Now, Bits of freedom Amnesty International, European Disability Forum, ProtectNotSurveil, AlgorithmWatch, European Central for Non-Profit-Law et al.

beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm.

The main issue with this provision is that it reveals that the AIA follows the same (traditional) approach to vulnerability of the UCPD. It considers vulnerability as originating from the characteristics of certain groups of people rather than from the structural dimension of AI technologies and the data-driven markets in which they are deployed (Galli, 2022).

To reinforce the protection of European citizens, one possible solution would be to include the deployment of emotion recognition systems for marketing or political microtargeting in the blacklist of unfair commercial practices contained in Annex I of the European Parliament and Council Directive 2005/29/EC. In fact, it is not clear, as noted above, whether exploiting emotions through AI emotional marketing techniques is to be considered an unfair commercial practice. The definition of aggressiveness, in particular, does not seem to involve the undue influence exercised on the irrational part of the brain (De Mari Casareto dal Verme, 2023).

There is a need for collective answers since enforcement in individual cases risks being ineffective in mitigating the harmful effects on society of certain deployments of emotional AI (Clifford, 2020). The massive scale of some practices may surpass the enforcement of individual rights (Valcke, Clifford and Dessers, 2021).

Given these considerations, another option would be the introduction under Art. 5 AIA of a clear ban on emotional AI for marketing purposes (Orlando, 2022). The exact meaning of "subliminal techniques" and "consciousness" under art. 5 (1) lett. a) is indeed far from clear and is uncertain to what extent practices such as 'digital nudging' or 'dark patterns' would fall under the prohibition contained therein.

The AI Act has been criticised also because it introduces a blanket exemption for all the AI systems developed or used solely for the purpose of national security, regardless of whether this is done by a public or private authority[27]. Disapproval rests on the assumption that exceptions should be on a case-by-case basis; national security should not become a digital rights-free zone[28]. In this view, the partial ban of ERSs contains dangerous loopholes and entails a risk: the fact that ERSs are prohibited in the workplace and education settings but are still allowed for other purposes such as law enforcement and border control could be interpreted as a signal that EU is likely to test these intrusive AI systems against the most marginalised and vulnerable people of our society, where the risks of the deployment of these systems are potentially the gravest[29].

---

[27] According to art. 2 (3) of AI Act: «This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities».

[28] EU's AI Act fails to set gold standard for human rights, Wednesday 3 April 2024, ARTICLE 19, Access Now, Bits of freedom Amnesty International, European Disability Forum, ProtectNotSurveil, AlgorithmWatch, European Central for Non-Protfit-Law et al.

[29] EU's AI Act fails to set gold standard for human rights, cit.

A partial ban on Emotional AI, according to this opinion, may have a negative impact since it could be perceived as a sign that mind-reading is allowed in the EU and this could set a dangerous precedent in a global scenario in which the EU aims to act and be seen as a game changer.
A very large opinion, as previously noted, is in favour of a comprehensive ban against any use of AI which is held to be not compatible with fundamental human rights and freedoms. Civil society organizations like *Article 19* wish the introduction of a general prohibition on emotion recognition. A study of January 2022 commissioned by the AIDA committee of the European Parliament, entitled *Identification and assessment of existing and draft EU legislation in the digital field*, stated that: «Emotion recognition systems powered by AI may have highly undesired discriminatory and dignity consequences, manipulative effects, and risk impact. Therefore, general prohibition might be an option to consider»[30].
The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), in their Joint Opinion on the AI Act, affirmed that the «use of AI to infer emotions of a natural person is highly undesirable and should be prohibited» further noting that exceptions should be made for «certain well-specified use-cases, namely for health or research purposes (*e.g.*, patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation»[31].
The main issue is that these systems are quite controversial and have been shown to be based on questionable scientific premises. For this reason, they should not be allowed in sensitive domains unless subject to rigorous clinical validation and the highest level of regulatory scrutiny[32]. Specifically, the deployment of ERSs for marketing should be prohibited. Emotional AI should be rather confined to the field of medical research and health care for diagnosis, treatment, and prevention of diseases (Orlando S, 2022). Even if the partial ban of ERSs is important, since it makes clear that the EU is prompt to draw red lines against harmful uses of AI, we should carefully reconsider the risks and opportunities of the datafication of emotions.

8. *Further shortcomings of the European legislative framework. Should the EU recognise a set of neurorights?*

Further shortcomings of the EU legal framework can be identified in the lack of specific regulation concerning mental data protection and consumer neuro-technologies. These are indeed specifically regulated only through soft law tools[33] which appear unable to

[30] Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf.
[31] EDPB-GEPD Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021 (35).
[32] See Prohibit emotion recognition in the Artificial Intelligence Act, p. 2: paper drafted by Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 and IT-Pol, further supported by AlgorithmWatch, Fair Trials, the European Centre for non-profit Law (ECNL) and Panoptykon Foundation, following the Joint Civil Society Statement An EU Artificial Intelligence Act for Fundamental Rights, signed by 123 organisations in November 2021.
[33] See OECD (Organisation for Economic Cooperation and Development) Recommendation on Responsible Innovation in Neurotechnology, adopted in 2019; The Ethics of Neurotechnology: UNESCO appoints international

meaningfully address the human rights challenges posed by these advanced technologies. There are protection gaps in non-medical contexts.

Policymakers need to ensure adequate protection of mental information and to adopt a more active approach in shaping a solid governance framework for emotional AI, providing specific safeguards which can prevent the accumulation and monopolisation by a limited number of private companies of data which refer to mental features of the individuals (emotions, intentions…)[34].

Given the *vacuum* of regulation concerning (non-invasive) neurotechnology in nearly every country, some scholars claim for the advancement of neuro-rights.

The Morningside Group identified five key neuro-rights: (1) the right to mental privacy, or the ability to keep mental activity protected against disclosure; (2) the right to identity, or the ability to control one's mental integrity and sense of self; (3) the right to agency, or the freedom of thought and free will to choose one's actions; (4) the right to fair access to mental augmentation, or the ability to ensure that the benefits of improvements to sensory and mental capacity through neurotechnology are distributed justly in the population and (5) the right to protection from algorithmic bias or the ability to ensure that technologies do not insert prejudices[35]. In particular, the Morningside Group coordinated by Professor Rafael Yuste of Columbia University suggests adding clauses protecting neuro rights to International Treaties such as the 1948 Universal Declaration of Human Rights[36].

Ienca and Andorno instead offer an alternative set of neuro rights: the right to cognitive liberty, the right to mental privacy, the right to mental integrity, and the right to psychological continuity (Ienca and Andorno, 2017).

These proposals have attracted criticism[37]. Some argue we need new laws not new rights (Ligthart, Bublitz and Alegre, 2023) and that neuro-specific mental privacy rights would be incomplete (Brown, 2024). Information about mental states (emotions, intentions, etc.) is indeed inferable by means other than neurotechnologies.

Some advocate the creation of an independent body to monitor developments in this domain (Wexler and Reiner, 2019).

A plausible solution would be to extensively interpret existing provisions to guide the development of European and national legal and regulatory frameworks: especially art. 8 ECHR, which provides for the "right to respect for private life"; Art. 9 ECHR, which provides "the right to freedom of thought"; art. 8 CFREU which provides for the "right to the protection of personal data"; art. 3 and art. 10 of CFREU, which respectively refer to "the right to mental integrity" and the "right to freedom of thought".

At the national level, several countries in the world have advanced or are advancing legislation and declarations aligned with the neuro rights framework. In 2021, Chile and

---

expert group to prepare a new global standard, UNESCO, 22 April 2024; León Declaration on European neurotechnology: a human focused and rights' oriented approach, Spanish Presidency of the Council of the EU, 24 October 2023; Charte de développement responsable des neurotechnologies, Ministère de l'Enseignement supérieur et de la Recherche, 17 November 2022.

[34] From vision to reality. Promises and risks of Brain-Computer Interfaces, cit., p. 20.

[35] The Neurorights Foundation, 2023; available from: https://neurorightsfoundation.org/.

[36] For more insights, see Errigo MC (2020) Neuroscienze, tecnologia e diritti: problemi nuovi e ipotesi di tutela Dirittifondamentali.it 3:215-245.

[37] For an overview of the criticisms see Brown C.M.L. (2024) Neurorights, Mental Privacy, and Mind Reading. Neuroethics 17 (2): 34 available at: https://doi.org/10.1007/s12152-024-09568-z.

Spain were pioneers in adopting stringent regulations for neurotechnology: Spain introduced its Charter on Digital Rights, which addresses "digital rights in the use of neurotechnologies" and emphasizes mental autonomy, privacy, and non-discrimination. Later that year, Chile amended its Constitution to safeguard brain data, mandating that such data be regulated and processed by a government agency. This amendment, which was unanimously approved by both chambers of Chile's Congress, recognizes "brain activity and the information derived from it" as a fundamental right. Additionally, the Chilean Senate passed a neuroprotection bill. In Brazil, the State of Rio Grande do Sul recently enacted legislation to protect brain activity and data. Uruguay has introduced a neuro rights bill in the Chamber of Deputies, and in the United States, Colorado, Minnesota, and California are developing state laws to protect neural data (Genser, Damianos and Yuste, 2024).

The General Assembly of the State of Colorado has just enacted a bill that expands the definition of "sensitive data" to include "biological data" and "neural data".

The data the brain produces is indeed unlike any other data enabling unique forms of insight into the individual and reflecting mental processing associated with thoughts, moods, feelings, and personality (Hallinan et al, 2014). Neural data is capable of revealing enormously sensitive information about the people from whom it was collected, including identifiable information about their mental health, physical health, and cognitive processing. Currently not specifically protected by regulation, neural data is just as sensitive as protected medical data. Neural data could afford companies unprecedented levels of insight into the cognitive states and inner worlds of consumers. Such information vests commercial entities with alarming knowledge and power over intimate dimensions of user's mental and social lives (Kreitmair, 2019).

In the coming years, neural data databases will function similarly to how genetic and biometric databases function. Hence, some claim that the regulation of genetic data may serve as templates for the regulation of neurodata (Hallinan et al, 2014).

As previously discussed, studies have found that when paired with generative AI, brain scans from non-invasive neurotechnologies allowed for the decoding of language, emotions, and imagery with high levels of accuracy (Minielly et al, 2020).

The human brain carries terabytes of valuable data. In the world of neuroscience, big data is truly, epically big (Landhuis, 2017).

In the future, more investments will result in improvements to the technical capabilities of both neurotechnology and multimodal digital technologies, affording increased resolution of brain scans and larger datasets of mental data being collected, while generative artificial intelligence will accelerate the ability to accurately decode these data. Since these developments have the aforesaid significant implications for mental privacy, we should put additional pressure on lawmakers.

Within the European Union, today, there is enormous ambiguity regarding whether neural data are to be considered a form of personal data: it is not clear whether data collected through neurotechnologies can be *per se* qualified as "personal data" under art. 4(1) of GDPR (even without any other identifier). In this respect, it can be reasonably assessed

that neural data and brain data are personal if, in combination with other data, allow to single out a data subject[38].
The subsequent legal issue to be addressed is obviously whether neural data, brain data, and, more in general, data concerning emotional states can or should be comprised within the special categories of personal data referred to in Art. 9 GDPR when they do not concern the health of a data subject (Montinaro, 2024).

8.1. *Calling for "mental data" protection.*

A preliminary review suggests that current legal standards, in the European Union legal framework, may require further interpretation or amendment to ensure that mental data (including neural data) fall unambiguously within the highest standard of legal protections: *i.e.*, within the protection of art. 9 GDPR[39].
To bolster human rights protection, the European legislator should consider the idea of introducing a new special category of personal data among those referred to in art. 9 GDPR: the "mental data" (*i.e.*, data referring to mental features of an individual) which should include "neural data" (*i.e.*, information concerning the activity of an individual's central nervous system or peripheral nervous systems, including the brain and spinal cord, and that can be processed by or with the assistance of a device). Mental data indeed entails all data about human brain structure, activity, and function, from neurobiological metrics, like EEG and fMRI, to non-neural data such as smartphone usage patterns (Ienca et al. 2022).
In the meantime, to regulate the process of mental data we could apply existing provisions on medical data either by analogy or extensively interpreting the concept of "mental health" which could be broadened so to include also any form of cognitive processes and affective states of the data subjects (Ienca and Malgieri, 2022). Emotions are not less "sensitive" than information about an individual's health. Mental data touches the *forum internum*. For this reason, it is probably even more "sensitive" than the data expressly mentioned in Art. 9 of GDPR.
Neural data in particular is electrical in nature and therefore is not necessarily covered by standard definitions of biometric data. It is even more difficult to qualify as sensitive data the emotion-related data inferred from written tests or voice records. For this reason, it would be valuable if the GDPR could specify that even indirect inferences affecting human emotions could be qualified as a "special category" of personal data. It could be reasonable to affirm that art. 9 (1) GDPR comes into application when the recognition of emotions based on the physical, physiological, and behavioral characteristics of the natural persons has the purpose of inferencing 'sensitive' data relating to an identifiable or identified individual (Montinaro, 2024).

---

[38] On the concept of personal data see Gruppo di lavoro art. 29, Opinion n. 4/2007 on the concept of personal data, WP136, (20.06.2007): «in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group». Actually, the jurisprudence of the Court of Justice of the European Union has gradually expanded the concept of personal data. For an overview of the most relevant case law on the matter see Sposini L (2024), Neuromarketing and Eye-Tracking Technologies Under the European Framework: Towards the GDPR and Beyond. Journal of Consumer Policy 47:330 ff.

[39] To which also the aforementioned art. 18 of the reg. EU 2024/900 on the transparency and targeting of political advertisement expressly refers.

As clarified above, information about emotions can be derived from brain observation but can also be inferred by data analytics based on retrospective data mining, pattern recognition, and aggregation of various data both physiological and non-physiological (Ienca and Malgieri, 2022).

Moreover, is to be remarked that legal consent is not required to capture data about emotions that are not personal: *i.e.*, capable of (directly or indirectly) identifying or singling out a person. The GDPR does not apply to personal data that has been adequately anonymized to ensure the individual can no longer be identified. But data that may be anonymous today could turn out to not be anonymous tomorrow, first of all, due to technological progress (Hallinan et al, 2014). There are privacy implications even when emotional AI practices use non-personally identifying data about people to infer human emotions (McStay, 2020).

In summary, there are normative gaps mostly because: (*i*) the list contained in Art. 9 GDPR is not comprehensive enough since it does not include mental data: the GDPR does not protect under the strict regime of Art. 9 personal data which are not related to the sensitive areas of health, sexuality, religious or political beliefs, etc. Emotions and moods would often be qualified as non-sensitive data, falling under the general regime set in Art. 6 of the GDPR (Ienca and Malgieri, 2022); (*ii*) the individual participation rights approach in the EU data protection law is inadequate: the concrete operation of individual rights granted by GDPR is sometimes difficult since we cannot understand which risks are involved in our privacy choices, especially with AI inferences (Cofone, 2023). The EU legislation does not address many of the modern data-processing initiatives involving large data sets since it either refers to personal data, which are strictly regulated, or to non-personal data, which are intentionally left unregulated. Whereas data-driven applications using Big Data, Artificial Intelligence and profiling techniques often do not rely on personal data, but make use of general data, statistical information and group profiles (Taylor, Floridi and van Der Sloot, 2017)[40]. We are underestimating the risks involved in the process of anonymised personal data and still adopting an anthropocentric and individualistic approach (Floridi, 2014).

New technologies and powerful analytics allow for the collection and analysis of large amounts of data that enable few gatekeepers of knowledge[41] to identify patterns in the behaviour of groups, communities, and even entire countries, extracting predictive inferences. The GDPR instead embraces an atomistic approach, which shows limits in the context of mass predictive analysis. It fails to take into account the collective dimension of data protection. Whereas, it would be important (*i*) to combine individual remedies with collective remedies and (*ii*) to recognise the role of entities representing collective interests since data subjects are often unable to negotiate their information and are unaware of the potential underlying prejudices (Mantelero, 2016). Changes in

[40] Van der Sloot B (2021) The Quality of Life: Protecting Non-personal Interests and Non-personal Data in the Age of Big Data. European Review of Private Law 29(5): 757-784 interestingly argues that the ECtHR "quality of life doctrine" could be used to broaden the scope of art. 8 ECHR: governments should have an obligation to inform citizens about the fact that data-driven applications might impact the quality of their lives, even when no personal data would be gathered.

[41] Control over information deriving from Big Data is not accessible to everyone, mainly because it is based on expensive technologies and specific human skills. For this reason, governments and big business are in the most favourable position to benefit from Big Data. See Mantelero A (2014) Social Control, Transparency, and Participation in the Big Data World. Journal of Internet Law April:23.

individual-centered privacy paradigm appear to be necessary since the main issues in the Big Data era, with the expansion of the Internet of Things, transcend individuals. We need to protect nonpersonal data and grant a bigger role for representative and collective actions (van der Sloot and van Schendel, 2021).
In order to protect the right to privacy some called for a completely different construction of the law which shields the individual from external interference and defines boundaries to protect the *forum internum* (Hallinan et al, 2014).
Notwithstanding the shortcomings, the GDPR still offers important safeguards: under EU data protection rules, according to the purpose limitation principle, the process of brain data or neural data collected for a specified, explicit, and legitimate purpose such as, for example, health self-monitoring could not be processed for commercial purposes; sensitive neural or brain data would be lawfully processed only under one of the conditions set by art. 9 (2) of the GDPR.
It could also be argued that the evaluation of the emotional state of a person for marketing purposes constitutes an automated processing pursuant to Art. 22 GDPR, when it implies a significant impact on the rights (including fundamental rights) of the data subject[42]. Moreover, under art. 35 GDPR processing of mental data that violates fundamental rights could be prevented in advance (Montinaro, 2024). The risk assessment obligations represent a more effective tool than information requirements since they mitigate harm upstream before products and services are placed on the market. The preventive approach based on *ex ante* risk assessments appears to be more efficient than *ex post* legal actions[43]. The main issue with this tool is that it mainly relies on self-assessment (Fassiaux, 2023).
To enhance the regulatory framework, an option would be to modify Art. 5 of the AIA to include among the AI systems subject to the prohibitions envisioned therein AI profiling systems for marketing purposes that process special categories of personal data under Art. 9 (1) GDPR (Orlando, 2022), including mental data.
In conclusion, even if the EU legislation offers safeguards against the potential harms of emotional AI, novel measures should strengthen the protection of mental privacy[44] and make sure that governments and companies properly safeguard not only neural data but any personal data that might be representative of mental features (Brown, 2024) however collected (Ienca, 2017). Despite the hype surrounding neuro rights, the necessity for stringent regulations governing emotional AI and neurotechnology advancements – especially their impact on agency, free will, consent, privacy, and data protection – remains crucial (Gilbert and Russo, 2024).
In light of possible data leaks, there is a need for closer monitoring of the private sector's use of brain data (Huang et al, 2024).

---

[42] The effectiveness of this provision is a matter of debate. Indeed, is uncertain whether it establishes a right or a prohibition. Secondly, the meaning of "legal effects" and "significantly affects" is not clear. In any case, is easy for the processor to use one of the exceptions envisioned in paragraph 2. See De Mari Casareto dal Verme T (2023), Artificial Intelligence, Neuroscience and Emotional Data. What Role for Private Autonomy in the Digital Market? Erasmus Law Review 3:92-93.

[43] Moreover, it contributes to address the risks of hidden forms of data processing. See Mantelero A (2014) Social Control, Transparency, and Participation in the Big Data World. Journal of Internet Law April:23–29.

[44] In order to protect mental freedom Bublitz and Merkel suggested to introduce a new criminal offence. See Bublitz JC, Merkel R (2014) Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. Crime Law and Philos 8:51-77.

More efforts in educating the public are also necessary since there is an evident gap in consumers' understanding of their mental data. Consumers should be able to better comprehend the implications of data that neurotechnologies and other mind-reading technologies can capture (Huang et al, 2024).
To protect the privacy of brain data, we should increase 'data literacy' in society (Kellmeyer, 2021).
Moreover, public EU legislation on consumers' protection should question its premises[45] and self-determination should be secured 'per se' irrespective of situations resulting in misperceptions and/or mistakes (De Mari Casareto dal Verme, 2023).
The current EU legal framework appears not fully capable of adequately accommodating the most recent technological developments. Neither the GDPR nor the DSA nor the AIA seem sufficient on their own. Nonetheless, the existing legislation offers several meaningful tools. Academics should therefore not only monitor the implementation of AI regulation and increase pressure on lawmakers but also promote a better coordination of existing European legislative acts (Orlando, 2022) especially of the Artificial Intelligence Act with the Digital Services Act (Tuccari, 2024) and the GDPR. It is fundamental to recalibrate legal safeguards and to ponder the adoption of a more holistic approach[46].
In light of the threats brought about by the deployment of emotional AI within the context of the data-driven economy, more studies are pivotal. Academics must contribute to shaping a regulatory framework that aims at preventing the targeting of cognitive or emotional weakness and governs the use of emotional AI in shaping public opinion to safeguard electoral integrity and democracy (Simchon et al, 2024). We need to ensure effective protection against manipulative emotional profiling for business or political goals.
Scholars should further explore interpretative solutions to fill in the gaps of the existing legislation, without relying only on future reforms. Research shall continue to further deeper investigate how to foster a regulatory environment that, in order to boost societal and economic progress, finds a balance between the promotion of innovation and defence of cognitive liberty and human dignity, advancing a modern approach to privacy and data protection to properly deal with the ongoing Big Data revolution and the rise of new forms of human vulnerability in the era of digital capitalism.

---

[45] In the classical economic model, the consumer is a rational agent. Cognitive psychology, though, has shown that most decisions are taken with the irrational part of the brain. The rational choice model is utopic. Consumers are subject to cognitive biases and emotions are one of the main factors determining economic choices. See in particular Kahneman D (2011) Thinking, fast and slow, Farrar, Straus and Giroux; Kahneman D and Tversky A (eds) Choices, Values, and Frames, Cambridge University Press, 2000; Sunstein CR (2000) Behavioral law and economics, Cambridge University Press. On the concept of "bounded rationality" see Simon A (1972) Theories of Bounded Rationality, in: Decision and Organization: A Volume in Honor of Jacob Marschak, C.B. McGuire and Roy Radner (eds), Minneapolis, University of Minnesota Press pp 161-176; Simon HA (1979) From substantive to procedural rationality, in: Philosophy and Economic Theory, Frank Hahn and Martin Hollis (eds), Oxford, Oxford University Press, pp. 65-85; Simon, Herbert A (1979) Rational Decision Making in Business Organizations. American Economic Review 69:493- 514; Simon HA (1987) Bounded Rationality. In Eatwell J, Milgate M and Newman P (eds) The New Palgrave - Utility and Probability, New York, W.W. Norton pp. 15-18; Zamir E and Teichman D (2018) Behavioral law and economics. Oxford University Press; Gerd G (2020) What is bounded rationality? Routledge.

[46] See Mantelero A (2022) Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI Springer, who advocates for an assessment model that overcomes the limitations of the current assessment models, considering the impact of data processing on fundamental rights and collective social and ethical values (Human Rights, Ethical and Social Impact Assessment-HRESIA).

References

AI Now Institute. (2018). *AI now report*. New York University. Retrieved 13 Apr 2022, from https://ainowinstitute.org/AI_Now_2018_Report.pdf

Alegre S (2021). Protecting freedom of thought in the digital age. Policy Brief No. 165. Centre for International Governance Innovation. Retrieved 13 Apr 2022, from https://www.cigionline.org/publications/protecting-free dom-of- thought- in- the- digital-age/

Bakir V, McStay A (2020) Empathic Media, Emotional AI, and the Optimization of Disinformation. In Boler M and Davis E (eds), Affective Politics of Digital Media (Routledge) p 263

Bakir V, McStay A (2022) Profiling, Targeting and the Increasing Optimisation of Emotional Life. In: Optimising Emotions, Incubating Falsehoods. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13551-4_6

Barrett L (2006) Are Emotions Natural Kinds? Perspectives on Psychological Science 1(1): 28-58 https://doi.org/10.1111/j.1745-6916.2006.0000

Barrett LF, Adolphs R, Marsella S, Martinez AM, Pollak SD (2019) Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. Psychological Science in the Public Interest 20(1): 1-68

Bartlett M, Littlewort G, Vural E, Lee K, Cetin M, Ercil A et al. (2008) Data mining spontaneous facial behavior with automatic expression coding. In Esposito et al (eds), Verbal and Nonverbal Features of Human-Human and Human-Machine Interaction, Springer, Berlin, Heidelberg p 1-20

Bartlett M, Hager JC, Ekman P, Sejnowski TJ (1999) Measuring facial expressions by computer image analysis. Psychophysiology 36(2): 253–263

Bartlett M, Littlewort G, Frank MG, Lainscsek C, Fasel IR, Movellan JR et al. (2006) Automatic recognition of facial actions in spontaneous expressions. J. Multimed. 1(6): 22–35

Brown CML (2024) Neurorights, Mental Privacy, and Mind Reading. Neuroethics 17 (2):34

Bublitz JC (2013) My Mind Is Mine!? Cognitive Liberty as a Legal Concept. In Hildt E, Franke AG (eds), Cognitive Enhancement: An Interdisciplinary Perspective, Springer, Netherlands

Bublitz JC, Merkel R (2014) Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. Crime Law and Philos 8:51-77

Burr C, Cristianini N (2019) Can Machines Read Our Minds? Minds and Machines 29:463

Burr C, Cristianini N, Ladyman J (2018) An Analysis of the Interaction between Intelligent Software Agents and Human Users. Minds and Machines 28:735–774

Bygrave LA (2020) Article 22. Automated Individual Decision-making, Including Profiling. In Kuner C, Bygrave LA and Docksey C (eds.), The EU General Data Protection Regulation (GDPR): A Commentary

Clifford D (2020), CitizenConsumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side? In Edwards L, Harbinja E, Shaffer B(eds) Future Law: Emerging Technology, Regulation and Ethics, Edinburgh University Press

Clifford D, The Legal Limits to the Monetisation of Online Emotions (PhD thesis, KU Leuven, Faculty of Law June 2019) p 110

Cofone I (2023) The Privacy Fallacy, Oxford University Press

Council of Europe, Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT) (2019) Responsibility and AI. A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework. Rapporteur: Yeung k. https://rm. coe.int/responsibility-and-ai-en/168097d9c5

Crivelli C, Carrera P, Fernández-Dols JM (2015) Are smiles a sign of happiness? Spontaneous expressions of judo winners. Evol. Hum. Behav 36: 52–58

De Mari Casareto dal Verme T (2023) Artificial Intelligence, Neuroscience and Emotional Data. What Role for Private Autonomy in the Digital Market? Erasmus Law Review 3:83-97 doi: 10.5553/ELR.000257

Dibeklioglu H., Salah AA, Gevers T (2015) Recognition of genuine smiles. IEEE Trans. Multimed. 17: 279–294. doi: 10.1109/TMM.2015.2394777

Du S, Tao Y, Martinez AM (2014) Compound facial expressions of emotion. Proceedings of the National Academy of Sciences of the USA, 111(15):1–9

Ekman P and Friesen WV (1978) Facial Action Coding System: A Technique for the Measurement of Facial Movement. Consulting Psychologists Press, Palo Alto, CA. https://doi.org/10.1037/t27734-000

Ekman P, Keltner D (1997) Universal facial expressions of emotion. In Nonverbal Communication: Where Nature Meets Culture, Segerstrale U, Molnar P (eds): California Mental Health Research Digest, Francisco, CA:27–46

European Parliament (2009) Science and Technology Options Assessment. Human Enhancement Study

Farahany N (2023), The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology, St. Martin's Press

Fassiaux S (2023) Preserving consumer autonomy through European Union regulation of artificial intelligence: A long-term approach. European Journal of Risk Regulation 14:710-730. https:// doi. org/ 10.1017/ err. 2023. 58.

Feldman D (1999) Human Dignity as a Legal Value, Public Law 4:688

Galli F (2022) Algorithmic marketing and EU law on unfair commercial practices. Rethinking consumer protection with AI. Cham: Springer

Genser J, Damianos S, Yuste R (2024), Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies

Goering S et al (2021) Recommendations for Responsible Development and Application of Neurotechnologies. Neuroethics 14:365-386, https://doi.org/10.1007/s12152-021-09468-6

Hallinan D, Schütz P, Friedewald M and De Hert P (2014) Neurodata and neuroprivacy: Data protection outdated? Surveill Soc 12 (1):55–72

Haselager P (2013) Did I Do That? Brain–Computer Interfacing and the Sense of Agency. Minds and Machines 23 (3):405-418

Huang et al (2024) U.S. public perceptions of the sensitivity of brain data. Journal of Law and the Biosciences 11(1):1–20 https://doi.org/10.1093/jlb/lsad032

Ienca M (2015) Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. Bioethica Forum 8(2): 51-53

Ienca M (2017) The Right to Cognitive Liberty, Scientific American, 317 (2):10

Ienca M (2019) Brain-Machine interfacing: Reflections on neurotechnology and neurorights Notizie di Politeia 33 (133):52-62

Ienca M, Andorno R (2017) Towards new human rights in the age of neuroscience and neurotechnology. Life Sci Soc Policy 13(1):5

Ienca M, Fins JJ, Jox RJ, Jotterand F, Voeneky S, Andorno R, Ball T, Castelluccia C, Chavarriaga R, Chneiweiss H and Ferretti A (2022) Towards a governance framework for brain data. Neuroethics 15:20

Ienca M, Haselager P (2016) Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics and Information Technology 18 (2):117-129

Ienca M, Haselager P, Emanuel EJ (2018) Brain leaks and consumer neurotechnology. Nature Biotechnology 36:805-810

Ienca M, Malgieri G (2022) Mental data protection and the GDPR, Journal of Law and the Biosciences 9 (1) https://doi.org/10.1093/jlb/lsac006

Floridi L (2014) Open Data, Data Protection, and Group Privacy. Philos. Technol. 27:1-3, https://doi.org/10.1007/s13347-014-0157-8

Gerd G (2020) What is bounded rationality? Routledge

Gilbert F, Russo I (2024) Mind-reading in AI and neurotechnology: evaluating claims, hype, and ethical implications for neurorights. AI Ethics 4:855-872 https://doi.org/10.1007/s43681-024-00514-6

Kahneman D (2011) Thinking, fast and slow, Farrar, Straus and Giroux

Kahneman D and Tversky A (eds) Choices, Values, and Frames, Cambridge University Press, 2000

Kellmeyer P (2021), Big Brain Data: On the Responsible Use of Brain Data from Clinical and ConsumerDirected Neurotechnological Devices. Neuroethics 14:83–98 https://link.springer.com/content/ pdf/10.1007/s12152-018-9371-x.pdf

Kollmer T, Eckhardt A (2023) Dark Patterns. Bus Inf Syst Eng 65:201-208 https://doi.org/10.1007/s12599-022-00783-7

Krausová A (2014) Legal Aspects of Brain-Computer Interfaces. Masaryk Univ. J. of Law and Technol. 8(2): 199-208

Kreitmair KV (2019) Dimensions of Ethical Direct-to-Consumer Neurotechnologies, AJOB Neuroscience 10 (4): 152–166

Landhuis E (2017) Neuroscience: Big brain, big data. Nature 541[7638]: 559–561

LeCun Y, Bengio Y, Hinton G (2015) Deep Learning. Nature 521: 436-444

Ligthart S, Bublitz C, Alegre S (2023) Neurotechnology: We need new laws, not new rights. Nature 620 (7976): 950

Mantelero A (2014) Social Control, Transparency, and Participation in the Big Data World. Journal of Internet Law April:23–29

Mantelero A (2016) Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer Law & Security Review 32 (2): 238-255

Mantelero A (2022) Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI Springer

Matz SC, Kosinski M, Nave G, Stillwell DJ (2017) Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the National Academy of Sciences, 114(48):12714–12719

McStay A (2016) Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (the Case for Intimacy) BD&S 3(1):3–6

McStay, A (2018) Emotional AI: The Rise of Empathic Media. London: Sage

McStay A (2020) Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy, Big Data & Society 7(1)

McStay A (2023) Automating Empathy: Decoding Technologies that Gauge Intimate Life. Oxford University Press

Minielly N, Hrincu V, Illes J (2020) Privacy Challenges to the Democratization of Brain Data, iScience 23 [101134] https://doi.org/10.1016/j.isci.2020.101134

Mollo A (2021) La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici European Journal of Privacy Law and Technology 1:199-210

Mollo A (2022) Neurorights. Una prospettiva di analisi interdisciplinare tra diritto e neuroscienze. In Orlando S and Capaldo G (eds), Annuario 2022. Osservatorio Giuridico sulla Innovazione digitale, Collana Materiali e documenti, Sapienza University Press p 191-215

A.A. Mollo (2023) Vulnerabilità e sostenibilità: primi spunti per uno studio dell'impatto sulle persone con disabilità e sulle future generazioni dei dispositivi [neuro]tecnologici. European Journal of Privacy Law & Technologies:28-49.

D'Aloia A, Errigo MC (eds) (2020) Neurosciences and Law: complicated crossings and new perspectives, Springer

Montinaro R (2024) Riconoscimento delle emozioni e marketing personalizzato. Persona e Mercato 3:847-894

OECD (Organisation for Economic Cooperation and Development) (2019) Recommendation on Responsible Innovation in Neurotechnology

Orlando S (2022) Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act. Persona e Mercato 3:346-367

Parenzo B (2024) Neuromarketing: un inventario di (spuntati) divieti contro il pericolo di una scelta manipolata. Persona e Mercato 2:539-558

Pasquale F (2015), The Black Box Society. The Secret Algorithms That Control Money and Information, Harvard University Press

Pasquale F (2024) Enforcing and Expanding Legal Protections for Vulnerable Subjects. In Crea C and De Franceschi A (eds) (2024) The New Shapes of Digital Vulnerability in European Private Law, Nomos doi.org/10.5771/9783748940913 p 21 ff

Pizzetti F (2017) A Proposal for a: 'Universal Declaration on Neuroscience and Human Rights'. Bioethical Voices (Newsletter of the UNSESCO Chair of Bioethics) 6 (10):3-6
Rhue L (2018) Racial Influence on Automated Perceptions of Emotions available at SSRN: https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765

Rhue L (2019) Affectively Mistaken? How Human Augmentation and Information Transparency Offset Algorithmic Failures in Emotion Recognition AI http://dx.doi.org/10.2139/ssrn.3492129

Rhue L (2018) Racial influence on automated perceptions of emotions SSRN, November https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765

Rude S, Gortner EM, Pennebaker J (2004) Language use of depressed and depression-vulnerable college students. Cognition and Emotion 18:1121–1133

Ruffolo U, Amidei A (2024) Diritto dell'Intelligenza Artificiale, vol. I, LUISS University Press p 193 ff

Russell J. A. (1994) Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies. Psychological Bulletin, 115(1):102-141 https://doi.org/10.1037/0033-2909.115.1.102

Simchon A, Edwards M, Lewandowsky S (2024) The persuasive effects of political microtargeting in the age of generative artificial intelligence, PNAS Nexus, 3(2):35 https://doi.org/10.1093/pnasnexus/pgae035

Simchon A, Sutton A, Edwards M, Lewandowsky S (2023) Online reading habits can reveal personality traits: towards detecting psychological microtargeting. PNAS Nexus. 2(6):gad191

Simon A (1972) Theories of Bounded Rationality. In: Decision and Organization: A Volume in Honor of Jacob Marschak, C.B. McGuire and Roy Radner (eds), Minneapolis, University of Minnesota Press pp 161-176

Simon A (1979) From substantive to procedural rationality, in: Philosophy and Economic Theory, Frank Hahn and Martin Hollis (eds), Oxford, Oxford University Press, pp. 65-85

Simon A (1979) Rational Decision Making in Business Organizations. American Economic Review 69:493- 514

Simon A (1987) Bounded Rationality. In: Eatwell J, Milgate M and Newman P (eds) The New Palgrave - Utility and Probability, New York, W.W. Norton pp. 15-18

Simoncini A, Longo E (2021), Fundamental Rights and the Rule of Law in the Algorithmic Society. In: Hans-W. Micklitz (ed) Constitutional Challenges in the Algorithmic Society, Cambridge University Press, p 35

Singla C, Singh S, Sharma P. et al. Emotion recognition for human–computer interaction using high-level descriptors. Sci Rep 14: 12122 (2024). https://doi.org/10.1038/s41598-024-59294-y

Stark L, Crawford K (2015) The Conservatism of Emoji: Work, Affect, and Communication'. Social Media+Society 1: 1-11

Stark L, Hutson J (2021) Physiognomic Artificial Intelligence (September 20, 2021). Fordham Intellectual Property, Media & Entertainment Law Journal, available at SSRN: https://ssrn.com/abstract=3927300 or http://dx.doi.org/10.2139/ssrn.3927300

Steindl E (2024) Consumer neuro devices within EU product safety law: Are we prepared for big tech ante portas? Computer Law and Security Review 52[105945] https://doi.org/10.1016/j.clsr.2024.105945

Sunstein CR (2000) Behavioral law and economics, Cambridge University Press

Taylor L, Floridi L, Van Der Sloot B (eds) (2017), Group Privacy, Springer

Thaler RH, Sunstein CR (2008) Nudge: Improving Decisions about Health, Wealth, and Happiness, Yale University Press

Tuccari E (2024) Neuromarketing: un'asistematica disciplina ... oltre il consenso? Persona e Mercato 2:511-537

UNESCO Recommendation the Ethics of AI, adopted on 23 Nov 2021

Valcke P, Clifford D, Dessers VK (2021) Constitutional Challenges in the Emotional AI Era. In Micklitz HW, Pollicino O, Reichman A, Simoncini A, Sartor G and De Gregorio G (eds), Constitutional Challenges in the Algorithmic Society, Cambridge University Press p 65 ff.

van der Sloot B (2021) The Quality of Life: Protecting Non-personal Interests and Non-personal Data in the Age of Big Data. European Review of Private Law 29(5):757-784

van der Sloot B, van Schendel S (2021) Procedural law for the data-driven society, Information & Communications Technology Law 30(3):304-332

Wexler A, Reiner PB (2019) Oversight of direct-to-consumer neurotechnologies. Science 363 [6424]: 234–235

Wright J. (2021) Suspect AI: Vibraimage, emotion recognition technology and algorithmic opacity. Science, Technology & Society, 1-20 https://doi.org/10.1177/09717218211003411

Yeung K (2017) 'Hypernudge': Big Data as a mode of regulation by design. Information, Communication & Society, 20(1):118-136 doi: 10.1080/1369118X.2016.1186713

Yuste R, Sara Goering S et al. (2017) Four Ethical Priorities for Neurotechnologies and AI, Nature 551:159-163, available at https://www.nature.com/articles/551159a

Yuste R, Genser J, Herrmann S (2021) It's Time for Neurorights: New Human Rights for the Age of Neurotechnology. Horizons 18: 154-55

Yuste R (2023) Advocating for neurodata privacy and neurotechnology regulation Nat Protoc. 18: 2869

Zamir E and Teichman D (2018) Behavioral law and economics. Oxford University Press

Ziegler K (2007) Introduction: Human Rights and Private Law − Privacy as Autonomy. In Ziegler K (ed) Human Rights and Private Law: Privacy as Autonomy, 1st ed., Hart Publishing, 2007

Zuboff S (2018) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs

Springer

To whom it may concern

Springer-Verlag, P.O. Box 10 52 80, 69042 Heidelberg, Germany

Springer-Verlag GmbH
Europaplatz 3
69115 Heidelberg, Germany
P.O. Box 10 52 80
69042 Heidelberg, Germany

T +49 6221 487 0
F +49 6221 487 8366
www.springer.com

Springer book project: 'Human Vulnerability in Interaction with AI in European Private Law'

To whom it may concern,

I hereby confirm that the book 'Human Vulnerability in Interaction with AI in European Private Law' edited by Claudia Amodio and Amalia Diurni will be published open access in 2025.

All chapters of this edited book, including the chapter **'Emotions Regognition Systems and Data Economy' authored by Claudia Confortini**, were subject to and approved by a strict anonymous peer review process of the highest international standards.

Best regards,

Anja Trautmann
Senior Editor Law