Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

REVIEW ARTICLE

Review Article

PRIVACY-BY-DESIGN IN EMOTION AI: DATA PROTECTION FRAMEWORKS AND COMPLIANCE STRATEGIES

Laroussi Chemlali* and Leila Benseddik

ABSTRACT

Background: *The rapid advancement of Emotion Artificial Intelligence (Emotion AI) has created significant opportunities for innovation across a broad variety of domains, including healthcare, marketing, and human-computer interaction. Emotion AI applications—which process, analyse, and respond to human emotions—rely heavily on sensitive personal data, resulting in privacy and ethical concerns. The implementation of Privacy-by-Design (PbD) principles within such systems is essential to counter these challenges and maintain compliance with changing legal frameworks. This paper discusses the interplay between PbD and Emotion AI, with a special emphasis on the privacy risks associated with the collection and processing of emotional data. The study is set against the broader background of developing ethical AI, emphasising the urgent need to balance technological innovation with robust privacy protection.*

Methods: *The paper provides a conceptual legal analysis of the intersection between Privacy-by-Design (PbD) and Emotion AI within modern data protection frameworks. It employs a comprehensive review of primary sources, including the EU GDPR,*

DOI:
https://doi.org/10.33327/AJEE-18-8.S-r000153

Date of submission: 21 Aug 2025
Date of acceptance: 02 Oct 2025
Online First publication: 04 Dec 2025

Disclaimer:

The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

the EU AI Act, CJEU and ECtHR jurisprudence, and guidance from Data Protection Authorities, alongside secondary sources like scholarly works and books. The discussion is structured first to provide an overview of Emotion AI, its applications, as well as individual privacy concerns it raises. This is followed by a consideration of existing data protection regimes and how they can be transferred to Emotion AI systems. The study then focuses on the fundamental principles of PbD, examining how they can be applied when developing and deploying Emotion AI technologies.

Results and Conclusions: *The analysis demonstrates that implementing PbD principles in Emotion AI systems is essential—not merely beneficial—for protecting users' privacy and ensuring legal compliance. Properly implemented PbD frameworks deliver three essential benefits: enhanced system transparency, stronger accountability mechanisms, and greater user control over their own data. These findings contribute significantly to the theoretical foundations of responsible AI design while offering actionable implementation guidance for organisations deploying Emotion AI systems. Finally, the study presents an unambiguous model for developers and organisations to successfully ride the wave of convergence between emotional intelligence technology and privacy regulations.*

1 INTRODUCTION

Emotion artificial intelligence technology, which can recognise and react to human emotions using information such as voice, facial expressions, and physiological signs, is a prevailing yet controversial invention as AI developments continue to transform sectors.[1] Although Emotion AI presents revolutionary prospects in healthcare, customer service, education, and other fields, it also poses serious questions around privacy, autonomy, and the ethical handling of sensitive emotional data. Traditional data protection paradigms are challenged by the capacity to collect and analyse such highly sensitive data, necessitating a strong and proactive reaction from companies, researchers, and regulators.[2]

This paper examines Privacy-by-Design (PbD) as a fundamental approach to addressing these ethical and legal issues. Stakeholders can guarantee adherence to data protection frameworks, including the General Data Protection Regulation (EU GDPR)[3] of the EU and comparable international regulations, as well as gain public trust in these cutting-edge

1 Andrew McStay, *Emotional AI: The Rise of Empathic Media* (SAGE Publications 2018) doi:10.4135/9781526451293.

2 Darlene Barker and others, 'Ethical Considerations in Emotion Recognition Research' (2025) 7(2) Psychology International 43. doi:10.3390/psycholint7020043; Andrew McStay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7(1) Big Data and Society 1. doi:10.1177/2053951720904386.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council 'On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' (27 April 2016) [2016] OJ L119/1.

technologies by incorporating privacy considerations into the development lifecycle of Emotion AI systems. The paper explores methods for implementing PbD principles into practice, while foreseeing future difficulties in striking a balance between human rights protection and technological progress.

By doing so, this paper aims to answer the following question: How can PbD principles be embedded into the development lifecycle of Emotion AI systems to foster robust data protection and compliance with privacy regulations? Therefore, this study offers a comprehensive understanding of how Emotion AI development can be aligned with contemporary compliance standards and ethical practices, ensuring a co-existence between innovation and privacy.

2 METHODOLOGY

This study was conducted as a conceptual legal analysis, aimed at understanding the intersection between the principle of PbD and the evolving use of Emotion AI within contemporary data protection frameworks. Although this study does not rely on empirical data collection, it employed a comprehensive review of primary and secondary legal materials. Primary sources included instruments, mainly the EU GDPR, along with the EU AI Act, ECtHR, and CJEU jurisprudence, as well as the Data Protection Authorities' Guidance. Secondary sources comprised mainly scholarly articles, books, and other relevant publications on the subject. The analysis proceeded in three stages. The paper presents a clarification of the conceptual foundations of PbD, drawing on its seven principles as articulated by Cavoukian. It then explores the implementation of the PbD in the Emotion AI setting. Finally, the paper was then followed by an examination of the compliance strategies proposed in existing frameworks, identifying practical enforcement challenges and gaps in regulatory guidance. By synthesising across legal systems and policy discourses, this conceptual analysis aimed not only to illustrate how PbD has been operationalised in the context of Emotion AI but also to point out where enforcement mechanisms fall short in practice.

3 UNDERSTANDING EMOTION AI AND ITS PRIVACY AND ETHICAL CONCERNS

3.1. Defining Emotion AI

Combining artificial intelligence with the intricate realm of human emotions, Emotion AI forms an intriguing link between technology and psychology. This field has increasingly evolved since Rosalind Picard's groundbreaking research in 1995,[4] and currently includes a variety of technologies that are able to recognise, understand, and react to human emotional

4 Rosalind W Picard, *Affective Computing* (Technical Report no 321, MIT Media Laboratory Perceptual Computing Section 1995).

states. To develop systems that can successfully interpret human emotional states, this complex field integrates machine learning, computer vision, and psychological insights.[5]

These systems analyse several signs at once, including subtle bodily movements, variations in voice patterns, minor changes in facial expressions, and quantifiable physiological reactions, such as alterations in skin conductance and heart rhythm fluctuations.[6] Through this inclusive approach, abstract emotional experiences can be converted into concrete, analysable data points that computers can process systematically.[7]

Emotion AI's real-world uses have grown significantly in a variety of industries. Measuring consumer responses to goods and services allows for more individualised shopping experiences in retail.[8] These technologies are used by medical professionals to track patients' emotional states throughout therapy and to spot early signs of mental health issues.[9] Emotion AI also plays a role in security applications, analysing crowd behaviour and detecting threats.[10]

The pervasive integration of Emotion AI highlights its profound impact on virtually every facet of human life. In fact, virtual assistants can now identify emotional undertones in speech patterns and modify their responses accordingly.[11] To improve comfort and safety, modern cars can now be equipped with technologies that monitor drivers' emotional states.[12] Smartphones increasingly feature advanced emotion-detection capabilities through their cameras and microphones.[13] Additionally, there has been a notable acceleration in the institutional adoption of Emotion AI: educational institutions use it to monitor students'

5 Sesha Bhargavi Velagaleti and others, 'Empathetic Algorithms: The Role of AI in Understanding and Enhancing Human Emotional Intelligence' (2024) 20(3) Journal of Electrical Systems 2051. doi:10.52783/jes.1806.

6 Smith K Khare and others, 'Emotion Recognition and Artificial Intelligence: A Systematic Review (2014-2023) and Research Recommendations' (2024) 102 Information Fusion 102019. doi:10.1016/j.inffus.2023.102019.

7 Bei Pan and others, 'A Review of Multimodal Emotion Recognition from Datasets, Preprocessing, Features, and Fusion Methods' (2023) 561 Neurocomputing 126866. doi:10.1016/j.neucom.2023.126866.

8 Thomas Davenport and others, 'How Artificial Intelligence Will Change the Future of Marketing' (2020) 48(1) Journal of the Academy of Marketing Science 24. doi:10.1007/s11747-019-00696-0.

9 Anoushka Thakkar, Ankita Gupta and Avinash De Sousa, 'Artificial Intelligence in Positive Mental Health: A Narrative Review' (2024) 6 Frontiers in Digital Health 1280235. doi:10.3389/fdgth.2024.1280235.

10 Lena Podoletz, 'We Have to Talk A bout Emotional AI and Crime' (2023) 38 AI & Society 1067. doi:10.1007/s00146-022-01435-w.

11 Ruhul Amin Khalil and others, 'Speech Emotion Recognition Using Deep Learning Techniques: A Review' (2019) 7 IEEE Access 117327. doi:10.1109/ACCESS.2019.2936124.

12 Sebastian Zepf and others, 'Driver Emotion Recognition for Intelligent Vehicles: A Survey' (2020) 53(3) ACM Computing Surveys (CSUR) 1. doi:10.1145/338879.

13 Imran A Zualkernan and others, 'Emotion Recognition Using Mobile Phones' (2017) 60 Computers & Electrical Engineering 1. doi:10.1016/j.compeleceng.2017.05.004.

emotional health and level of engagement during class activities,[14] while healthcare facilities employ it to monitor the psychological moods and recovery status of their patients.[15] In the same vein, corporate environments utilise these technologies to gauge employee engagement and workplace satisfaction.[16]

The extensive use of Emotion AI across diverse fields highlights both its possible advantages and the necessity of carefully weighing its effects on individual autonomy and privacy.

3.2. The Rise of Privacy and Ethical Concerns with Emotion AI

Although developers emphasise the importance of anonymity and collective emotional analysis, the collection of emotional data still poses serious privacy issues. While there might exist other factors, this section examines the issues and the implications associated with the collection of emotional data.

3.2.1. Bias and Discrimination

One of the most critical issues in AI is the ethical implications of bias and discrimination in Emotion AI systems. The training data these systems rely on has a fundamental impact on their performance. When this data includes pre-existing societal biases or prejudices, the emerging AI systems unavoidably reflect—and may even reinforce—these discriminatory patterns.[17]

When they arise, such biases can significantly impact different social and demographic groups. Emotion AI systems, in particular, may unfairly impact groups based solely on how the AI interprets their emotional responses.[18] This could then result in difficult situations where the technological tools intended to improve human connection end up being used in a discriminatory way.

Beyond racial biases, this issue includes cultural variations in emotional expression. For instance, Emotion AI systems that are usually trained on data from dominant cultural

14 Angel Olider Rojas Vistorte and others, 'Integrating Artificial Intelligence to Assess Emotions in Learning Environments: A Systematic Literature Review' (2024) 15 Frontiers in Psychology 1387089. doi:10.3389/fpsyg.2024.1387089.

15 Prashant Kumar Nag, Amit Bhagat and R Vishnu Priya, 'Expanding AI's Role in Healthcare Applications: A Systematic Review of Emotional and Cognitive Analysis Techniques' [2025] IEEE Access. doi:10.1109/ACCESS.2025.3562131.

16 McStay (n 2).

17 Varsha PS, 'How Can We Manage Biases in Artificial Intelligence Systems: A Systematic Literature Review' (2023) 3(1) International Journal of Information Management Data Insights 100165. doi:10.1016/j.jjimei.2023.100165.

18 Nomisha Kurian, 'AI's Empathy Gap: The Risks of Conversational Artificial Intelligence for Young Children's Well-Being and Key Ethical Considerations for Early Childhood Education and Care' (2023) 26(1) Contemporary Issues in Early Childhood 132. doi:10.1177/14639491231206004.

groups may struggle to accurately identify and interpret emotional responses from other cultures. In other words, when Emotion AI is deployed across various cultural contexts, its underlying cultural bias may lead to misinterpretations and inaccurate assessments.[19]

3.2.2. Transparency and Explainability

To build trust and accountability in human-machine interactions, Emotion AI systems must be transparent and understandable. Indeed, trust is a necessary condition for the effective deployment and uptake of Emotion AI technologies rather than just a desirable attribute.[20] In the absence of a solid foundation of trust, the most complex and powerful Emotion AI systems might fail to accomplish their purposes.

Therefore, maintaining and preserving trust requires Emotion AI systems to function with a high level of transparency in a number of crucial areas. This includes being transparent about how the system functions, how it processes information, and—above all—how it manages sensitive emotional data. Emotion AI users need a thorough awareness of the complete data lifecycle, from the initial phase of emotional reactions to the storage processes and the final uses of this data.[21]

However, recent studies demonstrate that many Emotion AI systems in use today function as "black boxes," with internal procedures that are frequently hidden from both users and observers.[22] This lack of transparency presents serious challenges. Consumers struggle to trust these systems' outputs or evaluate their reliability when they cannot comprehend how decisions are made. Furthermore, this opacity makes it more difficult to detect and resolve potential issues with the systems, such as algorithmic biases or systematic errors.[23]

This transparency issue has implications that go beyond user confidence. It affects the wider accountability of Emotion AI systems and raises significant questions about their responsible creation and application. Clear, intelligible, and transparent systems are

19 Peter Mantello and others, 'Machines that Feel: Behavioral Determinants of Attitude Towards Affect Recognition Technology—Upgrading Technology Acceptance Theory with the Mind sponge Model' (2023) 10(1) Humanities and Social Sciences Communications 430. doi:10.1057/s41599-023-01837-1.

20 Keng L Siau and Weiyu Wang, 'Building Trust in Artificial Intelligence, Machine Learning, and Robotics' (2018) 31(2) Cutter Business Technology Journal 47.

21 Ben Chester Cheong, 'Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making' (2024) 6 Frontiers in Human Dynamics 1421273. doi:10.3389/fhumd.2024.1421273.

22 Angelica Salvi del Pero, Peter Wyckoff and Ann Vourc'h, *Using Artificial Intelligence in the Workplace: What are the Main Ethical Risks?* (Social, Employment and Migration Working Papers no 273, OECD 2022). doi:10.1787/840a2d9f-en.

23 Karina Cortiñas-Lorenzo and Gerard Lacey, 'Toward Explainable Affective Computing: A Review' (2023) 35(10) IEEE Transactions on Neural Networks and Learning Systems 13101. doi:10.1109/TNNLS.2023.3270027.

becoming increasingly necessary as these technologies permeate more facets of our lives, ensuring they genuinely serve the interests of both their users and society as a whole.[24]

3.2.3. Consent and Data Security

A fundamental element of the ethical collection and use of personal information—especially emotional information—is informed consent. In the current digital environment, where Emotion AI systems are growing more common, this basic requirement has grown more complex. The alarming issue, however, is the lack of awareness among people regarding their emotions, which are being monitored and examined, let alone the possible consequences of such monitoring.[25] This lack of awareness is particularly concerning in situations where Emotion AI tools are used covertly or when people feel pressured to give their consent, such as a condition of employment or to access specific services.[26]

3.2.4. The Risk of Manipulation

There are serious ethical issues regarding Emotion AI's ability to assess and predict human emotions, particularly in relation to manipulation. The capacity of this technology to interpret physiological signs, speech patterns, facial expressions, and behavioural data opens up possibilities for impacting human behaviour.[27] Businesses, for instance, could employ Emotion AI in advertising to develop highly targeted advertisements that take advantage of people's emotional weaknesses.[28] An algorithm might, for example, detect when a person feels lonely or insecure and display advertisements intended to capitalise on these feelings. This could lead to impulsive purchasing decisions or even dependence on particular goods or services.[29]

24 Alejandro Barredo Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI' (2020) 58 Information Fusion 82. doi:10.1016/j.inffus.2019.12.012.

25 Adam J Andreotta, 'The Hard Problem of AI Rights' (2021) 36 AI & Society 19. doi:10.1007/s00146-020-00997-x

26 Adam J Andreotta, Nin Kirkham and Marco Rizzi, 'AI, Big Data, and the Future of Consent' (2022) 37 AI & Society 1715. doi:10.1007/s00146-021-01262-5.

27 Marcello Ienca, 'On Artificial Intelligence and Manipulation' (2023) 42(3) Topoi 833. doi:10.1007/s11245-023-09940-3.

28 V Kumar and others, 'Understanding the Role of Artificial Intelligence in Personalized Engagement Marketing' (2019) 61(4) California Management Review 135. doi:10.1177/0008125619859317.

29 Andrew McStay, 'Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (The Case for Intimacy)' (2016) 3(2) Big Data & Society. doi:10.1177/2053951716666868.

4 DATA PROTECTION FRAMEWORKS RELEVANT TO EMOTION AI

Existing data protection standards, along with newly emerging AI-specific laws and regulations, have created a complex web of compliance requirements, making the legal environment governing Emotion AI more comprehensive. Considering that the EU has the world's most comprehensive and stringent data protection and AI standards, serving as a benchmark, this section focuses primarily on the EU GDPR and the EU Artificial Intelligence Act—both of which serve as key instruments governing data protection and Emotion AI.

4.1. Emotion AI Through the Lenses of the GDPR

The GDPR serves as the cornerstone legislation governing personal data processing within the European Union. Its jurisdiction transcends geographical boundaries, extending to any entity, regardless of location, that monitors the behaviour of individuals in the EU.

Article 9(1) of the GDPR expressly prohibits the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Although emotional data is not explicitly listed in Article 9(1), there is a broad consensus that it qualifies as biometric data when it meets the personal data criteria outlined in Article 4(1) of the GDPR.[30]

As a result, companies using Emotion AI systems must carefully adhere to the GDPR's core requirements of purpose limitation, data minimisation, and storage limitation. This means restricting data collection to the most critical components, providing a clear explanation for the acquisition of emotional data, and retaining such data only for as long as necessary. The regulation also requires enterprises to disclose their use of Emotion AI in a transparent and understandable manner, while ensuring that data subjects have accessible means to manage their personal data.

To ensure regulatory compliance, organisations must also put in place thorough measures that combine organisational and technical safeguards. These include modern encryption techniques, strictly regulated access controls, and thorough documentation of all data processing operations, which should be part of these safeguards. Additionally, companies must conduct comprehensive Data Protection Impact Assessments to identify and mitigate potential risks before implementing large-scale Emotion AI systems that handle biometric data. By guaranteeing that privacy considerations are incorporated into the system's design from the beginning, these assessments act as essential preventive measures. In addition to demonstrating a commitment to compliance, adopting stringent security measures helps protect private emotional information from unethical or illegal use.

30 Leonhard Menges and Eva Weber-Guskar, 'Digital Emotion Detection, Privacy, and the Law' (2025) 38(2) Philosophy & Technology 1. doi:10.1007/s13347-025-00895-4.

4.2. Emotion AI Systems Under the EU AI Act

In 2024, the EU put forward an AI regulation,[31] marking the initial steps towards regulating AI and transforming the legal assessment of AI systems. This regulation uses a risk-based approach, categorising AI systems into four levels—unacceptable, high, limited, and minimal risk—based on the risk they pose to people and society.[32] Depending on its classification, every category of AI system is subject to specific rules and restrictions.

This thoughtful approach reflects a sophisticated understanding of the diverse implications that different AI technologies may have. The level of regulatory monitoring is directly correlated with the possible harm associated with each AI application under the hierarchical oversight framework established by the AI Act. The regulation thus establishes distinct lines between permissible and impermissible AI systems.

According to Article 5 (1)(f) of the AI Act, "the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons" is strictly prohibited. This rationale for this prohibition is further detailed in Recital 44, which lists several serious concerns regarding emotion identification systems. These concerns include its intrusive nature, lack of specificity and generalisability, power imbalance between those using it and those affected, its limited reliability, and the potential for discriminatory outcomes.[33]

Furthermore, Annexe III of the AI Act classifies emotion recognition systems as high-risk AI systems, subjecting them to stringent regulatory requirements. As a result, those who implement such systems must adhere to Article 50(3) of the AI Act, which stipulates that individuals who are exposed to these technologies must be made aware of how they work and that any personal information they handle must be processed in full compliance with the requirements of the GDPR.[34]

31 Regulation (EU) 2024/1689 of the European Parliament and of the Council 'Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (13 June 2024) <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> accessed 23 September 2025.

32 Natalia Díaz-Rodrígue and others, 'Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation' (2023) 99 Information Fusion 101896. doi:10.1016/j.inffus.2023.101896.

33 See: Regulation (EU) 2024/1689 (n 31) recital 44.

34 ibid, art 50(3).

4.3. European Case Law and Regulatory Guidance on Emotion AI

The use of biometric and emotion-inference technologies has been severely limited by European jurisprudence and supervisory guidelines, which stress the principles of necessity, proportionality and periodic review. The Court of Justice of the European Union (CJEU) has frequently ruled that national schemes authorising the systematic or blanket collection of biometric and genetic data violate the EU data-protection frameworks unless strictly limited and justified.

This principle was clearly articulated in the V.S. case, where the CJEU held that compulsory, systematic collection of biometric data for police records must meet a "strictly necessary" requirement in pursuit of specific, legitimate objectives.[35] Another landmark decision, *Digital Rights Ireland Ltd v Minister,* declared the EU Data Retention Directive invalid on the grounds that mass and indiscriminate retention of communications metadata without adequate protection is a severe interference with rights to data privacy.[36] According to this case, any automated or intrusive processing of personal data, especially sensitive or behavioural data, must adhere to stringent requirements for necessity, proportionality, transparency, and legal justification. Emotion AI, insofar as it infers inner emotional states, implicates several of those concerns.

In parallel, the ECtHR also considered intrusive biometric surveillance as a matter falling under Article 8 (private life). In *Glukhin v. Russia*, the ECtHR ruled that the use of facial-recognition technology by authorities was seen as "highly intrusive", highlighting that the use poses serious proportionality and clarity issues in domestic law.[37] Earlier, Gaughran v. the United Kingdom highlighted the dangers of stigmatisation and life-course harm and criticised schemes that permitted the indefinite retention of biometric data (photographs and fingerprints) as being incompatible with Convention provisions.[38]

Supervisory authorities have converted these principles into operational guidance. The European Data Protection Board's guidelines on facial recognition and law enforcement processing require stringent purpose limitation, data minimisation, and human oversight

35 Case C-205/21 *VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost* (CJEU, 26 January 2023) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62021CJ0205> accessed 23 September 2025.

36 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others* (**CJEU** (Grand Chamber), 8 April 2014) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CA0293> accessed 23 September 2025.

37 *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023) <https://hudoc.echr.coe.int/eng?i=001-225655> accessed 23 September 2025. **See:** Francesca Palmiotto and Natalia Menéndez González, 'Facial Recognition Technology, Democracy and Human Rights' (2023) 50 *Computer Law & Security Review* 105857. doi:10.1016/j.clsr.2023.105857.

38 *Gaughran v the United Kingdom* App no 45245/15 (ECtHR, 13 February 2020) <https://hudoc.echr.coe.int/eng?i=001-200817> accessed 23 September 2025.

safeguards before any biometric processing. They also call for customised necessity assessments rather than general authorisations.[39] Similarly, the European Data Protection Supervisor identified face emotion recognition as especially risky, pointing out the strong potential for discriminatory consequences and scientific ambiguity over accuracy.[40]

At the National DPA level, the UK Information Commissioner's Office (ICO) has frequently cautioned about the immaturity, bias, and intrusiveness of emotion-recognition technology. These concerns have been incorporated into the ICO's AI strategy and biometrics guidance.[41] In a similar vein, France's CNIL[42] and Spain's AEPD[43] published white papers and technical dispatches addressing automatic processing (speech, face, and neurodata) and underlining the concerns where inferred mental states meet with "special categories" of data. Regulators emphasise DPIAs, necessity, transparency, and purpose limitation. They also frequently caution against covert or workplace applications that lack robust protections.

5 COMPLIANCE STRATEGIES FOR PRIVACY-BY-DESIGN IN EMOTION AI

PbD emphasises the importance of incorporating privacy considerations throughout the development lifecycle to reduce risks and boost user confidence.[44] The present section offers a comprehensive insight into the underlying core principles of PbD and explores their implementation approaches in Emotion AI.

39 European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement* (version 2.0, 26 April 2023) <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf?utm_source=chatgpt.com> accessed 23 September 2025.

40 '*TechDispatch #1/2024 – Neurodata*' (*European Data Protection Supervisor*, 3 June 2024) <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata>accessed 26 September 2025.

41 '*Regulating AI: The ICO's Strategic Approach*' (*Information Commissioner's Office*, 30 April 2024) <https://ico.org.uk/about-the-ico/consultations/regulating-ai-the-icos-strategic-approach-a-response-to-the-dsit-secretary-of-state/> accessed 23 September 2025.

42 'Artificial Intelligence: the Opinion of the CNIL and its Counterparts on the Future European Regulation' (*CNIL Commission Nationale de l'Informatique et des Libertés*, 18 June 2021) <https://www.cnil.fr/en/artificial-intelligence-opinion-cnil-and-its-counterparts-future-european-regulation> accessed 23 September 2025.

43 TechDispatch (n 40).

44 Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2009) 5 Information and Privacy Commissioner of Ontario, Canada 12.

5.1. Privacy-by-Design Core Principles

PbD is a forward-thinking framework for safeguarding personal data, embedding privacy considerations into the design specifications of technologies, systems, and processes at the outset of personal data processing, rather than as an afterthought. This concept is further clarified by Cavoukian, who outlines seven fundamental principles that serve as a valuable reference for organisations seeking to comply with data protection regulations.[45] These are:

- **Proactive, not Reactive**: This approach anticipates and prevents privacy issues before they occur, rather than addressing them after violations have happened. It helps organisations maintain trust and avoid costly remediation efforts.
- **Privacy as the Default Setting**: Systems should safeguard user privacy automatically, without requiring user intervention. Every business procedure or IT system should automatically, by default, protect personal data.
- **Privacy Embedded into Design**: The system's architecture and design incorporate privacy protection from the start, rather than adding it after. This guarantees that privacy becomes a core feature.
- **Full Functionality – Positive-Sum, not Zero-Sum**: PbD seeks to accommodate all legitimate interests and objectives in a mutually beneficial "win-win" manner, rather than relying on an outdated zero-sum approach that requires needless trade-offs.
- **End-to-end Security**: Stringent procedures must be applied throughout the entire data lifecycle. This guarantees that all the data is securely collected, used, retained, and deleted at the end of the process.
- **Visibility and Transparency**: All components and operations should remain visible and transparent to both users and providers, fostering trust and accountability.
- **Respect for User Privacy**: Individuals' interests are crucial, requiring robust privacy defaults, and user-friendly options, as well as proper notice.

In recent years, the concept of PbD has gained widespread acceptance and has been formally incorporated into major data protection frameworks such as the GDPR. The principle is emphasised in Recital 78 of the GDPR, which states that:

> "When developing, designing, selecting, and using applications, services, and products that involve personal data processing, developers and manufacturers should consider the right to data protection, adhering to the state of the art, and ensuring that controllers and processors fulfil their obligations."[46]

45 ibid.
46 See: Regulation (EU) 2016/679 (n 3) recital 78.

Article 25(1) of the GDPR provides further guidance on implementing PbD. It requires controllers to take organisational and technical steps to implement data protection principles, such as data minimisation, and to incorporate the necessary safeguards to meet regulatory requirements and uphold individuals' rights. These measures should take into account various factors, including technological advancements, associated costs, and the nature, scope, and potential risks involved in data processing activities.

5.2. Implementing Privacy-by-Design in Emotion AI

PbD implementation in Emotion AI requires a thorough policy that covers every component of the technology, from data collection and processing to storage and utilisation.

5.2.1. Data Minimisation and Purpose Limitation

Fundamental PbD principles of purpose limitation and data minimisation necessitate that companies collect just the data necessary for a specific, legitimate purpose and use it only for that purpose. Therefore, applying PbD principles to emotional data poses substantial real-world challenges from an enforcement standpoint. Organisations must operationalise data minimisation and purpose limitation across intricate technical systems and business processes while navigating data protection regulations.

In practice, organisations must keep thorough records demonstrating their assessment of the importance of each emotional data point gathered. For instance, a mental health app would need to explain why specific emotional indicators are necessary for delivering therapeutic services, while omitting information that might be relevant but not essential for the service. This documentation becomes essential when Data Protection Authorities conduct regulatory audits and investigations.

The challenge of purpose limitation is reflected in data access controls and system architecture. Organisations must implement technical safeguards to prevent the use of emotional data for secondary purposes, such as product development or marketing, unless this is stated explicitly in the original consent. Addressing this challenge often requires sophisticated data governance frameworks and regular compliance audits. For instance, a workplace wellness program collecting emotional data must ensure strict separation between health-related processing and performance management systems to maintain compliance and protect individuals' privacy.

5.2.2. Transparency and Consent

Implementing informed consent for emotional data within EU frameworks poses several practical challenges. Organisations should set up clear, accessible consent mechanisms that effectively clarify the intricacies of emotional AI systems, while ensuring users are not overwhelmed by excessive consent requests. Information on an organisation's data collection

and processing procedures, including the type of emotional data it collects, its intended uses, and the security measures in place, should be easily comprehensible and available.[47]

The technical implementation of data subject rights raises significant challenges, particularly for emotional data that may be integrated into multiple systems or used for training AI models. For organisations to track emotional data throughout their infrastructure, fulfil access requests, and implement the right to be forgotten, they require strong data mapping and management systems. This becomes especially complex when emotional data is derived from multiple sources or combined with other personal data.

As emotional AI technologies evolve, organisations need to maintain ongoing transparency. For this, they are required to regularly update their documentation and communication channels. This includes incorporating practical processes for consent withdrawal at any time and the ability to view and request changes to their data.[48]

5.2.3. Security and Data Protection

Adopting thorough data security procedures is another essential component for protecting sensitive information. These precautions should ensure that this private information is protected from exposure, misuse, and unauthorised access.[49] Indeed, ways to implement such precautions include using advanced encryption methods, establishing strict access controls, and conducting systematic audits of data protection frameworks to identify weaknesses.[50] By prioritising these initiatives, organisations may improve accountability, lower risks, and maintain ethical principles while managing Emotion AI systems as well as protecting people's rights and privacy.

5.2.4. Accountability and Algorithmic Transparency

To ensure that Emotion AI systems function in a way that avoids discrimination, maintain fairness and stop bias, algorithmic accountability and transparency are crucial.[51] Thus, to make these algorithms as transparent as possible, organisations should provide a thorough, understandable explanation of the procedures and methods that underpin their operation.

47 Yugang Li and others, 'Developing Trustworthy Artificial Intelligence: Insights from Research on Interpersonal, Human-Automation, and Human-AI Trust' (2024) 15 Frontiers in Psychology 1382693. doi:10.3389/fpsyg.2024.1382693; Barker and others (n 2).

48 Salvi del Pero, Wyckoff and Vourc'h (n 22).

49 Ramanpreet Kaur, Dušan Gabrijelčič and Tomaž Klobučar, 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions' (2023) 97 Information Fusion 101804. doi:10.1016/j.inffus.2023.101804.

50 Jon D Elhai, Jason C Levine and Brian J Hall, 'Anxiety about Electronic Data Hacking: Predictors and Relations with Digital Privacy Protection Behavior' (2017) 27(3) Internet Research 631. doi:10.1108/IntR-03-2016-0070.

51 Julianne Cartwright, Marcus T Ellington and Amelia S Hawthorne, 'Exploring the Potential of Emotional Intelligence in AI through Emotion-Sensitive Learning Algorithms' [2024] Preprint. doi:10.13140/RG.2.2.18780.16005.

Transparency challenges derive from the complexity of AI systems, especially with Emotion AI's subjective nature. Organisations must address this by providing clear documentation and illustrative insights about how algorithms avoid bias, handle emotional input, and justify outputs, without overloading stakeholders with technical jargon.

Promoting accountability in Emotion AI systems requires not only transparency but also clarity on decision-making procedures. Companies should specify exactly how particular decisions are made using the algorithm, including the inputs and the justification for the results. By doing this, companies promote confidence among stakeholders such as regulators, users, and the public, in addition to enabling improved oversight.[52] Therefore, implementing such procedures strengthens the integrity and social responsibility of the Emotion AI systems.

5.2.5. User-Centric Design

User-centric design prioritises individuals' needs, preferences, and rights in the development and deployment of Emotion AI systems.[53] This approach necessitates continuous user engagement throughout the design processes to ensure that technologies align with human-centric values and respect user experiences. Practical enforcement involves integrating user feedback loops into the system development process. This could be done by facilitating participatory workshops or usability testing to enhance system responsiveness and meet user expectations. Designers must balance innovation with compliance, ensuring that emotional data is handled ethically, securely, and lawfully.

Furthermore, user-centric design empowers individuals with greater control over their emotional data. This includes enabling users to manage their data in ways that have personal significance, providing access to their emotional data, and offering simple methods to correct errors or delete the data if they choose. By prioritising consumers' autonomy and privacy first, this approach promotes both fairness and increases users' trust in the technology.

5.2.6. Impact Assessments

For businesses using Emotion AI systems, Data Protection Impact Assessments (DPIAs) are essential systematic methods for assessing and mitigating potential privacy issues prior to their deployment.[54] These assessments include a thorough examination of the

52 Cheong (n 21).

53 Lakshita Dodeja and others, 'Towards the Design of User-Centric Strategy Recommendation Systems for Collaborative Human–AI Tasks' (2024) 184 International Journal of Human-Computer Studies 103216. doi:10.1016/j.ijhcs.2023.103216.

54 Denise Almeida, Konstantin Shmarko and Elizabeth Lomas, 'The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks' (2022) 2 AI Ethics 377. doi:10.1007/s43681-021-00077-w; Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations' (2021) 11(2) International Data Privacy Law 125. doi:10.1093/idpl/ipaa020.

methods used to collect, process, store, and use personal and emotional data while taking into account the particular sensitivities related to Emotion AI technology. A comprehensive DPIA typically considers various factors, including the necessity and appropriateness of data processing, potential threats to people's rights and freedoms, and the effectiveness of existing protections.

DPIAs can be used by organisations to identify certain vulnerabilities, including dangers of emotional manipulation, potential bias or discrimination in emotional analysis, and illegal access to emotional data. Based on these results, organisations can create focused mitigation strategies, like enhanced data encryption, stringent access controls, explicit data retention guidelines, and transparent and honest communication with users regarding the processing of their emotional data. DPIAs are a dynamic tool for upholding ethical norms and privacy compliance, and regular revisions are crucial as Emotion AI technology develops and new privacy risks appear.

6 CONCLUSIONS

Incorporating PbD principles into the development of Emotion AI is not only required by law but also essential to the long-term, ethical development of this technology. As this paper demonstrates, the sensitive nature of emotional data necessitates a thorough, proactive approach to privacy protection that goes beyond mere compliance with current regulations. Implementing PbD in Emotion AI systems requires careful consideration of numerous factors, including data minimisation, transparency, consent, and robust security mechanisms. Therefore, organisations must strike a balance between the innovation of Emotion AI and the fundamental right to privacy to prevent technological innovation from compromising individual autonomy and trust.

The development and implementation of Emotion AI systems will likely be influenced by future regulatory changes, especially with the implementation of the EU AI Act and the ongoing impact of the GDPR. Businesses will be better positioned to adapt to these shifting demands while upholding public trust if they adopt PbD principles early in their development process.

Finally, organisations can develop solutions that are not just secure and compliant but also ethical and with long-lasting effects by integrating privacy concerns into the foundation of emotion AI systems. To ensure that the advancement of Emotion AI aligns with social values and expectations while encouraging innovation in this rapidly evolving sector, it will be crucial to conduct ongoing research, collaborate with stakeholders, and regularly evaluate privacy standards.

REFERENCES

1. Almeida D, Shmarko K and Lomas E, 'The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks' (2022) 2 AI Ethics 377. doi:10.1007/s43681-021-00077-w
2. Andreotta AJ, 'The Hard Problem of AI Rights' (2021) 36 AI & Society 19. doi:10.1007/s00146-020-00997-x
3. Andreotta AJ, Kirkham N and Rizzi M, 'AI, Big Data, and the Future of Consent' (2022) 37 AI & Society 1715. doi:10.1007/s00146-021-01262-5
4. Barker D and others, 'Ethical Considerations in Emotion Recognition Research' (2025) 7(2) Psychology International 43. doi:10.3390/psycholint7020043
5. Barredo Arrieta A and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI' (2020) 58 Information Fusion 82. doi:10.1016/j.inffus.2019.12.012
6. Cartwright J, Ellington MT and Hawthorne AS, 'Exploring the Potential of Emotional Intelligence in AI through Emotion-Sensitive Learning Algorithms' [2024] Preprint. doi:10.13140/RG.2.2.18780.16005
7. Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' (2009) 5 Information and Privacy Commissioner of Ontario, Canada 12
8. Cheong BC, 'Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making' (2024) 6 Frontiers in Human Dynamics 1421273. doi:10.3389/fhumd.2024.1421273
9. Cortiñas-Lorenzo K and Lacey G, 'Toward Explainable Affective Computing: A Review' (2023) 35(10) IEEE Transactions on Neural Networks and Learning Systems 13101. doi:10.1109/TNNLS.2023.3270027
10. Davenport T and others, 'How Artificial Intelligence Will Change the Future of Marketing' (2020) 48(1) Journal of the Academy of Marketing Science 24. doi:10.1007/s11747-019-00696-0
11. Díaz-Rodrígue N and others, 'Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation' (2023) 99 Information Fusion 101896. doi:10.1016/j.inffus.2023.101896
12. Dodeja L and others, 'Towards the Design of User-Centric Strategy Recommendation Systems for Collaborative Human–AI Tasks' (2024) 184 International Journal of Human-Computer Studies 103216. doi:10.1016/j.ijhcs.2023.103216

13. Elhai JD, Levine JC and Hall BJ, 'Anxiety about Electronic Data Hacking: Predictors and Relations with Digital Privacy Protection Behavior' (2017) 27(3) Internet Research 631. doi:10.1108/IntR-03-2016-0070

14. Ienca M, 'On Artificial Intelligence and Manipulation' (2023) 42(3) Topoi 833. doi:10.1007/s11245-023-09940-3

15. Kaminski ME and Malgieri G, 'Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations' (2021) 11(2) International Data Privacy Law 125. doi:10.1093/idpl/ipaa020

16. Kaur R, Gabrijelčič D and Klobučar T, 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions' (2023) 97 Information Fusion 101804. doi:10.1016/j.inffus.2023.101804

17. Khalil RA and others, 'Speech Emotion Recognition Using Deep Learning Techniques: A Review' (2019) 7 IEEE Access 117327. doi:10.1109/ACCESS.2019.2936124

18. Khare SK and others, 'Emotion Recognition and Artificial Intelligence: A Systematic Review (2014-2023) and Research Recommendations' (2024) 102 Information Fusion 102019. doi:10.1016/j.inffus.2023.102019

19. Kumar V and others, 'Understanding the Role of Artificial Intelligence in Personalized Engagement Marketing' (2019) 61(4) California Management Review 135. doi:10.1177/0008125619859317

20. Kurian N, 'AI's Empathy Gap: The Risks of Conversational Artificial Intelligence for Young Children's Well-Being and Key Ethical Considerations for Early Childhood Education and Care' (2023) 26(1) Contemporary Issues in Early Childhood 132. doi:10.1177/14639491231206004

21. Li Y and others, 'Developing Trustworthy Artificial Intelligence: Insights from Research on Interpersonal, Human-Automation, and Human-AI Trust' (2024) 15 Frontiers in Psychology 1382693. doi:10.3389/fpsyg.2024.1382693

22. Mantello P and others, 'Machines that Feel: Behavioral Determinants of Attitude Towards Affect Recognition Technology—Upgrading Technology Acceptance Theory with the Mind sponge Model' (2023) 10(1) Humanities and Social Sciences Communications 430. doi:10.1057/s41599-023-01837-1

23. McStay A, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7(1) Big Data & Society. doi:10.1177/2053951720904386

24. McStay A, *Emotional AI: The Rise of Empathic Media* (SAGE Publications 2018) doi:10.4135/9781526451293

25. McStay A, 'Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (The Case for Intimacy)' (2016) 3(2) Big Data & Society. doi:10.1177/2053951716666868

26. Menges L and Weber-Guskar E, 'Digital Emotion Detection, Privacy, and the Law' (2025) 38(2) Philosophy & Technology 1. doi:10.1007/s13347-025-00895-4

27. Nag PK, Bhagat A and Priya RV, 'Expanding AI's Role in Healthcare Applications: A Systematic Review of Emotional and Cognitive Analysis Techniques' [2025] IEEE Access. doi:10.1109/ACCESS.2025.3562131

28. Palmiotto F and González NM, 'Facial Recognition Technology, Democracy and Human Rights' (2023) 50 *Computer Law & Security Review* 105857. doi:10.1016/j.clsr.2023.105857

29. Pan B and others, 'A Review of Multimodal Emotion Recognition from Datasets, Preprocessing, Features, and Fusion Methods' (2023) 561 Neurocomputing 126866. doi:10.1016/j.neucom.2023.126866

30. Picard RW, *Affective Computing* (Technical Report no 321, MIT Media Laboratory Perceptual Computing Section 1995)

31. Podoletz L, 'We Have to Talk A bout Emotional AI and Crime' (2023) 38 AI & Society 1067. doi:10.1007/s00146-022-01435-w

32. Salvi del Pero A, Wyckoff P and Vourc'h A, *Using Artificial Intelligence in the Workplace: What are the Main Ethical Risks?* (Social, Employment and Migration Working Papers no 273, OECD 2022). doi:10.1787/840a2d9f-en

33. Siau KL and Wang W, 'Building Trust in Artificial Intelligence, Machine Learning, and Robotics' (2018) 31(2) Cutter Business Technology Journal 47

34. Thakkar A, Gupta A and De Sousa A, 'Artificial Intelligence in Positive Mental Health: A Narrative Review' (2024) 6 Frontiers in Digital Health 1280235. doi:10.3389/fdgth.2024.1280235

35. Varsha PS, 'How Can We Manage Biases in Artificial Intelligence Systems: A Systematic Literature Review' (2023) 3(1) International Journal of Information Management Data Insights 100165. doi:10.1016/j.jjimei.2023.100165

36. Velagaleti SB and others, 'Empathetic Algorithms: The Role of AI in Understanding and Enhancing Human Emotional Intelligence' (2024) 20(3) Journal of Electrical Systems 2051. doi:10.52783/jes.1806

37. Vistorte AOR and others, 'Integrating Artificial Intelligence to Assess Emotions in Learning Environments: A Systematic Literature Review' (2024) 15 Frontiers in Psychology 1387089. doi:10.3389/fpsyg.2024.1387089

38. Zepf S and others, 'Driver Emotion Recognition for Intelligent Vehicles: A Survey' (2020) 53(3) ACM Computing Surveys (CSUR) 64. doi:10.1145/338879

39. Zualkernan IA and others, 'Emotion Recognition Using Mobile Phones' (2017) 60 Computers & Electrical Engineering 1. doi:10.1016/j.compeleceng.2017.05.004

AUTHORS INFORMATION

Laroussi Chemlali*
PhD in Law, Associate Professor, Ajman University, College of Law, Ajman, United Arab Emirates
l.chemlali@ajman.ac.ae
https://orcid.org/0000-0002-4770-7121
Corresponding author, responsible for conceptualisation, methodology, writing – original draft, writing –review & editing, supervision, validation.

Leila Benseddik
PhD in Applied Linguistics, Assistant Professor, Canadian University of Dubai, Faculty of First Year, Dubai, United Arab Emirates
leila.benseddik@cud.ac.ae
https://orcid.org/0009-0000-4556-2961
Co-author, responsible for conceptualisation, methodology, writing – original draft, writing – review & editing, supervision.

Competing interests: No competing interests were disclosed. Any potential conflict of interest must be disclosed by authors.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

ACKNOWLEDGEMENTS

The authors wish to express their sincere appreciation to Ajman University for its financial support in covering the Article Processing Charges (APC) for this publication.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Chemlali L and Benseddik L, 'Privacy-By-Design in Emotion AI: Data Protection Frameworks and Compliance Strategies' (2025) 8(Spec) Access to Justice in Eastern Europe 1-24 <https://doi.org/10.33327/AJEE-18-8.S-r000153> Published Online 04 Dec 2025

DOI: https://doi.org/10.33327/AJEE-18-8.S-r000153

Keywords: *privacy-by-design, emotion AI, data protection, ethics in AI, emotion recognition, user privacy.*

DETAILS FOR PUBLICATION

Date of submission: 21 Aug 2025
Date of acceptance: 02 Oct 2025
Online First publication: 04 Dec 2025
Last date of publication: December 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The corresponding author confirms that this article was prepared with the assistance of AI tools. Specifically, ChatGPT (OpenAI) and Claude were used for language refinement during the drafting process. All content, arguments, and conclusions were generated independently and remain their sole responsibility. No AI tool was used for generating original research findings or analysis.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Оглядова стаття

КОНФІДЕНЦІЙНІСТЬ ЗА ЗАМОВЧУВАННЯМ В ЕМОЦІЙНОМУ ШІ: ЗАХИСТ ДАНИХ ТА СТРАТЕГІЇ ДОТРИМАННЯ ВИМОГ

Ларуссі Чемлалі* та Лейла Бенседдік

АНОТАЦІЯ

Вступ. *Швидкий розвиток емоційного штучного інтелекту (емоційний ШІ) створив значні можливості для інновацій у широкому спектрі галузей, зокрема в сфері охорони здоров'я, маркетингу та взаємодії людини з комп'ютером. Застосунки з емоційним ШІ, які обробляють, аналізують та реагують на людські емоції, здебільшого залежать від приватних персональних даних, що призводить до проблем із конфіденційністю та етичними нормами. Впровадження принципів конфіденційності за замовчуванням (PbD) у таких системах є важливим для протидії цим викликам та забезпечення відповідності змінам у правових системах. У цій статті розглядається взаємодія між PbD та емоційним ШІ, з наголосом на ризики для конфіденційності, що пов'язані зі збором та обробкою емоційних даних. Дослідження проводиться на тлі ширшого контексту розробки етичного ШІ. У роботі було підкреслено нагальну необхідність збалансувати технологічні інновації з надійним захистом конфіденційності.*

Методи. *У статті пропонується концептуальний юридичний аналіз взаємодії між концепцією конфіденційності за замовчуванням (PbD) та емоційним ШІ у сучасних системах захисту даних. У ній використовується комплексний огляд первинних джерел, зокрема GDPR ЄС, Акт ЄС про ШІ, судову практику Суду ЄС та ЄСПЛ, Рекомендації щодо захисту персональних даних, а також вторинні джерела, такі як наукові праці та книги. Дослідження структуровано таким чином: спочатку подано огляд емоційного ШІ, його застосування, а також проблеми конфіденційності, які він спричиняє. Далі йде розгляд наявних режимів захисту даних та того, як їх можна перенести на системи емоційного ШІ. Після чого увага зосереджується на*

фундаментальних принципах PbD, а також вивчається, як їх можна застосовувати під час розробки та впровадження технологій емоційного ШІ.

Результати та висновки. *Аналіз демонструє, що впровадження принципів PbD у системи емоційного ШІ є важливим, а не просто корисним для того, щоб захистити конфіденційність користувачів та забезпечити дотримання законодавства. Правильно впроваджені системи PbD мають три важливі переваги: підвищену прозорість системи, кращі механізми підзвітності та більший контроль користувачів над власними даними. Ці висновки роблять значний внесок у теоретичні основи відповідального проєктування штучного інтелекту, пропонуючи практичні рекомендації для організацій, що впроваджують системи емоційного ШІ. Зрештою, дослідження представляє чітку модель для розробників та організацій, яка допоможе їм успішно скористатися конвергенцією технологій емоційного інтелекту та нормативних вимог щодо конфіденційності.*

Ключові слова. *конфіденційність за замовчуванням, емоційний ШІ, захист даних, етика у ШІ, розпізнавання емоцій, конфіденційність користувачів.*

ABSTRACT IN ARABIC

مقالة مراجعة

الخصوصية المدمجة في التصميم ضمن تقنيات الذكاء الاصطناعي العاطفي: أطر حماية البيانات واستراتيجيات الامتثال

العروسي الشملالي* و ليلى بن صديق

الملخص

خلفية الدراسة: *أسهم التطور السريع في مجال الذكاء الاصطناعي العاطفي في فتح مجالات واسعة للابتكار في قطاعات متعددة تشمل الرعاية الصحية والتسويق والتفاعل بين الإنسان والآلة. وتعتمد تطبيقات هذا النوع من الذكاء الاصطناعي، القائم على تحليل الانفعالات البشرية ومعالجتها والتفاعل معها، على بيانات شخصية شديدة الحساسية، الأمر الذي يثير تحديات جوهرية تتعلق بالخصوصية وقضايا أخلاقية متنامية. ويعد تبني مبادئ الخصوصية المدمجة في التصميم داخل هذه الأنظمة خطوة أساسية لمواجهة هذه التحديات وضمان الامتثال للأطر القانونية المتغيرة. وتتناول هذه الدراسة العلاقة بين الخصوصية المدمجة في التصميم والذكاء الاصطناعي العاطفي، مع التركيز على المخاطر التي*

تهدد خصوصية الأفراد نتيجة جمع البيانات الانفعالية ومعالجتها. وتأتي الدراسة ضمن سياق أشمل يركز على تطوير ذكاء اصطناعي أخلاقي، مؤكدة الحاجة الملحة إلى المواءمة بين التقدم التقني وتوفير حماية قوية وفعّالة لخصوصية المستخدمين.

المنهجية: *يقدم هذا البحث تحليلًا قانونيًا مفاهيميًا للتقاطع بين الخصوصية المدمجة في التصميم والذكاء الاصطناعي العاطفي ضمن أطر حماية البيانات الحديثة. ويستند إلى مراجعة شاملة للمصادر الأولية، بما في ذلك اللائحة العامة لحماية البيانات في الاتحاد الأوروبي، وقانون الذكاء الاصطناعي الأوروبي، وأحكام محكمتي العدل الأوروبية وحقوق الإنسان الأوروبية، إلى جانب الإرشادات الصادرة عن هيئات حماية البيانات، فضلًا عن المصادر الثانوية مثل الدراسات الأكاديمية والكتب المتخصصة. وقد نُظمت المناقشة بحيث تبدأ بعرض شامل لمفهوم الذكاء الاصطناعي العاطفي وتطبيقاته والمخاوف الفردية المتعلقة بالخصوصية التي يثيرها. ويتبع ذلك تناولٌ للأطر الحالية لحماية البيانات وسبل تكييفها لتناسب أنظمة الذكاء الاصطناعي العاطفي. ثم تنتقل الدراسة إلى مناقشة المبادئ الأساسية للخصوصية المدمجة في التصميم، مع بحث كيفية تطبيق هذه المبادئ عند تطوير ونشر تقنيات الذكاء الاصطناعي العاطفي.*

النتائج والاستنتاجات: *يبيّن التحليل أن تطبيق مبادئ الخصوصية المدمجة في التصميم داخل أنظمة الذكاء الاصطناعي العاطفي ليس خيارًا إضافيًا، بل ضرورة أساسية لحماية خصوصية المستخدمين وضمان الامتثال القانوني. وعندما تُنفذ هذه المبادئ بصورة سليمة، فإنها توفر ثلاث فوائد محورية تتمثل في تعزيز شفافية النظام، وتقوية آليات المساءلة، وتوسيع قدرة الأفراد على التحكم في بياناتهم الشخصية. وتسهم هذه النتائج إسهامًا مهمًا في ترسيخ الأسس النظرية لتصميم ذكاء اصطناعي مسؤول، كما تقدم إرشادات عملية قابلة للتطبيق للجهات التي تعمل على تطوير ونشر تقنيات الذكاء الاصطناعي العاطفي. وتختتم الدراسة بطرح نموذج واضح يمكّن المطورين والمؤسسات من مواكبة التلاقي المتسارع بين تقنيات الذكاء العاطفي وتطورات التنظيمات المرتبطة بالخصوصية.*