Journal of Consumer Policy
https://doi.org/10.1007/s10603-023-09559-2

ORIGINAL PAPER

Neuromarketing and Eye-Tracking Technologies Under the European Framework: Towards the GDPR and Beyond

L. Sposini[1]

Received: 11 April 2023 / Accepted: 21 December 2023

Abstract
The Regulation (EU) 2016/679 on the protection of natural persons regarding the processing of personal data (GDPR) is one of the key fundamental pieces of European legislation to protect human rights and freedoms. However, the development of AI systems that are capable of collecting and processing large amounts of data and predicting user habits and emotional states has affected traditional legal categories and tested their resilience. This paper assesses the limits of the current formulation of the GDPR which does not take expressly into account the category of inferred data as a special category of data. Furthermore, it questions whether the toolbox put in place by the GDPR is still effective in protecting data subjects from practices such as neuromarketing and eye-tracking systems. It shows that it is certainly the essential starting point, but that, on the other hand, cannot be spared criticism. For this, in the recent years, the European legislator has adopted further legislations including, in particular, the Digital Services Act (DSA) and the Artificial Intelligence Act (AIA). Although representing a step forward in protection against such technologies, they each have critical aspects that need to be considered.

Keywords Artificial Intelligence Act · Biometric data · Digital Services Act · Eye-tracking · GDPR · Inferred data · Neuromarketing

Introductory Remarks

The combination of eye-tracking techniques and sophisticated AI systems allows very accurate conclusions of biometric data processing and drawings and also gives further understanding about the likelihood of the subject developing diseases or disorders in the future.

The first part of the paper provides a brief overview of the most widely used neuromarketing techniques such as eye tracking, which uses algorithms and machine learning systems and thanks to this technology, identification of human cognition and emotional weaknesses has become possible to collect and process, resulting in building more effective marketing techniques to push consumers into buying certain products or services.

✉ L. Sposini
Ludovica.Sposini@santannapisa.it

[1] Sant'Anna School of Advanced Studies, Pisa, Italy

Published online: 26 January 2024

The second part analyses the current legal framework with a particular reference to the GDPR and the recent Digital Services Act. This section aims to examine whether this legal regime is capable of adequately addressing the various challenges that the AI systems underlying neuromarketing techniques pose to the European law. Among which, particularly relevant and to point out, is that despite the sensitivity of the inferred data, the GDPR currently does not explicitly consider the techniques written above. This omission raises several critical issues, particularly the risk that they could be used unlawfully, which endangers the fundamental rights of individuals.

Finally, this concludes that although the current regulatory framework undoubtedly provides effective protection for the consumer, there are nevertheless several problematic nodes that need more attention from the EU legislator and that stem from the impact of AI systems with traditional types of law. In view of this, then a further tool to help build a safe, reliable, and trustworthy system could be proposed for a regulation on the AI which would aim to achieve "The objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence (…) and ensures the protection of ethical principles" (AIA, 2021).

However, they should not be regarded as an end point, but only a beginning to build an effective European framework with the development of technologies that would reach into the most intimate sphere of individuals.

When the Human Mind Is (No Longer) a "Black Box": Overcoming the Traditional Economic Theory in Favour of the New Emotional Agent

According to the classical economic model, consumers were perfectly rational and therefore always able to adopt the most efficient choices (Bauman, 2010). Their weakness derived essentially from asymmetric information that could be rebalanced by imposing stringent information obligations on the trader.

Consequently, cognitive processes could not traditionally be studied, so much so that the mind was considered a "black box" (Hildebrandt & Oliver, 2000; Seaman, 2008, pp. 427–488) because it was impenetrable and inaccessible from the outside.

Since the 1970s, behavioural sciences and neuroscience have shown that the *homo oeconomicus* paradigm is only a utopia because it does not correspond to the real behaviour of the economic agent moving in the market (Kahneman, 2011; Sunstein, 2000; Tversky and Kahneman 1974, pp. 1124–1131). On the contrary, it suffers from "bounded rationality" and is subject to various cognitive *biases* (Gerd, 2020; Simon et al., 1992; Zamir and Teichman, 2018). In other words, man is influenced in his purchasing choices by contingent and environmental factors, life experiences, and, above all, emotions (Fabris, 2010). In particular, these new studies have clearly shown that human behaviour is not a linear and perfect process, but is a result of mostly irrational and automatic cognitive mechanisms which man is never fully aware of. This is the theory of the so-called "Messy Middle" (Protheroe & Rennie, 2020, pp. 1–98) according to which the brain is not to be understood as a unit but consists of two constantly interacting systems. In particular, "System 1" represents the intuitive part and is focused on receiving and processing information quickly, without any mental effort; "System 2," on the other hand, operates rationally by processing data received from the outside in a more complex manner and, therefore, needs more time to act.

Subsequently, when a decision is made in a short time or with little information available, the part of the brain that acts most quickly is the irrational one and when the time comes for the mind to be made up to finally purchase the particular product, alternating confusion and chaos becomes the case rather than a perfectly rational procedure.

Therefore, emotion, rather than rationality, is the main factor that drives economic agents to behave in a certain way rather than another, and this new awareness contributes to the birth of neuromarketing, a discipline aimed precisely at identifying and exploiting unconscious factors.

The Birth of Neuromarketing and the Case Study of Eye-Tracking Systems

Algorithms and Neurotechnologies for the Exploitation of Consumer Emotions

Since the 1990s, thanks to technological development, building systems capable of studying emotions and the human unconscious with greater accuracy and precision has been made possible.

This new area of research was first defined by the well-known Professor Ale Smidts under the name "Neuromarketing" (Lee et al., 2007, pp. 199–204; Smidts, 2002) as an interdisciplinary subject combining neuroscience, engineering, and behavioural psychology and aiming to build AI systems capable of detection, extrapolation, and the processing of uncontrollable psychological factors to study, predict, and guide the behaviour of individuals (Arthmann & Li, 2017, pp. 1–10; McStay, 2018, pp. 60–61).[1]

The sector in which this discipline is most widely used is in marketing, where companies develop neurotechnologies to identify the factors that significantly influence consumers' purchasing decisions and, therefore, creating more effective marketing techniques based on these findings (Wilson et al., 2008, pp. 389–404).[2]

What Lies Beneath the Persuasive Power of Biotechnologies at the Heart of Neuromarketing: User Profiling and Algorithm Processing

The highly persuasive power of neuromarketing, thence, lies in its ability to exploit individual biases and emotions to push recipients to behave in a certain way. These marketing practices are based on the so-called "profiling" of users using algorithms to extrapolate and process a large amount of data. The peculiarity of these algorithms—and what makes them particularly efficient—lies in their ability to collect not only the information that users provide with their explicitly granted consent but also that derived from their physical and emotional reactions to a certain sensory stimulus as well as the activity they perform while surfing online.

[1] Arthmann and Li refer to Microsoft's Cognitive Service emotion recognition, which provides insights not only into what is available today but also into wider ranging opportunities to harness both verbal and non-verbal communications through semantic analysis as well as emotion recognition through video.

[2] They acknowledge that "When a consumer purchases a product based on a decision in which marketing stimuli unrelated to product characteristics cause affective neural systems to override cognitive processes, the final purchase outcome may not always be in the best interest of the consumer."

Profiling is defined by the Data Protection Regulation (GDPR 2016) as "Any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (Art. 2, GDPR). According to this definition, algorithm processes all personal data collected to analyse consumer behaviour and preferences and, in doing so, creates digital profiles of consumers.

At this point, it becomes extremely easy for companies to devise marketing strategies that are much more effective than traditional ones, precisely because they are tailored to consumers' preferences and behaviour. We speak, not by chance, of "customization" of content, i.e., the "strategic creation, modification and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors." (Bol et al., 2018, pp. 370–373).

Profiling is not a practice to be censored per se, because it brings innumerable benefits to both sides of the market. On the one hand, it allows companies to know more about the products that consumers want and to adapt them accordingly to their needs. However, consumers also gain the advantage of wasting less time in online research because they will only receive advertising of what the algorithm has already selected for them.

One of the most useful technologies—and, for this reason, most developed by the industry—is the so-called "eye tracking," which makes it possible to study the reactions and changes of the human eye when faced with a certain auditory or visual stimulus (Lee et al., 2018, pp. 1–49).

Let us take a brief look at how it works and why the data derived from studying the human eye is correlated.

When a Glance Is Worth More than a Thousand Words: Eye Tracking as the Most Widely Used Biometric Technique to Derive Users' Preferences and Purchasing Habits

The eye tracker allows eye behaviour to be tracked using a series of sensors. Presently, several different types are used and among them, the most common are, for example, the "screen-based" (also called "desktop") eye tracking, which is installed on a monitor; the "wearable" model, as it is installed on a device or on an accessory like glasses, mounted on the frame; and finally, the "mobile" model, which is incorporated into an electronic device such as a telephone, but which may be less accurate (Krueger et al., 2016; Bar-Haim, et al. 2006).

This technology can be based, alternatively, on an indirect measurement model, i.e., the so-called "corneal reflex"—whereby a source of light (usually infrared) is projected onto the eye and, with the help of high-definition cameras, its reflection on the cornea is observed—or eye movements recorded by a webcam device connected to a computer and are directly processed with the help of software. Both systems, therefore, require the use of algorithms to determine the exact behaviour of the eyes, given that the human eye alternates between moments of "fixation"—all the times that the gaze is fixed on a certain point in the field of vision—and "saccades," which are rapid eye movements that are produced when passing from one fixation point to another (Djamasbi, 2014, pp. 16–31; Featherman et al., 2011, pp. 1–25; Kamangar, 2020, pp. 73–91).

Similarly, with this technique, it is possible to detect the ocular electric field as well as its variations, even minute ones. Specifically, when the eyeball and eyelid move in response

to a certain external stimulus, they produce bioelectric signals called "Electro-Oculo-Gram" that can be recorded through electrodes placed on the side of the eyes. The eyes are electrically charged, and more specifically, the cornea is positively charged, while the retina is negatively charged.

For that reason, when one is subjected to a certain visual stimulus and their gaze in space changes, it produces a change in the electrical field of the eye, generating a large signal that can be recorded by the eye-tracking system. In particular, when the eyeball moves upwards, the cornea and the positive pole move closer to the sensor, producing a positive deviation of the electric field; similarly, for blinking: when the eyelid closes, the cornea moves closer to the sensor, producing a positive pulse that is recorded. Conversely, when the gaze moves downward, the cornea moves away from the sensor producing a negative electric field deviation, just as it does when the eyelid opens.

The Relevance of Ocular Data Between Opportunity for Companies and Risks for Fundamental Human Rights

For some time now, countless scientific studies have shown that accurate information on a person's health, emotional state, and behavioural tendencies can also be derived from eye analysis (Cherubino et al., 2019, pp. 1–41; Kröger et al., 2020, pp. 226–241; Morin, 2011, pp. 131–135).[3] In other words, it has been observed that pupil dilation reflects the cognitive reasoning of the central nervous system in response to a certain external stimulus and that the direction of gaze reflects the activity of the part of the brain responsible for emotional reactions (Ekman, 2004; Ekman & Friesen, 1978; Holmqvist et al., 2012).

This means that it is not only considered possible to deduce the subject's age but, above all, the presence of symptoms of a large number of neurological and behavioural disorders that can often manifest themselves precisely in the form of abnormalities of eye movement (Dalton et al., 2005, pp. 519–526; Laeng & Falkenberg, 2007, pp. 520–530; Partala et al., 2000).[4]

Taking into account these brief considerations, the possible risks to the fundamental rights of an individual are evident, ranging from physical and psychological integrity to the protection of their autonomy of decision-making and the protection of their personal data. This last hypothesis clearly correlates to the greatest critical issues that arise because, as neuroscientific studies have revealed, the eyes provide quantitatively and qualitatively superior information compared to traditional biometric factors (such as fingerprints or the face) because they are more accurate for substantial reasons (Jansson et al., 2015; Kindt, 2013). On the one hand, they are easier to detect and measure because they are unidimensional and have low frequency, and, on the other hand, they appear unique and different depending on the individual. One only has to think, for example, of the moment when the eyelid blinks: in this case, millions of electrical impulses are produced which, through the neural network, arrive to the brain where they are immediately processed, and it is evident that since each person is endowed with a unique neural network made up of numerous

[3] Think of the case of "Affidex," a particular software that identifies and classifies facial expressions into "emotion classifications" thanks to facial coding, AI and video analysis are able to record all the slightest facial expressions of the user, even the unconscious ones.

[4] For example, it has been shown that the way one observes the faces of others is strongly influenced by the so-called "Own-Race Face Bias," due to which an individual views the faces of those belonging to one's own ethnic group differently than others.

neurons, the electrical signals produced by the blinking of the eyelids are also exclusive to each individual (Abbas & Abo-Zahhad, 2017, pp. 122; Borji & Itti, 2014).[5]

Threats to Consumer Decision-Making Autonomy from the application of Eye Tracking in the Marketing Sector

There is, indeed, an obvious and general necessity to deal appropriately with such practices that are based, precisely, on the collection of particular data and the profiling of users. However, this need becomes even more pressing when these practices are used for commercial purposes.

Since in this sector, more than in others, there is a strong risk that the mere persuasion of consumers will be trapped into further manipulation, it suffices also to say that the GDPR, having a risk-based approach, takes into account that the dangers for data subjects arising from the processing of personal data are balanced against the benefits for the fundamental rights and freedoms of data controllers (Munoz et al., 1998), as well as the data subjects themselves. However, while in other sectors where eye-tracking technologies are widely used there may be various legal grounds to legitimize the processing of consumer data (for example, think of the grounds of "substantial public interest" in public health under Article 9.2, lett. g) of the GDPR), the same cannot be said for marketing. The latter is, in fact, a context in which companies have a substantial economic interest and where, on the other hand, the risk of violation of consumers' fundamental freedoms and rights is particularly high (Lee & Lee, 2004; Malhotra et al., 1982).

Given the essentiality of personal data for algorithms and AI systems used by neuromarketing, the first thing we must address is compliance with EU data protection legislation. In particular, it is a question of verifying the effectiveness of the current regulatory framework concerning the new issues raised by these commercial practices, with specific reference to those based on eye tracking. Once various regulations that come into play when talking about neuromarketing have been analysed, the attempt to offer some final considerations on possible future developments in the field will be possible (Rayner, 1998).

Eye Tracker and the European General Data Protection Regulation: Between Biometric and Inferred Data

The birth of neuromarketing has rapidly increased knowledge about brain functioning and unconscious processes because it has made data accessible that was previously considered, as seen above, completely inaccessible.

When talking about eye tracking, one can mentally distinguish two "stages" in which two different types of data are processed: "biometric data" and "inferred data." Then, it is a question of whether the GDPR provides adequate protection for these two categories of data.

[5] They report the results of a study on a biometric verification system based on eye movements: "The system was built using a database of 40 subjects (19 healthy subjects and 21 otoneurological patients) recorded with electro-oculography. Achieved verification results were in range of 86–97%.".

The History of European Legislation for the Regulation of Biometric Data

Focusing on the most popular types of eye tracker, namely, desktop and wearable, the person is first placed in front of a screen and subjected to a visual stimulus. Sensors embedded on the screen or directly on a wearable device detect the reaction of the eye by recording the size, colour, iris width, electric field, trajectory, and any eyelid movement or blinking.

Once these data have been collected, they are sent to the software that translates them into a computer language and then processes them, obtaining information on the cognitive and emotional processes of the person. Not only that, but more and more often, the eye tracker is integrated with AI systems capable not only of processing eye biometric data more precisely but also above all producing outputs in the form of inferences (even very accurate ones) about the presence of physical and mental illnesses as well as the possibility that the person may develop them in the future.

To date, the first of these two "stages" undoubtedly raises less concern than the second because, for some time now, fingerprints, pupil, and gaze have been considered "biometric identifiers." The latter, being unique to everyone, are distinctive and measurable characteristics capable of identifying an individual (McStay, 2020, pp. 1–12; see also Bhattacharyya et al., 2009).[6]

Beginning the Reflection on the Opportunity to Consider Biometric Data in the European Legal System

On closer inspection, before 2016, biometric data was given very little consideration and, above all, was not expressly considered in the relevant European legislation. The now-repealed EC Directive 95/46, on the protection of individuals concerning the processing of personal data and on the free movement of such data, made no explicit reference to this type of data, so much so that Article 8 (devoted precisely to special categories of data) referred exclusively to data that could reveal racial or ethnic origin, political, religious, or philosophical opinions, political affiliation, or data concerning health or sex life so there was no clear reference to the category of biometric data, which carried a risk of remaining outside the scope of the directive, with obvious risks to the privacy of the individual. To avoid this risk, an attempt was made to bring them interpretatively within the very broad definition of "personal data" defined by Art. 2(a) as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental economic, cultural or social identity."

Biometric data could (implicitly) be considered personal data since they process unique and identifying characteristics of an individual, regardless of the identification technique used (facial recognition, iris scan, or dactyloscopic data) as long as it allows for the identification of a living person (Schatten et al., 2008; Zaborska, 2019; Els, 2013).

[6] Gaze data fall into the category of "hard" biometrics, because they directly enable the identification of the subject, unlike "soft" biometrics.

The Work of the Article 29 Working Party as a Turning Point in the Recognition of Biometric Data

With technological development, identification techniques using biometric data have become increasingly sophisticated and widespread among the public for the most common purposes. This has further heightened the attention and concern about biometric data to such an extent that the same Article 29 Working Party (henceforth 29WP)[7] in 2007 reserved an entire opinion for specifying the definition of personal data (29WP, 2007) and even in 2012 another one precisely on the development of biometric technologies (29WP, 2012).

A29ccording to 29WP, biometric data "by their very nature, are directly linked to an individual" and consequently, biometric technologies differ from others because they use unique characteristics for identification or authentication purposes (Kindt, 2018, pp. 523–538; Jasserand, 2016; Sumer, 2022). For this particular quality, according to 29WP, they were to be defined "as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability" (29WP, 2007; Alterman, 2003, pp. 139–150; Rebera & Mordini, 2013). This means that not all physical or behavioural characteristics are in themselves biometric identifiers, but only those that are measurable (though independently of the technique used for detection) and, above all, representative of physical or behavioural traits that are unique to each individual such that they can be identified, even if only with a probabilistic degree of accuracy (Chinchilla, 2012, pp. 1–25).

Finally Here: The Adoption of GDPR, the Explicit Recognition of Biometric Data, and the Need to Go Further

With the entry into force of Regulation (EU) 2016/679, the European landscape has changed dramatically because the legislator has expressly and definitively clarified that biometric data represent a special category of personal data and, provided that they are intended to uniquely identify a natural person (Rec. No. 51, GDPR), are subject to stricter regulation (Art. 9.1, GDPR).

If this requirement is met, Article 9.1 GDPR requires that, as a rule, their processing is prohibited unless one of the hypotheses (considered a *numerus clausus*) derogating from this prohibition and typified in the following paragraph of the same provision occurs. If, on the other hand, the purpose is not to uniquely identify or authenticate a natural person, they cannot be considered within the meaning of this provision and will consequently be protected as normal personal data (Kuner & Gkotsopoulou, 2021).

The Other Side of the Coin: The European Evolution on the Regulation of Inferred Data

If the legal framework applicable to biometric data nowadays tends to be clear, what is different is what happens to "inferred data," which is, that is information that is not provided

[7] It was an independent European advisory body that dealt with issues relating to the protection of privacy and personal data until 25 May 2018, when the GDPR came into force. Its tasks were described in Article 30 of Directive 95/46/EC and Article 15 of Directive EC 2002/58.

directly by the data subject but is deduced, through AI systems and analytical processes, from the processing of previous data. This means, therefore, that the AI system, by processing the data obtained from the eye tracker on the gaze, iris, and pupils, can determine the probability (getting closer and closer to certainty as the systems become more sophisticated) that there are physical or mental disorders as well as the genetic tendency of that person to develop certain pathologies in the future (Arolt et al., 1996, pp. 564–579; Hochstadt, 2009, pp. 991–1011; Larrazabal et al., 2019, pp. 57–66).

However, inferred data is currently neither included among the particularly sensitive data under Article 9 of the GDPR nor in any other provision or recital, with the consequence that the entire European regulation may not apply. Since the dangers for fundamental rights are obvious in this situation of uncertainty, it is at this point that further consideration should be given to the rules that apply to them to verify whether they are sufficient to guarantee adequate protection.

First Things First: Can Inferred Data Be Considered Personal Data? An Analysis Starting from the GDPR

First, it must be understood whether inferred data can be considered personal data given that the legislation in question only applies "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filling system" (Art. 2.1, GDPR).

It is clear from this provision that there are two conditions for the applicability of the GDPR: the "personal" nature of the data and that it be "processed" (29WP, 2007, p. 136).

Starting from the first precondition, it should be noted that the regulation—as was the case with the previous directive—purposely constructs a definition of personal data that is as broad as possible, i.e., potentially covering all types of data and not only the most clearly personal ones (Borgesius, 2017; Finck & Pallas, 2020, pp. 11–36). Thus, it speaks of "any information relating to an identified or identifiable natural person (data subject)", as "can be identified, directly or indirectly, in particular by reference to an identifier" (Arts. 2 and 4.1, GDPR).

The expression "any information" contained therein must be interpreted, as stated above, in the most general sense possible and neutrally, without attributing any quality to the information. From this observation, it follows that the truthfulness of the information is irrelevant, meaning that it does not necessarily have to be proven or true but may also include the data that, just like the inferred data, does not represent a certain and incontrovertible fact, but a highly probable forecast. The 29WP itself also expressed its view on this point in Opinion 4/2007, according to which the concept of any information must be understood in a technologically neutral sense because, otherwise, it would already be completely obsolete at birth concerning the development of new technologies. In other words, it applies regardless of the type of format or technique used with the consequence that "the fact that the captured biometric samples have been manipulated and transformed into one or more numerical representations of the characteristics shall not determine whether the information is personal data or not" (29WP, 2007, p. 8). However, this condition does not allow us to conclude *ex se* that the inferred data are indeed personal data, but it is also necessary that they refer to an "identified or identifiable" natural person. Here again, the term "identify" must be understood in a general sense, and therefore, a (natural) person is

identified if it can be distinguished from the other members of the group (Finck & Pallas, 2020).

The same standard also specifies that a data subject is considered "identifiable" when his or her identity can be traced through identifiers such as name, location data, an online identifier (IP), or some characteristic of his or her physical, physiological, genetic, psychological, economic, cultural, or, finally, social identity (Art. 4.1, GDPR).

The Expansion of the Concept of Personal Data Through the Interpretation of the Court of Justice of the European Union: The Most Relevant Case Law on the Matter

This category should not be considered *sic et simpliciter*, so much as it has been the subject of constant expansion by the jurisprudence of the Court of Justice of the European Union. Among others, emblematic is the recent case *Nowak v Data Protection Commissioner* precisely concerning the definition of personal data (*Nowak v Data Protection Commissioner* 2017, p. 35).[8] Specifically, Mr. Nowak, a candidate on a professional examination, had requested transcripts of the answers given during the examination and the examiner's notes of those that were examined. The competent administrative authority (the professional organization of accountants) and the Irish Data Protection Commissioner rejected his access request, considering that such information could not be considered personal data (*Nowak v Data Protection Commissioner*, p. 18). The issue went all the way up to the Court of Justice of the European Union, which, contrary to the national courts, recognized that both a candidate's answers in an examination and the examiner's notes must be considered personal data, since "by reason of [their] content, purpose or effect, [they are] linked to a particular person" (*Nowak v Data Protection Commissioner*, p. 35). However, the use of the expression "any information" reflects the intention of the European legislator to give it a broader meaning, not limited to sensitive information but potentially extending to any kind of data, if it is linked, due to its content, purpose, or effect, to a particular person.

The Court went on to observe that the answers given by the candidate reflected their knowledge and skills in that field, as well as their thought processes, judgement, and critical mind and, consequently, concluded by recognizing that such information, depending on the specific circumstances, should be classified as personal data.

To determine whether a person is "identified or identifiable," the GDPR requires consideration of all the means that the data controller (or even a third party) may reasonably use to identify that natural person, either directly or indirectly (Rec. No. 26, GDPR). It follows that the regulation does not apply to personal information that has been rendered sufficiently anonymous so that the data subject can no longer be identified.

There are two types of identification, one direct and one indirect. The first hypothesis is when a person can be "directly" identified or identifiable, that is, when a person can be referred to by name, while the second type concerns "indirect" identification. This hypothesis is also recognized by the regulation itself which, in defining personal data, identifies the identifiable person as anyone who can be identified directly and indirectly, by referring to an identification number or one or more specific factors relating to his or her physical, psychological, mental, economic, cultural, or social identity. In other words, indirect

[8] In the same sense, cf. also *Breyer v Germany* 2016, p. 30.

identification occurs when it is possible to distinguish the person, but only through combination with other information.

Indeed, inferred data allows for (at least) indirect identification of the data subject, since they represent, although not to the degree of certainty, generally accurate predictions about the development of a disease. Suppose, for instance, that the AI system built into the eye tracker produces inferred data determining that, in all likelihood, that person will develop a rare neurodegenerative illness: it is evident that, in this case, the person can be said to be indirectly identifiable with respect to a group of persons, especially if these inferences are then combined with other information contained in an external server.

The Second Condition for the Applicability of GDPR: The Need for a Data Process

After proving that the inferred data can be considered, indeed, personal data, we must now focus on the other condition for the applicability of the European regulation: the "processing."

Here, too, the GDPR aims to construct a very broad definition, including "any operations or set of operations which is performed on personal data or sets of personal data, whether or not by automated means" (Art. 4.2, GDPR). Then, it provides an illustrative list of operations that must be considered processing for all purposes, including, for example, collection, recording, structuring, storage, adaptation, modification, and comparison (Hoofnagle et al., 2019, pp. 65–98).

As we have already observed, the eye tracker sensors collect and record eye movements and electrical impulses that are, first, translated into a computer language and, subsequently, sent to the software that processes them (Gama & Rodrigues, 2007, pp. 25–39; Stephens, 1997, pp. 491–541).[9] In other words, through deep learning and analytical and probabilistic processes, the algorithm can make inferences about the person's state of health which, through a comparison with an external database, can be identified.

This is particularly relevant when one considers that this data information is collected and processed to create a "digital profile" of the individual that contains all their preferences, habits, and biases that can be exploited with being sent highly personalized advertising. As we have already seen, profiling is considered by the GDPR itself as a form of automated processing of personal data to make assessments on certain aspects of the natural person, including behavioural habits, health, preferences, and interests.

Given all this, it must be concluded that this additional requirement is met and, therefore, we can say that these data fall within the scope of the European Data Protection Regulation.

Inferred Data as Personal Data: Is This (Really) Enough? Some Considerations for a Further Step Forward

Furthermore, the next question is whether inferred data can be subjected to stronger protection, including them among special categories of personal data and, in particular, within

[9] It should be noted that if the data once collected by the sensor is then saved on a durable medium, then this is referred to as "batch processing," whereby processing is carried out on groups of data later. On the contrary, we speak of "stream processing" when the data is sent to the AI system, without being saved in advance, to be processed at the same time as it is detected by the sensors.

"data concerning health" provided by Article 9.1 of the GDPR. This issue is indeed particularly relevant since, if the answer is yes, stricter rules rather than general ones would and should apply to them.

Some Hints from the European Court of Justice: The OT v Vyriausioji tarnybinés etikos komisija Case

On this point, the Court of Justice of the European Union has also recently pronounced itself, which, in the case *OT v Vyriausioji tarnybinés etikos komisija* (*OT v Vyriausioji tarnybinés etikos komisija* 2022), clarified that inferred data must be considered particularly sensitive data and, therefore, falling within the special category of personal data provided for in Article 9 GDPR.

The judgement stemmed from a Lithuanian case in which the director of an organization receiving public funds failed to submit the "declaration of private interests" required by Lithuanian anticorruption legislation, which was to be published online. However, the director refused to allow the publication of this document because it contained personal information that could reveal important aspects of his and his family's private life. The national court, having doubts about the compatibility of the anti-corruption legislation with Articles 6 and 9 of the GDPR, suspended the case and made a reference to the Court of Justice for a preliminary ruling, asking whether data capable of revealing, using a linking operation or an inference, the sexual orientation of a natural person fell within the special categories of personal data within the meaning of Article 9.1 GDPR.[10]

The Court noted that Article 9.1 GDPR places a general prohibition on the processing of data "revealing" a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data "relating" to a person's health, life, or sexual orientation.

In fact, from a literal analysis of the provision, the choice of the verb "disclose" also makes it possible to refer to processing that does not relate solely to intrinsically sensitive data, but also to data that can be indirectly derived from them using an intellectual deduction or comparison operation.

The same can also be said for the expression information "concerning health" since Article 4 defines it as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." Even more significant in this regard is Recital No. 35 of the regulation, according to which this category should include "all data pertaining to the health status of a data subject which reveal information relating to the past, the current or future physical or mental health status of the data subject."

[10] In this sense the referring court: "It takes the view that the personal data contained in a declaration of private interests are liable to reveal information on the private life of the declarant and his or her spouse and of the declarant's children, with the result that their disclosure is capable of infringing the right of the data subjects to respect for their private life. Indeed, those data are liable to reveal particularly sensitive information, such as the fact that the data subject is cohabiting or is living with another person of the same sex, the disclosure of which might well result in significant nuisance in the private life of those persons. The data concerning presents received and transactions carried out, by the declarant and his or her spouse, cohabitee or partner, also reveal certain details of their private life."

The Considerations of the European Legislator on the Suitability of Inferred Data as Special Category of Data

The feasibility of the thesis that inferred data should be qualified as particularly sensitive data and processed accordingly can also be deduced from the choice made by the European legislator regarding biometric data. In other words, to fall within the latter definition, there must be a finalistic element in that the data in question must be processed with a device specifically designed to unambiguously identify a natural person. However, when it comes to "data concerning health," this characteristic does not exist. If this is true, it can then be assumed that inferences of a sensitive nature do not even have to be corrected to fall within the scope of the GDPR, for which it is not the validity of the conclusions reached that is relevant, but only their processing.

From all these considerations, it emerges that the category of inferred data should also be explicitly considered, which, for the reasons mentioned above, should not only be considered personal data but even as "data concerning health." Therefore, inferred data should be subjected to the stricter rules established for this special category. Only in this way can the respect for the fundamental rights and freedoms of persons be guaranteed at the highest level.[11]

The Need to Find a Legal Basis to Allow the Processing of Inferred Data in the World of Neuromarketing

Having demonstrated, albeit briefly, that inferred data must be regarded as sensitive data, the question now arises as to the conditions under which they can be processed. First, the GDPR only allows the processing of personal data where it is lawful, meaning there must be a legal basis.

For this reason, Article 6 lists precisely the conditions under which processing is considered lawful and, therefore, permitted. Among these, the only condition that might be relevant concerning personalized marketing practices based on data collected by eye tracking is the explicit consent to the processing by the data subject for one or more specific purposes (Art. 6.1).

Explaining Why Explicit Consent Is the Only Way to Ensure Compliance with the Fundamental Rights of Consumers Exposed to Eye-Tracking Practices for Marketing Purposes

It is quite clear that the processing of the data, in this case, has a purely marketing purpose, so it cannot be said to be necessary to comply with a legal obligation to which the data controller is subject (c), to safeguard the vital interests of the data subject (d), or to perform a task carried out in the public interest or in the exercise of official authority (e).

Similarly, it is doubtful whether the condition in subparagraph (b) applies because the data are collected by the trader for the purpose of inducing the consumer to buy more. This purpose cannot then be said to be strictly necessary for the performance of the (possible)

[11] The Court of Justice of the EU had already interpreted the concept of "health data" broadly to include not only data relating to a person's physical but also mental health. See *Lindqvist*, 2003, p. 50.

contract concluded with the data controller. This statement is moreover confirmed by the 29WP itself, which acknowledged that this provision does not cover those situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller.

Furthermore, the fact that some data processing is covered by a contract does not automatically mean that processing is necessary for its performance. On user behavioural profiling, the 29WP stated that: "[this legal ground] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract" (29WP, 2014).

Finally, it is also doubtful whether such processing is necessary for the pursuit of the legitimate interests of the data controller or of third parties, provided that the interests, fundamental rights, and freedoms of the data subject do not prevail. Controllers may have a legitimate interest in getting to know the preferences of their customers to allow them to better personalize their offers and, ultimately, offer products and services that better meet the needs and desires of the customers.

The Features that Consent Must Have to Ground the Processing of Inferred Data: The Need for Qualified Consent

Considering this, Article 6(f) may be an appropriate legal ground to be used for some types of marketing activities, both online and offline. Anyway, the same 29WP specifies then that: ''However, this does not mean that controllers would be able to rely on Article 7(f) to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create – and, for instance, with the intermediary of data brokers, also trade in – complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject" (29WP, 2014, p. 26).

On the other hand, it is likely that the data subject, having had to accept the terms and conditions of the platform to be able to use the services provided by it, has given his or her consent to the processing of the data extrapolated by eye tracking and used for profiling him or her (Art. 6(a), GDPR).

However, the existence of consent is, by no means, sufficient. On the contrary, it is essential that it has certain specific qualities, or, in other words, it must be "qualified." Article 4 defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Therefore, it must be a positive act and voluntary and also be expressed in a paper, digital, or even in an oral declaration. What must be ensured is the awareness of the data subject, so much so that, if the request for consent is contained in a written document that also relates to other matters outside the one for which it is being requested, it must be clearly distinct, easily accessible, and formulated in clear and comprehensible language, under penalty of the declaration not being binding. This provision derives from the fact that processing is

always linked and strictly limited to a specific purpose (the so-called principle of data minimization), with the consequence that it would not be possible to consent generically to the processing of personal data. In other words, separate and specific consent would be needed for each purpose.

The regulation in question also admits consent manifested by *facta concludentia*, since the data subject may validly consent using—active—conduct that unequivocally indicates that he or she is aware of and accepts the proposed processing. In any case, from the specification that it must be an active action, it follows that silence, inactivity on the part of the data subject, or pre-filled online forms can never be considered valid consent.

The possibility of expressing it implicitly is never envisaged in the case of health data and all other categories of special data for which, on the other hand, explicit consent is required (Art. 9.2, GDPR). However, whether manifested explicitly or by active action, it must be "unambiguous," in the sense that there must be no doubt that the person concerned has accepted the proposed treatment. The latter must also have had the possibility of freely choosing whether to provide it, without any kind of conditioning, pressure, deception, or intimidation. Then, where the performance of a service or contract is conditional on the provision of consent to the processing of personal data that are not necessary for the performance of the service or contract, consent cannot be freely given (Art. 7.4, GDPR).

It is also clear that the necessary precondition for consent to be free is the right of the data subject to be adequately informed about the purposes, modalities, and duration of the processing, with the consequence that the person, on one hand, can withdraw her consent at any time and as easily as she gave it and, on the other hand, can request the deletion of the data according to Article 17.1(b).

The Adequacy of Explicit Consent Even when Considering Inferred Data as Health-Related Data as Stated by the European Court of Justice

The same considerations apply whether we adhere to the interpretation given by the European Court of Justice that recognizes inferred data as health-related data under Article 9.1 GDPR. As is well known, this provision places a general prohibition on processing data that fall within the category of special personal data. However, this prohibition is not absolute since certain mandatory exceptions are provided in the following paragraph.

Quickly reviewing them, we see again that, concerning the inferred data collected by eye tracking for marketing purposes, the only relevant basis would be the explicit consent of the user (Article 9.2(a), GDPR). Indeed, in this case, the processing of consumers' data does not concern obligations and rights in the field of labour law or social protection (subpara. b), nor the public interest, scientific, historical research for statistical purposes (subpara. j) as well as the public interest in the field of public health (subpara. i), neither, finally, the field of preventive or occupational medicine (subpara. h).

Since these neuromarketing techniques are mostly adopted by private companies which aim to profile their users for essentially commercial purposes, we can also exclude the nonprofit-making association or organization case (Art. 9.2(d), GDPR), as well as judicial activities (art. 9.2(f), GDPR), the public interest based on Union or MS law (Art. 9.2(g), GDPR), and, finally, the protection of a vital interest of the data subject or of another natural person in the event of his physical or legal incapacity (Art. 9.2(c), GDPR).

Having said that, even in this case, the consent of data subjects should have the same features as above because, otherwise, the processing of these type of data would be prohibited.

Troubles in Paradise: The Limits of Consent as a Legal Basis to Guarantee the Protection of Fundamental Rights of Data Subjects

While theoretically, the requirements for allowing the processing of inferred data are precisely identified, in reality, the situation is likely to be very different.

When speaking of inferences, one must bear in mind that they derive from an analytical and deductive process operated by algorithms that, starting from the biometric data of the data subject, arrive at further data that represent accurate predictions about the one's health—mental and physical, present, and future.

Even assuming that there was, indeed, explicit consent to the processing of the biometric data collected (perhaps stored) and processed by the eye tracker, there are several doubts concerning its validity about the processing of inferred data. This skepticism derives especially from the circumstance that the person often finds himself not even aware that she is providing additional data to those for which he has given his consent (always for a certain purpose).

In this case, this consent cannot be considered valid because it is not conscious and informed for at least two reasons. On the one hand, it must always be remembered that providing the user with a large amount of information does not serve the purpose because the user is not physiologically capable of handling it, nor will they have the desire to read it all. Therefore, the risk is that when faced with a very detailed and technical information sheet, the subject will simply consent without really being aware of the details of it. On the other hand, this danger should not be surprising given studies in the behavioural sciences that have clearly shown that excessive information does not benefit the recipient—who could be lazy to read the fine print—but, on the contrary, generates an "overload effect" (Bawden et al., 1999; Ben-Shahar & Schneider, 2016; Herbig & Kramer, 1994).

Particularly for inferred data, it becomes difficult to ensure that the consent of the person is conscious, free, and informed as required by GDPR, precisely because this kind of data derives from algorithmic processing from previous information. This situation has important negative consequences for fundamental rights, including especially the risk that they may be processed by circumventing the requirements of European legislation (Eppler & Mengis, 2004, pp. 1–20).

Therefore, the inferences bring to light several critical issues and doubts about the actual ability of GDPR to provide adequate protection.

Indeed, there is a need to also qualify the data inferred under Art. 9, to provide them with the highest possible protection. On the other hand, the considerations made so far have also shown some difficulties in ensuring in practice that the consent given by the data subject has all the qualities required to be considered valid (to allow the processing of these data).

This means that its function as a legal basis may have to be reconsidered, since qualified consent cannot guarantee that the data subject is aware of all the consequences of profiling by means of neuromarketing techniques.

Concluding Remarks: The Current Importance of GDPR for the Protection of Individuals Against Eye-Tracking and Neuromarketing Technologies

Aware of the danger of user profiling for human autonomy and dignity, the GDPR provides specific provisions aimed precisely at regulating such practices. According to Article 22.1, the data subject "shall have the right not to be subject to a decision based solely on

automated processing, including profiling, which produces legal effects concerning him or her similarly significantly affects him or her."

Two conditions are necessary for it to apply. First, the decision must be entirely automated ("based solely on automated processing") without human intervention. The latter, as also recognized by the 29WP, must be understood in a substantial sense. In other words, the mere human presence is not sufficient, but it is required that the intervention be meaningful, i.e., made by one who has the authority to change the decision (29WP, 2017a, b, p. 9). Second, this decision must generate "legal" or, alternatively, "similarly significant" effects. Since no indication has been given on its interpretation, it is considered to refer to automated processing operations that have an effect of a nonsignificant magnitude but are designed to influence the data subject's behaviour and choices in a relevant way. In regard to commercial practices that are based on the processing of biometric and inferred data for user profiling, this expression is particularly problematic. In point of fact, their nature as covert practices (in that they seek to unwittingly influence the consumer by pushing emotional rather than rational factors) does not always make it easy for the supervisory authorities or for the recipients to detect them. Furthermore, it should also be noted that "In many typical cases targeted advertising does not have a significant effect on individuals. (…) However, it may do, depending on the particular characteristics of the case" (29WP, 2017a, b, p. 11).

In any case, the data subject has the right to be informed about the existence of automated decisions (Art. 13–14) as well as to access (Art. 15) and to object (Art. 21).

By adopting a risk management strategy, the GDPR not only provides information obligations but also shows awareness of the dangers that certain technologies may pose to fundamental human values in the long term. In this sense, then, Article 35 of GDPR requires the data controller to carry out the so-called "data protection impact assessment" (DPIA). That is, when processing, involving the use of new technologies, is likely to present a high risk to the rights and freedoms of individuals, the controller is required, before the processing itself, to carry out a data protection impact assessment of the intended processing. Such an assessment is required in certain situations considered particularly risky, among which the legislator includes precisely "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Art. 35.3(a), GDPR). The DPIA is not always compulsory, but only where processing is "likely to result in a high risk to the rights and freedoms of natural persons" which, according to the interpretation of the 29WP, is the case of "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" as well as in the case of "innovative use or applying technological or organizational solutions" (29WP, 2017a, b, p. 7; Liebling & Preibusch, 2014).[12]

[12] It is interesting that the 29WP continues saying that: "combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. The personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain 'Internet of Things' applications could have a significant impact on individuals' daily lives and privacy; and therefore, require a DPIA."

The Latest Developments in European Law to Contain the Risks Arising from the Use of Algorithms, Artificial Intelligence, and Neuromarketing: The Provisions of the New Digital Services Act and the Artificial Intelligence Act

Again, to make data controllers responsible for the processing carried out, the recent Regulation (EU) 2022/2065 (the so-called "Digital Services Act") introduced, first and foremost, new information obligations. Thus, online platforms that use recommender systems must indicate the main parameters in their contractual terms and conditions (Art. 27 DSA 2022) and provide users, at least, with an option not to be profiled (Art. 38 DSA 2022).

Like the impact assessment under the GDPR, Article 34 of the DSA requires very large online platforms to assess the systemic risks arising from the design (including algorithmic systems), operation, and use of services.[13] It must be prepared at least once a year and, in any case, before the introduction of new functionalities. On an annual basis, they are also required to conduct an independent audit to assess adherence to the DSA itself (Art. 37 DSA 2022). Once systemic risks have been identified, platforms must take reasonable, proportionate, and effective measures to mitigate them (Art. 35.1 DSA 2022).

The Artificial Intelligence Act as a Highly Criticised Piece of Legislation: The Exclusion of Neuromarketing Among Prohibited Technologies

The Artificial Intelligence Act (AIA 2021) is also crucial. As is well known, AI systems are divided into three categories based on the risk they pose to fundamental rights.

Article 5.1 first prohibits two types of practices that are considered manipulative, namely, an AI system that deploys subliminal techniques "beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm" (Art. 5.1(a), AIA 2021) and "that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, to materially distort the behaviour of a person about that group in a manner that causes or is likely to cause that person or another person physical or psychological harm" (Art. 5.1(b), AIA 2021).

This rule then seems to apply exclusively to those AI systems that, by manipulating the behaviour of the persons involved, causing (or are likely to cause) physical or psychological harm. This means that if the AI practice is manipulative, but not causally capable of causing physical or psychological harm, it will not in itself be considered a high-risk system within the meaning of Sect. 5 of the AIA (STOA, 2022, pp. 12–13). As noted already, not every neuromarketing practice can be said to be subliminal and manipulative per se because otherwise, the entire discipline would be illegitimate.

[13] Systemic risks include the dissemination of illegal content; possible current or foreseeable negative effects on the exercise of fundamental rights; possible current or foreseeable negative effects on civic debate, electoral processes, and public safety; and, finally, in relation to gender-based violence, the protection of public health and minors, and serious negative consequences for the physical and mental well-being of the individual.

Neuromarketing Practices as High-Risk or Low-Risk AI Systems? The Provisional Decision of the European Legislator

The other category to which reference is made is the one governed by Title III of the AIA which includes those IA systems considered "high risk" that are subject, for this reason, to stringent mandatory requirements that suppliers must comply with right from the design phase (Hof, 2022; Hupont et al., 2023; Mökander et al., 2022).

Neuromarketing techniques, however, do not seem to fall even within the cases of Article 6(1) of the AIA or even less so among those listed in Annex III (to which Article 6(2) refers) where, at most, paragraph 1 speaks of those systems used for the biometric identification and categorization of natural persons. However, since the purpose of neuromarketing is neither real-time nor a posteriori identification of a natural person, it does not seem to be possible to include such practices among high-risk AI systems (Alì & Yu, 2021; De Cooman, 2022; Hildebrandt, 2021, pp. 4–5).

Turning, instead, to AI systems deemed to be "low risk," the Draft Regulation refers, in Article 52.2, to emotional recognition and biometric categorization systems (Art. 52, AIA 2021). Nevertheless, since they are considered low-risk systems, their implementation and application will be subject to transparency obligations which, however, do not appear to be sufficient concerning the dangerousness of these practices because: "These systems are based on highly problematic evidence while nevertheless generating potentially highly detrimental output (in the form of decisions or behavior)" resulting in "chilling effects, exclusion and disrespect for individuals of groups that do not fit the categorizations that are taken for granted" (Hildebrandt, 2021, p. 46).[14]

Awareness of the problems this shortcoming could cause for the protection of fundamental human rights, the European Parliament, at its first reading in the ordinary legislative procedure, adopted several amendments to the Commission Proposal. Among these, the category of high-risk IA systems in Annex III was amended and expanded further. Thus, it now includes, among others, emotion recognition systems and, more generally, those AI systems intended to be used to draw conclusions about the personal characteristics of natural persons based on biometric data or based on biometric elements (Barrett et al., 2019, p. 46; Orlando, 2023, pp. 378–381).

What is the Future of Eye-Tracking Systems in Europe? Some Final Considerations

The explicit inclusion of such practices among high-risk AI systems is a very important step forward in providing more effective protection against violation of fundamental rights. Indeed, because of this choice, the supplier is required to implement and document a risk management system to identify and analyse the possible risks arising from the use of the AI system and to adopt appropriate measures for its proper management (Art. 9, AIA 2021) and to guarantee a qualitative level of dataset and data governance (Art. 10, AIA 2021). Moreover, the supplier must draught and maintain detailed, complete, and up-to-date technical documentation and ensure the verifiability and traceability

[14] The author comments that: "the current categorization of emotion recognition and biometric categorization as not necessarily high risk, whereas depending on use or context they may nevertheless qualify as high risk or even be prohibited, is confusing and unnecessarily complicated" and concludes that: "If not prohibited, they should be added under point 1 in Annex III."

of the processes used by AI systems by providing instruments both for recording purposes and to allow adequate human supervision of their operation (Arts. 11–14, AIA 2021). In other words, they must be designed and developed to ensure a high level of accuracy, robustness, and cybersecurity, as well as transparency through the provision of clear, concise, and understandable instructions for use (Art. 13.1, AIA 2021).

However, we can wonder whether the regulatory tools provided by the AIA might be appropriate to address long-term autonomy concerns, especially when it comes to eye-tracking technologies and biometric recognition technologies, in general. In fact, it is true that the instrument of risk assessment obligations is more effective than information requirements since it mitigates harm upstream when products and services are not yet placed on the market. On the other hand, the main issue with risk assessments is that they mainly rely on self-assessment and should thus be subject to external review to be meaningful (Fassiaux, 2023, pp. 1–21).

In conclusion, the development of technologies capable of recognizing human emotions and exploiting them to guide consumer behaviour requires the presence of appropriate legislation to ensure a reliable system that respects fundamental values.

Although the current regulatory framework, including above all the GDPR and the DSA, undoubtedly provides effective protection for the consumer, there are nonetheless several problematic nodes that need more attention from the EU legislator and that stem from the impact of AI systems with traditional legal categories (Veale & Borgesius 2021, pp. 97–112).

Undoubtedly, then, further tool to help build a safe, reliable, and trustworthy system could be the AIA because "against this background, the call for transparency rests on the need to look inside AI technology, to try to fully understand its logic and regulate its behavior" (Alì and Yu, 2021, pp. 5–6). Precisely due to the ability of such technologies to touch many fundamental values and to get to the essence of the person, the need to adopt a holistic approach is now undeniable. In this sense, then, GDPR, although still proving to be indispensable, is no longer sufficient on its own (Dìaz-Rodriguez et al., 2023).

Author Contribution The author wrote and reviewed the manuscript for important intellectual content, approved the manuscript, and made the final decision for submission.

Funding Open access funding provided by Scuola Superiore Sant'Anna within the CRUI-CARE Agreement.

Data Availability Not applicable.

Declarations

Ethics Approval Not applicable.

Consent to Participate Not applicable.

Consent for Publication Not applicable.

Competing Interests The author declares no competing interests.

References

Abbas, S. N., & Abo-Zahhad, M. (2017). *Eye blinking EOG signals as biometrics*. Springer International Publishing. https://doi.org/10.1007/978-3-319-47301-7_5

Alì, G. S., & Yu, R. (2021). Artificial intelligence between transparency and secrecy: From the EC whitepaper to the AIA and beyond. *European Journal of Law and Technology, 12, 3*. https://ejlt.org/index.php/ejlt/article/view/754 (accessed 13 November 2023).

Alterman, A. (2003). 'A piece of yourself': Ethical issues in biometric identification. *Ethics and Information Technology, 5*, 139–150. https://doi.org/10.1023/B:ETIN.0000006918.22060.1f

Arolt, V., Lencer, R., Müller-Myhsok, B., Purmann, S., Schürmann, M., Leutelt, J., Pinnow, M., & Schwinger, E. (1996). Eye tracking dysfunction is a putative phenotypic susceptibility marker of schizophrenia and maps to a locus on chromosome 6p in families with multiple occurrence of the disease. *American Journal of Medical Genetics, 67*, 564–579. https://doi.org/10.1002/(SICI)1096-8628(19961122)67:6%3c564::AID-AJMG10%3e3.0.CO;2-R

Arthmann, C., & Li, I. P. (2017). Neuromarketing-The art and science of marketing and neurosciences enabled by IoT technologies. *IIC Journal of Innovation,* 1–10. https://www.iiconsortium.org/pdf/2017_JoI_Neuromarketing_IoT_Technologies.pdf (accessed 15 November 2023).

Bar-Haim, Y., Ziv, T., Lamy, D., & Hodes, R. M. (2006). Nature and nurture in own-race face processing. *Psychological Science, 17*, 159–163. https://doi.org/10.1111/j.1467-9280.2006.01679.x

Barrett, L. F., Adolphs, R., Martinez, A., Marsella, S., & Pollak, S. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest, 20*, 1–68. https://doi.org/10.1177/1529100619832930

Bauman, Z. (2010). *I consume, therefore I am*. Laterza.

Bawden, D., Holtham, C., & Courtney, N. (1999). *Perspectives on information overload*. MCB UP Ltd.

Ben-Shahar, O., & Schneider, C. E. (2016). *More than you wanted to know: The failure of mandated disclosure*. Princeton University Press.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Minkyu C. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology, 2*, 13–28. https://faculty.kutztown.edu/frye/secure/CSC541/papers/BiometricAuthReview2009.pdf (accessed 20 September 2023).

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & De Vreese, C. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication, 23*, 370–388. https://doi.org/10.1093/jcmc/zmy020

Borgesius, F. Z. (2017). The Breyer case of the court of justice of the European Union: IP addresses and the personal data definition. *European Data Protection Law Review, 3*, 130–137. https://doi.org/10.21552/edpl/2017/1/21

Borji, A., & Itti, L. (2014). Defending Yarbus: Eye movements reveal observers' task. *Journal of Vision, 14*, 1–22. https://doi.org/10.1167/14.3.29

Cherubino, P., Martinez-Levy, A. C., Caratù, M., Cartocci, G., Di Flumeri, G., Modica, E., Rossi, D., Mancini, M., & Trettel, A. (2019). Consumer behaviour through the eyes of neurophysiological measures: State-of-the-art and future trends. *Computational Intelligence Neuroscience, 2019*, 1–41. https://doi.org/10.1155/2019/1976847

Chinchilla, R. (2012). Ethical and social consequences of biometric technologies: Implementation in engineering curriculum. *ASEE Annual Conference & Exposition.* https://doi.org/10.18260/1-2—21340.

Dalton, K. M., Nacewicz, B. M., Johnstone, T., Schaefer, H. S., Gernsbacher, M. A., Goldsmith, H. H., Alexander, A. L., & Davidson, R. J. (2005). Gaze fixation and the neural circuitry of face processing in autism. *Nature Neuroscience, 8*, 519–526. https://doi.org/10.1038/nn1421

De Cooman, J. (2022). Humpty dumpty and high-risk AI systems: The ratione materiae dimension of the proposal for an EU Artificial Intelligence Act. *Market & Competition Law Review, 6*, 49–88. https://doi.org/10.34632/mclawreview.2022.11304

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy artificial intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion, 99*, 1–24. https://doi.org/10.1016/j.inffus.2023.101896

Djamasbi, S. (2014). Eye tracking and web experience. *AIS Transactions on Human-Computer Interaction, 6,* 37–54. https://aisel.aisnet.org/thci/vol6/iss2/2 (accessed 15 September 2023).
Ekman, P. (2004). *Emotions revealed: Recognizing faces and feelings to improve communication and emotional life*. Henry Holt and Company.
Ekman, P., & Friesen, W. V. (1978). Facial action coding system: A technique for the measurement of facial movement. *Consulting, Paolo Alto, 22*.
Els, K. (2013). *Privacy and data protection issues of biometric applications*. Springer.
Eppler, M. J., & Mengis, J. (2004). The concept of information overload-A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The Information Society: An International Journal, 20*(5), 1–20. https://doi.org/10.1080/01972240490507974
Fabris, G. (2010). *Il nuovo consumatore: Verso il postmoderno ("The new consumer: towards postmodernism")*. Franco Angeli.
Fassiaux, S. (2023). Preserving consumer autonomy through European Union regulation of artificial intelligence: A long-term approach. *European Journal of Risk Regulation,* 1–21. https://doi.org/10.1017/err.2023.58.
Featherman, M., Wright, R. T., Thatcher, J. B., Zimmer, J. C., & Pak, R. (2011). The influence of interactivity on E-service offerings: An empirical examination of benefits and risks. *AIS Transactions on Human-Computer Interaction, 3*, 1–25. https://aisel.aisnet.org/thci/vol3/iss1/1 (accessed 30 September 2023).
Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*, 11–36. https://doi.org/10.1093/idpl/ipz026
Gama, J., & Rodrigues, P. P. (2007). *Learning from data streams: Processing techniques in sensor networks*. Springer.
Gerd, G. (2020). *What is bounded rationality?* Routledge.
Herbig, P. A., & Kramer, H. (1994). The effect of information overload on the innovation choice process: Innovation overload. *Journal of Consumer Marketing, 11*, 45–54. https://doi.org/10.1016/0046-8177(91)90167-N
Hildebrandt, C., & Oliver, J. (2000). The mind as black box: A simulation of theory building in psychology. *Teaching of Psychology, 27*, 195–197. https://doi.org/10.1207/S15328023TOP2703_06
Hildebrandt, M. (2021). *A brief commentary by Mireille Hildebrandt,* (pp. 1–7). https://www.cohubicol.com/assets/uploads/hildebrandt-feedback-eu-aia.pdf. Accessed 30 Sep 2023.
Hochstadt, J. (2009). Set-shifting and the on-line processing of relative clauses in Parkinson's disease: Results from a novel eye-tracking method. *Cortex, 45*, 991–1011. https://doi.org/10.1016/j.cortex.2009.03.010
Hof, M. J. (2022). *Human-AI teaming for conformity assessment of welded joints: A human factors perspective* (pp. 1–53). University of Twente.
Holmqvist, K., Nyström, M., & Mulvey, F. (2012). Eye tracker data quality: What it is and how to measure it. *Proceedings of the Symposium on Eye Tracking Research and Applications,* 45–52. https://doi.org/10.1145/2168556.2168563.
Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *InFormation & Communications Technology Law, 28*, 65–98. https://doi.org/10.1080/13600834.2019.1573501
Hupont, I., Micheli, M., Delipetrev, B., Gòmez, E., & Garrido, J. S. (2023). Documenting high-risk AI: A European regulatory perspective. *Computer, 56*, 18–27. https://doi.org/10.1109/MC.2023.3235712
Jansson, D., Medvedev, A., Axelson, H., & Nyholm, D. (2015). *Stochastic anomaly detection in eye-tracking data for quantification of motor symptoms in Parkinson's disease*. Springer International Publishing.
Jasserand, C. (2016). Legal nature of biometric data: From generic personal data to sensitive data. *European Data Protection Law Review, 2*, 297–311. https://doi.org/10.21552/EDPL/2016/3/6
Kahneman, D. (2011). *Thinking, fast and slow*. Farrar.
Kamangar, A. (2020). A literature review of customer behaviour patterns on e-commerce websites using an eye tracker. *The Marketing Review, 20*, 73–91. https://doi.org/10.1362/146934720X15929907504102
Kindt, E. J. (2013). *An introduction into the use of biometric technology. Privacy and data protection issues of biometric applications: A comparative legal analysis*. Springer Netherlands.
Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review, 34*, 523–538. https://doi.org/10.1016/j.clsr.2017.11.004
Kröger, J. L., Lutz, O. H., & Müller, F. (2020). *What does your gaze reveal about you?* Springer International Publishing.

Krueger, R., Koch, S., & Ertl, T. (2016). Saccadelenses: Interactive exploratory filtering of eye tracking trajectories. *IEEE Second Workshop on Eye Tracking and Visualisation (ETVIS),* 31–34.

Kuner, C., & Gkotsopoulou, O. (2021). *Article 9. Processing of special categories of personal data. The EU general data protection regulation: A commentary/update of selected articles*. Oxford University Press.

Laeng, B., & Falkenberg, L. (2007). Women's pupillary responses to sexually significant others during the hormonal cycle. *Hormones Behavior, 52*, 520–530. https://doi.org/10.1016/j.yhbeh.2007.07.013

Larrazabal, A. J., Cena, C. G., & Martínez, C. E. (2019). Video-oculography eye tracking towards clinical applications: A review. *Computers in Biology and Medicine, 108*, 57–66. https://doi.org/10.1016/j.compbiomed.2019.03.025

Lee, B. K., & Lee, W. N. (2004). The effect of information overload on consumer choice quality in an online environment. *Psychology & Marketing, 21*, 159–183. https://doi.org/10.1002/mar.20000

Lee, N., Broderick, A. J., & Chamberlain, L. (2007). What is 'neuromarketing'? A discussion and agenda for future research. *International Journal of Psychophysiology, 63*, 199–204. https://doi.org/10.1016/j.ijpsycho.2006.03.007

Lee, N., Chamberlain, L., & Brandes, L. (2018). Welcome to the jungle! The neuromarketing literature through the eyes of a newcomer. *European Journal of Marketing, 52*, 4–38. https://doi.org/10.1108/EJM-02-2017-0122

Liebling, D., & Preibusch, S. (2014). Privacy considerations for a pervasive eye tracking world. *UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing,* 1169–1177. https://doi.org/10.1145/2638728.2641688.

Malhotra, N. K., Jain, A. K., & Lagakos, S. W. (1982). The information overload controversy: An alternative viewpoint. *Journal of Marketing, 46*, 27–37. https://doi.org/10.2307/3203338

McStay, A. (2018). *Emotional AI: The rise of empathic media*. SAGE Publications.

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society, 7*. https://doi.org/10.1177/2053951720904386

Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: A guide to the role of auditing in the proposed European AI regulation. *Minds and Machines, 32*, 241–268.

Morin, C. (2011). Neuromarketing: The new science of consumer behavior. *Society*, *48*, 131–135. https://doi.org/10.1007/s12115-010-9408-1

Munoz, D. P., Broughton, J. R., Goldring, J. E., & Armstrong, I. T. (1998). Age-related performance of human subjects on saccadic eye movement tasks. *Experimental Brain Research, 121*, 391–400. https://doi.org/10.1007/s002210050473

Orlando, S. (2023). Diritto e nuove tecnologie. Rubrica di aggiornamento dell'OGID. *Persona e Mercato, 4,* 697–728. http://www.personaemercato.it/wpcontent/uploads/2023/01/Osservatorio.pdf (accessed 30 October 2023).

Partala, T., Jokiniemi, M., & Surakka, V. (2000). Pupillary responses to emotionally provocative stimuli. *Proceedings of Eye Tracking Research & Application Symposium (ETRA).*https://doi.org/10.1145/355017.355042

Protheroe, J., & Rennie, A. (2020). Decoding decisions: Making sense of the messy middle. https://www.thinkwithgoogle.com/_qs/documents/9998/Decoding_Decisions_The_Messy_Middle_of_Purchase_Behavior.pdf (accessed 30 September 2023).

Rayner, K. (1998). Eye movements in reading and information processing: 20 years of research. *Psychological Bulletin, 124*, 372–422. https://doi.org/10.1037/0033-2909.124.3.372

Rebera, A. P., & Mordini, E. (2013). Biometrics and ageing: Social and ethical considerations. In M. Fairhurst (Ed.), *Age factors in biometric processing* (pp. 37–62). Springer.

Schatten, M., Baca, M., & Rabuzin, K. (2008). International conference on a taxonomy of biometric methods. Information Technology Interfaces (ITI). https://www.frontex.europa.eu/assets/Publications/Research/Technology_Foresight_on_Biometrics_for_the_Future_of_Travel_Annex_II.pdf (accessed 30 September 2023).

Seaman, J. A. (2008). Black box. *Emory Law Journal, 58*, 427–488.

Simon, H. A., Egidi, M., Marris, L. R., & Viale, R. (1992). *Economics, bounded rationality and the cognitive revolution*. Edward Elgar Publishing Limited.

Smidts, A. (2002). *Kijken in Het Brein: Over de Mogelijkheden Van Neuromarketing*. Erasmus Research Institute of Management (ERIM).

Stephens, R. (1997). A survey of stream processing. *Acta Informatica, 34*, 491–541. https://doi.org/10.1007/s002360050095

STOA. (2022). *Regulatory divergences in the draft AI Act. Differences in public and private sector obligations.* Study. EPRS. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729507 (accessed 30 September 2023).
Sumer, B. (2022). When do the images of biometric characteristics qualify as special categories of data under the GDPR?: A systemic approach to biometric data processing. *IElectrical and Electronics Engineers (IEEE) Xplore, 329*. https://doi.org/10.1109/BIOSIG55365.2022.9897034.
Sunstein, C. R. (2000). *Behavioral law and economics*. Cambridge University Press.
Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*, 1124–1131.
Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*, 97–112. https://doi.org/10.9785/cri-2021-220402
Wilson, R. M., Gaines, J., & Hill, R. P. (2008). Neuromarketing and consumer free will. *Journal of Consumer Affairs, 42*, 389–410. https://doi.org/10.1111/j.1745-6606.2008.00114.x
29Working Party. (2007). *Opinion 4/2007 on the concept of personal data* (No. WP 136).
29Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies* (No. WP 193).
29Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, (No. 844/14/EN WP 217).
29Working Party. (2017a). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (No. 17/EN WP 251).
29Working Party. (2017b). *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679* (No. WP 248 rev.01).
Zaborska, S. (2019). Legal regulation of the protection of biometric data under the GDPR. *Studia Iuridica Lublinensia, 28*, 97–115.
Zamir, E., & Teichman, D. (2018). *Behavioral law and economics*. Oxford University Press.

Cases

Lindqvist (case C-101/01)
ECLI:EU:C:2003:596
OT v Vyriausioji tarnybinės etikos komisija (case C-184/20)
ECLI:EU:C:2022:601
Peter Nowak v Data Protection Commissioner (case C-434/16)
ECLI:EU:C:2017:994

Legislation

Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (2021) COM/2021/206 final
Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016) OJ L 119/1
Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (2022) OJ L 277/1

This contribution was written as part of the Ph.D. programme in which the author is enrolled (2021–2024).