ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2026-03-09

Deposited version:
Accepted Version

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Pereira, A. da C. (2025). Data, AI systems, and society: Ethical dilemmas in the digital age. AI and Ethics. 5 (6), 6007-6016

Further information on publisher's website:
10.1007/s43681-025-00834-1

Publisher's copyright statement:
This is the peer reviewed version of the following article: Pereira, A. da C. (2025). Data, AI systems, and society: Ethical dilemmas in the digital age. AI and Ethics. 5 (6), 6007-6016, which has been published in final form at https://dx.doi.org/10.1007/s43681-025-00834-1. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

Data, AI Systems, and Society: Ethical Dilemmas in the Digital Age

Abstract:

Collecting and using biometric data in AI systems presents significant ethical, legal, and societal challenges. This paper critically examines the interplay between emergent AI technologies, normative ethics, and governance, drawing from an experiment on emotionally embedded cognition and applications used during the COVID-19 pandemic. Ethical and regulatory frameworks underscore the pivotal role of governance in mitigating risks associated with AI. The European Union's Artificial Intelligence Act establishes critical boundaries by categorizing AI systems based on risk levels, prohibiting those deemed unacceptable, and imposing strict compliance requirements on high-risk systems, including biometric surveillance tools. The text explores key concerns such as data privacy, consent, and normative regulation, proposing an ethical framework grounded in regulation, digital literacy, and shared responsibility. This paper contributes to ongoing debates on ensuring ethical and equitable AI innovation by situating data governance within broader AI ethics.

Keywords: AI ethics, digital literacy, AI governance, risk, regulation, responsible AI.

Introduction

The rapid advancement of artificial intelligence (AI) and data-collection technologies has led to complex ethical dilemmas and risks, particularly regarding privacy, autonomy, and societal impact. Biometric tools, encompassing facial recognition and emotion detection, have transformative potential but also introduce the likelihood of misuse, bias, and lack of transparency.

Scholars in surveillance and biometric studies [1; 2; 3; 4] have long emphasized power asymmetries, institutional control, and trust deficits that shape how biometric data is collected, interpreted, and governed. While this paper does not elaborate on their work in depth, it engages with the broader ethical conversation they have helped define.

Risks and challenges include:

1. **Privacy and consent** are crucial, as biometric and personal data collection often lack informed consent and transparency, raising significant ethical concerns regarding surveillance and unauthorized data usage.
2. **Algorithmic bias**, as AI systems trained on non-representative datasets risk reinforcing inequalities in biometric recognition and physiological assessments, disproportionately affecting marginalized groups.

3. **Commodification**, as data, whether personal, physiological, or biometric, is increasingly monetized, raising concerns about ownership, commercial exploitation, and autonomy.

Besides biometric technologies, other techniques concerning the collection of broader physiological data, including neuroimaging, bio signal monitoring, and brain-computer interfaces (BCIs), raise similar ethical dilemmas. Although not all of these technologies fall under the legal definition of biometrics, they similarly engage with sensitive personal information. They are increasingly subject to regulatory scrutiny, particularly within the framework of the EU AI Act [5].

The EU AI Act (2024) [5] defines "biometric data" as information that enables the authentication, identification (Art. 3(15)), or recognition of individuals' emotions (Art. 3(39)). Additionally, the EU AI Act (2024, recital 17, p.9) adopts the GDPR definition of "personal data" as "any information relating to an identified or identifiable natural person" (GDPR Art. 4(1), p. 13 of the Official Journal of the European Union, Regulation (EU) 2016/679). Therefore, any data that can be linked to a person, directly or indirectly, constitutes personal data, including behavioral patterns, physiological signals, and other similar data. However, not all personal data falls into the categories of biometric data or physiological data.

Under the EU AI Act, AI systems processing biometric data for identification purposes are treated as high-risk (Art. 3(15), Annex III). However, the Act also classifies AI systems processing other forms of sensitive physiological or health-related data, such as emotion recognition systems (Art. 3(39)) or AI embedded in medical devices, as high-risk. This means that even when physiological or neurocognitive data do not fall under biometric identification, they remain ethically and legally significant within the EU regulatory framework.

Leveraging insights from an experiment on emotionally embedded cognition [6] and drawing on examples from applications launched during the COVID-19 pandemic [7], the paper discusses how AI tools for collecting biometric, personal, and physiological data challenge traditional ethical frameworks. It emphasizes the need to integrate regulatory, educational, and technological measures to address these emerging challenges.

The following question guides this reflection: *How can ethical governance frameworks address the challenges posed by biometric, physiological, and personal data in AI systems*? To address this question, the paper considers: what regulatory instruments, such as the EU AI Act, offer in terms of legal safeguards; how digital literacy can be differentiated across societal actors to foster meaningful engagement; and what models of shared responsibility are needed to balance innovation with ethical accountability.

To guide this reflection and answer such questions, this paper proposes a conceptual framework based on three interconnected pillars: regulation, digital literacy, and shared responsibility. Regulation provides legal safeguards such as those outlined in the EU AI Act; digital literacy empowers stakeholders to engage with technologies critically; and shared responsibility encourages cooperative governance among institutions, corporations, and individuals. This framework will be used to examine the ethical and societal dilemmas posed by biometric, physiological, and personal data in AI systems. This framework aims to align technological innovation with transparency, accountability, and ethical governance, thereby promoting an inclusive digital future.

The Ethical Landscape of Emerging Data Types in AI Systems

The ethical landscape of biometric AI technologies is shaped not only by technological capabilities but also by the complex social, political, and institutional contexts in which these systems operate. Scholars such as Ajana [1], Molnar [3], Lyon [2], and Aas [4] emphasize that biometric technologies are embedded within power relations that often disproportionately affect marginalized groups, raising concerns about surveillance, control, and systemic inequalities. These technologies do not exist in a vacuum but interact with societal structures that influence who benefits and who is disadvantaged. Complementing this sociological perspective, Lupton's [8] analysis of risk highlights how digital and biometric surveillance reconfigure traditional notions of safety, vulnerability, and agency, producing new forms of uncertainty and exposure for individuals. Similarly, Beck's risk society framework [9] is essential for understanding how biometric AI systems contribute to a reflexive modernization process, where societies must manage emergent technological risks that are complex, global, and often unintended. Together, these perspectives underscore the necessity of moving beyond purely technical or legalistic understandings of biometric AI ethics toward a more holistic view that accounts for social justice, governance, and cultural implications. Recognizing the interplay between risk, power, and ethical responsibility is critical to developing frameworks that ensure equitable, transparent, and accountable deployment of AI technologies, dealing not just with biometrics but also with other identification, personal, medical, or physiological types of data.

Emerging trends in neuroscience and machine learning highlight the potential of biometric neuro data and physiological data to enhance our understanding of cognitive and emotional states, as well as health and well-being. As we build on these technological advances, it's essential to consider these innovations within their broader ethical and societal contexts. While machine learning enables detailed classifications of mental and physiological states through EEG and PPG data, the collection and use of this sensitive information present significant risks that go beyond technical problems, including risks of misuse, commodification, and privacy breaches. Addressing these risks requires a comprehensive ethical framework that tackles privacy, security, and social justice concerns inherent in the deployment of AI systems. Hence, legislative frameworks must strike a balance between the benefits of these data types for scientific, medical, or societal advancements and the risks they pose to individual autonomy and security.

It is essential to emphasize the distinction between neuro data, other types of physiological data, and biometric data in legal and ethical terms. Patterns of brain activity, such as alpha, beta, or theta waves measured through EEG, are not considered biometric data per se unless they are processed to identify or verify an individual's identity. According to Article 3(15) of the EU AI Act, biometric data refers specifically to physical, physiological, or behavioral characteristics used for identification or authentication. Therefore, while neurotechnological tools may process physiological signals, their outputs only qualify as biometric if used in a context where identification is the objective, such as, e.g., in brain print-based authentication systems. In this paper, we refer to such types of data in a broader ethical sense, acknowledging their sensitivity and potential implications without asserting that all of them are the same, particularly under EU law.

For instance, various machine-learning techniques can differentiate between different mental states, including neutral, rested, or focused states, as well as positive and negative emotional states. EEG brainwave data, as demonstrated by Bird et al. [10], showed that a low-resolution EEG headband can effectively classify a person's emotional state, providing concrete evidence of the practical applications of classification algorithms in real-world decision support systems. Another example cited by Kellmeyer [11] is the model used in thalamocortical dysrhythmia (TCD), which identifies connectivity oscillation patterns in patients with Parkinson's disease, neuropathic pain, tinnitus, and depression [12].

However, there are also valid concerns regarding privacy and security when these technologies are used directly by consumers or patients. The data collected can be vulnerable to risks such as unauthorized use, commodification, and dissemination, including personal data on blood pressure, heart conditions, sleep patterns, and fitness application records. According to Kellmeyer [11], companies responsible for safeguarding this information may face technological obstacles, including issues with encryption and data transfer.

Finally, regarding personal, biometric, and physiological data, careful handling and efficient decision-making are necessary when implementing programs involving public participation during emergencies, such as the COVID-19 pandemic. In such cases, it is crucial to consider how data collection should be managed, the extent to which risk management is vital for successful compliance, and the role of advanced technological research in the process. Governments, tech companies, and the general public must address issues of equal access, privacy, security, relevance, and usefulness. To achieve this, it is essential to emphasize the importance of responsibility, accountability, law or regulation, and digital literacy as three key factors that warrant exploration.

The Role of Responsibility in Ethical Data Practices

Accountability in the context of data collection requires recognizing its innovative and transformative dimensions while mitigating harm. Ethical responsibility extends to researchers, developers, and policymakers who must collaborate to establish trust, uphold transparency, and ensure biometric data usage aligns with societal values. Thus, the paper argues for a collective approach to ethical decision-making in the biometric field based on Tomasello's concept of shared intentionality. Being a responsible member of society involves recognizing and attributing expertise to specific behavioral patterns and upholding trustworthiness to maintain moral standards within a given cultural context. It is essential to collaborate with others who share the same objectives and values, and to cooperate in decision-making processes and exchange ideas. This involves emotional understanding, empathy, and insight, as Tomasello et al. described through their concept of "shared intentionality," i.e., participation in collaborative activities requires a unique form of cognitive representation and motivation to share psychological states. Empathy and emotional intelligence are essential in understanding and sharing others' feelings, but competition and power struggles can also arise [13]. So, negotiating and weighing the benefits and risks of physiological and biometric data management when working towards shared goals (like in the case of the pandemic) is essential to ensure ethical

behavior and regulation efficacy, like the proper implementation of social and legal structures, and a positive impact.

However, the case of creating artificial agents or operators with recognizable ethical reasoning capabilities is daunting for those in robotics and artificial intelligence. It necessitates the ability of machines to compute judgments on potential decisions and explain why a decision is ethical or not. This is a challenging endeavor because of the multiple sources of human subjectivity involved in ethical dilemmas and decision-making processes that machine learning and deep learning algorithms cannot fully replicate (yet). As Bryson [14] puts it, since humans are accountable for designing and determining the features and commercial exchange of these agents, the issue of ethics is not just a descriptive matter of the moral status of these agents. It is a normative issue of whether the intended societal outcomes of their successful implementation are ethically acceptable. For instance, Europe's "Stay-away COVID-19 app" has created concerns about security, data privacy, and legitimacy. [7] It was free and voluntary, but it lacked ensuring the privacy of individuals and proper data handling by analysts or intelligent systems. It is also crucial to establish the legal status of robots and applications. Particularly now that Tesla, OpenAI, and possibly others are already preparing to create robots and operators on a large scale in the next few years.

According to Bryson [14], normative ethics is about recommendations on what should be done to achieve ethical outcomes. According to our reflection, such recommendations could foster literacy and awareness among the public. Nevertheless, the innovation of norms depends on the mechanisms by which new norms are conceived, the conditions under which they extend and advance through a society, the people involved, whom they reach, and how they become instrumentalized by certain powers and interests. For instance, as discussed earlier, this was evident when implementing the COVID-19 app, which was presented as a good choice for protection and public health benefits. Despite privacy fears, it was recommended that the app be used, as it was a voluntary action. However, in some countries, it was unclear whether it violated the general principles of the data protection EU law [15], like transparency, integrity, security, accountability, and confidentiality. Besides, according to the data guidance, Law 52/2020 established directives for the voluntary use of the application. This legislation ensured that the app's usage remained optional, aligning with data protection principles and safeguarding personal freedoms and privacy [7]. However, there were issues with its design, especially the Bluetooth connection, which allowed users' locations to be easily detected. The app's low usage was probably due to a failure to uphold such ethical standards and provide complete explanations of its usefulness and purpose. This is problematic, showing that ethical explanations on usefulness and the proper regulation are needed whenever a new device or application for general public use is produced or installed. The COVID-19 contact tracing app, while not a biometric identifier in a narrow legal sense, exemplifies public concern around datafication, ethical accountability, and digital trust in times of crisis. It serves here as an example to reflect on the broader dynamics of regulation, transparency, and digital literacy.

Ethical Regulation and Innovation

Ethics is a set of norms, rules, or regulations that ensure technological behavior is consistent with human values, as making ethical decisions leads to good choices and efficient action [16]. While legal requirements, rulings, and sanctions are central to decision-making and individual roles, norms are not fixed or timeless. They may require negotiation for a new social order to emerge. However, discussions over critical issues may be extended until a new social order is established. The new principles form a complex set of rules that govern conduct and ensure compliance with the prescribed standards within a specific culture, group, or institution. They are a social mechanism that controls human interactions and conflicting interests, allowing for efficient everyday life.

Therefore, technological advancement raises crucial questions about the ethical treatment of data and the responsible use of emerging devices and applications. This is especially relevant when such devices collect multivariate physiological data to decode neurophysiological and behavioral states, such as sleep, readiness, and oxygen levels, or when used in biometric identification. [cf. 11; 17; 18]. This underscores the need for interdisciplinary dialogue among professionals to understand the impact on society and to integrate it with public health and education policy questions, to name a few sectors of society.

Understanding the links between technological dimensions and their health, cultural, and symbolic implications raises critical normative questions. These include how neuronal, biometric, and physiological data are treated and the ethical assessment of their benefits and risks. This includes rules on data access, literacy regarding physiological and biometric data collection and analysis, and the responsible conception and use of technological tools. Regulatory issues concerning the protection of personal, physiological, and biometric data, as well as the management of associated risks, are central to ethical reflections in technologically advanced societies. This is particularly true in the context of the ongoing digital transformation.

To understand the complex relationships between different dimensions of technology and society, we must examine their unique characteristics. This includes the neurobiological, sociocultural, and historical contingencies of technology, and how they connect to social, cultural, and symbolic systems (cf., e.g., [19]).

These aspects, along with how people interpret them, allow for a critical assessment of their potential for broader real-world applications. Digital literacy and ethical awareness are now fundamental topics of discussion, especially in a world where disproportionate power is increasingly concentrated.

Digital Literacy and Ethical Awareness in Scientific Research

Digital literacy empowers individuals to navigate the ethical landscape of physiological and biometric technologies. Therefore, the paper advocates public and institutional education programs to enhance awareness of data rights, security practices, and the implications of research in this field, highlighting the importance of fostering critical thinking and ethical reflection in an increasingly digital society.

Digital literacy [20] involves various skills, including essential computer operations, navigating the internet, evaluating digital information, effective communication via digital platforms, and media literacy. Additionally, it involves understanding the importance of protecting personal information online and recognizing potential dangers and threats associated with digital technologies. Thus, ethical awareness plays a crucial role in digital literacy and societies, encompassing ethical considerations about digital citizenship, integrity, and inclusion. These aspects are critical because people must make informed decisions and choices while fully aware of the implications of digital applications, AI operators and systems, their uses, potential dangers, benefits, disadvantages, and reach. To enhance digital literacy and ethics awareness, it would be good to implement government programs and educational curricula in schools, universities, and public libraries [21; 22] to promote responsible and ethical use of digital technologies and systems.

Individuals should be empowered to make informed decisions and navigate digital environments responsibly and informedly. Critical thinking skills are vital for evaluating digital information and recognizing bias, which can help individuals become discerning digital consumers and creators or providers of information and data. To engage responsibly and ethically online, digital citizens must respect others' rights and privacy and practice ethical online behavior, including sharing accurate and reliable information. Companies also have ethical responsibility and should be accountable for such matters. So, efforts should be made to bridge the digital divide and ensure, or at least promote, equal access to digital resources and opportunities for all to participate in studies, networks, and platforms, and be well-informed and aware, besides making those in charge of information and data responsible for its management. Therefore, it is fundamental that governments, other systems, and institutions promote discussions and awareness about digital literacy and ethics (as a common good), as they can help shape policies, regulations, and ethical frameworks governing digital interactions. This way, individuals can confidently and ethically navigate the digital world by prioritizing digital literacy and ethics, contributing to developing inclusive and thriving digital societies and research [23].

Case Study: Emotionally Embedded Cognition Research

This example serves to underscore the importance of integrating digital literacy, regulation, and responsibility into ethical governance, particularly in the context of physiological data, biometric data, health-related data, and personal data. By fostering collaboration and public engagement, society can handle the challenges posed by these technologies while maximizing their benefits. The following case study, grounded in multidisciplinary research on cognition, illustrates the complexities of physiological data collection and provides further insight into the issue.

This case study reports an experiment on emotionally embedded cognition conducted during the COVID-19 pandemic. The study utilized EEG and PPG data to assess emotional and cognitive responses in digital environments. The objective was to explore emotional responses to different environments and their effects on cognition, comparing Zoom-based classes with in-person classes. However, several obstacles emerged: participant dropout due to pandemic-related restrictions, technical constraints in physiological data collection, and risks regarding safety,

transparency, and voluntary participation. This case study underscores the importance of ethical governance in research, such as biomedical research, including design, data collection, and treatment, highlighting the need for adaptive regulations and public awareness of data rights.

The loss of research participants in collecting data (from April to July 2021) due to COVID-19 led to a small experimental sample. Additionally, the pandemic led to the abandonment of the classes' in-person condition, which prevented a comparison of both situations as previously intended. The pandemic constraints posed many ethical challenges and compromised the accuracy of results, leading to a profound reflection on the study design, risks, and implications.

Ethical Reflections on Research Design and Execution

Although the research design prioritized ethical approval, transparency, informed consent, and participant well-being, various obstacles emerged due to the COVID-19 pandemic. Difficulties included logistical constraints, such as limited participant access, schedule disruptions, and adapting to new protocols that complied with pandemic-related safety measures. Despite these difficulties, ethical rigor was maintained, enhancing participant trust and the validity of the research data collection.

The study consisted of two phases: an initial survey on literacy and perceptions of technological tools, involving 300 students, and a lab experiment assessing physiology metrics, emotions, and environmental engagement. The lab experiment involved 16 students, during which physiological data were collected using a headband that recorded EEG and PPG signals. The Stroop test evaluated cognitive interference, while two neuropsychological scales measured emotional states: the Maslach Burnout Inventory for Students and the Profile of Mood States. The assessment included multiple-choice questions and a five-point Likert scale to evaluate environmental engagement, administered via Google Forms.

However, the pandemic required significant adaptations. For example, while the initial survey of 300 participants was feasible without direct contact, the in-person experiment faced restrictions, as direct contact and laboratory visits were required. Ultimately, data collection was limited to the digital environment, excluding participants from in-person classes and relying primarily on PPG data due to issues with EEG recordings and other technical constraints related to access. This meant that balancing the study's objectives with logistical and ethical considerations proved complex in such a scenario. Additionally, pandemic-related delays, class cancellations, and participant availability posed significant barriers. The research had to adopt continuous safety measures that were rigorously followed, including sanitization, physical distancing, and protocols that addressed COVID-19-specific risks, such as regular testing requirements to use faculty facilities and labs.

The case study on emotionally embedded cognition underscored the critical intersection of research ethics, education, and public health, highlighting the complex interplay between these fields. However, the feedback from participants was positive. They appreciated being part of the study, particularly during isolation, highlighting this factor as a reason to participate, and were curious about it. They appreciated the transparency of the process and the precautions being taken. While the logistical limitations prevented simultaneous experiments with multiple students, the study's

adaptation to individual lab sessions ensured controlled, safe, and ethical data collection standards. Despite these efforts, the sample size and data robustness were compromised due to a lack of people, and the results were ultimately treated as exploratory rather than definitive. Nevertheless, fundamental lessons from this experience, which are the subject of reflection in this article, include the importance of flexibility in research design, securing a reliable data collection process, and maintaining responsible ethical practices under constrained conditions. In conclusion, in this case, the pandemic impacted data collection, research design, and, ultimately, the process of analysis and data management. The impacts are summarized in the following table.

Table 1- EECH Case-study data collection research impacts

Research Impacts	Description
Inference limitations	The sample size limited the inferences from the findings, rendering the results exploratory rather than representative and precluding a comparison of both situations or conditions as initially planned.
Participant dropout	Recurrent COVID testing and rigorous safety measures mitigated risks but did not eliminate participant dropout from the first phase (survey) to the second phase (the experiment).
Technical constraints	Ensuring proper technical procedures regarding access rights, records, functionality, and licensed materials and applications is crucial for achieving the best results; despite all care, technical constraints, such as access to servers and the state of data recordings, may still arise.
Innovation and adaptability	The study demonstrated innovation and adaptability, providing a foundation for future research with more diverse participant groups and enhanced preparation for unexpected events and occurrences.

Discussion: Ethical Implications of Data Collection Tools

The case study on emotionally embedded cognition provides a lens through which to examine the dual-edged nature of intelligent data collection tools and applications. On the one hand, these technologies offer transformative possibilities in fields such as neurology, psychiatry, and public health. Several tools have shown potential in the early detection of Alzheimer's and Parkinson's disease through neuroimaging, predicting responses to chemotherapy, and distinguishing between typical and atypical Parkinson's syndromes [11]. In psychiatry, machine-learning techniques have been used to anticipate psychosis, detect depressive symptoms, and predict suicidal behavior from social media activity [11]. These studies highlight the growing role of artificial intelligence in analyzing human emotions, physiology, and mental health states.

Despite these benefits, data reliability, technical limitations, and participant disengagement as presented through the example above underscore the need for robust ethical measures and safeguards. However, in online applications, concerns over privacy and the potential misuse of autonomously gathered data present additional barriers to widespread adoption. Even when physical risks to individuals are minimal, security, privacy, and the impact of real-time interactions

between users and devices raise concerns about autonomy and agency [11]. Questions also arise about participants' awareness and understanding of data use [24; 25]. Furthermore, ethical dilemmas intensify when machine-learning models autonomously interpret neural data or intervene in brain states through closed-loop systems [11]. To ensure that technologies fulfill their promise without exacerbating existing inequalities, policymakers, researchers, and developers must collaborate to establish inclusive and transparent practices and innovation with responsibility. As outlined earlier, this analysis is guided by a three-pillar framework—regulation, digital literacy, and shared responsibility—that together offer a basis for ethical governance in AI systems.

Risk, Ethics, and Data Governance

Ulrich Beck's [9] concept of the risk society provides a valuable framework for understanding how technological progress introduces new and unpredictable uncertainties. Beck argues that modernization produces global risks that exceed the control of traditional social institutions. Technological advancements, ranging from biomedical and neuroscientific research to physiological apps and biometric technologies, align with this paradigm, calling for new governance approaches. Beck's concept of reflexive modernization emphasizes that societies must critically assess and regulate these risks rather than accept them as inevitable [9].

Like Beck, sociologist Deborah Lupton [8] recognizes risk as central to governance, shaping how institutions and individuals respond to uncertainty. Expanding Beck's work by incorporating a Foucauldian perspective, Lupton highlights how risk operates as a form of social control, arguing that governments, corporations, and the media shape public perceptions of risk, influencing behaviors through surveillance, discourse, and emotional appeals. The COVID-19 pandemic exemplifies this dynamic, where risk narratives justified health surveillance measures. To counter this, Lupton encourages individuals to take responsibility for managing their own risks, for instance, by monitoring digital self-tracking tools, adopting healthier lifestyles, or making informed choices (cf. [8], pp. 114-122).

The collection and analysis of physiological and biometric data—mainly when driven by artificial intelligence (AI)—must be governed by robust ethical frameworks that prioritize transparency, security, and respect for individual autonomy. Ensuring that individuals understand how their data is used remains a pressing challenge. As emerging technologies evolve, fostering ethical literacy and institutional accountability becomes essential for managing the risks and uncertainties inherent in our increasingly digital society.

The responsible use of biometric and digital technologies in domains such as surveillance, biomedical research, public health, and personal care requires ongoing ethical reflection. The pandemic highlighted tensions between public health imperatives and individual rights, demonstrating that exceptions to standard ethical protocols may sometimes be necessary. Still, concerns about participant safety, data privacy, and research transparency must never be overlooked. Open, informed public debate is crucial for legitimizing policies governing biometric data and related technological advances.

Even with consent, commercialization and monopolization of personal data remain critical concerns [11]. Hence, transparency in data use is essential, particularly in research settings where normative confidentiality measures and distinctions between participation and data disclosure consent must be communicated.

The classification of personal data sources—including medical records, neurophysiological data, fitness trackers, wearables, and social media activity—requires rigorous ethical scrutiny. Whether data arises from medical imaging, movement-tracking apps, or online behavior, organizations must ensure the proportional and responsible use of this data (e.g., [26]). Skilled data analysts are vital for the correct interpretation of biometric data to prevent misrepresentation and misuse [11]. While academic institutions often uphold strict ethical standards and promote digital literacy, such safeguards are inconsistently applied in private and public sector biometric and surveillance systems. The use of electronic health records or AI analysis of social media data to infer neurophysiological states raises urgent ethical and privacy concerns, demanding comprehensive legislation across sectors.

The EU Artificial Intelligence Act

Addressing ethical dilemmas related to data use requires clear distinctions between acceptable and unacceptable outcomes, especially when repurposing big data analytics beyond their original intent. Digital literacy is essential, and governments must implement targeted programs to empower individuals and organizations with the skills to critically assess how data is collected, processed, and used.

Several initiatives illustrate this educational push. For example, the European Commission's *Digital Education Action Plan (2021–2027)* promotes AI and data literacy across EU member states by supporting targeted initiatives in schools, higher education, and lifelong learning [27]. Similarly, UNESCO's *Media and Information Literacy* program promotes critical thinking and digital skills globally, helping citizens understand and navigate digital ecosystems, including AI and data-driven technologies [28].

Equally important is robust regulation to prevent indiscriminate or harmful use of data. The EU AI Act [5] provides a comprehensive legal and ethical framework covering diverse AI applications, including biometric AI. It sets legal, technical, and procedural standards to ensure AI systems are safe, transparent, accountable, and respectful of fundamental rights.

The EU AI Act [5] offers a risk-based framework for all AI applications, including biometric systems. Article 3(15) defines biometric data as physical, physiological, or behavioral characteristics used for identification or verification, while Article 3(39) introduces emotion recognition systems. Both categories are classified as high-risk under Annex III when used in sectors such as education or employment, triggering specific obligations for AI providers, including ensuring transparency, enabling human oversight, and implementing risk mitigation measures.

As summarized in Table 2 below, the EU AI Act categorizes AI systems into four risk levels—prohibited, high-risk, limited-risk, and minimal-risk—each carrying specific legal obligations. For instance, real-time biometric surveillance is prohibited in most contexts, while AI used in education or employment is subject to strict oversight requirements.

Table 2 - AI Risk Classification (Adapted from Annex III, EU AI Act 2024) [5]

Risk Type	Description
Prohibited AI practices	AI applications that pose threats to fundamental rights, such as social scoring or real-time biometric surveillance in public spaces, except in specific policing contexts.
High Risk	AI systems in critical sectors (e.g., education, law enforcement, healthcare) must comply with requirements such as risk assessment and human oversight.
Limited Risk	Systems that use biometric categorization or generate deepfakes must ensure transparency towards users.
Minimal Risk	Low-risk applications (e.g., spam filters, video games) that are not subject to binding obligations but are encouraged to follow ethical principles.

The EU AI Act also includes specific provisions for biometric identification, emotion recognition, and deep-fake technologies. Emotion recognition systems are banned in educational and workplace settings due to ethical concerns and risks of misuse. AI-generated deepfakes must be clearly labeled to prevent misinformation [5].

The regulation applies to all AI systems placed on the EU market, used within the EU, or affecting EU citizens, regardless of the provider's location. It excludes applications used solely for military, defense, or research purposes. Its overarching goal is to foster trustworthy, human-centric AI while safeguarding fundamental rights, democracy, and sustainability [5].

The COVID-19 app case (see "Role of Responsibility" section) similarly illustrates how emergency-driven data collection must balance public health imperatives with privacy safeguards. While public health needs may justify temporary surveillance, governments must ensure data collection remains transparent, time-limited, and proportionate. Additionally, policies related to user consent, third-party access, and data reuse must be clearly communicated to avoid erosion of trust and democratic accountability.

Ensuring ethical data handling requires understanding how agencies and governments approach technology, digital literacy, data protection, and risk assessment—factors that are shaped by political, historical, and systemic contexts. When properly regulated, predictive analytics can safely support emergency response during crises such as pandemics, natural disasters, and armed conflict, where swift, informed decision-making is essential.

Democratic institutions must develop comprehensive data-classification frameworks that both protect individual rights and enable socially beneficial uses of data. Secure offline storage and well-defined legal access controls are especially critical for managing sensitive health-related

information. Finally, ongoing public debate and interdisciplinary oversight are essential to ensure that emerging technologies ethically extend and enhance human capacities [cf. e.g., 29].

Conclusion

The ethical challenges of biometric and physiological data in AI extend from ensuring informed consent and transparent data practices to securing ethical oversight. Individuals must fully understand the objectives, potential risks (such as data sharing or pandemic-related safety measures), and the limitations of third-party data use. These safeguards uphold human dignity and rights as technological capabilities expand.

In response to the central question guiding this reflection, we argue that addressing the challenges posed by biometric and physiological data in AI systems requires a triangulated approach. Regulation provides the normative backbone through instruments like the EU AI Act, ensuring basic legal safeguards. Digital literacy, when differentiated by stakeholder group, empowers engagement with these systems in meaningful and rights-preserving ways. Finally, shared responsibility, grounded in relational ethics and cooperative intentionality, enables a governance model in which states, corporations, and citizens co-produce accountability. Together, these mechanisms offer a framework that is ethically responsive to the complexity of biometric and physiological data governance.

Tomasello's concept of shared intentionality supports a relational model of responsibility, where ethical governance emerges from mutual recognition and coordinated action. Applied to biometric AI, this suggests that ethical outcomes depend not on isolated actors but on institutions co-designing safeguards, corporations upholding transparent data practices, and individuals engaging critically with the technologies they use.

To navigate these complexities, the paper proposed a three-pillar framework:

1. **Regulation**: Robust legal instruments, such as the EU AI Act, establish baseline protections and obligations.
2. **Digital Literacy**: Tailored programs empower policymakers, developers, and citizens to understand and contest data practices.
3. **Shared Responsibility**: Coordinated action across state, corporate, and civil actors ensures accountability.

This paper is not intended to produce generalizable conclusions but rather to reflect on the ethical, methodological, and regulatory complexities of research data collection, management, and uses in constrained real-world contexts. The examples of case studies provided served to illustrate precisely this point.

Ensuring that data-driven technologies align with democratic values and human dignity will require more than regulation – it demands sustained digital literacy, public accountability, and cooperative governance rooted in shared ethical responsibility.

Author contributions

The author is solely responsible for researching and writing the manuscript.

Funding

No funding was received to support the preparation of this manuscript.

Data availability

Datasets were generated and analyzed during the study on EECH. However, the findings are not presented here, as they are not the core focus of the paper's argument. They can be provided by sending an email request to the author or by consulting reference [6].

Declarations

Conflict of interest

The author declares no competing interests.

References

[1] Ajana, B. (2013). *Governing through Biometrics: The Biopolitics of Identity*. Palgrave Macmillan.

[2] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.

[3] Molnar, P. (2019). "Technologies of Immigration Control: Biopolitics and the Border Regime," in A. Dijstelbloem & E. van Reekum (Eds.), *Imagining the Nation in Nature* (pp. 142–158). Routledge.

[4] Aas, K. F. (2006). "The body does not lie: Identity, risk and trust in technoculture." *Crime, Media, Culture*, 2(2), 143–158

[5]. Artificial Intelligence Act. (2024). http://.ai-act-law.eu

[6]. Pereira, A.: Emotional Response and Cognitive performance in digital environments: an exploratory study. Master's Dissertation. IBEB - Institute of Biomedical Engineering. Faculty of Sciences, University of Lisbon (2023). http://hdl.handle.net/10451/58938

[7]. DataGuidance. (2020). Portugal: Law No. 52/2020 on StayAway COVID App published. Retrieved August 19, 2024, from https://www.dataguidance.com/news/portugal-law-no-522020-stayaway-app-published

[8]. Lupton, D. (2013). *Risk* (2nd ed.). Routledge.

[9]. Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

[10]. Bird, J. J., Ekart, A., Buckingham, C. D., & Faria, D. R. (2019). Mental, emotional sentiment classification with an EEG-based Brain-Machine Interface. In *Proceedings of the International Conference on Digital Image and Signal Processing* (DISP'19), St Hugh's College, University of Oxford, UK. Retrieved from https://www.researchgate.net/publication/329403546

[11]. Kellmeyer, P. (2018). Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices. *Neuroethics, 11*(1), 1-16. https://doi.org/10.1007/s12152-018-9371-x

[12]. Vanneste, S., Song, J. J., & De Ridder, D. (2018). Thalamocortical dysrhythmia detected by machine learning. *Nature Communications, 9*, 1103. https://doi.org/10.1038/s41467-018-02820-0

[13]. Tomasello, M., Carpenter, M., Call, J., Behne, T., & Moll, H. (2005). Understanding and sharing intentions: The origins of cultural cognition. *Behavioral and Brain Sciences, 28*(5), 675-735. https://doi.org/10.1017/S0140525X05000129

[14]. Bryson, J. (2018). Patience is not a virtue: The design of intelligent systems and systems of ethics. *Ethics and Information Technology, 20*(1),15–26.https://doi.org/10.1007/s10676-018-9448-6

[15]. GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).1 (2016, May 4). *Official Journal of the European Union*, L 119, 1–88. https://gdpr-info.eu/

[16]. Greene, J. D., Sommerville, R. B., Nystrom, L. E., Darley, J. M., & Cohen, J. D. (2001). An fMRI investigation of emotional engagement in moral judgment. *Science, 293*(5537), 2105–2108. https://doi.org/10.1126/science.1062872

[17]. Farah, M. J. (2005). Neuroethics: The practical and the philosophical. *Trends in Cognitive Sciences, 9*(1), 34–40. https://doi.org/10.1016/j.tics.2004.12.001

[18]. Farah, M. J. (2012). Neuroethics: The ethical, legal, and societal impact of neuroscience. *Annual Review of Psychology, 63*, 571–591. https://doi.org/10.1146/annurev.psych.093008.100438

[19]. Damásio, A. (2018). *The strange order of things: Life, feeling, and the making of cultures*. Pantheon Books.

[20]. Gilster, P. (1997). *Digital literacy*. Wiley Computer Publishing.

[21]. McKeown, A. (2016). *Overcoming information poverty: Investigating the role of public libraries in the twenty-first century*. Chandos Publishing. https://doi.org/10.1016/B978-0-08-101110-2.00006-2

[22]. Nicholson, K. (2017). *Innovation in public libraries: Learning from international library practice*. Chandos Publishing. https://doi.org/10.1016/B978-0-08-101276-5.00001-1

[23]. Fulton, C., & McGuinness, C. (2017). Your learning in a digital world. In *Digital Detectives: Solving Information Dilemmas in an Online World* (pp. 9–17). Chandos Publishing. https://doi.org/10.1016/B978-0-08-100124-0.00002-7

[24]. Jamali, A., Berger, C., Spiteri, R. (2023). Momentary Depressive Feeling Detection Using X (Formerly Twitter) Data: Contextual Language Approach. Journal of Medical Internet Research AI 2:e49531. http://doi:10.2196/49531/ ai.jmir.org/2023/1/e49531

[25] Leis, A., Ronzano, F., Mayer, M., Furlong, L., & Sanz, F. (2019). Detecting Signs of Depression in Tweets in Spanish: Behavioral and Linguistic Analysis. *Journal of Medical Internet Research*. 21(6): e14199 https://www.jmir.org/2019/6/e14199 (DOI: 10.2196/14199)

[26]. Markus, B., Nzamba, B., Peeter, R., Sadok, B.Y., & Dirk, D., (2024). Evaluation of deep learning-based depression detection using medical claims data, *Artificial Intelligence in Medicine*,147 (102745), https://doi.org/10.1016/j.artmed.2023.102745.

[27] European Commission. (2020). *Digital Education Action Plan 2021–2027: Resetting education and training for the digital age* (COM/2020/624 final). Brussels: European Commission. https://education.ec.europa.eu/system/files/2022-01/deap-communication-sept2020_en.pdf

[28] UNESCO. (2021). *Media and Information Literate Citizens: Think critically, Click wisely*. Paris: UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000377068

[29]. Clark, A., & Chalmers, D. (1998). *The extended mind*. Analysis, 58(1), 7-19. https://doi.org/10.1093/analys/58.1.7