

MASTER THESIS | MASTER'S THESIS

Titel | Title

The regulation of emotion recognition systems in the EU

verfasst von | submitted by

Katja Kolman

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 992 942

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on
the student record sheet:

Informations- und Medienrecht

Betreut von | Supervisor:

Univ.-Prof. Mag. Dr. Nikolaus Forgó

Table of Contents

List of abbreviations	1
1 Introduction	2
2 About emotion recognition systems	4
2.1 The development and use of emotion recognition systems	4
2.2 The definition of emotion recognition systems	13
2.2.1 First element: AI system	13
2.2.2 Second element: Emotions and intentions	15
2.2.3 Third element: The identification/inference of emotions and intentions	18
2.2.4 Fourth element: Biometric data basis	18
3 The regulation of emotion recognition systems under EU law – selected aspects	23
3.1 The AI Act.....	24
3.1.1 The applicability of the AI Act to emotion recognition systems.....	25
3.1.1.1 Prohibited AI practices	26
3.1.1.1.1 AI systems to infer emotions of persons in workplace and education institutions	26
3.1.1.1.2 Exceptions from the prohibition of emotion recognition systems in workplace and education institutions	28
3.1.1.1.3 Other prohibited AI practices	29
3.1.1.2 High-risk AI practices.....	31
3.1.1.2.1 Exceptions from the high-risk classification.....	31
3.1.1.3 Other exceptions to the applicability of the AI Act.....	32
3.1.1.3.1 Exceptions from the overall scope of the AI Act.....	32
3.1.1.3.2 Exceptions from the definition of emotion recognition systems under the AI Act	34
3.1.2 Requirements under the AI Act	35
3.1.2.1 High-risk AI systems	35
3.1.2.2 Transparency obligations.....	37
3.2 The interplay of the AI Act with EU fundamental rights and data protection law	37
3.2.1 EU fundamental rights law	38
3.2.1.1 The applicability of EU fundamental rights law	38
3.2.1.2 Requirements under fundamental rights law: selected risks	40
3.2.1.2.1 Human dignity	40
3.2.1.2.2 Right to integrity of the person.....	41
3.2.1.2.3 Freedom of thought.....	41
3.2.1.2.4 Right to respect for private life.....	42

3.2.1.2.5	Right to protection of personal data	44
3.2.1.2.6	Non-discrimination	45
3.2.1.2.7	The potential adverse impact on other rights	46
3.2.1.2.8	The need for new human rights?	47
3.2.1.2.9	Necessity and proportionality	48
3.2.1.3	Fundamental rights protection in practice and the interplay with the AI Act...	49
3.2.1.3.1	Fundamental rights due diligence	49
3.2.1.3.2	The role of oversight and enforcement	50
3.2.1.3.3	The review of prohibited and high-risk AI practices	52
3.2.2	The EU data protection acquis	53
3.2.2.1	The applicability of the EU data protection acquis	53
3.2.2.1.1	Processing of personal data	54
3.2.2.1.2	Processing of sensitive data	56
3.2.2.2	Requirements under data protection law	60
3.2.2.2.1	The lawfulness of processing	60
3.2.2.2.2	The fairness of processing	62
3.2.2.2.3	Accuracy requirements	62
3.2.2.2.4	Other requirements	63
3.2.2.2.5	Necessity and proportionality	63
3.2.2.3	Data protection in practice and the interplay with the AI Act	63
3.2.2.3.1	Data subject rights	64
3.2.2.3.2	Data protection impact assessment	65
3.2.2.3.3	The role of oversight and enforcement	65
4	Conclusions: Emotion recognition <i>de lege ferenda</i>	67
5	Annex I: Abstract in English and German	70
6	Annex II: List of sources	72
6.1	Books	72
6.2	Articles	72
6.3	Legal sources	77
6.4	Case law	79
6.5	Reports	79
6.6	Other online sources	82

List of abbreviations

AI	Artificial intelligence
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
ECG	Electrocardiogram
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEG	Electroencephalogram
EMG	Electromyogram
FRIA	Fundamental Rights Impact Assessment
EU	European Union
EUDPR	Data Protection Regulation for EU institutions, bodies, offices and agencies (Regulation 2018/1725)
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
GSR	Galvanic skin response
LED	Law Enforcement Directive (Directive (EU) 2016/680)
LLM	Large language model
MSA	Market surveillance authority
OJ	Official Journal of the European Union
PPG	Photoplethysmogram
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
WP29	Article 29 Data Protection Working Party

1 Introduction

In recent years, a growing trend of emotion recognition systems can be observed.¹ At the same time, criticism about their scientific basis and reliability as well as intrusiveness is mounting. This led also to increased regulatory attention in such systems, resulting in the explicit regulation of AI-based emotion recognitions systems under the EU AI Act.²

The master thesis examines key pieces of the EU regulatory framework that govern emotion recognition systems. Chapter 2 first looks in Section 2.1 into the development and use of emotion recognition systems, summarising both its technical aspects, (potential) applications in practice as well as criticism faced. This is the basis for examining the definition of emotion recognition systems, as contained in Article 3(39) of the AI Act, in Section 2.2.

Chapter 3 discusses selected aspects of the regulation of emotion systems under EU law. Section 3.1 first examines the applicability of the AI Act, which follows a risk-based approach to regulating emotion recognition systems, and its relevant requirements. Section 3.2 then explores the interplay of the AI Act with EU fundamental rights law, most notably the Charter of Fundamental Rights of the European Union (hereinafter: the Charter),³ and EU data protection law.⁴ It examines the applicability of these legal requirements to the development and use of emotion recognition systems, examines legal challenges as well as looks into practical ways forward in ensuring the respect for fundamental rights, including the right to data protection, in this context.

The thesis explores the following three questions, the answers to which will be summarised in the conclusions:

1. To what extent are emotion recognition systems covered by the AI Act and the different risk categories contained therein?
2. To what extent can the development and use of emotion recognition systems, when not prohibited by the AI Act, be permitted under EU fundamental rights law and more specifically the EU data protection acquis?

¹ See e.g. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (2025) Fifth edition, 3, 32 <www.autoriteitpersoonsgegevens.nl/en/current/ap-recognising-emotions-using-ai-is-questionable-and-risky> last accessed 19 October 2025. It should be also noted that several companies are making market size predictions for emotion recognition that predict its growth, however, it is difficult to verify the robustness of these analyses. See e.g. MarketsandMarkets, 'Emotion AI Market', December 2024 <www.marketsandmarkets.com/Market-Reports/emotion-ai-market-134111673.html> last accessed 19 October 2025.

² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) OJ L, 2024/1689.

³ Charter of Fundamental Rights of the European Union, OJ C 326/391.

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L 119/1; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive, LED), OJ L 119/89; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (EUDPR), OJ L 295/39.

3. How should such systems be regulated *de lege ferenda*?

Methodology

The thesis is based on desk research consisting of a review of literature, hard and soft laws as well as case law. The thesis analyses in particular relevant provisions of the AI Act, the Charter and the EU data protection acquis consisting of the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the Data Protection Regulation for EU institutions, bodies, offices and agencies (EUDPR). Next to analysing the operative provisions of the respective laws, the thesis frequently considers accompanying recitals and scholarly work to further the understanding of issues at hand. To this end, the non-binding legal nature of recitals has to be acknowledged.⁵ Even if recitals are not legally binding in themselves, they, however, provide guidance on the intent of the legislators and thus interpretation of the articles.⁶ Throughout the analysis of the legal framework, different examples, both from real life and theory, are embedded.

While there are important ethical considerations surrounding the use of emotion recognition systems, the thesis aims to focus on its legal aspects.⁷ Both aspects are, however, closely intertwined.

⁵ Pursuant to the EU's Joint practical guide on legislative drafting, Recitals should not contain normative provisions. European Union, 'The Joint practical guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation' (2015) Publications Office of the European Union, 31 <<https://op.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-en/format-PDF/source-341338175>> last accessed 19 October 2025.

⁶ As Klimta and Vaiciukaite note: 'Recitals in EC law are not considered to have independent legal value, but they can expand an ambiguous provision's scope. They cannot, however, restrict an unambiguous provision's scope, but they can be used to determine the nature of a provision, and this can have a restrictive effect.' Tadas Klimas, Jurate Vaiciukaite, 'The Law of Recitals in European Community Legislation' (2008) ILSA Journal of International & Comparative Law, Volume 15, Issue 1, 3. Den Heijer, van Os van den Abeelen and Maslyka note that recitals are used in EU law to state reasons for adoption (as per the Treaties) as well as provide an interpretative legal tool (as per the CJEU's case law). In their study, which looked into the use of recitals in EU directives in practice, they found that recitals often contain normative statements. Maarten den Heijer, Teun van Os van den Abeelen, Antanina Maslyka, 'On the Use and Misuse of Recitals in European Union Law' (2019) Amsterdam Law School Research Paper No. 2019-31, 4–6, 12, 19. See on this also: Sandra Wachter, Brent Mittelstadt, Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2019) International Data Privacy Law, Volume 7, Issue 2, 80.

⁷ For an overview of ethical concerns, see: Amelia Katirai, 'Ethical considerations in emotion recognition technologies: a review of the literature' (2023) AI and Ethics, Volume 4, 927–948.

2 About emotion recognition systems

This Chapter first briefly outlines the current state of development of emotion recognition systems with a view to understand their (potential) use in practice. While such systems can be used in many different areas, which is demonstrated also by a broad spectrum of patents and products on the market, there appears to be limited evidence about their use in the EU. The developments and use of such systems have been subjected to criticism by different actors, including from academia, civil society organisations and the media as well as by the European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) and the United Nations (UN) High Commissioner for Human Rights, primarily due to their disputed scientific basis and reliability as well as due to their intrusiveness, as will be further explained in Section 2.1.⁸

The Chapter then looks in Section 2.2 into the definition of an ‘emotion recognition system’ under the AI Act, which is key for the subsequent analysis of the EU legal framework that governs the development and use of such systems. It points towards several uncertainties connected to the definition, which stipulates that these are ‘AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data’ (Article 3(39) of the AI Act). The Commission has published non-binding Guidelines on the definition of an AI system under the AI Act,⁹ however, some open questions remain as to its exact scope, in particular the extent to which less complex systems are covered by it. The Commission has also published non-binding Guidelines on the prohibitions under the AI Act.¹⁰ While these provide guidance on the other elements of the definition of emotion recognition system, a major point of uncertainty remains the definition of ‘emotions’, on which no consensus exists in literature. Even less clear is the concept of ‘intentions’, which remains largely undefined. The AI Act also broadens the definition of biometric data from the EU data protection acquis, which helps to ensure a broader application of it to emotion recognition systems in practice, as such systems do not need to allow for the unique identification of a person.¹¹

2.1 The development and use of emotion recognition systems

Emotion recognition systems belong to ‘affective computing’ technologies, which aim to recognise and interpret emotions and affective states¹² with a view for computers to

⁸ See the corresponding references below in Section 2.1.

⁹ European Commission, Annex to the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final, 6.2.2025 <<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>> last accessed 19 October 2025 (hereinafter: Commission Guidelines on the definition of an artificial intelligence system).

¹⁰ European Commission, Annex to the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 6.2.2025 <<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>> last accessed 19 October 2025 (hereinafter: Commission Guidelines on prohibited artificial intelligence practices).

¹¹ See the corresponding references below in Section 2.2.

¹² EDPS, ‘TechDispatch #1/2021 - Facial Emotion Recognition’, 26 May 2021, 1 <www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf> last accessed 19 October 2025.

intelligently react to human emotions.¹³ It is based on the premise that emotions ‘can be surveyed, measured and remembered’.¹⁴ Affective computing is a multidisciplinary research field that deals with emotion recognition and sentiment analysis¹⁵ – two distinct issues that can to a certain degree overlap.¹⁶ Approaches in the affective computing field rely on the idea of basic emotions, described below (so-called discrete emotion models, which categorise emotions into limited categories) and more complex 2- or 3-dimensional emotion models, which measure the valence (magnitude of joy/distress), arousal (activation of physiological and psychological changes in a person) and dominance (influence by/on the environment and others) experienced by a person.¹⁷

According to a 2020 survey on emotion recognition and detection models, four methods were predominantly used for the detection of emotions (facial expressions, speech signals, physiological signals¹⁸ and text semantics detection), leading to the recognition of a number of basic emotions.¹⁹ A further systematic review of emotion recognition and AI from 2024 followed a similar categorisation by distinguishing between emotion recognition using questionnaires, physical signals (focusing on most commonly used facial expressions and speech²⁰) and emotion recognition using physiological signals (focusing on most commonly used signals obtained through electroencephalography (EEG; measuring brain activity), electrocardiography (ECG; measuring heart activity), galvanic skin response (GSR; measuring the change in the electrical properties of the skin²¹) and eye tracking).²² While visual-based emotion recognition systems are prevalent due to the ease with which such data can be captured,²³ physiological signals collected through wearable sensors are preferred for

¹³ Yan Wang and others, ‘A systematic review on affective computing: emotion models, databases, and recent advances’ (2022) *Information Fusion Volumes* 83–84, 19. The authors refer to R.W. Picard, E. Vyzas, J. Healey, *Toward machine emotional intelligence: analysis of affective physiological state*, *IEEE Trans. Pattern Anal. Mach. Intell.* 23 (2001) 1175–1191.

¹⁴ Javier Sánchez-Monedero and Lina Dencik, ‘The Politics of Deceptive Borders: “Biomarkers of Deceit” and the Case of iBorderCtrl’ (2022) *Information, Communication & Society*, Volume 25, Issue 3, 415.

¹⁵ The idea of affective computing was first proposed by Prof. Rosalind Picard in 1997. Wang and others (n 13) 19.

¹⁶ Sentiment analysis mostly focuses on evaluations of text and opinion mining, and its results are usually described as a positive, negative, or neutral sentiment, as opposed to a specific emotion. Wang and others (n 13) 20. The authors refer to E. Cambria, Affective computing and sentiment analysis, *IEEE Intell. Syst.* 31 (2016) 102–107; S. Poria, E. Cambria, A. Gelbukh, Aspect extraction for opinion mining with a deep convolutional neural network, *Knowl. Based Syst.* 108 (2016) 42–49; E. Cambria, R. Speer, C. Havasi, A. Hussain, SenticNet: a publicly available semantic resource for opinion mining, in: *AAAI2010*, 2010: pp. 14–18.

¹⁷ Smith K. Khare and others, ‘Emotion Recognition and Artificial Intelligence: A Systematic Review (2014–2023) and Research Recommendations’ (2024) *Information Fusion*, Volume 102, 102019, 1–2. Wang and others (n 13) 23–24. See also: Andreas Häuselmann and others, ‘EU law and emotion data’ (2023) *arXiv:2309.10776*, 2 <<https://arxiv.org/abs/2309.10776v1>> last accessed 19 October 2025. Andrew McStay, ‘Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy’ (2020) *Big Data & Society*, Volume 7, Issue 1, 2.

¹⁸ These are biochemical signals that occur in response to stimuli, such as electrocardiographic signals (recording heart activity), electroencephalographic signals (recording brain activity), or electromyography signals (recording muscle activity). Anvita Saxena, Ashish Khanna, Deepak Gupta, ‘Emotion Recognition and Detection Methods: A Comprehensive Survey’ (2020) *Journal of Artificial Intelligence and Systems* 2, 62, 74.

¹⁹ The studies mentioned in the paper were detecting up to seven emotions, such as happiness, sadness and fear. *Ibid.*, 53–55, 62, 65.

²⁰ Other, less commonly used physical signals for emotion recognition are text, gestures, and body posture. Khare and others (n 17) 2. The authors refer to Lin Shu and others, ‘A Review of Emotion Recognition Using Physiological Signals’ (2018) *Sensors* 2018, 18(7), 2074.

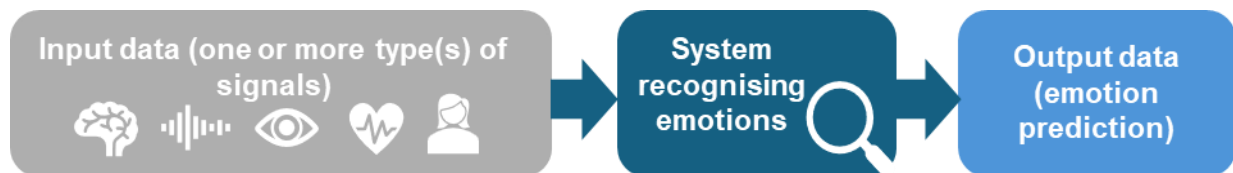
²¹ Science Direct, ‘Galvanic Skin Response’ <www.sciencedirect.com/topics/computer-science/galvanic-skin-response> last accessed 19 October 2025. The term Electrodermal Activity (EDA) can be also used for it.

²² Other signals used for emotion detection are electromyogram, respiration, skin temperature and photoplethysmography. Khare and others (n 17) 1–2. The authors refer to: Lin Shu and others, ‘A Review of Emotion Recognition Using Physiological Signals’ (2018) *Sensors* 2018, 18(7), 2074.

²³ Wang and others (n 13) 41.

emotion identification in the system development community, as they cannot be easily controlled by a person,²⁴ i.e. subjected to so-called social masking.²⁵ These different signals are fed into an automated emotion recognition system, which then extracts and assesses their features to arrive to an output (emotion prediction).²⁶ Systems can be thereby either unimodal (processing one kind of signal) or multimodal (processing different kinds of signals), with the latter gaining more attention owing to the multimodal way in which humans express emotions or sentiment²⁷ and the improved performance that such systems can achieve.²⁸

Figure 1: The functioning of emotion recognition systems²⁹



Emotion recognition systems can be used in different areas, for example healthcare, education, employment, law enforcement and public safety, customer behaviour analysis and targeted advertising, as well as in the entertainment industry.³⁰ Different providers around the globe are developing emotion recognition systems that can be integrated into different software solutions³¹ – the potential use cases are therefore manifold. For example, Google released in December 2024 the vision-language model PaliGemma 2 which identifies emotions.³² The Amazon Rekognition API allows for detecting emotions in images and

²⁴ Khare and others (n 17) 14. See also: Wang and others (n 13) 20, 25, 41.

²⁵ Wang and others (n 13) 25, 34. The authors refer to J. Zhang, Z. Yin, P. Chen, S. Nichele, Emotion recognition using multi-modal data and machine learning techniques: a tutorial and review, *Inf. Fusion*. 59 (2020) 103–126.

²⁶ See: Khare and others (n 17) 3–4. The authors analyse the steps in an automated emotion recognition system, considering also aspects pertaining to the development of the system (feature selection, classification, and model evaluation).

²⁷ Wang and others (n 13) 20. The authors refer to P. Tzirakis, G. Trigeorgis, M.A. Nicolaou, B.W. Schuller, S. Zafeiriou, End-to-end multimodal emotion recognition using deep neural networks, *IEEE J. Sel. Top. Signal Process*. 11 (2017) 1301–1309.

²⁸ Wang and others (n 13) 41.

²⁹ See the analysis and corresponding references above. For a more detailed illustration of how emotion recognition systems work, see: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 35.

³⁰ European Commission, 'Multi-stakeholder consultation for Commission guidelines on the application of the definition of an AI system and the prohibited AI practices established in the AI Act', Section F <<https://ec.europa.eu/eusurvey/runner/Prohibitions-and-Definition-Survey-2024#page3>> accessed 23 November 2024. See also: EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 2. The EDPS mapped out potential areas of use of facial emotion recognition. See also: Khare and others (n 17) 1. The authors of the survey noted that emotion recognition can be used for affective computing, healthcare, human-robot interactions and market research. See also: McStay (n 17) 1. The author notes emotion recognition can be used in everyday objects and practices as well as different spaces. See also: Elisabeth Steindl, 'Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in Light of the Draft AI Act and its Interplay with the GDPR' (2022) *European Data Protection Law Review*, Volume 8, Number 2, 312. The author observes that emotion technology can be used 'in literally every context'. See also: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 41.

³¹ For some commercial examples, see: AI Superior, 'Best Emotion Recognition Companies', 9 July 2024 <<https://aisuperior.com/emotion-recognition-companies/>> last accessed 19 October 2025; Fora Soft, '7 Leading Real-Time AI Emotion Recognition Software Solutions', 29 August 2024 <www.forasoft.com/blog/article/real-time-ai-emotion-software> last accessed 19 October 2025.

³² Google for Developers, 'Introducing PaliGemma 2: Powerful Vision-Language Models, Simple Fine-Tuning', 5 December 2024 <<https://developers.googleblog.com/en/introducing-paligemma-2-powerful-vision-language-models-simple-fine-tuning/>> last accessed 19 October 2025.

videos.³³ Amazon and Spotify for example also registered patents for emotion recognition in their voice assistants.³⁴ Snap patented emotion recognition for workforce analytics.³⁵ NEC introduced already in 2018 an emotion analysis solution that could infer emotions of employees from physiological signals collected through wearable devices, which was implemented in various industries, including transportation, manufacturing, construction, and healthcare.³⁶ Another well-known provider in the field, Affectiva, is providing solutions for ad and entertainment content testing, qualitative research, behavioural research, in-cabin sensing in vehicles as well as a software development kit that can be incorporated into different apps.³⁷ Another provider, Realeyes, offers an automated emotion recognition technology, which is being used in different fields, including advertising, education, wellbeing, gaming, anti-fraud, customer feedback and human-robot interaction.³⁸ At EU level, different projects looking into this technology were funded by the Horizon2020 program, most notably the iBorderCtrl project that explored the use of facial emotion recognition at EU borders.³⁹ The current Horizon program is funding research into an emotion recognition system for real-time and continuous patient monitoring in psychiatry.⁴⁰ These are only a few examples that demonstrate the diverse use cases of such technology.⁴¹

The 2024 systematic review of emotion recognition and AI by Khare and others showed that there is, however, little discussion on applications of such systems in literature.⁴² The authors therefore outlined several areas which emotion recognition can help to accelerate in their view: detection and monitoring of medical conditions (building on existing research on, for example, emotions and Parkinson's disease, schizophrenia or Alzheimer's disease),⁴³ children's health (for example to teach children with autism or dyslexia), environmental health studies (to better understand the impact of various environmental factors on mental health), human-robot interaction (for models to interpret human emotions and adjust their behaviour), patient

³³ AWS, 'Detecting and analyzing faces' <<https://docs.aws.amazon.com/rekognition/latest/dg/faces.html>> last accessed 19 October 2025.

³⁴ Google Patents, 'Systems and methods for enhancing responsiveness to utterances having detectable emotion', US10566010B2 <<https://patents.google.com/patent/US10566010B2/en?q=US+10566010+B2>> last accessed 19 October 2025. Google Patents, 'Voice-based determination of physical and emotional characteristics of users', US10096319B1 <<https://patents.google.com/patent/US10096319B1/en?q=US+10096319>> last accessed 19 October 2025.

³⁵ Google Patents, 'Emotion recognition for workforce analytics', US10496947B1 <<https://patents.google.com/patent/US10496947B1/en>> last accessed 19 October 2025.

³⁶ NEC, 'NEC's Emotion Analysis Solution Supports Work Style Reform and Health Management', NEC Technical Journal, Vol.14 (2019) <www.nec.com/en/global/techrep/journal/g19/n01/190109.html> last accessed 19 October 2025. It is unclear whether this solution was adopted only in Japan (the article refers at the beginning to the Japanese government and Japanese corporations). No further information about the solution is available on the NEC website. NEC and Realeyes have, however, announced a joint emotion analysis technology in 2020. NEC, 'NEC and Realeyes jointly develop emotion analysis service in support of video communications', 23 October 2020 <www.nec.com/en/press/202010/global_20201023_03.html> last accessed 19 October 2025.

³⁷ Affectiva, 'Solutions' <www.affectiva.com/solutions/> last accessed 19 October 2025.

³⁸ Realeyes, 'Emotion' <www.realeyesit.com/technology/emotion/> last accessed 19 October 2025.

³⁹ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 1. See also: European Commission, 'Smart lie-detection system to tighten EU's busy borders', 24 October 2018 <<https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders>> last accessed 19 October 2025. For a critical analysis of the system, see: Sánchez-Monedero and Dencik (n 14) 413–430.

⁴⁰ European Commission, 'A novel and accurate emotion recognition system for real-time and continuous patient monitoring in psychiatry' <<https://cordis.europa.eu/project/id/190129251>> last accessed 19 October 2025.

⁴¹ For some mapping of the potential use of facial emotion recognition, see for example: EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 2.

⁴² Khare and others (n 17) 5.

⁴³ The authors note that very few studies on the detection of various disorders from emotions are available due to a lack of publicly available datasets. Ibid, 13.

assistance, driving assistance (to detect driver's fatigue), education (to understand students' levels of satisfaction), marketing (to read real-time emotions of customers and adjust marketing strategies to them), recruitment (to monitor stress levels of candidates during interviews), business models (to gather people's perception about a product/experience) and e-learning (to identify students' emotions and understanding in real-time and adjust class content).⁴⁴

As this overview demonstrates, such systems are being developed and could be potentially used in many different areas. They could be also used in combination with biometric identification systems.⁴⁵ It is also important to consider the trend of emotion recognition being more broadly integrated into large language models.⁴⁶ McStay and Bakir distinguish for example between AI systems that simulate empathic behaviours or responses either intentionally (by design) or unintentionally. In the latter case, emotion recognition and pre-trained emotion classifiers are not deliberately included in the system, but systems still simulate empathic behaviours as they are programmed to include context sensitivity in the predicted outputs.⁴⁷ This ultimately means that systems down the value chain, which use such models, can perform emotion recognition, despite this not being the key objective of the systems.⁴⁸ Overall, it remains unclear to what extent emotion recognition systems (with the exception of LLMs) are being used in practice in the EU, especially by public bodies and more broadly in asymmetrical power relationships, as the current discussions focus mostly on its potential use.⁴⁹

Concerning the use of emotion recognition systems falling under the AI Act (see Section 2.2), there will be some more clarity on which systems are placed on the market/put into service/used in the EU once the AI Act's provisions on high-risk AI systems will become applicable, as they will generally require providers to register such systems in an EU database⁵⁰ (for more on the classification of emotion recognition systems under the AI Act, see Section 3.1). Moreover, if public authorities or Union institutions or bodies will be deploying such systems, they will have to register the use in the database too.⁵¹ This data will be publicly

⁴⁴ Ibid, 13–14.

⁴⁵ See: Article 3(35) and (41) AI Act. EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 1.

⁴⁶ Andrew McStay and Vian Bakir, 'Soft law for unintentional empathy: addressing the governance gap in emotion-recognition AI technologies' (2025) *Journal of Responsible Technology*, Volume 23, 2. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 36.

⁴⁷ McStay and Bakir (n 46) 1–2.

⁴⁸ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 44.

⁴⁹ The author's own research, albeit not surveying this topic in a structured manner, revealed limited evidence of such systems (in a narrower sense) being used in practice in the EU, especially by public bodies and more broadly in asymmetrical power relationships. Ultimately, the scope of use would depend also on the scope of the definition of an emotion recognition system (see Sub-section 2.2). For example, as the Dutch Department for the Coordination of Algorithmic Oversight observed in its recent Report AI & Algorithms Netherlands, the use of wearables such as smart watches that measure stress levels of consumers is gaining popularity. If emotions include 'stress' (noting that Recital 18 of the AI Act excludes from the scope of the definition systems used for detecting physical states, see Sub-section 3.1.1.3.2.1), this would amount to emotion recognition. See: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 42.

⁵⁰ With some exceptions for systems used in the critical infrastructure field that should be registered at national level. Article 49(1) and (5) as well as Article 71 AI Act.

⁵¹ Articles 26(8) and 49(3) AI Act.

available, except for systems provided or deployed in the areas of law enforcement, migration, asylum and border control management.⁵²

At the same time, it should be noted that emotion recognition technologies have faced criticism by different actors – including from academia,⁵³ civil society organisations⁵⁴ and the media⁵⁵ as well as by the EDPS and EDPB⁵⁶ and UN High Commissioner for Human Rights⁵⁷ – primarily due to their disputed scientific basis and reliability as well as due to their intrusive nature.⁵⁸ As will be further explain in Chapter 2.2.2, emotions are difficult to define and vary between persons, subject also to the social and cultural context.⁵⁹ A frequently cited 2019 study conducted by Feldman Barrett and others, which was indirectly referred to also in the impact assessment of the AI Act,⁶⁰ challenged the ‘common view’ that it is possible to read

⁵² The data about these will be available only to the Commission and relevant national market surveillance authorities. Article 49(5) AI Act.

⁵³ For a critique of the scientific basis, see: Lisa Feldman Barrett and others, ‘Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements’ (2019) *Psychological Science in the Public Interest*, Volume 20, Number 1, 1–68. For a critique of the intrusive nature, see e.g.: Nathalie A. Smuha and others, ‘How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission’s Proposal for an Artificial Intelligence Act’ (2021) SSRN, 27 <<http://dx.doi.org/10.2139/ssrn.3899991>> last accessed 19 October 2025. Mateja Durovic and Tommaso Corno, ‘The Privacy of Emotions’ in Martin Ebers and Karin Sein (eds.), *Privacy, Data Protection and Data-driven Technologies* (1st edition, Routledge 2024) 375.

⁵⁴ See e.g.: Joint civil society amendments to the Artificial Intelligence Act, ‘Prohibit emotion recognition in the Artificial Intelligence Act’ <www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf> last accessed 19 October 2025.

⁵⁵ See e.g.: Hannah Devlin, ‘AI systems claiming to ‘read’ emotions pose discrimination risks’ *The Guardian* (16 February 2020) <www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks> last accessed 19 October 2025. Kate Crawford, ‘Artificial Intelligence is Misreading Human Emotion’ *The Atlantic* (27 April 2021) <www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/> last accessed 19 October 2025. Kyle Wiggers, ‘Google says its new AI models can identify emotions — and that has experts worried’ *TechCrunch* (5 December 2024) <<https://techcrunch.com/2024/12/05/google-says-its-new-open-models-can-identify-emotions-and-that-has-experts-worried/>> last accessed 19 October 2025.

⁵⁶ EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, 13 <www.edps.europa.eu/node/7140_en> last accessed 19 October 2025.

⁵⁷ UN High Commissioner for Human Rights, ‘The right to privacy in the digital age’ (2021) A/HRC/48/31.

⁵⁸ See also the results of a recent public consultation by the Dutch Data Protection Authority, where respondents have raised their concerns about the reliability of emotion recognition technology and related risks of discrimination, as well as its intrusiveness and related privacy risks. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, ‘AI systems for emotion recognition in the areas of workplace or education institutions’ (2025) 2 <www.autoriteitpersoonsgegevens.nl/en/documents/summary-and-next-steps-call-for-input-on-prohibition-on-ai-systems-for-emotion-recognition-in-the-areas-of-workplace-or-education-institutions> last accessed 19 October 2025.

⁵⁹ Scarantino points out the work of psychological constructionists (Russell, 2003 and Barrett, 2006) who considered that there is no empirical evidence to support the claim that emotions correspond to unavoidable changes in the body. He also summarises the work on the ‘cultural variability’ and ‘social role’ of emotions. Andrea Scarantino, ‘The Philosophy of Emotions and Its Impact on Affective Science’ in Lisa Feldman Barrett, Michael Lewis, Jeannette M. Haviland-Jones (eds.), *Handbook of Emotions* (4th edition, Guilford Press 2016) 21. In the public consultation by the Dutch Data Protection Authority, respondents for example also noted that the concept of ‘emotions’ is hard to define as they are highly context dependent. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, ‘AI systems for emotion recognition in the areas of workplace or education institutions’ (n 58) 7.

⁶⁰ When noting the ‘serious doubts as to the scientific nature and reliability of [emotion recognition] systems’, the impact assessment refers to James Vincent’s article ‘AI ‘emotion recognition’ can’t be trusted’ in *The Verge* of 25 July 2019 <www.theverge.com/2019/7/25/8929793/emotion-recognition-analysis-ai-machine-learning-facial-expression-review> last accessed 19 October 2025, which refers to the 2019 study from Lisa Feldman Barrett and others. European Commission, Commission staff working document, Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, SWD(2021) 84 final,

emotions from facial expressions.⁶¹ This systematic literature review highlighted three key shortcomings of the scientific research in this field, namely its limited reliability, lack of specificity and limited generalisability⁶² (these shortcomings of emotion recognition systems were also acknowledged in Recital 44 of the AI Act). Limited reliability refers to the fact that emotions are not reliably expressed and perceived through specific facial movements. The lack of specificity refers to the lack of a unique mapping between some facial movements and emotion categories (i.e. a facial configuration would need to express only one specific emotion, and not potentially others). General conclusions are therefore limited due to the insufficient documentation and consideration of how context and culture affect expressions of emotions in research.⁶³ In addition, the study observed that when it comes to measuring emotions through dynamic changes in the autonomic nervous system (e.g. cardiovascular or respiratory changes) or in the central nervous system (e.g. changes in the electrical activity in the brain), there are currently also ‘no objective measures [...] that reliably, uniquely, and replicably identify an instance of one emotion category compared with an instance of another’.⁶⁴

As Crawford notes, despite the critiques emotion recognition from facial expressions received, the idea of emotion recognition took off as it fit well the potential of computer vision and automation at scale – as the author puts it, ‘[t]he theory fit what the tools could do.’⁶⁵ This aligns with some broader concerns about the resurgence of pseudoscience in the era of machine learning, in particular of physiognomy (i.e. methods that aim to predict character traits of a person from their appearance).⁶⁶

At the same time, it should be acknowledged that Feldman Barrett and others did not dismiss in their 2019 study the idea of emotion recognition, but rather underlined the limits of existing research, primarily on facial expressions. They included recommendations for improving future research on emotions by ‘sampling individuals deeply’ through multimodal data analysis.⁶⁷ Such multimodal approaches can be in turn even more data demanding and invasive.⁶⁸

Another issue connected to such systems, and AI systems more broadly,⁶⁹ is bias that can be present in such systems and can lead to discrimination. Previous research has for example demonstrated that emotion recognition systems can be biased based on a person’s race (by

21.4.2021, 19 <<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>> last accessed 19 October 2025.

⁶¹ Feldman Barrett and others (n 53) 1, 3.

⁶² Ibid.

⁶³ Ibid, 3, 10.

⁶⁴ Ibid, 16.

⁶⁵ Kate Crawford, ‘Artificial Intelligence is Misreading Human Emotion’ (n 55).

⁶⁶ Mel Andrews, Andrew Smart, Abeba Birhane, ‘The reanimation of pseudoscience in machine learning and its ethical repercussions’ (2024) *Patterns*, Volume 5, Issue 9, 1–2. Meredith Whittaker and others, ‘AI Now Report 2018’ (2018) 13 <https://ainowinstitute.org/wp-content/uploads/2023/04/AI_Now_2018_Report.pdf> last accessed 19 October 2025. See also: McStay and Bakir (n 46) 3–6.

⁶⁷ Feldman Barrett and others (n 53) 48–49.

⁶⁸ Andrew McStay and Lachlan Urquhart, ‘This time with feeling?’ Assessing EU data governance implications of out of home appraisal based emotional AI’ (2019) *First Monday*, Volume 24, Number 10, 3, 8.

⁶⁹ See e.g., European Union Agency for Fundamental Rights (FRA), ‘Bias in algorithms - Artificial intelligence and discrimination’ (2022) Publications Office of the European Union <<https://fra.europa.eu/en/publication/2022/bias-algorithm>> last accessed 19 October 2025.

more frequently assigning 'negative emotions' to black persons⁷⁰) or age (by more 'accurately' predicting emotions in younger persons⁷¹).

Most importantly, regardless of the potential accuracy of such systems (that could be achieved in the future), a key legal issue connected to the use of such systems lies in their intrusiveness and related datafication of persons,⁷² which could be also misused for manipulation, as well as their chilling effect. The risks that public authorities' use of emotion recognition systems poses to human rights were for example acknowledged by the UN High Commissioner for Human Rights in her 2021 annual report.⁷³

Experts from academia raised concerns over the intrusive nature and chilling effect of such systems. Smuha and others considered for example that 'even if [such systems] were scientifically sound, automatically reading every single person's emotional state is a highly intrusive act, with potentially huge chilling effects'.⁷⁴ They called for banning their use by public authorities with coercive powers.⁷⁵ McStay and Urquhart also raised particular concerns about such technologies entering the public sphere, flagging how such technologies lead to a loss of ephemerality of emotions and are prone to be misused for manipulation (especially of consumers). They also bring challenges for individuals' identity and their possibility to resist such observation and monitoring, as well as could result in unfair and pre-emptive treatment of persons.⁷⁶ Häuselmann and others pointed out how such systems can interfere with people's privacy and dignity, and result in discrimination, oppression or manipulation, with the latter not only undermining people's autonomy, but also potentially harming their health or leading to economic and time losses.⁷⁷ Durovic and Corno questioned the acceptability of public and private actors using such systems 'to incentivise certain outcomes over others or to interfere with [people's] lives under the pretext of safety and security'.⁷⁸ Steindl also raised concerns about such technology making people vulnerable to manipulation and leading to increased surveillance of people's emotions.⁷⁹ Concerns over potential manipulation through emotional AI used in social media or toys were also raised by the majority of respondents to

⁷⁰ Lauren Rhue, 'Racial Influence on Automated Perceptions of Emotions' (2018) SSRN <<https://dx.doi.org/10.2139/ssrn.3281765>> last accessed 19 October 2025.

⁷¹ Eugenia Kim and others, 'Age Bias in Emotion Detection: An Analysis of Facial Emotion Recognition Performance on Young, Middle-Aged, and Older Adults' (2021) AIES '21: AAAI/ACM Conference on AI, Ethics, and Society.

⁷² As Mejias and Couldry put it 'datafication is a contemporary phenomenon which refers to the quantification of human life through digital information, very often for economic value' and 'datafication combines two processes: *the transformation of human life into data through processes of quantification, and the generation of different kinds of value from data.*' Furthermore, 'it signals a historically new method of quantifying elements of life that until now were not quantified to this extent.' Ulises A. Mejias and Nick Couldry, 'Datafication' (2019) Internet Policy Review, Volume 8, Issue 4. As the authors acknowledge, the term 'datafication' was coined by Mayer-Schönberger and Cukier (Mayer-Schönberger and Cukier, 2013, chapter 5). See also: McStay and Urquhart (n 68) 4. Steindl (n 30) 312. Thomas Gremsl and Elisabeth Hödl, 'Emotional AI: legal and ethical challenges' (2022) Information Polity 27, 163.

⁷³ '[T]he use of emotion recognition systems by public authorities, for instance for singling out individuals for police stops or arrests or to assess the veracity of statements during interrogations, risks undermining human rights, such as the rights to privacy, to liberty and to a fair trial.' UN High Commissioner for Human Rights, 'The right to privacy in the digital age' (2021) A/HRC/48/31, 8.

⁷⁴ Smuha and others (n 53) 27.

⁷⁵ Ibid, 56.

⁷⁶ McStay and Urquhart (n 68) 2, 4–5.

⁷⁷ Häuselmann and others (n 17) 2–3. See further references used by the authors.

⁷⁸ Durovic and Corno (n 53) 375.

⁷⁹ Steindl (n 30) 311–312. See also: EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 4.

a 2022 UK-based survey.⁸⁰ In an earlier UK-based survey, over half of the respondents were not comfortable with emotion detection, even if working in an anonymous manner that does not lead to their personal identification.⁸¹ Ultimately, as pointed out in the AI Now's 2018 report, the use of emotion recognition systems 'raises troubling ethical questions about locating the arbiter of someone's "real" character and emotions outside of the individual, and the potential abuse of power that can be justified based on these faulty claims.'⁸²

In the run up to the AI Act, civil society organisations,⁸³ including the European Disability Forum,⁸⁴ the EDPS and EDPB⁸⁵ and Austria⁸⁶ called in principle for the full ban of emotion recognition systems (in some cases with narrowly defined exceptions for research and assistive technologies⁸⁷), given the interference of such systems with fundamental rights. Civil society organisations and other stakeholders continue with raising concerns about such systems.⁸⁸ In the Commission's public consultation on the prohibitions under the AI Act, respondents underlined that emotion recognition systems need to be strictly regulated to prevent their use in sensitive contexts.⁸⁹ While some respondents noted that the use of emotion recognition systems could help to enhance user experiences or improve mental health support, many were concerned about their impact on privacy and autonomy as well as

⁸⁰ Vian Bakir and others, 'On manipulation by emotional AI: UK adults' views and governance implications' (2024) *Frontiers in Sociology*, Volume 9, 1, 15.

⁸¹ McStay (n 17) 9–10.

⁸² Meredith Whittaker and others, 'AI Now Report 2018' (n 66) 14–15.

⁸³ A Civil Society Statement, 'An EU Artificial Intelligence Act for Fundamental Rights' 30 November 2021, 3 <<https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf>> last accessed 19 October 2025. Joint civil society amendments to the Artificial Intelligence Act, Prohibit emotion recognition in the Artificial Intelligence Act, 1 <www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf> last accessed 19 October 2025. The civil society organisations consider that exceptions could be permitted for assistive technologies if there is evidence about their usefulness from affected groups (such as organisations representing persons with disabilities) and experts (p. 4). See also the joint civil society statement on the compromise AI Act text, 'EU's AI Act fails to set gold standard for human rights', 3 April 2024, 5 <www.amnesty.eu/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf> last accessed 19 October 2025.

⁸⁴ European Disability Forum, 'Resolution on the EU Artificial intelligence Act for the inclusion of persons with disabilities', adopted by the Board of Directors of the European Disability Forum on 1 April 2023 <www.edf-feph.org/publications/resolution-on-the-eu-artificial-intelligence-act-for-the-inclusion-of-persons-with-disabilities/> last accessed 19 October 2025. The resolution calls for the ban of emotion recognition system, unless used for well-defined research purposes and in assistive technologies, which comply with strict privacy safeguards, including informed consent (point 7).

⁸⁵ The EDPS and EDPB considered that the use should be exceptionally permitted only for 'for certain well-specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation.' EDPS - EDPB Joint Opinion on the AI Act proposal (n 56) 13.

⁸⁶ Council of the EU, Draft Regulation 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) (first reading) - Adoption of the legislative act = Statements, 2021/0106(COD), 3 <<https://data.consilium.europa.eu/doc/document/ST-9645-2024-ADD-1-REV-2/en/pdf>> last accessed 19 October 2025.

⁸⁷ See the corresponding references above.

⁸⁸ See e.g. Electronic Privacy Information Center, 'AI Systems for Emotion Recognition in the Areas of Workplace or Education Institutions: Prohibition in EU Regulation 2024/1689 (AI Act)' (2024) 6–11 <<https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/>> last accessed 19 October 2025. See also: Durovic and Corno (n 53) 400. The authors conclude that generally prohibiting emotion recognition systems under the AI Act, permitting only very few and very specific exceptions, would be preferred.

⁸⁹ European Commission, 'Analysis of EU AI Office stakeholder consultations: defining AI systems and prohibited applications' (2025) Final study report, written by CEPS, 45 <<https://digital-strategy.ec.europa.eu/en/library/european-commission-releases-analysis-stakeholder-feedback-ai-definitions-and-prohibited-practices>> last accessed 19 October 2025.

people's mental health and wellbeing due to invoked feelings of surveillance.⁹⁰ The Dutch Department for the Coordination of Algorithmic Oversight recently also conducted an in-depth study of emotion recognition systems, calling on organisations to critically approach their potential adoption due to risks they pose to fundamental rights and public values as well as their questionable effectiveness.⁹¹

2.2 The definition of emotion recognition systems

The present thesis follows the definition of emotion recognition systems in the AI Act. Article 3(39) of the AI Act defines an emotion recognition system as an '*AI system* for the purpose of *identifying or inferring emotions or intentions* of natural persons on the basis of their *biometric data*'.⁹² When considering what kind of technology falls under 'emotion recognition systems' it is therefore important to consider (1) what is an AI system, (2) what are emotions or intentions of natural persons, (3) what does it mean that a system can identify or infer them and (4) what are biometric data. These elements and challenges with their interpretation will be explained further in Sub-sections 2.2.1 to 2.2.4 below.

2.2.1 First element: AI system

The AI Act clarifies in Article 3(1) that an AI system 'means a *machine-based* system that is designed to operate with varying levels of *autonomy* and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, *infers*, from the *input* it receives, how to generate *outputs* such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'.⁹³ Recital 12 of the AI Act explains that this means that the system has to run on machines and operate with some degree of independence from human involvement.⁹⁴ It further states that the capability to infer – i.e. to obtain outputs and to derive models and/or algorithms from inputs or data – is a key characteristic of AI systems and 'transcends basic data processing by enabling learning, reasoning or modelling'. While the AI Act aims to draw a distinction between AI systems and simpler traditional software systems or programming approaches,⁹⁵ this distinction requires further clarifications in practice.

To this end, the Commission published non-binding Guidelines on the application of the definition in February 2025, in line with Article 96(1)(f) of the AI Act. These explain inter alia that the concept of inference, which is key for the definition of an AI system, needs to be understood not only 'as an ability of a system to derive outputs from given inputs', but as referring to the building phase of a system, 'whereby a system derives outputs through AI

⁹⁰ Ibid, 44.

⁹¹ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 3.

⁹² Emphasis added.

⁹³ Emphasis added. This definition follows the revised 2023 OECD definition: 'An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.' Marko Grobelnik, Karine Perset, Stuart Russell, 'What is AI? Can you make a clear distinction between AI and non-AI systems?' OECD.AI, 6 March 2024 <<https://oecd.ai/en/wonk/definition>> last accessed 19 October 2025.

⁹⁴ Feiler and König however consider that autonomy is only a descriptive but not defining element of the definition in line with the OECD AI Principles. Lukas Feiler and Beat König, 'Article 3 Definitions' in Ceyhun Necati Pehlivan, Nikolaus Forgó, Peggy Valcke (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer 2024) 58.

⁹⁵ See Recital 12 AI Act.

techniques enabling inferencing.⁹⁶ Recital 12 of the AI Act outlines techniques that enable inference when building an AI system, such as machine learning approaches and logic- and knowledge-based approaches. The Guidelines on the definition set out AI techniques that enable inference based on Recital 12, clarifying that machine learning approaches include ‘a large variety of approaches enabling a system to ‘learn’, such as supervised learning, unsupervised learning, self-supervised learning and reinforcement learning.’⁹⁷ Logic- and knowledge-based approaches, which ‘infer from encoded knowledge or symbolic representation of the task to be solved’,⁹⁸ include based on the Guidelines ‘knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, expert systems and search and optimisation methods’.⁹⁹

Importantly, the Guidelines foresee that the following systems *may* be excluded from the definition of an ‘AI system’: systems for improving mathematical optimisation (such as linear or logistic regression), basic data processing, systems based on classical heuristics and simple prediction systems.¹⁰⁰ Some of these exclusions raise questions, as for example linear or logistic regression could lead to adjustments of decision making models, and thereby inevitably be within the AI Act’s scope.¹⁰¹ The Guidelines also acknowledge that such models have the capacity to infer, but exclude them from the definition as ‘they do not transcend basic data processing’,¹⁰² which contradicts Recital 12 that foresees that the capacity of an AI system to infer by enabling learning, reasoning or modelling in itself transcends basic data processing.¹⁰³ This appears to limit the key aspect of the definition – the capacity to infer – further, by covering only some AI systems with such capacity.

During the Commission’s public consultation on the definition, which contributed to the above-mentioned Guidelines, several respondents raised concerns over the possibility of providers circumventing the AI Act’s requirements by reclassifying their systems as traditional software, on the one side, and the definition being too broad, on the other.¹⁰⁴ Ultimately, the definition and accompanying Guidelines remain quite abstract (the Guidelines clarify that ‘[n]o automatic determination or exhaustive lists of systems that either fall within or outside the definition of an AI system are possible’¹⁰⁵), which could lead to different interpretations in practice, posing challenges for legal certainty.¹⁰⁶ For example, views seem to differ on the extent to which less complex systems, which can be used also for emotion recognition,¹⁰⁷ are covered by the definition.¹⁰⁸ Given that the AI Act primarily applies to systems used for high-risk purposes that

⁹⁶ Commission Guidelines on the definition of an artificial intelligence system (n 9) para 29.

⁹⁷ Ibid, para 32.

⁹⁸ Recital 12 AI Act.

⁹⁹ Commission Guidelines on the definition of an artificial intelligence system (n 9) para 39.

¹⁰⁰ Ibid, paras 42–59.

¹⁰¹ Irish Council for Civil Liberties, ‘AI system definition guidelines fail to provide clarity’, 7 February 2025 <www.iccl.ie/news/ai-system-definition-guidelines-fail-to-provide-clarity> last accessed 19 October 2025.

¹⁰² Commission Guidelines on the definition of an artificial intelligence system (n 9) para 42.

¹⁰³ Irish Council for Civil Liberties (n 101).

¹⁰⁴ European Commission, ‘Analysis of EU AI Office stakeholder consultations: defining AI systems and prohibited applications’ (n 89) 22–23.

¹⁰⁵ Commission Guidelines on the definition of an artificial intelligence system (n 9) para 62.

¹⁰⁶ The author acknowledges that the definition of an ‘AI system’ is inevitably a highly technical issue which would require further expertise in computer science for a fully-fledged analysis.

¹⁰⁷ See e.g. Agnes Jacob, ‘Modelling speech emotion recognition using logistic regression and decision trees’ (2017) *International Journal of Speech Technology*, Volume 20, 897–905.

¹⁰⁸ See: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, ‘Report AI & Algorithms Netherlands’ (n 1) 26. The Dutch DCA considers that simpler algorithms are covered by the AI Act. See also: Rania Wazir, ‘The European Commission’s guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Comment by the

can significantly interfere with people's lives, a broad interpretation of the definition seems thereby suitable in the author's view to ensure the AI Act's objective of ensuring a high level of fundamental rights protection (Article 1(1) AI Act) in practice. It remains to be seen if the definition will be at some point further clarified through an authoritative interpretation by the Court of Justice of the European Union (CJEU).¹⁰⁹

It should be also noted that the AI Act definition covers emotion recognition systems that are AI systems, however, emotions can be 'recognised' also through non-AI approaches such as questionnaires.¹¹⁰

2.2.2 Second element: Emotions and intentions

The AI Act does not provide for a definition of emotions or intentions. Some clarifications are included in Recital 18 of the AI Act, which stipulates that these could be for example 'happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement', albeit this seems to refer only to emotions. The non-binding Commission Guidelines on the prohibitions explain that the concept of emotions or intentions should be interpreted broadly and not circumvented with references to 'attitudes'.¹¹¹ Recital 18 further excludes from the definition systems used for detecting physical states (such as pain or fatigue) and systems used for merely detecting readily apparent expressions, gestures and movements (such as a frown, smile, movement of hands or raised voice), unless used for identifying or inferring emotions.

Emotions have been studied in different fields, including psychology, neuroscience, sociology, and philosophy.¹¹² How to decode emotions has been also studied in the Human Computer Interaction (HCI) field.¹¹³ The American Psychological Association defines emotions for example as 'a complex reaction pattern, involving experiential, behavioral, and physiological elements, by which an individual attempts to deal with a personally significant matter or event. The specific quality of the emotion (e.g., fear, shame) is determined by the specific significance of the event. For example, if the significance involves threat, fear is likely to be generated; if the significance involves disapproval from another, shame is likely to be generated. Emotion typically involves feeling but differs from feeling in having an overt or implicit engagement with the world.'¹¹⁴ However, there is no uniform definition of what emotions are, even though consensus on their characteristics is growing.¹¹⁵

Advisory Committee on the Ethics of Artificial Intelligence of the Austrian Commission for UNESCO' (2025) 2 <www.unesco.at/fileadmin/user_upload/Stellungnahme_zu_den_Leitlinien_der_EU-Kommission_zur_Definition_von_KI-Systemen_auf_Englisch_21_Maerz_2025.pdf> last accessed 19 October 2025. The author observes that the Guidelines on the definition of an AI system try to distinguish between simple and more complex methods.

¹⁰⁹ See: Commission Guidelines on the definition of an artificial intelligence system (n 9) para 7.

¹¹⁰ Khare and others (n 17) 2. See also EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12), which mentions that for example facial emotion recognition technology is often, but not always, based on AI (p. 1).

¹¹¹ Commission Guidelines on prohibited artificial intelligence practices (n 10) paras 247–248.

¹¹² See Lisa Feldman Barrett, Michael Lewis, Jeannette M. Haviland-Jones (eds.), *Handbook of Emotions* (4th edition, Guilford Press 2016) and Häuselmann and others (n 17) 2. The authors refer to the handbook.

¹¹³ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 1 (referring to Cowie et al. (2001); Abdat et al. (2011)).

¹¹⁴ American Psychological Association, 'Emotion', updated on 19 April 2018 <<https://dictionary.apa.org/emotion>> last accessed 19 October 2025.

¹¹⁵ Scarantino (n 59) 4, 36–37. The author considers that theorists of emotions tend to agree on diagnostic features of emotions that are used for inferring emotions, i.e. causes, constituents and effects of emotions (p. 5).

Historically, there were different attempts at classifying emotions. Some of the most known ones are Robert Plutchik's work on eight primary emotions (joy, sadness, trust, disgust, fear, anger, surprise and anticipation) from which other emotions can be derived¹¹⁶ and Paul Ekman's work on six basic emotions (anger, disgust, fear, happiness, sadness and surprise).¹¹⁷ Ekman considered that emotions are specific evolutionary adaptations and studied the distinct facial expressions associated with these emotions.¹¹⁸ He also considered that basic emotions are connected to unavoidable changes in the body that can be regulated only *ex post*,¹¹⁹ which was criticised by psychological constructionists, who considered that 'there is no one-to-one correspondence between anger, fear, happiness, sadness, or any other basic emotion, and any neurobiological, physiological, expressive, behavioural, or phenomenological responses, and that such diagnostic markers are not strongly correlated with one another.'¹²⁰ Different stakeholders also point out that emotions can be culturally¹²¹ and contextually shaped.¹²² While the present thesis deals with the legal aspects of emotion recognition systems, these examples illustrate the difficulty of reaching a consensus on what emotions are and to what extent they can be identified or inferred in psychology, which is in turn intrinsically connected to the definition of emotion recognition systems and their regulation. Some aspects of this will be further analysed in Sub-section 3.1.1.

It is even less clear what was meant with the notion of 'intentions' and if the legislator wished to cover any additional technologies with this element of the definition. Recital 18 of the AI Act

He distinguishes between three emotion theories: (1) the feeling tradition, which considers that emotions are feelings of a distinctive type, (2) the motivational tradition, which considers that they are motivational states or behavioural patterns of a distinctive type and (3) the evaluative tradition, which considers that emotions entail different evaluations (cognition, interpretation, judgement, thought etc.) (pp. 7–8, 15, 24). The author concludes, referring to Russel (2013, p. 146) that a universal theory of emotions seems to be not possible as folk emotion categories are too heterogeneous, and suggests that componentialism (looking at building blocks of emotions) or pluralism (further revising emotion categories) could be the way forward (pp. 37–38). Smith K. Khare and others for example consider them to be 'a dynamic cognitive and physiological condition that develops in reaction to inputs, like experiences, thoughts, or interactions with people [and] includes subjective experience, cognitive processes, behavioral influences, physiological responses, and communication'. Khare and others (n 17) 1. See also: McStay and Urquhart (n 68) 5.

¹¹⁶ Scarantino (n 59) 20. The author referred to Plutchik (1970).

¹¹⁷ Paul Ekman, 'An argument for basic emotions' (1992) *Cognition and Emotion*, 6(3–4), 169–200. According to the author, these six basic emotions have nine characteristics that distinguish them from one another and from other affective phenomena (i.e. distinctive universal signals, presence in other primates, distinctive physiology, distinctive universals in antecedent events, coherence among emotional response, quick onset, brief duration, automatic appraisal and unbidden occurrence). These can be shared also by contempt, shame, guilt, embarrassment, and awe (pp. 170, 175). Lisa Feldman Barrett and others observe that the work on six basic emotions can be traced back to the work of Charles Darwin. Overall, these are the most frequently studied emotional perceptions in cross-cultural studies. Feldman Barrett and others (n 53) 12.

¹¹⁸ Scarantino (n 59) 20 (the author refers to Ekman's work over the years). Ekman co-developed the facial action coding system, which is a system to describe facial movements, used among others for facial recognition research. See: Paul Ekman Group, 'Facial action coding system' <www.paulekman.com/facial-action-coding-system/> last accessed 19 October 2025.

¹¹⁹ Scarantino (n 59) 21. The author, referring to Ekman & Cordaro (2011, p. 367), outlines Ekman's suggestions that facial changes can be regulated in less than a second whereas regulating changes in the respiration, perspiration and cardiac activity takes longer.

¹²⁰ *Ibid*, 21 (referring to Russell (2003) and Barrett (2006)). Ekman was sceptical about the possibility of emotions not having a unique, universal signal (this would not necessarily need to be a facial one though but could be also vocal or a set of movements). Ekman (n 117) 192.

¹²¹ Ute Frevert, 'The History of Emotions' in Lisa Feldman Barrett, Michael Lewis, Jeannette M. Haviland-Jones (eds.), *Handbook of Emotions* (4th edition, Guilford Press 2016) 49, 53. The author observes that in recent years, historians started to question the premise that emotions are innate and universal, highlighting the impact of language and culture on how they are experienced (p. 49).

¹²² Feldman Barrett and others (n 53) 1.

addresses emotions and intentions jointly¹²³ and does not provide any specific clarifications or examples concerning intentions. The same goes for the Commission Guidelines on the prohibitions.¹²⁴ The American Psychological Association defines intention for example as ‘1. a prior conscious decision to perform a behavior [...] [and] 2. more generally, any directedness in one’s thoughts or behaviors, whether or not this involves conscious decision making.’¹²⁵ Therefore, intentions are understood to be distinct from emotions and could cover systems that predict how a person intends to act next.¹²⁶

It should be noted that during the trilogue, the European Parliament called for expanding the definition of emotion recognitions systems to include, next to the identification or inference of emotions and intentions, also the identification or inference of ‘thoughts’ and ‘states of mind’ to it. The Council suggested to cover in addition ‘psychological states’.¹²⁷ None of these suggestions made it to the final text, which raises the question whether these were assumed to be covered by ‘emotions or intentions’ or indeed were distinct categories for which it was decided to remain outside the scope of this definition.¹²⁸ Wendehorst and Duller have in a 2021 study for the European Parliament on biometric recognition and behavioural detection proposed to expand the definition of emotion recognition systems in the proposed AI Act by including the identification or inference of ‘thoughts’ to it.¹²⁹ They further considered that such systems belong to a broader category of ‘biometric detection techniques’, which aim to detect certain human conditions, such as emotions, thoughts, intentions or a particular disease.¹³⁰ To this end it should be also noted that the Commission Guidelines on the prohibitions explicitly state that a system that predicts if a person is sick does not constitute an emotion recognition system.¹³¹

¹²³ Feiler and König observe that the examples in Recital 18 likely refer only to emotions. Feiler and König (n 94) 72.

¹²⁴ It should be also noted that in the public consultation on the prohibitions under the AI Act, which fed into the guidelines, the European Commission did not mention ‘intentions’ neither in the proposed elements of the definition nor in the questions addressed to stakeholders. European Commission, ‘Multi-stakeholder consultation for Commission guidelines on the application of the definition of an AI system and the prohibited AI practices established in the AI Act’, Section F <<https://ec.europa.eu/eusurvey/runner/Prohibitions-and-Definition-Survey-2024#page3>> accessed 23 November 2024. The only example provided in the Guidelines that could relate also to intentions is that of a system that infers from voice or body gestures that a person is furious and will become violent. Commission Guidelines on prohibited artificial intelligence practices (n 10) para 247.

¹²⁵ American Psychological Association, ‘Intention’, updated on 19 April 2018 <<https://dictionary.apa.org/intention>> last accessed 19 October 2025.

¹²⁶ Intention recognition is for example used in robotics. See: Karim A. Tahboub, ‘Intelligent Human-Machine Interaction Based on Dynamic Bayesian Networks Probabilistic Intention Recognition’ (2006) *Journal of Intelligent and Robotic Systems* 45, 31–52.

¹²⁷ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021/0106(COD), DRAFT 20-06-2023 at 16h53 (AI Act trilogue mandates), 215 (point 161). Available at <www.kaizenner.eu/post/long-journey-towards-aiact> under ‘Trilogue negotiations’, last accessed 19 October 2025.

¹²⁸ It should be noted that also the concept of ‘thought’ lacks a clear legal definition, and views differ on whether it encompasses emotions. Sjors Ligthart and others, ‘Rethinking the Right to Freedom of Thought: A Multidisciplinary Analysis’ (2022) *Human Rights Law Review*, Volume 22, Issue 4, December 2022, 4. Ahmed Shaheed, ‘Interim report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed: Freedom of thought’, A/76/380, 5 October 2021, 5 (referring to: <https://engineering.mit.edu/engage/ask-an-engineer/what-are-thoughts-made-of/>).

¹²⁹ Christiane Wendehorst and Yannic Duller, ‘Biometric Recognition and Behavioural Detection’ (2021) Study requested by the JURI and PETI committees, European Parliament, 71 <[www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf)> last accessed 19 October 2025.

¹³⁰ *Ibid.*, 21, 57.

¹³¹ Commission Guidelines on prohibited artificial intelligence practices (n 10) 79.

Given the uncertainties connected to the part of the definition referring to intentions,¹³² this thesis focuses only on systems that identify or infer emotions, although conclusions could be applicable also to systems recognising human intent. The issue of intentions may, however, warrant a separate discussion.

2.2.3 Third element: The identification/inference of emotions and intentions

The AI Act does not define what constitutes the identification or inference of emotions or intentions of individuals by an AI system. The European Commission has, however, in its Guidelines on the prohibitions further clarified that identification happens when ‘the processing of the biometric data (for example, of the voice or a facial expression) of a natural person allows to directly compare and identify an emotion with one that has been previously programmed in the emotion recognition system’.¹³³ It further noted that an inference happens when the system deduces information by analytical or other processes and ‘the information about the emotion is not solely based on data collected on the natural person, but it is inferred from other data, including machine learning approaches that learn from data how to detect emotions’.¹³⁴ The concept of inference is linked to the concept of profiling,¹³⁵ which implies probability statements about emotions or intentions of a person based on various sources and statistical extrapolations.¹³⁶ It is understood that the key distinction between the concepts of ‘identification’ and ‘inference’ in this context lies in the data and techniques used for the ‘emotion recognition’, while at the same time acknowledging that, given the disputed scientific basis of emotion recognition described under Section 2.1, the outputs of such systems would in any case result in an inference (assumption) and not identification of an emotion.

This focus on identifying and inferring emotions and intentions risks overlooking, as McStay and Bakir put it, ‘unintentionally emphatic’ AI systems, as recent LLMs function in a way that emulates empathy, even if not specifically trained to classify emotions.¹³⁷

2.2.4 Fourth element: Biometric data basis

The AI Act defines ‘biometric data’ in Article 3(34) as ‘personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data’. The definition follows from the definition of biometric data in the EU data protection acquis (Article 4(14) GDPR, Article 3(13) LED, Article 3(18) EUDPR) which defines it as ‘personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, *which allow or confirm the unique identification of that natural person*, such as facial images or dactyloscopic data’.¹³⁸ The AI Act definition does, however, not include a reference to the need that such data allow or confirm the unique identification of a person (i.e. no specific

¹³² Respondents to a recent public consultation by the Dutch Data Protection Authority also considered that the meaning of intentions remains unclear. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, ‘AI systems for emotion recognition in the areas of workplace or education institutions’ (n 58) 2, 7.

¹³³ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 246.

¹³⁴ *Ibid.*

¹³⁵ Els J. Kindt and Catherine Jasserand, ‘Article 5 Prohibited AI Practices’ in Ceyhun Necati Pehlivan, Nikolaus Forgó, Peggy Valcke (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer 2024) 160.

¹³⁶ See *ibid.*, 146–147. The authors refer to the work of the Art. 29 AP (2018) and Council of Europe (2011).

¹³⁷ McStay and Bakir (n 46) 4.

¹³⁸ Emphasis added.

technical processing¹³⁹ that compares the data with a certain reference linked to the identity of a person is needed, neither does the processing need to lead to the possibility to establish or confirm a person's identity¹⁴⁰).¹⁴¹ Recital 14 of the AI Act foresees that the notion should be interpreted in line with the data protection acquis, and further explains that '[b]iometric data can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions'.¹⁴² It appears that this aimed to expand the definition from the data protection acquis. This was also confirmed by the Commission in its Guidelines on the prohibitions, which acknowledge that the AI Act's definition is broad.¹⁴³

This was a deliberate choice by the co-legislators, as the initial AI Act proposal followed the definition from the EU data protection acquis.¹⁴⁴ The initial proposal would lead to a more restrictive definition of emotion recognition systems, requiring that the data, and ultimately also the way it is processed, allow for the identification or authentication of a person. A closer look at the negotiation mandates of the EU institutions during the trilogue reveals that this change was introduced by the Council during the negotiations.¹⁴⁵ At the same time, the European Parliament called for amending the definition of emotion recognition systems by including the possibility of the AI system identifying or inferring emotions on the basis of 'biometric-based data',¹⁴⁶ which would be 'data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person'.¹⁴⁷ The wording contained in the final text of the AI Act therefore seems to cover both of these proposals and addresses concerns of an overly narrow scope of the initial wording. To this end, Wendehorst and Duller called in the 2021 study for the European Parliament for detaching the definition of 'emotion recognition

¹³⁹ As Bygrave and Tosoni observe, while pointing to the work of Wayman et al. (2004), Liu (2011) and Kindt (2013), specific technical processing would in general consist of several steps, including measuring one or more physical, physiological or behavioural characteristics of a person, creating a 'master template' of the measurement linked to that person, and storing it in a database; creating new measurements of these characteristics ('live template') and comparing them, through algorithms, to the master template. Lee A. Bygrave and Luca Tosoni, 'Article 4(14). Biometric data' in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 212.

¹⁴⁰ For a brief explanation of the three cumulative criteria to establish biometric data under the GDPR (i.e. (1) the nature of the data; (2) the means/manner of processing and (3) its purpose), see: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), 'Rules for the Use of Biometrics' <www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics> last accessed 19 October 2025.

¹⁴¹ For a discussion on this see also: Kindt and Jasserand (n 135) 163.

¹⁴² Biometric identification automatically establishes the identity of a natural person by comparing their biometric data against biometric data of individuals stored in a database (Article 3(35) and Recital 15 AI Act). Biometric authentication falls under biometric verification, which aims to automatically verify the identity of a natural person by comparing their biometric data to previously provided data (Article 3(36) and Recital 15 AI Act). Biometric categorisation means an assignment of natural persons to specific categories, which is based on their biometrics (Article 3(40) and recital 16 AI Act). See on this e.g. European Union Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) Publications Office of the European Union, 7–8 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> last accessed 19 October 2025. The focus paper describes identification as a 'one-to-many comparison', verification as a 'one-to-one comparison' and categorisation as 'matching general characteristics'.

¹⁴³ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 252. See also: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 48–49.

¹⁴⁴ Article 3(33), Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>> last accessed 19 October 2025.

¹⁴⁵ AI Act trilogue mandates (n 127) point 160.

¹⁴⁶ *Ibid*, point 161.

¹⁴⁷ *Ibid*, point 160a.

system' in the AI Act 'from the concept of 'biometric data' as defined in the GDPR and rather base it on a new definition of 'biometrics-based data''.¹⁴⁸ They considered the requirement that the data must allow or confirm the unique identification of a person too restrictive and not up-to-date with technological developments, as it would exclude from the scope of the definition 'an emotion recognition system based on pulse frequency, body temperature and nonunique facial expressions (such as smiling, raising of the brow or yawning) or non-unique voice signals (such as volume or trembling)'.¹⁴⁹

Under the final wording of the AI Act, when it comes to emotion recognition systems, personal data that results from specific technical processing of physical, physiological or behavioural characteristics of a natural person is considered biometric data. This definition addresses the above concerns of limiting the definition of emotion recognition systems only to systems that process data that allow/confirm the unique identification of a person. At the same time, the definition of biometric data under the data protection acquis also focuses on the technical process of generating biometric data with the aim to enable the unique identification.¹⁵⁰ It appears that is not necessary under the AI Act, as the data do not need to be processed in a way that allows or confirms the unique identification of a person. An example would be a photograph of a person, which would be considered as biometric data under the data protection acquis if processed to identify or authenticate a natural person.¹⁵¹ If such an image is processed by an AI system to identify or infer emotions, and the process does not allow to authenticate or identify a person, it would, in light of Article 3(34) and Recital 14, still amount to processing of biometric data under the AI Act in the author's view.

When it comes to the definition of the sources of biometric data, i.e. 'physical, physiological or behavioural characteristics', the Commission's guidelines do not define them and follow instead a similar taxonomy to one of the Biometrics Institute, distinguishing between physiological biometrics and behavioural biometrics.¹⁵² The former include a person's 'physical, structural, and relatively static attributes', such as fingerprints, iris patterns, face contours, veins geometry, DNA and odour, and the latter include a person's 'distinctive characteristics of movements, gestures, and motor-skills' when performing a task, such as gait, keystrokes, signatures, voice, eye tracking and heartbeats.¹⁵³ The Commission additionally considered that electroencephalography (EEG) and electrocardiography (ECG) constitute behavioural biometrics.¹⁵⁴ This appears to diverge from their classification in literature, where such signals are considered to be physiological, as explained above in Section 2.1.¹⁵⁵ Importantly, the Commission emphasised that an AI system inferring emotions from written text does not constitute an emotion recognition system, as it is not based on

¹⁴⁸ Wendehorst and Duller (n 129) 61. They proposed the following definition of biometrics-based data: 'personal data resulting from specific technical processing relating to physical, physiological or behavioural signals or characteristics of a natural person, such as facial expressions, movements, pulse frequency, voice, keystrokes or gait, which may or may not allow or confirm the unique identification of a natural person' (p. 69).

¹⁴⁹ Ibid, 67.

¹⁵⁰ Bygrave and Tosoni (n 139) 211.

¹⁵¹ Recital 51 GDPR. See also: FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (n 142) 5.

¹⁵² Commission Guidelines on prohibited artificial intelligence practices (n 10) para 251.

¹⁵³ Biometrics Institute, 'Physiological and Behavioural Biometrics' <www.biometricsinstitute.org/physiological-and-behavioural-biometrics/> last accessed 19 October 2025. Commission Guidelines on prohibited artificial intelligence practices (n 10) para 251.

¹⁵⁴ Commission Guidelines on prohibited artificial intelligence practices (n 10) 84.

¹⁵⁵ See: Khare and others (n 17) 1–2.

biometric data.¹⁵⁶ This links to the idea that biometrics are always to a certain extent immutable and therefore do not include behaviour that can be to a higher extent controlled by a person, such as text (the content of communication) and a person's browsing history.¹⁵⁷

In comparison, commentators of the AI Act observe that physical characteristics relate to observable human body features (e.g. height, body shape, face, body mass index), physiological characteristics relate to observable characteristics of the human body's functions and abilities (e.g. heart rate, blood pressure, odour, fingerprint, iris¹⁵⁸) and behavioural characteristics relate to observable features of human behaviour (e.g. voice, prosody, eye movements, gait, posture, keystrokes rhythm).¹⁵⁹

Considering this, the distinction in Table 1 is proposed for the purposes of this thesis. Whether these data could in practice allow for the unique authentication or identification of a person, considering also the state of technological development, is another question which is not important for determining whether the data constitute biometric data in the context of emotion recognition systems under the AI Act. The data have to, however, amount to 'personal data', i.e. 'any information relating to an identified or identifiable natural person' pursuant to Article 4(1) of the GDPR.¹⁶⁰ It should be also noted that this classification, evolving around the AI Act's definition, can differ from classifications in literature dealing with emotion recognition, as outlined previously in Section 2.1.

Table 1: Sources of biometric data in the context of emotion recognition systems under the AI Act¹⁶¹

Characteristic	Relates to	Examples based on emotion recognition systems ¹⁶²
Physical	Body features	These features, which are relatively static, are generally not used for recognising emotions (e.g. emotions are not being inferred from a person's height, body shape, or fingerprint). However, they may be processed when detecting behavioural characteristics (e.g. a body shape to detect gestures, a facial image to detect facial expressions, or voice to detect speech).
Physiological	Body functioning	Heart activity (electrocardiogram, ECG), ¹⁶³ brain activity (electroencephalogram, EEG), ¹⁶⁴ galvanic skin

¹⁵⁶ Commission Guidelines on prohibited artificial intelligence practices (n 10) 80.

¹⁵⁷ Wendehorst and Duller (n 129) 21.

¹⁵⁸ The author considers fingerprints and irises would rather constitute physical characteristics.

¹⁵⁹ Feiler and König (n 94) 70 (referring also to EDPB 2021, para. 31).

¹⁶⁰ See Art. 3(50) AI Act.

¹⁶¹ Based on/inspired by the following sources: Art. 3(34) AI Act; Commission Guidelines on prohibited artificial intelligence practices (n 10) 80; Feiler and König (n 94) 70; Khare and others (n 17) 1–2 (see the corresponding references).

¹⁶² These are not exhaustive as the technology is developing. For some it could be argued to what extent they are physiological or behavioural characteristics (e.g. eye movements).

¹⁶³ See e.g.: Muhammad Anas Hasnul and others, 'Electrocardiogram -Based Emotion Recognition Systems and Their Applications in Healthcare—A Review' (2021) *Sensors* (Basel, Switzerland) vol. 21, 15 5015.

¹⁶⁴ See e.g.: Xiang Li and others, 'EEG Based Emotion Recognition: A Tutorial and Review' (2023) *ACM Computing Surveys*, Volume 55, Issue 4, 1–57.

		response, ¹⁶⁵ muscle activity (electromyogram, EMG), ¹⁶⁶ respiration, ¹⁶⁷ eye tracking, ¹⁶⁸ blood volume changes (photoplethysmogram, PPG) ¹⁶⁹
Behavioural	Behaviour	Facial expressions, ¹⁷⁰ speech, ¹⁷¹ gestures, ¹⁷² posture, ¹⁷³ keystroke, mouse, and touchscreen movements ¹⁷⁴

Overall, moving away from the definition of biometric data under the data protection acquis ensured a more inclusive coverage of emotion recognition systems. This conceptual change might, however, cause some confusion in practice. Therefore, it might have been a better solution to follow the above proposals to include a definition of and reference to biometric-based data instead. The interplay with the EU data protection acquis will be further discussed below in Sub-section 3.2.2.

¹⁶⁵ See e.g.: Atefeh Goshvarpour and Ateke Goshvarpour, 'The potential of photoplethysmogram and galvanic skin response in emotion recognition using nonlinear features' (2020) *Physical and Engineering Sciences in Medicine*, Volume 43, 119–134.

¹⁶⁶ See e.g. Mangesh Ramaji Kose, Mitul Kumar Ahirwal, Anil Kumar, 'A new approach for emotions recognition through EOG and EMG signals' (2021) *Signal, Image and Video Processing*, Volume 15, 1863–1871.

¹⁶⁷ See e.g.: Qiang Zhang and others, 'Respiration-based emotion recognition with deep learning' (2017) *Computers in Industry*, Volumes 92–93, 84–90.

¹⁶⁸ See e.g.: Jia Zheng Lim, James Mountstephens, Jason Teo, 'Emotion Recognition Using Eye-Tracking: Taxonomy, Review and Current Challenges' (2020) *Sensors* (Basel, Switzerland), 20(8), 2384.

¹⁶⁹ See e.g.: Goshvarpour and Goshvarpour (n 165) 119–134.

¹⁷⁰ See e.g.: Sze Chit Leong and others, 'Facial expression and body gesture emotion recognition: A systematic review on the use of visual data in affective computing' (2023) *Computer Science Review*, Volume 48, 100545.

¹⁷¹ See e.g.: Taiba Majid Wani, 'A Comprehensive Review of Speech Emotion Recognition Systems' (2021) *IEEE Access*, Volume 9, 47795–47814.

¹⁷² See e.g.: Chit Leong and others (n 170).

¹⁷³ See e.g.: Sekar Vijayanthi, J. Arunnehr, 'Human Emotion Recognition from Body Posture with Machine Learning Techniques' in: Mayank Singh and others (eds.), *Advances in Computing and Data Sciences. ICACDS 2022* (Springer 2022).

¹⁷⁴ See e.g.: Liying Yang, Sheng-Feng Qin, 'A Review of Emotion Recognition Methods From Keystroke, Mouse, and Touchscreen Dynamics' (2021) *IEEE Access*, Volume 9, 162197–162213.

3 The regulation of emotion recognition systems under EU law – selected aspects

The development and use of emotion recognition systems in the EU are regulated, and partly prohibited, under the AI Act. The Act entered into force on 1 August 2024 and will gradually enter into application over the next few years.¹⁷⁵ The AI Act is, however, not the sole instrument governing such systems at EU level – other pieces of EU law that apply to providers and deployers of emotion recognition systems need to be considered too.¹⁷⁶

This Chapter first looks in Section 3.1 into the applicable regulatory regime under the AI Act, which is the first instrument to explicitly addresses emotion recognition systems.¹⁷⁷ It considers the extent to which emotion recognition systems are covered by the AI Act and the different risk categories contained therein. The analysis shows that due to some rather restrictive definitions and exceptions from the AI Act's scope, its application to emotion recognition systems is limited in practice.

Section 3.2 then examines the interplay of the AI Act with two selected aspects of EU law – EU fundamental rights law and data protection law – exploring whether the use of emotion recognition systems can be compatible with these whenever not prohibited under the AI Act. It explains when and how these areas of law apply to providers and deployers of emotion recognition systems. While providers and deployers need to comply with certain fundamental rights due diligence processes under the AI Act, further obligations arise under EU and international law. When it comes to data protection law, it would likely frequently apply to the development and use of emotion recognition systems, however, the data processed by such systems might not always be considered sensitive. The Section then highlights several compliance challenges under both legal areas. In particular, the development and use of permitted emotion recognition systems under the AI Act might be often at odds with necessity and proportionality requirements under fundamental rights and data protection law. The Section therefore also looks into ways through which fundamental rights protection and data protection can be duly considered and ensured in practice.

Finally, it should be acknowledged that, depending on the area of deployment, such systems could be subjected to further EU law, such as the EU consumer law acquis or rules on online platforms or political advertising,¹⁷⁸ as well as national law.¹⁷⁹ These are beyond the scope of

¹⁷⁵ See Article 113 AI Act.

¹⁷⁶ See Recital 9 AI Act: 'The harmonised rules laid down in this Regulation should apply across sectors and, in line with the New Legislative Framework, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety, to which this Regulation is complementary.'

¹⁷⁷ As Steindl noted, the AI Act is 'the first hard law to address emotion recognition de lege ferenda'. Steindl (n 30) 311.

¹⁷⁸ Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act) and Regulation (EU) 2024/900 on the transparency and targeting of political advertising. See also: Häuselmann and others (n 17) 6–7. Steindl (n 30) 318.

¹⁷⁹ See Recital 9 AI Act: 'Furthermore, the obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to national law, in compliance with Union law, having the effect of limiting the use of certain AI systems where such law falls outside the scope of this Regulation or pursues legitimate public interest objectives other than those pursued by this Regulation. For example, national labour law and law on the protection of minors, namely persons below the age of 18, taking into account the UNCRC General Comment No 25 (2021) on children's rights in relation to the digital environment, insofar as they are not specific to AI systems and pursue other legitimate public interest objectives, should not be affected by this Regulation.'

this thesis. While a fragmented approach to the regulation of emotion systems was subjected to criticism in the past,¹⁸⁰ it appears unavoidable given the variety of contexts in which such systems can be used. A case-by-case examination is therefore required in practice to identify relevant applicable law.

3.1 The AI Act

The AI Act follows a risk-based approach to regulating AI, meaning that the more risks an AI system poses in light of the purpose of its use, the stricter are the requirements with which the operators¹⁸¹ of the AI system, in particular the providers¹⁸² and deployers¹⁸³ of the system, have to comply. In cases where the risks posed by a system are deemed as unacceptable, their placement on and use in the EU market is prohibited.¹⁸⁴

The regulation of emotion recognition systems led to diverging views during the negotiations of the AI Act. While the initial Commission proposal did not foresee their ban, but only high-risk classification if used in law enforcement or migration,¹⁸⁵ the European Parliament called for their ban in the areas of law enforcement and border management as well as in the workplace and education institutions.¹⁸⁶ Some experts from academia called for their high-risk classification.¹⁸⁷ Civil society organisations¹⁸⁸ and the EDPS and EDPB¹⁸⁹ went even further, calling in principle for their full ban during the trilogues, given the interference of such systems with fundamental rights. This was for example also the position of Austria in its final statement before the formal approval of the AI Act by the Council on 21 May 2024.¹⁹⁰

Under the final text of the AI Act, emotion recognition systems are prohibited if used in educational institutions and the workplace, with exceptions applying for medical and safety reasons. In all other cases, they are considered high-risk AI systems, to which additional transparency requirements apply. The applicability of the AI Act to emotion recognition systems will be further explained in Sub-section 3.1.1 below.

¹⁸⁰ McStay and Urquhart (n 68) 5.

¹⁸¹ Article 3(8) of the AI Act defines 'operator' as 'provider, product manufacturer, deployer, authorized representative, importer or distributor'.

¹⁸² See Article 3(3) AI Act.

¹⁸³ See Article 3(4) AI Act.

¹⁸⁴ See Recital 26 AI Act as well as its Chapter II on prohibited AI practices, Chapter III on high-risk AI systems, Chapter IV on transparency obligations for providers and deployers of certain AI systems and Chapter V on general-purpose AI models.

¹⁸⁵ Annex III, AI Act proposal (n 144).

¹⁸⁶ Amendment 226, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, P9_TA(2023)0236 <www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> last accessed 19 October 2025.

¹⁸⁷ Gianclaudio Malgieri and Marcello Ienca, 'The EU regulates AI but forgets to protect our mind', European Law Blog, 7 July 2021 <www.europeanlawblog.eu/pub/the-eu-regulates-ai-but-forgets-to-protect-our-mind/release/1> last accessed 19 October 2025.

¹⁸⁸ A Civil Society Statement, 'An EU Artificial Intelligence Act for Fundamental Rights' (n 83) 3. See also the joint civil society statement on the compromise AI Act text, 'EU's AI Act fails to set gold standard for human rights' (n 83) 5.

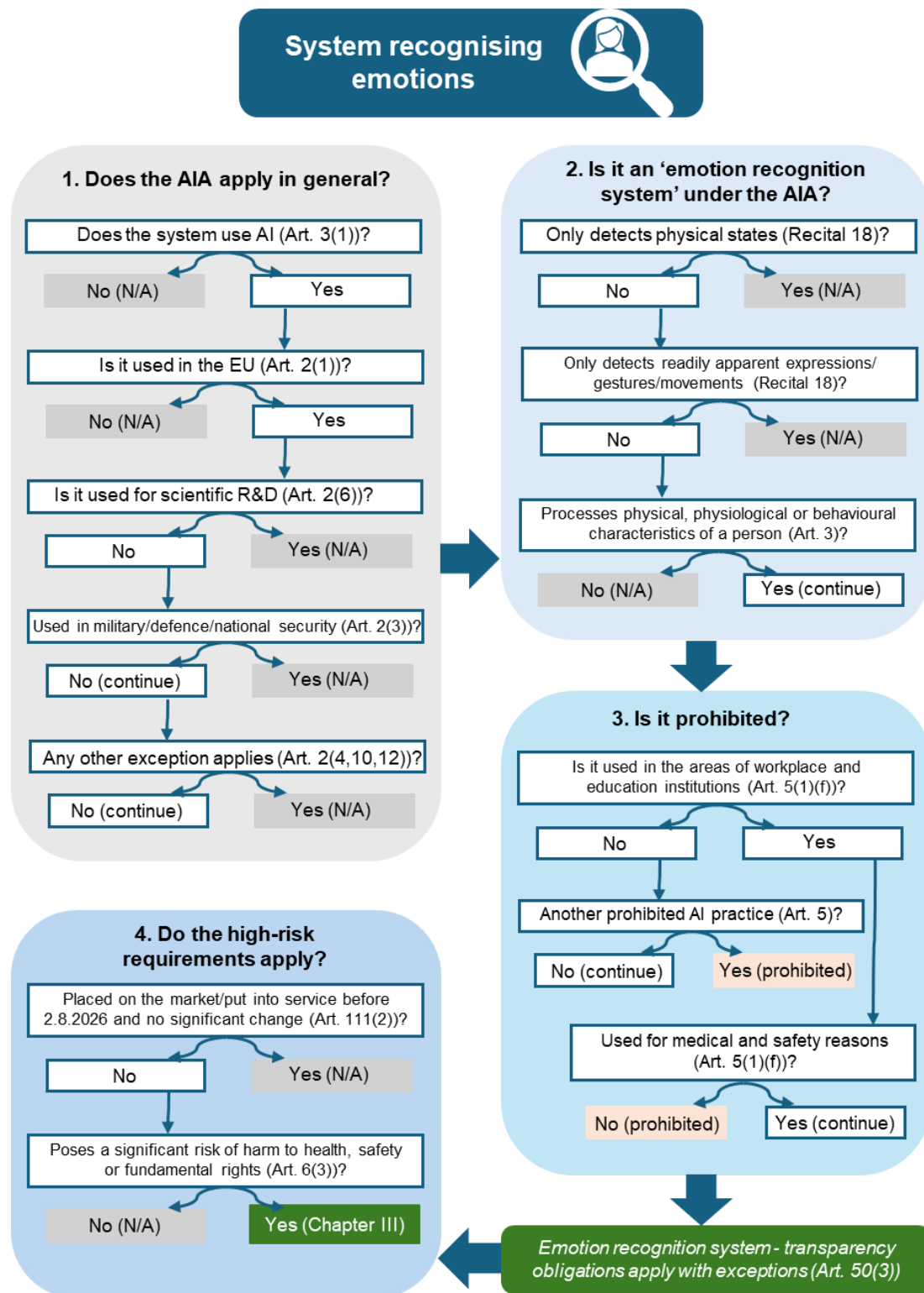
¹⁸⁹ The EDPS and EDPB considered that the use should be exceptionally permitted only for 'for certain well-specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation.' EDPS - EDPB Joint Opinion on the AI Act proposal (n 56) 13.

¹⁹⁰ Council of the EU, 2021/0106(COD) (n 86) 3.

3.1.1 The applicability of the AI Act to emotion recognition systems

The AI Act contains some restrictive definitions and exceptions from its scope, which could limit its application to emotion recognition systems in practice, as will be demonstrated by the below analysis.

Figure 2: Applicability of the AI Act to systems recognising emotions



These can be summarised as follows. First, some of these systems might fall outside the general scope of the AI Act, for example because they do not fulfil all the criteria of the definition of an ‘AI system’ or are used for scientific research and development. Second, some AI systems that recognise emotions might not meet the criteria of an ‘emotion recognition system’ under the AI Act, as they are not based on biometric data. Third, the prohibitions apply to emotion recognition systems in rather limited number of cases, linked to the use in educational institutions and the workplace (with exceptions applying for medical and safety reasons). Moreover, they could be prohibited if amounting to another prohibited practice under Article 5. For all other emotion recognition systems that fall within the scope of the AI Act and the relevant definitions, transparency obligations and in principle also high-risk requirements would apply. With the latter, a temporal exception applies and more importantly, the so-called filter in Article 6(3) would allow providers to self-assess if their emotion recognition system is indeed high-risk due to posing a significant risk of harm to health, safety or fundamental rights.¹⁹¹ Figure 2 above illustrates the considerations that need to be taken into account to establish whether a system that recognises emotions amounts to (1) a prohibited practice or a (2) high-risk AI system or a (3) system for which transparency measures need to be taken in practice.

3.1.1.1 Prohibited AI practices

The AI Act prohibits manipulative, exploitative and social control AI practices, which ‘contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter’.¹⁹² These prohibitions, which apply since 2 February 2025,¹⁹³ are outlined in Article 5 of the AI Act. Article 5 prohibits inter alia the placing on the market, putting into service or use¹⁹⁴ (hereinafter: the development or use) of AI systems to infer emotions of a person in the areas of workplace and education institutions, unless used for medical or safety reasons (Article 5(1)(f) AI Act).

3.1.1.1.1 AI systems to infer emotions of persons in workplace and education institutions

The legislator opted for the prohibition of AI systems to infer emotions of persons in the areas of workplace and education institutions due to the imbalance of power that is present in these institutions on the one side, and the intrusive nature of these systems on the other.¹⁹⁵ At the same time, Recital 44 of the AI Act acknowledges the dubious scientific basis of emotion recognition systems ‘particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual.’ It further points out their ‘limited reliability, the lack of specificity and the limited generalisability.’¹⁹⁶ Nevertheless, their prohibition under the AI Act extends in principle only to their use in the workplace and education institutions.

¹⁹¹ See the corresponding references below in Sub-section 3.1.1.1.

¹⁹² Recital 28 AI Act.

¹⁹³ Article 113(3)(a) AI Act.

¹⁹⁴ The Commission guidelines on the prohibitions underline that deployers are prohibited from using such systems regardless of whether such use was excluded by the provider in the contract with the deployer. Commission Guidelines on prohibited artificial intelligence practices (n 10) 5.

¹⁹⁵ Recital 44 AI Act.

¹⁹⁶ Concerns about the data accuracy of facial emotion recognition were raised also by EDPS. See: EDPS, ‘TechDispatch #1/2021 - Facial Emotion Recognition’ (n 12) 3. See also: Joint civil society amendments to the Artificial Intelligence Act, Prohibit emotion recognition in the Artificial Intelligence Act, 1 <www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf> last accessed 19 October 2025.

The AI Act does, at the same time, not define what workplace or education institutions mean. The Commission explained in the Guidelines on the prohibitions that both notions should be interpreted broadly.¹⁹⁷ Workplace thereby means ‘any specific physical or virtual space where natural persons engage in tasks and responsibilities assigned by their employer or by the organisation they are affiliated to’.¹⁹⁸ This therefore covers people engaging in work independently of their status (be it as an employee, contractor or trainee, for example) in any space where work is performed (in the author’s understanding, albeit not explicitly mentioned in the Guidelines, also home offices). The Commission seems to acknowledge through its interpretation modern-day work dynamics,¹⁹⁹ advancing in this context the definition of workplace from the 1989 EU Workplace Directive. The latter is still in force and limits the notion of workplace ‘to the premises of the undertaking and/or establishment and any other place within the area of the undertaking and/or establishment to which the worker has access in the course of his employment’.²⁰⁰ Importantly, the Guidelines confirm that the prohibition of emotion recognition systems covers also recruitment activities.²⁰¹ This is in line with the position of Kindt and Jasserand that the term ‘workplace’ should be interpreted broadly to also protect candidates, especially in light of the legislator’s intent in Recital 57 of the AI Act.²⁰² It should be noted that such recruitment practices have led to public outcry in the past, with the company HireVue discontinuing their emotion recognition system from its recruitment software.²⁰³

Concerning education institutions, the Commission clarified in its Guidelines that both public and private institutions fall under this notion, regardless of the age of the students and the environment where the educational programme takes place (covering also online sessions). The prohibition applies also to admissibility processes.²⁰⁴ It is important to note that the Commission explicitly confirmed that vocational education schools and continuous training are covered by the prohibition too, as these are not explicitly mentioned in Article 5(1)(f) AI Act as opposed to Annex III, which distinguishes between ‘educational and vocational training institutions’ in the context of high-risk AI systems. The Commission’s clarification, albeit non-binding, is important for the uniform application of the AI Act, as EU law does not provide for a definition of this notion and the interpretation would otherwise depend on national law. The Commission’s approach also follows the views of commentators. Kindt and Jasserand considered that the prohibition should include private and public institutions, providing education at all levels (including vocational training and continuing training), both in-person

¹⁹⁷ Commission Guidelines on prohibited artificial intelligence practices (n 10) paras 254, 255.

¹⁹⁸ *Ibid.*, para 254.

¹⁹⁹ For example, according to Eurostat, in 2023, 8.9% of employed persons worked from home as a percentage of the total employment. Eurostat, ‘Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%)’, last update 12 December 2024 <[https://ec.europa.eu/eurostat/databrowser/view/lfsa_ehomp\\$defaultview/default/table?lang=en](https://ec.europa.eu/eurostat/databrowser/view/lfsa_ehomp$defaultview/default/table?lang=en)> last accessed 19 October 2025.

²⁰⁰ Article 2 of Council Directive of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC) (89/654/EEC), Consolidated text <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01989L0654-20190726>> last accessed 19 October 2025.

²⁰¹ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 254.

²⁰² Kindt and Jasserand (n 135) 163.

²⁰³ Will Knight, ‘Job Screening Service Halts Facial Analysis of Applicants’ *Wired* (12 January 2021) <www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/> last accessed 19 October 2025.

²⁰⁴ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 255.

and online.²⁰⁵ The line might be sometimes blurred if emotion recognition systems are deployed in settings that could also subject employees to such recognition, such as shops, health facilities, public administration or prisons.²⁰⁶

Furthermore, Article 5(1)(f) does not refer to the concept of ‘emotion recognition systems’ which is defined in Article 3(39) of the AI Act, but rather to ‘AI systems to infer emotions of a natural person’. It is unclear if the legislator wished to draw a distinction between these two terms and further narrow down the scope of prohibition, given that on the other side Recital 44, which corresponds to Article 5(1)(f) refers to ‘AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data’ in this context.²⁰⁷ Kindt and Jasserand observed that such a distinction might have been intended in order to prohibit emotion recognition also from sources other than biometric data, such as written text, given the vulnerable situation of persons exposed to emotion recognition systems in the workplace and education institutions.²⁰⁸ At the same time, it should be noted that the wording in Article 5(1)(f) covers only the inference, but not identification of emotions. The Commission clarified in its Guidelines that ‘[i]nferring generally encompasses identifying as a prerequisite, so that the prohibition should be understood as including both AI systems identifying or inferring emotions or intentions.’²⁰⁹ It also underlined the relevance of the definition in Article 3(39) in the context of the prohibition, as ‘[f]or consistency reasons, it is also important to construe the prohibition in Article 5(1)(f) AI Act as having a similar scope as the rules applicable to other emotion recognition systems (Annex III, point 1(c), and Article 50 AI Act) and to limit it to inferences based on a person’s biometric data.’²¹⁰

3.1.1.1.2 Exceptions from the prohibition of emotion recognition systems in workplace and education institutions

As mentioned above, Article 5(1)(f) of the AI Act foresees that emotion recognition systems can be used in the areas of workplace and education institutions if used for medical or safety reasons. The AI provides only a limited explanation of what constitutes such reasons – it mentions in Recital 44 that this could be for example therapeutical use. Kindt and Jasserand considered that the interpretation of the concept of ‘medical and safety’ in the workplace could be aligned with the Directives on Occupational Safety and Health, although these follow a broader concept that obliges employers to take measures for making the workplace healthier and safer.²¹¹

The Commission clarified in the Guidelines on the prohibitions that this exception should be interpreted narrowly. Therapeutic use means the use of CE-marked medical devices and does not cover emotion recognition systems that are used to detect wellbeing aspects, such as stress levels of employees.²¹² A medical exception is foreseen also in the case of manipulative and exploitative practices, albeit enshrined only in Recital 29, which stipulates that such

²⁰⁵ Kindt and Jasserand (n 135) 163–164 (referring to the UNESCO Institute for Statistics, the impact assessment of the AI Act proposal and Art. 14 of the Charter).

²⁰⁶ See: Commission Guidelines on prohibited artificial intelligence practices (n 10) 82. The Commission notes that deployments in such settings are allowed if there are sufficient safeguards in place that employees are not being tracked.

²⁰⁷ See also: Kindt and Jasserand (n 135) 160.

²⁰⁸ *Ibid*, 160.

²⁰⁹ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 245.

²¹⁰ *Ibid*.

²¹¹ Kindt and Jasserand (n 135) 164.

²¹² Commission Guidelines on prohibited artificial intelligence practices (n 10) paras 256–257.

practices need to be ‘carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives’. By analogy, this could apply also for the medical exception when it comes to emotion recognition systems used in the workplace and education institutions. Indeed, the Commission underlined in the Guidelines that other applicable law needs to be taken into account and that such use must be strictly necessary and proportionate.²¹³ An example that would constitute such use, according to the Commission, would be emotion recognition used by employees or students with autism, or to improve accessibility for blind or deaf persons.²¹⁴

Concerning the safety exception, the AI Act does also not clarify what could constitute safety reasons in the areas of workplace and education institutions, which would justify the use of emotion recognition systems. The Commission clarified in its Guidelines that this covers only strictly necessary and proportionate use to protect life and health.²¹⁵ The Commission pointed out as an example the use of systems to detect anxiety in an employee dealing with dangerous machines or chemicals, where increased stress levels could lead to specific danger.²¹⁶ At the same time, it noted that systems to detect fatigue in professional drivers or pilots are already outside the scope of the prohibition, as per Recital 18 of the AI Act.²¹⁷ However, it should be noted that the Recital excludes only systems aimed at detecting drivers’ fatigue from the definition of emotion recognition systems. In case such in-cabin sensing technology would be detecting the driver’s emotional state (e.g. to measure if a driver is ‘angry’), this would warrant a necessity and proportionality assessment to see if the safety exception could apply.

On the other side, the exception of use for medical and safety purposes could be further restricted by Member States pursuant to Article 2(11) of the AI Act, i.e. ultimately also removed under national law.²¹⁸

3.1.1.1.3 *Other prohibited AI practices*

Additionally, the use of emotion recognition systems could be further prohibited under the AI Act if amounting to manipulative or exploitative practices, which aim to materially distort a person’s behaviour and (are reasonably likely to) cause significant harm to that or another person.²¹⁹ Recital 29 explains that AI-enabled manipulative techniques deploy subliminal components or other manipulative or deceptive techniques that subvert or impair the autonomy, decision-making and free choices of a person. Pursuant to Article 5(1)(a), the distortion caused by such systems must appreciably impair a person’s ability to make an informed decision. In the case of exploitative practices, these must exploit the vulnerability of persons due to their age, disability or specific social or economic situation.²²⁰ However, both prohibitions do not apply to lawful medical practices or common and legitimate commercial practices.²²¹

²¹³ Commission Guidelines on prohibited artificial intelligence practices (n 10) paras 259, 262.

²¹⁴ Ibid, 84.

²¹⁵ Ibid, paras 258, 259.

²¹⁶ Ibid, 84.

²¹⁷ Ibid, 79.

²¹⁸ See: ibid, para 264.

²¹⁹ See Article 5(1)(a) and (b) of the AI Act. See also: Kindt and Jasserand (n 135) 127. The authors consider this could be e.g. the case if ‘used in combination with persuasive marketing techniques and neuromarketing.’ See also: Commission Guidelines on prohibited artificial intelligence practices (n 10) para 262.

²²⁰ Recital 29 and Art. 5(1)(b) AI Act.

²²¹ Recital 29 AI Act.

In the context of emotion recognition systems, these systems could amount to manipulative or exploitative practices if used to identify or infer emotions of a person with a view to exploit their emotional state by distorting their behaviour in a substantial way.²²² Generally, in this scenario, there would be no limitation in terms of system modalities (i.e. it would not need to be based on biometrics, so emotion recognition from written text would be for example covered too). While no intent to cause harm is required on the side of the deployer or provider, there would need to be a plausible or reasonably likely causal link and the resulting harm would need to be significant²²³ – i.e. have a significant adverse impact, including on a person's physical or psychological health or financial and economic interests.²²⁴ There is extensive case law, also by the CJEU, on serious and/or significant harm in different fields²²⁵ and the Commission highlighted the following key considerations for considering if a harm is 'significant': the severity of the harm, the context and cumulative effects, its scale and intensity, the vulnerability of the affected persons, and the duration and reversibility of the harm.²²⁶ Generally, to establish significant harm, a careful case-by-case analysis would be needed.²²⁷

In practice, it might prove challenging to, first, prove the use of such practices (as their use is to a large extent by definition not noticeable to a person²²⁸) and second, their causal link to significant harm, especially when it comes to psychological harm. The Commission acknowledged too that: '[t]here are numerous cases where the threshold of significant harm will likely not be reached even if the systems may be deploying subliminal, purposefully manipulative, or deceptive techniques'.²²⁹ On top of these requirements, the Commission Guidelines clarify that the prohibition of manipulative practices does not apply to lawful persuasion practices, which are transparent and respect individual autonomy. An example of lawful persuasion provided in the Guidelines is the use of emotion recognition systems that analyse in a transparent manner emotions of customers to improve interactions and provide support. On the other side, according to the Guidelines, if such a system would be used in a hidden way to offer products at higher prices when consumers are more likely to buy a product, this would result in manipulation.²³⁰ In practice, lawful persuasion would presumably always require free and informed consent by the person subjected to such a system,²³¹ and ensuring

²²² The Commission Guidelines explain that material distortion implies a substantive impact and that a minor influence would not meet this threshold. Commission Guidelines on prohibited artificial intelligence practices (n 10) para 76.

²²³ Commission Guidelines on prohibited artificial intelligence practices (n 10) 24, 27–28, 38.

²²⁴ Recital 29 AI Act. Commission Guidelines on prohibited artificial intelligence practices (n 10) para 115.

²²⁵ Kindt and Jasserand (n 135) 147.

²²⁶ Commission Guidelines on prohibited artificial intelligence practices (n 10) para 92.

²²⁷ *Ibid*, para 91.

²²⁸ The Commission Guidelines explain that 'subliminal techniques' are beyond a person's conscious awareness. 'Purposefully manipulative techniques' could be susceptible to the awareness of a person, but they may not be able to control/resist their effect. When it comes to 'deceptive techniques', a person may not be consciously aware of them or if aware, may still be deceived or unable to control their response/resist them. In the case of 'exploitative practices', they exploit the vulnerabilities of some groups and the persons belonging to them may have limited capacity to recognise or resist such practices. *Ibid*, 20–22, 34. See also: Kindt and Jasserand (n 135) 139–146.

²²⁹ Commission Guidelines on prohibited artificial intelligence practices (n 10) 30.

²³⁰ *Ibid*, 41–43.

²³¹ See also: *Ibid*, para 130. The Commission considers consent would play an important role in certain cases.

it is given in such a way could pose additional challenges.²³² Overall, the use of such practices also interplays with EU consumer law.²³³

3.1.1.2 High-risk AI practices

Under the AI Act, emotion recognition systems, whenever not prohibited (i.e. not used in workplace and education institutions), will be considered high-risk AI systems. Annex III of the AI Act stipulates that AI systems used in the area of biometrics for emotion recognition, in so far as permitted under EU or national law, should be considered high-risk AI systems. As explained in Sub-section 2.2.4, the AI Act's definition of biometrics in Article 3(34) expands the definition of biometrics from the data protection acquis,²³⁴ as it does not require that the 'personal data resulting from the specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person' allow or confirm the unique identification of a person, neither does the data need to be processed in such a way. This is supported by Recital 14, which confirms that '[b]iometric data can allow [...] for the recognition of emotions'. In light of the physical and physiological signals that are commonly used by emotion recognition systems, such as facial images, speech, EEG signals and ECG signals, the majority of such systems would be considered to use biometrics as defined under the AI Act, as these data relate to the physical, physiological or behavioural characteristics of a natural person. Only if such AI systems would not process data relating to such characteristics, such as written text, and would not be deployed for any other high-risk purpose listed in Annex III of the AI Act, they would be considered as 'limited risk' under the AI Act.²³⁵

The rules for high-risk AI systems falling under Annex III of the AI Act, including emotion recognition systems, will start to apply on 2 August 2026, pursuant to Article 113(2) of the AI Act, with some temporal exceptions (see Sub-section 3.1.1.2.1.1).

3.1.1.2.1 Exceptions from the high-risk classification

3.1.1.2.1.1 Emotion recognition systems that will be placed on the market or put into service before 2 August 2026

Pursuant to Article 111(2) of the AI Act, the AI Act will generally not apply to high-risk AI systems, including emotion recognition systems, that will be placed on the market or put into service before 2 August 2026, unless they will undergo a significant change in their designs. However, if such systems are used by public authorities, providers and deployers should ensure compliance with the AI Act by 2 August 2030.

This temporal scope exception means that existing systems that are offered or used on the EU market, with the exception of prohibited AI practices, will not need to comply with the requirements for high-risk AI systems. Recital 177 clarifies to this end that a significant change

²³² Cf. with the issue of meaningful choices for cookie banner consent, see e.g.: Paul Graßl and others, 'Dark and Bright Patterns in Cookie Consent Requests' (2021) *Journal of Digital Social Research*, Volume 3, Number 1, 1–38.

²³³ See the Unfair Commercial Practices Directive. Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), OJ L 149/22.

²³⁴ Article 4(14) GDPR, Article 3(13) LED, Article 3(18) EUDPR.

²³⁵ On the other side, Kindt and Jasserand considered that emotion recognition systems, will be always considered at least high-risk. This is indeed that case provided they fulfill all the elements of the definition of emotion recognition systems under the AI Act. See: Kindt and Jasserand (n 135) 165.

should mean the same as a substantial modification, as defined in Article 3(23) of the AI Act.²³⁶ The concept of substantial modification refers to changes not planned or foreseen in the initial conformity assessment of the system. It is therefore understood that the change would need to result in a modification to the design or intended purpose of the system, which could be interpreted in different ways.

3.1.1.2.1.2 Emotion recognition systems not posing a significant risk of harm to health, safety or fundamental rights

In addition, the AI Act negotiations resulted in the final text including a so-called filter or derogation from the high-risk AI requirements in Article 6(3) of the AI Act. Providers will be able to assess whether their systems that fall under Annex III, including emotion recognition systems, pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Should this be answered in the negative, the system would be exempt from the high-risk AI requirements in the AI Act, unless established otherwise during oversight. Article 6(3) of the AI Act clarifies that this means that the system does not *inter alia* materially influence the outcome of decision making. These would be systems that (a) perform a narrow procedural task, (b) improve the results of a previously completed human activity, (c) detect decision-making patterns or deviations and do not replace or influence a previously completed human assessment without a proper human review and (d) perform a preparatory task. However, if the system profiles persons, it should be always considered high-risk. Providers will have to document this assessment (Articles 6(4) and 49(2) of the AI Act), which could be subject to a re-assessment by the market surveillance authority (MSA; Article 80(1) of the AI Act) and fines if the MSA considers that the system was misclassified to circumvent the AI Act (Article 80(7) of the AI Act).

Concerns over this self-regulatory exercise were raised by civil society.²³⁷ The filter could lead to misclassifications in practice – even if there is no intent to circumvent the AI Act requirements, there might be misunderstandings on the interpretation of this exception and of the exceptions to the exception. Especially in the case of emotion recognition systems, risks to fundamental rights would need to be carefully considered (for more, see Sub-section 3.2.1.2).

3.1.1.3 Other exceptions to the applicability of the AI Act

The AI Act contains further material and temporal exceptions to the scope of its applicability. The relevance of these for emotion recognition systems is outlined below.

3.1.1.3.1 Exceptions from the overall scope of the AI Act

3.1.1.3.1.1 Emotion recognition systems not using AI

Emotion recognition systems under the AI Act have to, by definition, use AI. As demonstrated in Sub-section 2.2.1, there are, however, some uncertainties connected to the definition of AI, in particular when a system is considered AI or rather a simpler traditional software system or

²³⁶ The Article stipulates that “‘substantial modification’ means a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed”.

²³⁷ Joint civil society statement, ‘EU’s AI Act fails to set gold standard for human rights’ (n 83) 6.

programming approach.²³⁸ While systems that recognise emotions seem to use machine learning- or deep learning-based techniques,²³⁹ there might be some systems that are based on excluded approaches such as logistic regression.²⁴⁰ This would require further examination in such cases, and ultimately such systems might fall outside the scope of the AI Act.

3.1.1.3.1.2 Emotion recognition systems used for scientific research and development

Pursuant to Article 2(6) of the AI Act, emotion recognition systems that are developed and put into service only for scientific research and development are excluded from the scope of the AI Act. The AI Act does not define what scientific research and development mean, but draws a distinction to product-oriented research in Recital 26. The Recital clarifies that the AI Act does also not apply to the latter before the system is placed on the market or put into service, with the exception of testing in real world conditions (Article 2(8) AI Act).²⁴¹ While such research needs to be conducted in line with recognised ethical and professional standards as well as applicable law,²⁴² and the AI Act would apply as soon as a system is placed on the market or put into service, this exception ultimately means that any kind of emotion recognition systems, even those prohibited under the AI Act, could fall under the scientific research and development exception. In connection to this, it should be also noted that the AI Act does not apply to EU providers that export otherwise prohibited systems outside the EU.²⁴³ It is understood that the rationale behind this solution was to support innovation, however, by enabling experimenting with prohibited practices and not prohibiting their export, significant risks to fundamental rights could arise.

3.1.1.3.1.3 Emotion recognition systems used for military, defence or national security purposes

Furthermore, if an emotion recognition system would be used for military, defence or national security purposes, it would be excluded from the scope of the AI Act in line with Article 2(3) of the AI Act. When it comes to national security, a distinction has to be drawn with the use for law enforcement or public security purposes, which would fall within the AI Act (Recital 24 of the AI Act). The Commission also underlined in its Guidelines on the prohibitions that this exception would depend on the purpose of use, and not the entities that use the AI system, and would apply only when systems are used exclusively for such purposes.²⁴⁴ It should be also noted that this exception has to be interpreted in light of the CJEU's case law, which established a narrow interpretation of the term. The Court considered in its 2020 *La Quadrature du Net* ruling that national security 'corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.'²⁴⁵

²³⁸ Recital 12 AI Act.

²³⁹ Wang and others (n 13) 20–21. Khare and others (n 17) 3–4.

²⁴⁰ See e.g. Jacob (n 107) 897–905.

²⁴¹ See also Recital 25 AI Act.

²⁴² Recital 25 AI Act.

²⁴³ Cf. Article 2 AI Act. Civil society organisations raised concerns about this, see: Joint civil society statement, 'EU's AI Act fails to set gold standard for human rights' (n 83) 4.

²⁴⁴ Commission Guidelines on prohibited artificial intelligence practices (n 10) paras 22–24.

²⁴⁵ Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and Others* [2020]

ECLI:EU:C:2020:791, para 135. See: Plixavra Vogiatzoglou, 'The AI Act National Security Exception: Room for

3.1.1.3.1.4 Other exceptions

In addition, the AI Act includes further exclusions from its scope, which could be to some extent relevant also for emotion recognition systems. Pursuant to Article 2(4) of the AI Act, the law does not apply to AI systems used by third country public authorities or international organisations in the framework of law enforcement and judicial cooperation with the EU or its Member States, provided adequate safeguards for protecting the fundamental rights and freedoms of individuals are in place within those cooperation frameworks.²⁴⁶ Article 2(10) also excludes from the scope of the AI Act AI systems, including emotion recognition systems, used by individuals for personal non-professional activities. However, providers of such systems will still have to comply with the AI Act and other applicable law, and individuals using them will also need to ensure that such systems are used in line with other applicable law.²⁴⁷ Lastly, the AI Act does pursuant to Article 2(12) of the AI Act not apply to AI systems released under free and open source licences, unless they are placed on the market or put into service as prohibited or high-risk AI systems or systems subjected to transparency obligations under Article 50. This will have in practice some limited implications for certain general purpose AI models.²⁴⁸

3.1.1.3.2 Exceptions from the definition of emotion recognition systems under the AI Act

3.1.1.3.2.1 Systems used for detecting physical states and readily apparent expressions, gestures and movements

As explained under Sub-section 2.2.2, the AI Act does not define what emotions are, however, its Recital 18 provides for several examples to this end (listing happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement). Recital 18 excludes from the scope of the definition systems used for detecting physical states (such as pain or fatigue), such as systems for detecting fatigue in professional pilots or drivers in order to prevent accidents. It also excludes systems used for merely detecting readily apparent expressions, gestures and movements, unless used for identifying or inferring emotions. The examples provided are basic facial expressions (such as a frown or a smile), the movement of hands, arms or head, or voice characteristics, such as a raised voice or whispering.

As these are features that are typically processed by an emotion recognition system, these distinctions might cause some confusion in practice. In a 2024 public consultation by the Dutch Data Protection Authority, respondents for example raised the need for further guidance to this end as ‘interpretations such as stress, pain and fatigue can be both an emotion and a physical state’.²⁴⁹ It is understood that the key difference lies in the output of the system, which must not result in the prediction of an emotion,²⁵⁰ although, as explained under Sub-section

Manoeuvres?’ Verfassungsblog, 9 December 2024 <<https://verfassungsblog.de/the-ai-act-national-security-exception/>> last accessed 19 October 2025. The author analyses the national security exception under the AI Act, pointing out the CJEU’s strict interpretation of national security derogations from EU law and concluding that developing separate, non-AI Act compliant systems for national security purposes might not be economically viable in practice. See also: Commission Guidelines on prohibited artificial intelligence practices (n 10) para 23.

²⁴⁶ See: Commission Guidelines on prohibited artificial intelligence practices (n 10) para 29.

²⁴⁷ Ibid, paras 34, 35.

²⁴⁸ See Articles 53(2) and 54(6) AI Act.

²⁴⁹ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, ‘AI systems for emotion recognition in the areas of workplace or education institutions’ (n 58) 7.

²⁵⁰ See also: Kindt and Jasserand (n 135) 166–167. The authors point out that the sentence ‘the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring

2.2.2, there is no clear consensus on the definition and classification of emotions in psychology and the lines might be often blurred. As one respondent to the Dutch Data Protection Authority's public consultation rightly pointed out, recognising emotions is ultimately the same as recognising readily apparent expressions, since it is impossible to establish correctly what people feel in their inner world.²⁵¹ McStay and Bakir note that Recital 18 of the AI Act relies on a narrow understanding of emotions and creates a loophole, as providers and deployers could claim that they do not want to recognise emotions or intentions but only outward behaviour and expressions of people. This is indeed already the case with some products on the market.²⁵² At the same time, it should be noted that the processing of data relating to physical states and expressions can be still intrusive and might not always justify such a distinction (see Section 3.2).

3.1.1.3.2.2 Emotion recognition systems not processing physical, physiological or behavioural characteristics

In line with the definitions of an emotion recognition system and biometric data under the AI Act (Article 3(34) and (39) of the AI Act), a system has to process physical, physiological or behavioural characteristics of a natural person in order to be considered an emotion recognition system. As explained under Sub-section 2.2.4, not all inputs used by emotion recognition systems would qualify as physical, physiological or behavioural characteristics, such as for example the content of written text. On the other side, an analysis of the way the text was written on the screen – i.e. through keystroke, mouse and touchscreen moves – would amount to behavioural characteristics and therefore biometric data in this sense.²⁵³

3.1.2 Requirements under the AI Act

3.1.2.1 High-risk AI systems

Pursuant to Article 16 of the AI Act, providers of high-risk AI systems, including emotion recognition systems, will have to comply with a number of obligations entailed in Chapter III of the AI Act. These include:

- *Putting in place a quality management system (Article 17 AI Act), including by establishing, implementing, documenting and maintaining a risk management system.* As part of the risk management system, providers need to, inter alia, identify and analyse 'the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights' and put in place 'appropriate and targeted risk management measures' (Article 9 of the AI Act).
- *Having in place appropriate data governance and management practices.* Among other things, training, validation and testing data sets needs to be 'relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose' (Article 10 of the AI Act).

emotions' appears to authorise the detection and possibly collection of this data, but not use for emotion recognition. However, the collection of such data, which could be used for such purposes, is already problematic as it already starts interfering with fundamental rights (p. 166; referring to Kindt (2018) 523–538 and the case law of the ECtHR). See also: McStay and Bakir (n 46) 3.

²⁵¹ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, 'AI systems for emotion recognition in the areas of workplace or education institutions' (n 58) 8.

²⁵² McStay and Bakir (n 46) 3–4.

²⁵³ See: Commission Guidelines on prohibited artificial intelligence practices (n 10) 80.

- *Drawing up technical documentation relating to the high-risk AI system.* This documentation needs to demonstrate compliance of the system (containing as a minimum information from Annex IV of the AI Act). It needs to be in place before the system is placed on the market or put into service, as well as regularly updated (Article 11 of the AI Act).
- *Record-keeping.* The system needs to technically allow for automated record-keeping (Article 12 of the AI Act) and providers need to keep the logs as long as they are under their control (Article of the 19 AI Act).
- *Ensuring transparency and providing information to deployers.* Providers need to design and develop an AI system in a way that ensures that deployers are able to interpret the system's outputs and use it in an appropriate way. Providers need to provide instructions for the use of the system (Article 13 of the AI Act).
- *Ensuring human oversight.* Providers also need to design and develop an AI system in such a way that natural persons can effectively oversee it during its use (Article 14 of the AI Act).
- *Ensuring an appropriate level of accuracy, robustness and cybersecurity.* Providers will have to ensure these throughout the lifecycle of the system (Article 15 of the AI Act).
- *Keeping documentation relating to the system.* This includes the technical documentation mentioned above. The documentation needs to be kept for 10 years after the placement of the high-risk AI system on the market/putting it into service (Article 18 of the AI Act).
- *Ensuring the system undergoes a conformity assessment.* The conformity assessment can be based on harmonised standards or, where applicable, common specifications, if they are available (Article 43 of the AI Act). Providers of emotion recognition systems will be able to decide if they want to follow an internal control procedure to this end, meaning that they will conduct a self-assessment, or to involve a notified body into the assessment (Article 43(1) of the AI Act).²⁵⁴
- *Taking corrective actions and providing information in case of certain risks.* If a system is (no longer) in conformity with the AI Act, providers need to take corrective actions. They also need to inform MSAs about AI systems presenting a risk to the health, safety or to fundamental rights of persons (Articles 20 and 79(1) of the AI Act and Article 3(19) of Regulation (EU) 2019/1020).

While the AI Act primarily addresses the providers of high-risk AI systems, deployers of such systems, including emotion recognition systems, will have to comply with certain requirements under the Regulation too. These include:

- *Taking appropriate technical and organisational measures.* Deployers need to ensure the system is used in line with its instructions (Article 26(1) of the AI Act).
- *Assigning human oversight.* Persons with the necessary competence, training, authority and support should be assigned this role (Article 26(2) of the AI Act).

²⁵⁴ For a critique of the general self-assessment approach in the AI Act, under which providers are both involved in the creation of standards and able to self-assess their conformity with the AI Act, see: Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) Yale Journal of Law & Technology, Volume 26, Issue 3, 692–693.

- *Ensuring the relevance and sufficient representativeness of input data.* Deployers need to ensure this whenever they have control over the input data (Article 26(4) of the AI Act).
- *Monitoring the operation of the high-risk AI system.* If deployers notice certain issues with the system, they need to inform the provider and relevant authorities about it (Article 26(5) of the AI Act).
- *Keeping of logs.* Deployers who have control over the system logs need to keep them for an appropriate period of time (Article 26(6) of the AI Act).
- *Conducting a fundamental rights impact assessment.* Deployers that are bodies governed by public law, provide public services or deploy risk assessment and pricing systems pertaining to creditworthiness or life and health insurance will have to conduct a fundamental rights impact assessment (Article 27 of the AI Act).

In certain cases, the deployer of an emotion recognition system could also become a provider of the system, for example if they make a substantial modification to the system or put their name or trademark on the system, contrary to contractual arrangements. In such cases they would need to comply with all obligations for providers of such systems (Article 25 of the AI Act).

3.1.2.2 Transparency obligations

The AI Act introduces in Article 50 also transparency obligations for providers and deployers of certain AI systems which aim to interact with users or otherwise pose a risk for their manipulation, regardless of whether the system is considered high-risk under the AI Act or not.²⁵⁵ All deployers of emotion recognition systems will therefore, pursuant to Article 50(3) and (5) of the AI Act, have to inform in a clear and distinguishable manner persons exposed to the system about it. Such information needs to be provided at the latest when the person is for the first time exposed to the system.

Exceptions apply in the field of law enforcement if (1) the system is permitted by law to detect, prevent or investigate criminal offences and (2) appropriate safeguards are in place for the rights and freedoms of third parties. This exception is in place to not jeopardise criminal investigations, for example by a person knowing that they are subjected to such a system and therefore changing their behaviour.²⁵⁶

The transparency obligations will start to apply on 2 August 2026 (Article 113(2) of the AI Act).

3.2 The interplay of the AI Act with EU fundamental rights and data protection law

The AI Act underlines on several occasions that its provisions do not affect other applicable EU law, including the prohibitions of certain practices. Recital 9 of the AI Act emphasises that the AI Act 'should apply across sectors and [...] should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights [...] to which

²⁵⁵ Durovic and Corno (n 53) 385.

²⁵⁶ Vagelis Papakonstantinou and Evangelos Zarkadoulas, 'Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement', eucrim issue 2/2023, 3–4 <<https://eucrim.eu/articles/remote-biometric-identification-and-emotion-recognition-in-the-context-of-law-enforcement/>> last accessed 19 October 2025.

[the] Regulation is complementary.²⁵⁷ The AI Act is therefore a *lex specialis* that addresses gaps in Union and national legislation.²⁵⁸

More specifically, when it comes to prohibited AI practices, Article 5(8) of the AI Act underlines that its provisions ‘shall not affect the prohibitions that apply where an AI practice infringes other Union law.’ In addition, Recital 45 of the AI Act clarifies that ‘[p]ractices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation.’ Similarly, in the case of high-risk AI systems, Recital 63 of the AI Act clarifies that the classification of an AI system as high-risk under the AI Act does not mean that the use of a system is lawful under other applicable law, including the Charter. It also underlines that the AI Act does not provide a legal basis for the processing of personal data under EU data protection law, unless explicitly provided for otherwise.²⁵⁹ Moreover, in the case of the additional transparency obligations under Article 50 of the AI Act that will apply to providers and deployers of certain AI systems, Article 50(3) underlines that deployers of emotions recognition systems have to process the personal data in accordance with the EU data protection acquis. At the same time, Recital 137 of the AI Act underlines that the compliance with transparency obligations does not mean that the use of the system is *per se* lawful.

The above demonstrates the co-legislators’ intention that the regime established under the AI Act should not impact prohibitions or restrictions relating to AI development and use under existing EU and national law. This Section therefore examines to what extent the use of emotion recognition systems, even when not explicitly prohibited under the AI Act, could be in fact permitted under two selected aspects of EU law, namely EU fundamental rights and data protection law. It focuses on the applicability of these two areas of law to the development and use of emotion recognition systems, selected requirements that might be at odds with such systems as well as the protection of rights in practice.

3.2.1 EU fundamental rights law

3.2.1.1 The applicability of EU fundamental rights law

One of the AI Act’s objectives is to ensure a high level of protection of fundamental rights contained in the Charter when improving the functioning of the internal market and promoting the uptake of human-centric and trustworthy AI (Article 1(1) AI Act). The AI Act, which forms part of EU secondary law, thereby needs to be in line with primary EU law, most notably the Charter.²⁶⁰

²⁵⁷ See also Article 2(9) of the AI Act, which stipulates that the AI Act is without prejudice to the EU consumer protection acquis. See also Article 2(7) of the AI Act and its accompanying Recital 10 stipulate that the provisions of the AI Act do not affect the EU data protection acquis, which applies to all personal data processing by AI systems regulated under the AI Act.

²⁵⁸ See also: Kindt and Jasserand (n 135) 137.

²⁵⁹ Pursuant to Article 2(7) of the AI Act, the Act applies without prejudice to Article 10(5) of the AI Act, which clarifies the legal basis of personal data processing for bias detection, and Article 59 of the AI Act, which governs personal data processing in AI regulatory sandboxes for developing certain AI systems in the public interest.

²⁶⁰ Charter of Fundamental Rights of the European Union, OJ C 326/391. See also: EUR-Lex, EU hierarchy of norms <<https://eur-lex.europa.eu/EN/legal-content/glossary/eu-hierarchy-of-norms.html>> last accessed 19 October 2025.

Moreover, EU institutions and bodies as well as Member States when implementing EU law need to respect the rights contained in the Charter,²⁶¹ next to their other human rights²⁶² obligations stemming from national, European and international law.²⁶³ The Charter provisions have to be interpreted in line with the corresponding provisions in the European Convention on Human Rights (ECHR) and case law of the European Court of Human Rights (ECtHR), as well as other relevant international law instruments, common constitutional traditions of Member States and, in some cases of explicit references to it, relevant national laws.²⁶⁴

Businesses too need to respect human rights (i.e. address adverse human rights impacts of their activities by preventing, mitigating and remediating them), including by exercising human rights due diligence, in line with the UN Guiding Principles on Business and Human Rights (UNGPs), which apply to all businesses.²⁶⁵ While discussions on the horizontal direct effect of human rights are on-going, and case law is evolving,²⁶⁶ it should be noted that the AI Act obliges providers and certain deployers of high-risk AI systems, which could be both public and private entities, to assess their systems' risks to fundamental rights. Providers have to do this through the risk management system under Article 9 of the AI Act and certain deployers, notably public authorities but also entities providing public services, banks and insurance companies, through the fundamental rights impact assessment (FRIA) under Article 27 of the AI Act.²⁶⁷

Some fundamental rights obligations can be further specified in EU secondary law, such as the EU data protection, non-discrimination, or consumer protection acquis. Certain due

²⁶¹ Article 51 of the Charter.

²⁶² The thesis uses the terms fundamental rights and human rights interchangeably. It is understood they broadly cover the same substance, however, the term 'fundamental rights' is usually used in an EU or constitutional context, whereas the term 'human rights' is usually used in international law. FRA, 'What are fundamental rights?' <<https://fra.europa.eu/en/content/what-are-fundamental-rights>> last accessed 19 October 2025.

²⁶³ See e.g.: Janneke Gerards (ed.), *Fundamental Rights, The European and International Dimension* (Cambridge University Press 2023).

²⁶⁴ European Union Agency for Fundamental Rights (FRA), 'Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level - Guidance' (2018) Publications Office of the European Union, 44 <<https://fra.europa.eu/en/publication/2018/applying-charter-fundamental-rights-european-union-law-and-policymaking-national>> last accessed 19 October 2025.

²⁶⁵ United Nations, 'Guiding Principles on Business and Human Rights' (2011) HR/PUB/11/04, 1, 13–26 (Guiding Principles 11–24)

<www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> last accessed 19 October 2025. While the UNGPs are a soft law instrument and states are 'the primary duty-bearers under international human rights law' (see pp. 1 and 7 of the UNGPs), they have been, as Byrnes and Renshaw observe, included in different business standards and occasionally referred to in case law. Their significant impact lies though in encouraging compliance through stepping up the expectations and pressure from consumers and investors. Andrew Byrnes and Catherine Renshaw, 'Within the State' in Daniel Moeckli, Sangeeta Shah, Sandesh Sivakumaran (eds.), *International Human Rights Law* (4th edition, Oxford University Press 2022) 513. The authors refer to Debevoise and Plimpton LLP, Business and Human Rights Center, *UN Guiding Principles on Business and Human Rights at 10: The Impact of the UNGPs on Courts and Judicial Mechanisms* (2021) and Australian Human Rights Commission and Australian Human Rights Institute, *At the Crossroads: 10 years of implementing the UN Guiding principles on Business and Human Rights in Australia* (2011). See also: European Union Agency for Fundamental Rights (FRA), 'Getting the future right – Artificial intelligence and fundamental rights' (2020) Publications Office of the European Union, 8 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf> last accessed 19 October 2025.

²⁶⁶ See Sub-section 3.2.1.3.2.

²⁶⁷ The fundamental rights impact assessment will have to be conducted by deployers that are bodies governed by public law, that provide public services or that deploy creditworthiness or life and health insurance risk assessment and pricing systems. Article 27(1) AI Act.

diligence obligations could also arise through the Directive on corporate sustainability due diligence, which applies to some large companies.²⁶⁸

3.2.1.2 Requirements under fundamental rights law: selected risks

This part will briefly examine how different fundamental rights could be adversely impacted by the development and use of emotion recognition systems, whenever they are not prohibited under the AI Act (i.e. used outside of the workplace and education institutions). The thesis thereby focuses on some selected aspects, to illustrate issues that could arise with emotion recognition systems. These are by no means exhaustive, as ultimately an assessment of a fundamental rights interference (resulting in a violation) would be always case, and context, specific.

It should be acknowledged that certain use cases of emotion recognition systems could also help to uphold people's fundamental rights, for example through providing better healthcare and personalised services that individuals choose to use, in an informed manner, to improve their wellbeing (for example wearables to monitor their stress levels).²⁶⁹ This would be, however, again a context specific assessment. For example, while proponents of emotion recognition often advocate for their potential in supporting persons with autism,²⁷⁰ some stakeholders have challenged this.²⁷¹ As noted for example by the Electronic Privacy Information Center, emotions can be neurologically diverse.²⁷²

3.2.1.2.1 Human dignity

Subjecting persons to emotion recognition systems can adversely impact their human dignity, which is protected by Article 1 of the Charter as well as several other human rights instruments,²⁷³ and constitutes the basis for all fundamental rights.²⁷⁴ While it is difficult to define human dignity legally, as Dupré observes, 'it has to do with notions of (self-) respect, autonomy,[²⁷⁵] privacy, integrity and self-determination.'²⁷⁶ All these notions can be impacted by the development and use of emotion recognition systems, which claim to 'read' the innermost states of persons, record them and use them for different purposes, including in

²⁶⁸ Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L <<https://eur-lex.europa.eu/eli/dir/2024/1760/oj>> last accessed 19 October 2025. See also: FRA, 'Getting the future right – Artificial intelligence and fundamental rights' (n 265) 8.

²⁶⁹ See: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 32–33.

²⁷⁰ See e.g. Fatma M. Talaat, 'Real-time facial emotion recognition system among children with autism based on deep learning and IoT' (2023) *Neural Computing & Applications*, Volume 35, 12717–12728. Maja Pantic, 'This is why emotional artificial intelligence matters', TEDxCERN, 2018 <https://youtu.be/4QjZDUaDxQU?si=g3g_BaR_DhW1qgxF> last accessed 19 October 2025.

²⁷¹ Kerry McInerney and Os Keyes, 'The Infopolitics of feeling: How race and disability are configured in Emotion Recognition Technology' (2024) *New Media & Society*, 27(7), 4246–4264. See also: Report of the Special Rapporteur on the rights of persons with disabilities, 'Rights of persons with disabilities', A/HRC/49/52, 28 December 2021, 15–16.

²⁷² Electronic Privacy Information Center (n 88) 7.

²⁷³ For an overview see Catherine Dupré, 'Article 1 – Human Dignity' in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 7–12.

²⁷⁴ Explanations relating to the Charter of Fundamental Rights, OJ C 303/17, Explanation on Article 1 — Human dignity.

²⁷⁵ See on this: Mejias and Couldry (n 72). The authors observe, while referring to Hildebrandt (2015), Couldry and Mejias (2019) and Rouvroy (2015), that 'we are, through datafication, becoming dependent on (external, privatised) data measurements to tell us who we are, what we are feeling, and what we should be doing, which challenges our basic conception of human agency and knowledge.'

²⁷⁶ Dupré (n 273) 16–17.

situations of power asymmetries, such as in a law enforcement, migration or public administration context. More generally, human dignity is impacted in situations where persons subjected to emotion recognition systems are not aware of it and/or do not consent to it in an informed manner.²⁷⁷ Gremsl and Hödl pointed out for example that the use of emotion recognition systems, in particular if linked to a scoring system, would lead to a restriction of a person's autonomy. Moreover, the objectification (classification) of emotions through technical means also undermines human dignity.²⁷⁸

3.2.1.2.2 *Right to integrity of the person*

Article 3 of the Charter protects the right to physical integrity, i.e. a person's right to be free from interferences with their body, and the right to mental integrity, i.e. a person's right to be free from psychological pressure and to not be imposed to mental suffering.²⁷⁹ It is conceivable that the use of emotion recognition systems could impact the mental integrity of a person. For example, the (continuous) monitoring of a person's emotions could induce stress, anxiety or other mental suffering to the person. In certain scenarios, if a person would be required to wear sensors to 'recognise' their emotions, this could also impact their physical integrity. Article 3 furthermore requires the free and informed consent of person's subjected to medical treatment, which would apply also in cases where emotion recognition systems are used for medical reasons (which form an exception to the prohibition of their use in the workplace and education institutions, as explained in Sub-section 3.1.4.3.1). This could be, however, challenging, given the disputed scientific basis of these systems on the one hand, and opaqueness of AI systems on the other.²⁸⁰

3.2.1.2.3 *Freedom of thought*

The right to freedom of thought, conscience and religion is guaranteed by Article 10 of the Charter, as well as a number of other instruments.²⁸¹ While the impact of emotion recognition systems on the freedom of thought has been acknowledged by the European Commission in its Guidelines on the prohibitions under the AI Act,²⁸² existing interpretations and case law on Article 10 of the Charter and Article 9 of the ECHR, as well as other international human rights law instruments,²⁸³ focus predominantly on the protection of (non-)religious beliefs in the

²⁷⁷ See: European Union Agency for Fundamental Rights (FRA), Getting the future right – Artificial intelligence and fundamental rights, 14 December 2020, 60 <<https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>> last accessed 19 October 2025. The report notes that 'preserving dignity includes avoiding subjecting people to AI without their knowledge and/or informed consent, which is strongly linked to privacy and data protection.'

²⁷⁸ Gremsl and Hödl (n 72) 171–172. See also: Marcello Lenca and Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) *Journal of Law and the Biosciences*, Volume 9, Issue 1, 6. The authors note how access to mental data by third parties undermines personal autonomy, as 'the informational boundaries of the self blur with the infosphere.'

²⁷⁹ Steve Peers, 'Article 3 – Right to the Integrity of the Person' in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 45. The author also notes that under the ECHR, the right to integrity is part of the right to private life (Article 8 ECHR) (p. 43).

²⁸⁰ It should be noted that the AI Act aims to address this opaqueness through proper documentation that allows for traceability and explainability (see Recital 27 and Chapter III AI Act).

²⁸¹ Ronan McCrea, 'Article 10 – Right to Freedom of Thought, Conscience and Religion' in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 324–325.

²⁸² Commission Guidelines on prohibited artificial intelligence practices (n 10) 81.

²⁸³ The UN Special Rapporteur on freedom of religion or belief noted in its 2021 report on the freedom of thought that '[d]espite its proclaimed importance and absolute nature, the right's scope and content remain largely underdeveloped and poorly understood. The right receives scant attention in jurisprudence, legislation and scholarship, international and otherwise.' Shaheed (n 128) 3.

context of this right.²⁸⁴ However, as McGoldrick notes, this right is actually wider in its scope as it protects also the ‘right of the individual to have independent thoughts, ideas, and beliefs.’²⁸⁵ This aspect of the right seemed to have received little to no prominence in jurisprudence so far (with some authors considering it ‘is something of a legal enigma’²⁸⁶). At the same time, it is receiving increasing attention at the international level²⁸⁷ and in academia,²⁸⁸ especially with the rise of neurotechnology²⁸⁹ and other intrusive digital technologies.

The UN Special Rapporteur on freedom of religion or belief published in 2021 a report on the freedom of thought, in which he proposed the following four attributes of this right: the ‘(a) freedom not to disclose one’s thoughts; (b) freedom from punishment for one’s thoughts; (c) freedom from impermissible alteration of one’s thoughts; and (d) an enabling environment for freedom of thought.’²⁹⁰ In the context of emotion recognition, the freedom of thought could be impacted as emotions are interlinked with thoughts, forming a part of them.²⁹¹ In particular, its use could lead to the ‘disclosure’ of the innermost states of persons, so-called *forum internum* (point (a)) or possibly even punishment or sanctioning for one’s emotions if used in a law enforcement, migration or other asymmetric power relationships (point (b)).

3.2.1.2.4 *Right to respect for private life*

The interference with a person’s right to private life, protected by Article 7 of the Charter and other human rights instruments, including Article 8 of the ECHR,²⁹² is a core issue of emotion recognition systems. The concept of ‘private life’ is thereby broad, covering a person’s physical and psychological integrity and encompassing multiple aspects of their physical and social

²⁸⁴ McCrea (n 281) 325, 330. The Charter commentary does not engage into the analysis of ‘freedom of thought’ as an independent concept beyond conscience and religion. See also: Registry of the ECHR, ‘Guide on Article 9 of the European Convention on Human Rights’ (2024) <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_9_eng> last accessed 19 October 2025.

²⁸⁵ Dominic McGoldrick, ‘Thought, Expression, Association, and Assembly’ in Daniel Moeckli, Sangeeta Shah, Sandesh Sivakumaran (eds.), *International Human Rights Law* (4th edition, Oxford University Press 2022) 212.

²⁸⁶ Patrick O’Callaghan and others, ‘The right to freedom of thought: an interdisciplinary analysis of the UN special rapporteur’s report on freedom of thought’ (2023) *The International Journal of Human Rights*, Volume 28, Issue 1, 16. They also refer in their article to Dwight Newman, who considered freedom of thought is a ‘forgotten freedom’ (Dwight Newman, ‘Interpreting Freedom of Thought in the Canadian Charter of Rights and Freedoms’ (2019) *Supreme Court Law Review* 91, 107–122).

²⁸⁷ Shaheed (n 128).

²⁸⁸ See e.g.: Jan Christoph Bublitz, ‘Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right’ (2014) *Archives for Philosophy of Law and Social Philosophy*, Volume 100, Number 1, 1–25. Ligthart and others (n 128) 1–14. O’Callaghan and others (n 286) 1–23.

²⁸⁹ O’Callaghan and others note, as also observed in the report of the UN Special Rapporteur on freedom of religion or belief, that neurotechnology is ‘an area of potential concern, but the relevant technology is still sufficiently primitive that there is adequate time to develop ethical standards to govern dilemmas which might arise when – and if – ‘neurotechnology’ develops to a point where it can decipher thoughts outside ‘tightly controlled laboratory conditions.’ It is far from that point at present.’ O’Callaghan and others (n 286) 11.

²⁹⁰ Shaheed (n 128) 9.

²⁹¹ As the UN Special Rapporteur on freedom of religion or belief notes: ‘[s]ome neuroscientists distinguish “thought” from other cognitive processes, including emotion, based on the primary part of the brain engaged. Others emphasize the complex, highly interrelated nature of anatomical aspects of the brain that support cognitive functions, comparing efforts to “trace a thought from beginning to end” to “asking where the forest begins”.’ Ibid, 5 (referring to: <https://engineering.mit.edu/engage/ask-an-engineer/what-are-thoughts-made-of/>). Jan Christoph Bublitz considered that thoughts include emotions. Bublitz (n 288) 18, 24. For a brief analysis of the impact of emotion recognition systems on the freedom of thought, see also: Gremsl and Hödl (n 72) 167.

²⁹² See: David Mangan, ‘Article 7 (Private Life, Home and Communications) – Respect for Private and Family Life’ in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 153.

identity.²⁹³ The ECtHR has developed a concept of ‘reasonable expectation of privacy’, i.e. a person’s expectation of privacy outside of their home or private premises, which can be a factor in determining a violation of their right to privacy.²⁹⁴ With emotion recognition systems, especially the mental privacy of a person could be impacted, i.e. their ‘right to not reveal any unexpressed mental state.’²⁹⁵ More broadly, emotion recognition systems risk to undermine the informational privacy of a person by interfering with their control over these data²⁹⁶ and with privacy as a group right if resulting in general surveillance.²⁹⁷

The ECtHR held in the past that there can be an interference with private life as soon as ‘any systematic or permanent record of [...] personal data comes into existence.’²⁹⁸ Emotion recognition systems imply the creation of a record, albeit only for a short period of time, relating to a person’s emotion. The data processed, subject to how a given system works, might however not always amount to personal data, as will be further explained Sub-section 3.2.2.1.1.

While at present no case law on emotion recognition systems by the CJEU and ECtHR exists, the question arises to what extent parallels can be drawn between the issue of (video) surveillance, where case law exists, and emotion recognition. Some overlap between these two issues can be noted, for example when recordings are used as input data, i.e. to recognise facial expressions or gestures from which emotions are inferred. However, in the author’s opinion, a key distinction lies in their intrusiveness, with emotion recognition systems allegedly ‘recognising’ and recording the innermost states of a person. The level of intrusiveness can, however, vary subject to the modalities of a given system, including how it processes, stores and uses the data gathered.²⁹⁹ For example, such systems can capture ‘emotions’ from sensors that touch a person, or use remote sensors not noticeable to the person that collect information about their physical, physiological and behavioural characteristics.³⁰⁰ Such data

²⁹³ *Denisov v. Ukraine* App. no. 76639/11 (ECtHR, 25 September 2018) para 95.

²⁹⁴ See e.g.: *López Ribalda and Others v. Spain* App. nos. 1874/13 and 8567/13 (ECtHR, 17 October 2019) para 89. See also: Registry of the ECHR, ‘Guide on Article 8 of the European Convention on Human Rights’ (2024) 35 <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng> last accessed 19 October 2025. FRA, ‘Getting the future right – Artificial intelligence and fundamental rights’ (n 265) 61.

²⁹⁵ Ligthart and others (n 128) 8 (referring to Bublitz, ‘The Nascent Right to Psychological Integrity and Mental Self-Determination’ in Von Arnould, Von der Decken and Susi (eds), *The Cambridge Handbook of New Human Rights* (2020) 400).

²⁹⁶ Häuselmann and others (n 17) 2.

²⁹⁷ See: McStay (n 17) 2–3. The author refers to the work of Floridi (2014), Edwards (2016) and the EDPS Opinion 4/2015.

²⁹⁸ *López Ribalda and Others v. Spain* App. nos. 1874/13 and 8567/13 (ECtHR, 17 October 2019) para 89. Referring to previous case law (*Peck v. the United Kingdom*, *Perry v. the United Kingdom* and *Vukota-Bojić v. Switzerland*).

²⁹⁹ Cf. *Antović and Mirković v. Montenegro* App. no. 70838/13 (ECtHR, 28 November 2017), Joint Dissenting Opinion of Judge Spano, Bianku and Kjølbro, para 8. In their joint dissenting opinion in *Antović and Mirković v. Montenegro*, Judges Spano, Bianku and Kjølbro deduced from the ECtHR’s existing case law that: ‘video monitoring or surveillance does not in itself amount to an interference with the private lives of the persons monitored. Whether that is the case depends on an assessment of the specific circumstances of the case, including where the monitoring takes place, the nature of the activities monitored, whether the monitoring is targeted and systematic, whether the persons monitored had a reasonable expectation of privacy, whether notice had been given or whether the person irrespective of such notice had a reasonable expectation of privacy having regard to the nature of the activities, whether the information is stored, processed and made use of, including whether it is disseminated. In other words, it depends on an assessment of the video monitoring as such as well as the storing, processing and use of the data or information gathered.’ These factors could be relevant also for the assessment of how emotion recognition systems interfere with a person’s privacy.

³⁰⁰ McStay and Urquhart (n 68) 3.

may be combined with other data about the person, collected both from their devices and the wider context.³⁰¹

3.2.1.2.5 *Right to protection of personal data*

Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the EU (TFEU)³⁰² guarantee everyone the right to the protection of their personal data. Article 8(2) of the Charter further requires that personal data are processed fairly, for specified purposes and that the processing is based on a person's consent or some other legitimate basis enacted by law. It also guarantees everyone the right to access their data and to have it rectified. The right to data protection is, based on Article 16 of the TFEU, further defined in secondary EU law, namely the GDPR, LED and EUDPR. Both the Charter and the TFEU foresee that compliance with data protection rules has to be overseen by independent authorities. The right to data protection is also intricately connected to the right to private life – indeed the ECtHR considers it as part of Article 8 of the ECHR.³⁰³ At the Council of Europe level, the right is further protected by Convention 108+.³⁰⁴

When it comes to the development and use of emotion recognition systems, the right to data protection can be impacted in several ways. Data protection issues could arise when such systems are being developed, as the development of AI often requires large amounts of data, which can include personal data, especially when it comes to AI models used as a basis for such systems.³⁰⁵ Problems arise in particular when such data is unlawfully obtained, e.g. through the scraping of websites.³⁰⁶ Once such systems are operational, they process physical, physiological or behavioural characteristics of a person, leading to the datafication of the innermost states of persons. As McStay and Urquhart note, emotion recognition 'enables a shift from emotive states being transient and ephemeral to becoming datafied, catalogued, scored and potentially retrospectively assessed.'³⁰⁷ This raises questions about the lawfulness of such processing and compliance with other data protection principles.³⁰⁸ The data processing by emotion recognition systems might, however, not always amount to the processing of personal data as defined under the EU data protection acquis. This limits the protection afforded by the right to data protection only to some cases where emotion recognition systems are being used. Sub-section 3.2.2 will examine in more detail these and other issues relating to the development and use of emotion recognition systems under the EU data protection acquis.

³⁰¹ Ibid.

³⁰² Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326/47 <https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng> last accessed 19 October 2025.

³⁰³ See: Joined Cases C 92/09 and C 93/09 *Volker und Markus Schecke and Eifert* [2010] ECLI:EU:C:2010:662, paras 47, 52. See also: Herke Kranenborg, 'Article 8 – Protection of Personal Data' in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 238–242. The author concludes that the CJEU in its case law does not consistently draw a distinction between the right to privacy and the right to data protection, as often the two rights are assimilated (p. 242).

³⁰⁴ Convention for the protection of individuals with regard to the processing of personal data, as amended by Protocol CETS No. 223 (Convention 108+).

³⁰⁵ See: Recital 105, Article 3(63) AI Act. Some authors therefore for example propose to use federal learning instead of centralised learning for developing such models, meaning that the data is not stored on a central server but rather client devices. Khare and others (n 17) 15.

³⁰⁶ Electronic Privacy Information Center (n 88) 10.

³⁰⁷ McStay and Urquhart (n 68) 4.

³⁰⁸ Art. 5 GDPR, Art. 4 LED, Art. 4 EUDPR.

3.2.1.2.6 Non-discrimination

The prohibition of discrimination is enshrined in Article 21 of the Charter as well as numerous other international instruments.³⁰⁹ The Charter includes in the first paragraph of Article 21 an open-ended list of prohibited status grounds of discrimination³¹⁰ and in the second one a specific prohibition of discrimination on the grounds of nationality. The right is further specified in a several pieces of EU secondary law, such as the Racial Equality Directive (2000/43/EC) or the Employment Equality Directive (2000/78/EC).³¹¹ Secondary EU law prohibits discrimination in certain areas based on age, disability, ethnic origin, race, religion or belief, sex and sexual orientation.³¹² To this end, both direct discrimination, i.e. situations where a person is treated less favourably than another in a comparable situation based on a protected characteristic, and indirect discrimination, i.e. situations where a person with a protected characteristic is put at a particular disadvantage compared to others on the basis of an apparently neutral provision, criterion or practice, are generally prohibited. Indirect discrimination can be, however, justified if there is a legitimate aim for this provision, criterion or practice, and the means to achieve that aim are necessary and proportionate.³¹³

The use of emotion recognition systems can lead to discrimination. Previous research has for example demonstrated that emotion recognition systems can be biased based on a person's race (by more frequently assigning 'negative emotions' to black persons³¹⁴) or age (by more 'accurately' predicting emotions in younger persons³¹⁵). Bias in algorithms, that could lead to discrimination, is indeed a broader issue connected to the development and use of AI.³¹⁶ As noted by the Dutch Department for the Coordination of Algorithmic Oversight, when it comes to AI systems inferring emotions, such bias can be more difficult to detect in general AI

³⁰⁹ See: Claire Kilpatrick and Hanna Eklund, 'Article 21 – Non-Discrimination' in Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022) 618–620.

³¹⁰ Such as 'sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation' (Article 21(1) of the Charter). The Explanations further clarify that '[i]n contrast [to Article 19 TFEU], the provision in Article 21(1) does not create any power to enact anti-discrimination laws in these areas of Member State or private action, nor does it lay down a sweeping ban of discrimination in such wide-ranging areas. Instead, it only addresses discriminations by the institutions and bodies of the Union themselves, when exercising powers conferred under the Treaties, and by Member States only when they are implementing Union law.' Explanations relating to the Charter of Fundamental Rights, OJ C 303/17, Explanation on Article 21 — Non-discrimination.

³¹¹ The Charter right offers additional possibilities for judicial review of acts of EU institutions and bodies as well as Member States when they implement EU law that amount to discrimination based on other grounds protected by the Charter. Kilpatrick and Eklund (n 309) 615–616, 628. See also: FRA and Council of Europe, 'Handbook on European non-discrimination law' (2018) Publications Office of the European Union, 23 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf> last accessed 19 October 2025.

³¹² The Racial Equality Directive (2000/43/EC) prohibits discrimination based on race or ethnicity in employment, as well as when it comes to the access to the welfare system, social security and to goods and services; the Employment Equality Directive (2000/78/EC) prohibits discrimination based on age, disability, religion or belief and sexual orientation in the area of employment; the Gender Goods and Services Directive (2004/113/EC) prohibits discrimination based on sex in the area of goods and services; and the Gender Equality Directive (recast) (2006/54/EC) prohibits discrimination based on sex in the area of social security. See also Article 10 TFEU. FRA and Council of Europe, 'Handbook on European non-discrimination law' (n 311) 21–22.

³¹³ Kilpatrick and Eklund (n 309) 627. The authors refer to relevant provisions in secondary EU law, such as Art. 2(2) of the Racial Equality Directive, which define the meaning of direct and indirect discrimination. They note that direct discrimination generally cannot be justified, or needs to be subject to stricter justification as indirect discrimination.

³¹⁴ Rhue (n 70).

³¹⁵ Kim and others (n 71).

³¹⁶ See more generally on bias in algorithms and the issue of discrimination: FRA, 'Bias in algorithms - Artificial intelligence and discrimination' (n 69).

systems (such as LLMs) than narrow AI systems, as the former are based on larger datasets and are not focusing solely on emotion recognition.³¹⁷

3.2.1.2.7 *The potential adverse impact on other rights*

Depending on the purpose of use, the development and use of emotion recognition systems could adversely impact also many other rights enshrined in the Charter. For example, there could be an adverse impact on the freedom of expression, which is interlinked with the freedom of thought,³¹⁸ if people refrain from manifesting emotions to the outside world due to the potential surveillance and datafication of their emotions. As pointed out for example by Wachter, the use of emotion recognition systems can force individuals to act in a way which is in line with an algorithmic standard, impacting their 'autonomy to express themselves freely'.³¹⁹ The EDPS also considered that unwanted exposure to advanced facial emotion recognition systems, which may detect facial movement not fully comprehensible to the human eye, could lead to people feeling vulnerable and lead to behavioural changes and a chilling effect.³²⁰

Moreover, if such systems are used in law enforcement and/or for the administration of justice, the right to liberty protected in Article 6 of the Charter as well as the right to fair trial or the presumption of innocence, protected under Articles 47 and 48 of the Charter, could be adversely impacted. Generally, as with the use of AI systems more broadly, also the rights to an effective remedy (Article 47 of the Charter) and to good administration (Article 41 of the Charter) could be adversely impacted, if persons subjected to such systems would not be made aware of it in an appropriate manner and receive necessary information that allows them to challenge the use. Consumer rights, guaranteed by Article 38 of the Charter and the EU consumer law acquis, could be impacted if exposing consumers to such systems, potentially amounting to unfair commercial practices.³²¹ Persons belonging to specific groups granted additional protection under Title III of the Charter, such as children or persons with disabilities, could be adversely impacted too if for example emotion recognition systems are biased towards them or used to exploit their potential vulnerabilities.³²² The development of AI can also impact intellectual property rights, protected under Article 17(2) of the Charter, if copyrighted or trademarked data is used in the process.³²³

³¹⁷ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 36.

³¹⁸ Shaheed (n 128) 7–8. Ligthart and others (n 128) 5 (referring to Taylor, A Commentary on the International Covenant on Civil and Political Right (2021) 501 and Evans, Religious Liberty and International Law in Europe (1997) 285).

³¹⁹ Sandra Wachter, 'Every smile you fake' — an AI emotion-recognition system can assess how 'happy' China's workers are in the office' Berkman Klein Center (15 June 2021) <<https://cyber.harvard.edu/story/2021-06/every-smile-you-fake-ai-emotion-recognition-system-can-assess-how-happy-chinas>> last accessed 19 October 2025.

³²⁰ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 4.

³²¹ The Unfair Commercial Practices Directive defines such practices as a practice that is 'contrary to the requirements of professional diligence' and 'materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.' Article 5(2) Directive 2005/29/EC.

³²² For a general analysis of the impact of the development and use of AI systems on selected fundamental rights mentioned here (rights of special groups, the right to an effective remedy and to a fair trial, consumer protection and the right to good administration), see e.g. FRA, 'Getting the future right – Artificial intelligence and fundamental rights' (n 265) Chapter 4.

³²³ For an analysis on intellectual property issues, see e.g.: OECD, 'Intellectual Property Issues in Artificial Intelligence Trained on Scraped Data' (2025) OECD Artificial Intelligence Papers, Number 33, 20–21 <<https://doi.org/10.1787/d5241a23-en>> last accessed 19 October 2025.

This is only an illustration of the wide-reaching adverse impact that the development and use of emotion recognition systems could have on fundamental rights, as protected under EU law. It should be also noted that all these fundamental rights are ultimately also interrelated and interdependent. For example, by respecting the right to privacy, also human dignity is upheld.³²⁴ Some fundamental rights could be restricted if the conditions in Article 52 of the Charter are fulfilled, as will be further discussed under Sub-section 3.2.1.3.

3.2.1.2.8 *The need for new human rights?*

Scholars have also discussed whether there is a need to introduce new human rights to adequately protect the mind (and one could therefore argue also emotions, especially when inferred from EEG signals) of a person.³²⁵ Proponents of so-called neurorights advocate for the introduction of one or more new human rights to ensure adequate protection of the integrity, privacy and freedom of mental processes of a person in a time where neurotechnology is advancing.³²⁶

On the other side, there are views that the existing human rights framework can offer sufficient protection.³²⁷ Hertz for example argues that freedom of thought can be interpreted in a way (for example through general comment, protocol or soft law documents) that ensures 'comprehensive protection of mental processes and brain data.'³²⁸ An example of a soft law instrument would be the Commission guidelines on the prohibitions under the AI Act, which contribute to such legal development by explicitly acknowledging the impact that emotion recognition systems have on the freedom of thought.³²⁹

In light of the above, the author considers that when it comes to the development and use of emotion recognition systems, existing frameworks applying within the EU could offer sufficient protection. As outlined above, the Charter, together with other international human rights instruments, offers broad protection. While it is true that some fundamental rights are at present rarely referred to in jurisprudence or other legal instruments, their interpretation could be further clarified and expanded in the future both through soft law and scholarly interpretation as well as (strategic) litigation. One specific aspect that discussions about the need for new human rights seem not to pay close attention to is the protection afforded by the right to human dignity. As noted by Dupré, the broad concept of human dignity as enshrined in the Charter offers flexibility, as it could be used to afford protection in situations that have not been foreseen when the Charter was drafted.³³⁰ Ultimately, fundamental rights should be interpreted in light of modern day circumstances – this 'living instrument' doctrine has been for example developed by the ECtHR for the interpretation of the ECHR already in 1978.³³¹

³²⁴ See e.g. Dupré (n 273) 6.

³²⁵ For an overview of arguments, see: Nora Hertz, 'Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought' (2023) *Neuroethics*, Volume 16, Article number 5.

³²⁶ Ibid, 1–2, 11. Ienca and Andorno for example proposed new human rights to cognitive liberty, mental privacy, mental integrity and the right to psychological continuity. Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) *Life Sciences, Society and Policy*, Volume 13, Number 5, 10–23.

³²⁷ Ienca and Andorno advocated for new human rights, but at the same time acknowledged that another possibility would be to further develop existing rights. Ibid, 8.

³²⁸ Hertz (n 325) 2, 11.

³²⁹ Commission Guidelines on prohibited artificial intelligence practices (n 10) 81.

³³⁰ Dupré (n 273) 7, 14.

³³¹ *Tyrer v. The United Kingdom* App no. 5856/72 (ECtHR, 25 April 1978) para 31: 'The Court must also recall that the Convention is a living instrument which, as the Commission rightly stressed, must be interpreted in the light of present-day conditions.' Hertz (n 325) 9.

How this could occur in practice, as well as other opportunities and challenges for fundamental rights protection in the context of emotion recognition systems, will be further explored in Sub-section 3.2.1.3.

3.2.1.2.9 *Necessity and proportionality*

As illustrated, the development and use of emotion recognition systems could adversely impact several fundamental rights. This raises the question of the extent to which the development and use of emotion recognition systems, when not prohibited under the AI Act, can be permitted under EU fundamental rights law.

When it comes to the fundamental rights that can be impacted by the development and use of emotion recognition systems, it should be noted that some of these are absolute (such as human dignity and freedom of thought³³²), meaning that they cannot be restricted.³³³ The exercise of other rights, such as the rights to the integrity of the person, privacy or data protection, could be restricted provided that the conditions for their limitation contained in Article 52 of the Charter are fulfilled. This means that any limitations need to be provided for by law and respect the essence of these rights. The essence of a right, as noted by Lenaerts, refers to the very substance of a fundamental right. A limitation would therefore, both in light of its intensity and extent, question the right as such and be therefore automatically disproportionate.³³⁴ In addition, provided the essence of a right is respected, limitations also need to genuinely meet objectives of general interest or the need to protect the rights and freedoms of others (such as for example the freedom to conduct a business enshrined in Article 16 of the Charter), and be necessary and proportionate.³³⁵ Such balances in individual cases are ultimately struck by courts in the ever-evolving jurisprudence pertaining to fundamental rights.³³⁶

It is questionable how certain fundamental rights interferences could be justified when emotion recognition systems are used. While emotion recognition systems could be used for legitimate objectives, such as the fight against (serious) crime,³³⁷ the question arises whether this would be indeed necessary to achieve these objectives, especially in light of their disputed scientific basis. Smuha and others for example questioned whether the impact of such systems on fundamental rights 'can be even legitimised as necessary and proportionate.'³³⁸ They called for their prohibition when used by law enforcement and other public actors that have coercive powers, as well as *ex ante* control by an independent body whenever such systems are not prohibited (i.e. such systems should undergo a prior independent conformity assessment).³³⁹

³³² Shaheed (n 128) 7.

³³³ Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) German Law Journal, Volume 20, Special Issue 6, 783. See the corresponding references to case law.

³³⁴ Ibid, 779, 781, 785. See the corresponding references to case law. The author notes that: 'it is argued, in the light of the seminal judgment of the CJEU in Schrems, ²² that the concept of the essence of a fundamental right implies that every fundamental right has a "hard nucleus" that guarantees to each and every individual a sphere of liberty that must always remain free from interference.' (p. 781).

³³⁵ Article 52 of the Charter.

³³⁶ See: Gianclaudio Malgieri and Cristiana Santos, 'Assessing the (Severity of) Impacts on Fundamental Rights' (2024) Computer Law & Security Review, 2025, forthcoming, SSRN version, 10, 13–14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875937> last accessed 19 October 2025.

³³⁷ As Lenaerts notes, the CJEU held in *Ministerio Fiscal* (C-207/16) that a serious interference with fundamental rights may be justified only if done to fight serious crime. Lenaerts (n 333) 787.

³³⁸ Smuha and others (n 53) 31.

³³⁹ Ibid, 56–57.

Ultimately, it should be noted that emotion recognition systems could be used for multiple purposes and their impact on fundamental rights would depend on the specific context, taking into account their purpose and aim of use, legal basis, likely affected persons and groups, interests driving such use as well as safeguards taken.³⁴⁰

3.2.1.3 Fundamental rights protection in practice and the interplay with the AI Act

The question therefore arises how fundamental rights considerations can shape up the practice of developing and using emotion recognition systems. The thesis will explore the following three aspects: (1) fundamental rights assessments by providers and certain deployers of such systems under the AI Act, (2) the role of oversight and enforcement in protecting fundamental rights, and (3) the annual Commission review of the prohibited and high-risk AI practices.

3.2.1.3.1 Fundamental rights due diligence

As briefly explained under Sub-section 3.2.1.1, the AI Act foresees that both providers and certain deployers of emotion recognition systems have to assess their systems' risk to fundamental rights. Providers will have to, in line with Article 9 of the AI Act, have in place a continuous iterative risk management system that will identify and analyse the known and the reasonably foreseeable risks that their system can pose to fundamental rights. They will have to adopt appropriate and targeted measures to address these risks. This risk management system will be further elaborated upon through standards that are currently being developed by two European standardisation organisations, CEN and CENELEC.³⁴¹

In addition, certain deployers of such systems – namely bodies governed by public law and private entities providing public services³⁴² – will have to conduct a Fundamental Rights Impact Assessment (FRIA) under Article 27 of the AI Act. They will have to do so prior to the deployment of the system with a view to address further context-specific risks that can occur when the system is used. The assessment will have to be updated in case of changes to its elements during the deployment of the system.³⁴³ The assessment will complement data protection impact assessments (see Sub-section 3.2.2.3.2) and other existing assessments by the providers.³⁴⁴ The template for the FRIA will be developed by the AI Office.³⁴⁵ Possible approaches for both assessments under Articles 9 and 27 of the AI Act are currently being discussed, and different ways forward are being proposed.³⁴⁶

³⁴⁰ See also Art. 27 AI Act and Ienca and Malgieri (n 278) 8.

³⁴¹ Article 40 AI Act. European Commission, Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, C(2023)3215, 22 May 2023 <[https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en)> last accessed 19 October 2025.

³⁴² In addition, also deployers of high-risk AI systems covered in points 5 (b) and (c) of Annex III (i.e. deployers of systems used for creditworthiness assessments and of systems used for risk assessment and pricing in life and health insurance) will have to conduct a FRIA. See Art. 27(1) AI Act.

³⁴³ Art. 27(2) AI Act.

³⁴⁴ Art. 27(2) AI Act.

³⁴⁵ Art. 27(5) AI Act.

³⁴⁶ See e.g. Mélanie Gornet, Winston Maxwell, 'The European approach to regulating AI through technical standards' (2024) Internet Policy Review, Volume 13, Issue 3. Catalan Data Protection Authority, 'FRIA model: Guide and use cases' (2025) <www.dpdexarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_en_def.pdf> last accessed 19 October 2025.

While it remains to be seen how such impact assessments should be conducted in practice, it is clear that under the AI Act providers and deployers should refrain from developing or deploying emotion recognition systems that pose too high risks for fundamental rights. This might inevitably lead to questions about the overall appropriateness of using such systems, especially in asymmetrical power relationships, and without sufficient safeguards in place.

Despite the fundamental rights assessments under Articles 9 and 27 of the AI Act being ultimately self-assessments, and the FRIA obligation under Article 27 of the AI Act having only a limited personal scope (meaning that private entities will be largely exempt from it), the documentation created during these processes can help to improve the enforcement of fundamental rights obligations by competent authorities as well as broader oversight by civil society stakeholders in practice.³⁴⁷ Moreover, providers will be also obliged to report serious incidents, including infringements of fundamental rights, to MSAs.³⁴⁸ Deployers also have to inform the providers, distributors and MSAs about such incidents.³⁴⁹ The MSAs will then need to inform national authorities protecting fundamental rights about it.³⁵⁰ While this will be also a self-reporting exercise, it can help to enhance oversight in practice.

3.2.1.3.2 *The role of oversight and enforcement*

The effective oversight and enforcement over emotion recognition systems will be key to uphold the fundamental rights of persons affected by such systems. While providers and (some) deployers will be obliged to perform fundamental rights due diligence under the AI Act and to comply with other applicable law (see also Sub-section 3.2.2), it has to be acknowledged that the current legal framework leaves some ambiguity concerning the permitted development and use of emotion recognition systems. Providers and deployers of such technologies, who are driven by different public and commercial interests, might be therefore incentivised to comply with the legally prescribed minimum.³⁵¹ At the same time, as observed by the Dutch Department for the Coordination of Algorithmic Oversight, the challenge remains for both supervisory authorities and policy makers to assess if and when the use of emotion recognition could be desirable.³⁵²

Under the AI Act, the supervision and enforcement of rules concerning emotion recognition systems is entrusted to one or more MSAs in each Member State.³⁵³ Member States can generally choose which authorities they wish to establish or designate for this purpose.³⁵⁴ However, the AI Act foresees that data protection authorities need to act as MSAs in cases where emotion recognition systems are used for law enforcement purposes, border management and the administration of justice and democratic processes.³⁵⁵ MSAs, acting in line with Regulation (EU) 2019/1020, can start investigations into emotion recognition

³⁴⁷ See also: Eike Graef, Paul Nemitz, 'Addressing the Challenge of Protecting Fundamental Rights Through AI Regulation in the European Union' (2024) 71 UCLA L. Rev. Disc. 144, 148–149.

³⁴⁸ Arts. 73 and 3(49) AI Act.

³⁴⁹ Art. 26(5) AI Act.

³⁵⁰ Arts. 73(7) and 77 AI Act.

³⁵¹ See: Durovic and Corno (n 53) 399.

³⁵² Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 40.

³⁵³ Art. 70 AI Act.

³⁵⁴ Art. 70(1) AI Act. The list of designated single points of contact for MSAs in Member States is available here: European Commission, 'Market Surveillance Authorities under the AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act#1720699867912-2>> last accessed 19 October 2025. It shows that as of October 2025, several designations still need to take place.

³⁵⁵ Art. 74(8) AI Act.

systems³⁵⁶ and are empowered to deal with complaints by companies and individuals pertaining to their development and use.³⁵⁷ They can access documentation needed for fulfilling their tasks.³⁵⁸ In cases of non-compliance, they can issue penalties.³⁵⁹ So far, it appears that no supervisory cases concerning the prohibition of emotion recognition systems in the workplace and education institutions emerged in EU Member States,³⁶⁰ which might be also due to the early days of the establishment of the AI Act's governance structure.³⁶¹

In addition, Article 77 of the AI Act foresees that national authorities or bodies with supervisory or enforcement powers concerning fundamental rights obligations under Union law will have the possibility to request documentation under the AI Act concerning emotion recognition systems when this necessary for fulfilling their mandates. They will be also able to request testing through technical means with MSAs. This provision can contribute to fundamental rights protection in practice, as it will enable national authorities protecting fundamental rights to obtain relevant information for their investigations.

Persons affected by emotion recognition systems as well as others concerned about their compliance with the AI Act will be able, as mentioned, to complain about it to MSAs.³⁶² Importantly, affected persons will have to be informed about the use of emotion recognition systems³⁶³ and be able to request a clear and meaningful explanation from deployers of emotion recognition systems about the system's role in decisions affecting them, with some exceptions applying.³⁶⁴ This information can be used both for complaining to MSAs and to substantiate claims under other applicable remedies. Guaranteeing such a right is particularly important as a lack of explainability of outcomes through existing emotion identification techniques has been observed.³⁶⁵ This right complements the information provision regime under data protection law (see Sub-section 3.2.2.3.1), as it applies also to 'semi-automated' decision-making with the support of AI.³⁶⁶ It remains to be seen however how the interests of affected persons will be balanced against interests of deployers (such as trade secrets) when the right to an explanation is evoked.³⁶⁷

Importantly, existing remedies provided for under other applicable law, such as data protection, equality and consumer law, remain fully applicable also when emotion recognition

³⁵⁶ Art. 74(1) AI Act. Art. 14(4) of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169/1 <<https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng>> last accessed 19 October 2025.

³⁵⁷ Art. 85 AI Act.

³⁵⁸ Art. 74(12) and (13) AI Act.

³⁵⁹ Art. 99 AI Act.

³⁶⁰ At the time of writing, the AI Act's provisions on high-risk AI systems were not yet applicable (see Art. 113 AI Act).

³⁶¹ Governance provisions entered into application on 2 August 2025 (see Art. 113(1)(b) AI Act).

³⁶² Art. 85 AI Act.

³⁶³ Art. 50 AI Act.

³⁶⁴ Art. 86 AI Act.

³⁶⁵ Khare and others (n 17) 12. See also p. 15.

³⁶⁶ Margot E. Kaminski and Gianclaudio Malgieri, 'The Right to Explanation in the AI Act' (2025) University of Colorado Law Legal Studies Research Paper No. 25-9, SSRN draft, 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5194301> last accessed 19 October 2025. See also Art. 22 GDPR and Case C-203/22 *Dun & Bradstreet Austria* [2025] ECLI:EU:C:2025:117.

³⁶⁷ Wachter, Mittelstadt and Floridi considered the impact of such limitations also in case a right to explanation were to be established in the future under the GDPR. They considered auditing of automated decision-making by trusted third parties as a key measure to overcome these limitations. Wachter, Mittelstadt, Floridi (n 6) 93, 98. See also: Case C-203/22 *Dun & Bradstreet Austria* [2025] ECLI:EU:C:2025:117, para 76.

systems are used.³⁶⁸ Affected persons could therefore complain to existing competent authorities, as well as seek judicial redress in front of national courts. While EU institutions, bodies, offices and agencies as well as Member States when implementing EU law are obliged to comply with the Charter,³⁶⁹ it should be noted that individuals could invoke some Charter rights also directly in disputes with providers and deployers who are not public authorities, as some fundamental rights enshrined in the Charter can have a horizontal direct effect. So far, the CJEU has established that the right to non-discrimination (Article 21 of the Charter), workers' right to limited working hours, rest periods and paid annual leave (Article 31(2) of the Charter) and right to an effective remedy and to a fair trial (Article 47 of the Charter) may have such an effect.³⁷⁰ The condition for it is, as noted by Lenaerts, that 'a Charter provision is sufficient in itself and does not need to be made more specific by other provisions of EU or national law to confer on individuals a right on which they may rely as such'.³⁷¹ Further rights could have such an effect too in the future.³⁷²

National courts could, through a request for a preliminary ruling under Article 267 of the TFEU, ask the CJEU for guidance on the interpretation of the AI Act. The CJEU could, ultimately, invalidate parts of the AI Act based on its incompatibility with the Charter.³⁷³ So far, there has been no ruling on the issue of emotion recognition either by the CJEU or the ECtHR, in light of which judgements the Charter has to be interpreted too. Strategic litigation could therefore also play an important role in the future. Ultimately, fundamental rights as broad and ever-evolving notions could help to ensure that emotion recognition systems are used only when necessary and proportionate.

3.2.1.3.3 *The review of prohibited and high-risk AI practices*

Another important instrument to ensure protection of fundamental rights in light of technological and societal developments is the possibility to review the list of prohibited AI practices and high-risk systems in Annex III. The Commission is empowered to propose

³⁶⁸ Recital 9 AI Act. See also: Paul Nemitz and Eike Gräf, 'Artificial Intelligence Must Be Used According to the Law, or Not at All' *Verfassungsblog* 28 March 2022 <<https://verfassungsblog.de/roa-artificial-intelligence-must-be-used-according-to-the-law/>> last accessed 19 October 2025.

³⁶⁹ Art. 51(1) of the Charter.

³⁷⁰ Lenaerts (n 333) 788. The author refers to relevant case law and Koen Lenaerts & Jose A. Gutiérrez-Fons, *The European Court of Justice as the Guardian of the Rule of "EU Social Law,"* in *A European Social Union: After the Crisis* 446 (Frank Vandenbroucke, Catherine Barnard & Geert De Baere eds., 2017).

³⁷¹ Lenaerts (n 333) 788. See e.g. also Case C-414/16 *Egenberger* [2018] ECLI:EU:C:2018:257, para 76: 'The prohibition of all discrimination on grounds of religion or belief is mandatory as a general principle of EU law. That prohibition, which is laid down in Article 21(1) of the Charter, is sufficient in itself to confer on individuals a right which they may rely on as such in disputes between them in a field covered by EU law (see, with respect to the principle of non-discrimination on grounds of age, judgment of 15 January 2014, *Association de médiation sociale*, C-176/12, EU:C:2014:2, paragraph 47).' See also para 78: '[I]t must be pointed out that, like Article 21 of the Charter, Article 47 of the Charter on the right to effective judicial protection is sufficient in itself and does not need to be made more specific by provisions of EU or national law to confer on individuals a right which they may rely on as such.'

³⁷² For example, as Dupré argues, the fact that human dignity is 'inviolable' and a foundational concept under Article 2 of the TEU as well as the Charter, as well as existing references to Article 3 ECHR case law in the CJEU case law on human dignity indicate the horizontal effect of human dignity (to be possibly developed also in future CJEU case law). Dupré (n 273) 19–20. As Lenaerts notes, the essence of further rights that satisfy the condition of being 'sufficient in itself' could have horizontal direct effect too based on the *a maiore ad minus* argument. Lenaerts (n 333) 789.

³⁷³ Cf. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238. In this case, the CJEU invalidated the Data Retention Directive (Directive 2006/24/EC) due to its infringement of the rights to privacy and data protection (para 69: 'it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.')

amendments, under Article 112(1) and (10) of the AI Act, once a year. In assessing the need for changes, the Commission should take into account information provided by Member States and their competent authorities as well as the European Parliament, Council and other relevant bodies and sources.³⁷⁴ The findings of the assessment need to be submitted to the European Parliament and the Council.³⁷⁵ In light of this, further restrictions could be imposed on the development and use of emotion recognition systems where evidence would show their adverse impact on fundamental rights.

3.2.2 The EU data protection acquis

3.2.2.1 The applicability of the EU data protection acquis

The EU data protection acquis will in principle apply to the development and use of emotion recognition systems whenever EU based controllers or processors process personal data or personal data of natural persons in the EU is processed (i.e. any operation is performed on such personal data, such as their collection, recording, storage, consultation, use or erasure³⁷⁶). More specifically, the GDPR applies to all activities falling within EU law, with exceptions applying if Member States process personal data for activities falling within the common foreign and security policy, if natural persons process personal data for purely personal or household activities (e.g. in terms of deployment, if an emotion recognition system processes personal data solely on a user device and the data is not transmitted outside of the device³⁷⁷) or if the processing takes place for law enforcement purposes³⁷⁸ (in the latter case, the LED applies³⁷⁹). The GDPR applies to all controllers and processors established in the EU as well as those established outside of the EU, if the processing activities are related to the offering of goods or services to data subjects in the EU or to the monitoring of data subjects' behaviour that takes place within the Union.³⁸⁰ In case the data is processed by Union institutions and bodies, the EUDPR applies.³⁸¹

In order to determine if and to what extent the EU data protection acquis applies to the development and use of emotion recognition systems, it must be first established whether data processed by such systems constitute 'personal data'. In addition, it needs to be considered whether stricter rules for the processing of sensitive personal data under the EU data protection acquis could apply to emotion recognition systems.³⁸²

³⁷⁴ Art. 112(8), (9) and (11) AI Act.

³⁷⁵ Art. 112(1) AI Act.

³⁷⁶ Art. 4(2) GDPR, Art. 3(1) LED, Art. 3(3) EUDPR.

³⁷⁷ Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (2015) 5 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> last accessed 19 October 2025.

³⁷⁸ Art. 2(2) GDPR.

³⁷⁹ Art. 2 LED.

³⁸⁰ Art. 3 GDPR. On the material and personal scope of application of the GDPR, see e.g.: Pierre Dewitte, 'AI Meets the GDPR' in Nathalie A. Smuha (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press 2025) 137–145.

³⁸¹ Art. 2 EUDPR.

³⁸² Art. 9 GDPR, Art. 10 LED, Art. 10 EUDPR.

3.2.2.1.1 Processing of personal data

Personal data is defined in EU data protection law as ‘any information relating to an identified or identifiable natural person’.³⁸³ When considering if a person is identifiable (i.e. it is possible to identify them, directly or indirectly, by distinguishing them from others within a group of persons³⁸⁴), all means that are reasonably likely to be used by the controller or someone else to identify the person need to be considered, including the costs and time required for it in light of available technology.³⁸⁵ The CJEU confirmed in *Nowak* that such information encompasses both objective and subjective information, such as opinions or assessments, as long as it is linked to the data subject.³⁸⁶ It also ultimately followed the Article 29 Working Party (WP29)’s view that different information can relate to a natural person – not only information about a person (‘content element’), but also data (likely to be) used for evaluating a person, treating them in a certain way or influencing their status or behaviour (‘purpose element’) or data that is likely to impact a person’s rights or interests (‘result element’).³⁸⁷ The CJEU considered over the years that different pieces of information constitute personal data, from telephone numbers³⁸⁸ to written answers during an exam and the examiner’s comments on them³⁸⁹ and in certain circumstances dynamic IP addresses.³⁹⁰ At the same time, however, anonymous data, i.e. information that cannot be linked (through an identifier³⁹¹) to a specific person, is excluded from the ambit of data protection law.³⁹² Achieving anonymisation is, however, challenging as risks for information being linked back to persons persist, to some extent even in the case of aggregated data.³⁹³ As Purtova concluded back in 2017 based on the analysis of the WP29’s opinion on the concept of personal data and the CJEU’s case law, everything therefore is or will become personal data in the future.³⁹⁴

Despite the broad notion of personal data under EU data protection law, Durovic and Corno for example questioned the applicability of this definition to emotion recognition systems.³⁹⁵

³⁸³ Art. 4(1) GDPR, Art. 3(1) LED, Art. 3(1) EUDPR.

³⁸⁴ Article 29 Data Protection Working Party (2007), ‘Opinion 4/2007 on the concept of personal data’ 01248/07/EN, 12.

³⁸⁵ Recital 26 AI Act, Recital 21 LED, Recital 16 EUDPR.

³⁸⁶ Case C-434/16 *Nowak* [2016] ECLI:EU:C:2017:994, paras 34, 35. See also: Article 29 Data Protection Working Party’s Opinion 4/2007 (n 384) 6.

³⁸⁷ Case C-434/16 *Nowak* [2016] ECLI:EU:C:2017:994, para 35. Article 29 Data Protection Working Party’s Opinion 4/2007 (n 384) 10–11. For an analysis of how the CJEU’s position changed from *YS and others* to *Nowak*, see: Nadezhda Purtova, ‘The law of everything. Broad concept of personal data and future of EU data protection law’ (2018) *Law, Innovation and Technology*, Volume 10, Issue 1, 66–72.

³⁸⁸ Case C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596.

³⁸⁹ Case C-434/16 *Nowak* [2016] ECLI:EU:C:2017:994,

³⁹⁰ Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779. See also: Lee A. Bygrave and Luca Tosi, ‘Article 4(1). Personal data’ in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 109–110.

³⁹¹ Art. 4(1) GDPR, Art. 3(1) LED, Art. 3(1) EUDPR list the following examples: ‘a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.

³⁹² Recital 26 AI Act, Recital 21 LED, Recital 16 EUDPR.

³⁹³ Andrea Gadotti and others, ‘Anonymization: The imperfect science of using data while preserving privacy’ (2024) *Science Advances*, Volume 10 Issue 29, 5–8, 17. The authors conclude that while there is evidence of individual level information being leaked from aggregate data, it is less clear how realistic such attacks are in practice (p. 17). See also: Purtova (n 387) 44. Article 29 Data Protection Working Party (2014), ‘Opinion 05/2014 on Anonymisation Techniques’ 0829/14/EN. See also: Vansh Narula, Kexin Feng, Theodora Chaspari, ‘Preserving Privacy in Image-based Emotion Recognition through User Anonymization’ (2020) *Proceedings of the 2020 International Conference on Multimodal Interaction (ICMI '20)*, 453. The authors acknowledge that user anonymisation is becoming significantly challenging with the uptake of multimodal behavioural data.

³⁹⁴ Purtova (n 387) 55–56, 78.

³⁹⁵ Durovic and Corno (n 53) 372, 375.

They noted that ‘the nature of the data collected by these systems is such that it often falls outside the meaning of “personal” data’.³⁹⁶ They considered that providers and deployers of such systems could easily fall outside the scope of data protection law by using anonymisation techniques that prevent the ‘singling out of a natural person’.³⁹⁷ Steindl also noted that systems only detecting information about a person’s emotions would fall outside the scope of the GDPR, reflecting on an example from Germany where the Bavarian data protection supervisory authority did not object a retailer’s use of a software that records customers age and gender for ad engagement, as in their view personal data were not processed by the system.³⁹⁸ Similarly, Häuselmann and others observed that providers tend to claim that their systems store only anonymised data such as age or gender, referring to the same German case.³⁹⁹ Research on different privacy-preserving techniques is indeed on-going in the field of emotion recognition, looking for example at how to preserve user privacy in image-,⁴⁰⁰ speech-⁴⁰¹ or gait-based⁴⁰² emotion recognition.

This is, however, a restrictive interpretation of the GDPR.⁴⁰³ It can be argued that data processed by emotion recognition systems, as long as they can be linked back to a person through reasonable means, constitute personal data. In this context, it is also important to consider all data that are processed when a person is subjected to emotion recognition systems. For example, as soon as the system processes facial images to extract facial expressions, this would amount to personal data processing.⁴⁰⁴ Even if the personal data is immediately deleted or anonymised (e.g. by noise being added to it or filtering being applied⁴⁰⁵), the initial processing (including the deletion and anonymisation process) would need to comply with data protection law.⁴⁰⁶ As WP29 noted, anonymisation of personal data itself constitutes processing and needs to therefore comply with data protection law.⁴⁰⁷ There seems to be a misconception that this is not the case in practice. As McStay pointed out, providers of emotion recognition systems using soft biometrics frequently claim that in such cases a person is not identified in the process of emotion recognition.⁴⁰⁸ He, however, considers that such data should be ‘considered personal upfront’,⁴⁰⁹ in light of the EDPS

³⁹⁶ Ibid, 372.

³⁹⁷ Ibid, 377.

³⁹⁸ Steindl (n 30) 314. Heike Anger, ‘Gesichtsscan im Supermarkt ist unbedenklich’, *Handelsblatt* (12 June 2017) <www.handelsblatt.com/politik/deutschland/datenschuetzer-zu-real-werbebildschirm-gesichtsscan-im-supermarkt-ist-unbedenklich/19921456.html> last accessed 19 October 2025. Such systems are indeed being offered in practice. See e.g. the website of a provider: Reco 3.26, ‘Emotion Recognition’ <www.reco326.com/en/solutions/smart-recognition/emotion-recognition> last accessed 19 October 2025.

³⁹⁹ Häuselmann and others (n 17) 3.

⁴⁰⁰ Narula, Feng, Chaspari (n 393) 452–460.

⁴⁰¹ Vasileios Tsouvalas, Tanir Ozcelebi, Nirvana Meratnia, ‘Privacy-preserving Speech Emotion Recognition through Semi-Supervised Federated Learning’ (2022) arXiv:2202.02611 <<https://arxiv.org/abs/2202.02611>> last accessed 19 October 2025.

⁴⁰² Carmen Bisogni and others, ‘Walk as you feel: Privacy preserving emotion recognition from gait patterns’ (2024) *Engineering Applications of Artificial Intelligence*, Volume 128.

⁴⁰³ Michael Veale and Frederik Zuiderveen Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act’ (2021) *Computer Law Review International*, Volume 22, Issue 4, 107.

⁴⁰⁴ The Article 29 Working Party has for example stated in its 2007 Opinion on the concept of personal data that images of individuals can be personal data to the extent a person is recognisable on them. Article 29 Data Protection Working Party’s Opinion 4/2007 (n 384) 8.

⁴⁰⁵ For an overview of some anonymisation techniques, see: Narula, Feng, Chaspari (n 393) 453–454.

⁴⁰⁶ For an explanation of the concept of ‘processing’, see Art. 4(2) GDPR, Art. 3(2) LED, Art. 3(3) EUDPR and Bygrave and Tosoni (n 390) 109–110.

⁴⁰⁷ Article 29 Data Protection Working Party’s Opinion 05/2014 (n 393) 3, 7.

⁴⁰⁸ McStay (n 17) 1.

⁴⁰⁹ Ibid, 3.

Opinion 4/2015 that highlighted the limitations of data anonymisation in the context of big data.⁴¹⁰

In addition, using privacy preserving techniques might still imply the processing of personal data. For example, a paper dealing with privacy preserving gait-based emotion recognition considered that a system preserves privacy by not relying on facial cues. At the same time, it acknowledges that gait can be used for remote identification.⁴¹¹ This confirms that this is personal (biometric) data, and the system still processes personal data, even if not processing facial cues. The means required for the identification might be however more sophisticated.

In addition, even if the system captures data that may not amount to personal data, if such systems process this data together with other identifiers (such as a person's location or IP address), this could be used to create a profile about the person and to identify them.⁴¹² The CJEU confirmed in *Breyer* that not all information that enables the identification 'must be in the hands of one person'.⁴¹³ The question is therefore how reasonably likely it is that the means that could lead to the identification will be used.⁴¹⁴ If the provider or deployer would put in place appropriate technical and organisational measures that a person subjected to an emotion recognition system could not be identified neither by them nor someone else through reasonable means (i.e. anonymises the data), the data processing would fall – if the data is collected in an anonymous way/once the data is anonymised – outside the scope of EU data protection law. This needs to be assessed on a case-by-case basis.⁴¹⁵ It seems, however, difficult to conceive situations where data protection law would not apply at least at some stage of emotion recognition through AI systems, as at least the capturing of the data would be presumably linked to processing personal data or other identifiers. The data about a person also does not need to be true in order to amount to personal data,⁴¹⁶ which is important to note in light of the disputed scientific basis of emotion recognition systems. To conclude, as indicated in Table 2, which includes the most commonly processed data by emotion recognition systems, these data will always amount to personal data if the data can relate to an identifiable person, i.e. they can be linked to them.

3.2.2.1.2 Processing of sensitive data

The EU data protection acquis grants special protection to sensitive data, the processing of which could create significant risks to the fundamental rights and freedoms of persons.⁴¹⁷ It defines sensitive data as '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'. While the data

⁴¹⁰ Ibid, 3.

⁴¹¹ Bisogni and others (n 402) 1–2.

⁴¹² Recital 30 GDPR, Recital 18 EUDPR. See also: Ienca and Malgieri (n 278) 8. The authors conclude that 'mental data, in combination with other data that allow to single out a data subject, are personal data.'

⁴¹³ Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779, para. 43. See also: Luca Tosoni and Lee A. Bygrave, 'Article 4(2). Processing' in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 116–122.

⁴¹⁴ See: Article 29 Data Protection Working Party's Opinion 4/2007 (n 384) 15–17. Purtova (n 387) 46–47, 64–65. As Purtova notes, the CJEU considered in *Breyer*, in contradiction to the WP29, that identification is not reasonably likely if it is prohibited by law, i.e. data breaches are excluded from this criterion (pp. 64–65).

⁴¹⁵ See: Article 29 Data Protection Working Party's Opinion 4/2007 (n 384) 17, 21.

⁴¹⁶ Article 29 Data Protection Working Party's Opinion 4/2007 (n 384) 6.

⁴¹⁷ Recital 51 GDPR, Recital 37 LED, Recital 29 EUDPR.

protection acquis does not define emotions as sensitive data explicitly, which some authors consider as a ‘lack of comprehensive protection’,⁴¹⁸ both the input data that such systems process (such as facial images/expressions, voice/speech, or brain data – see Chapter 2) and the output data of such systems (information about ‘emotions’ of a person)⁴¹⁹ could be considered sensitive. Häuselmann and others have for example argued that only emotion recognition systems that process physiological information, and do not use visual approaches, would amount to sensitive data under Article 9 GDPR.⁴²⁰ This approach requires, however, further nuancing. Keeping in mind that information revealing sensitive data indirectly can fall under Article 9 if processed to deduce such data,⁴²¹ input and/or output data of emotion recognition systems could amount to sensitive data under the EU data protection acquis in particular under the following three scenarios.

First, emotion recognition systems could process biometric data that enables the unique identification of a person. Overall, as explained under Sub-section 2.2.4, the definition of ‘biometric data’ under the EU data protection acquis is narrower than the one under the AI Act, as such data needs to allow/confirm the unique identification of a person,⁴²² meaning they need to be unique to a person and measurable.⁴²³ While emotion recognition systems can process data that could allow for such identification or verification (for example facial images or voice),⁴²⁴ they would amount to biometric data under data protection law only if undergoing technical processing aimed at biometric verification or identification, in addition to ‘recognising’ emotions.⁴²⁵ In addition, only biometric data processed for identification (and not verification purposes) amount to sensitive data under EU data protection law.⁴²⁶ This indicates the limited applicability of the concept of biometric data under data protection law to emotion recognition systems. While some of the input data processed by such systems could be used to uniquely identify persons subjected to the system, the data would be presumably rarely processed in such a way. The processing would thereby need to be done through specific technical means allowing for the unique identification of the person (i.e. the data would need to be compared against previously captured templates in a reference database to establish that the person from whom a specific emotion is being inferred is indeed the person in the database).⁴²⁷

Second, health data, i.e. personal data that relate to the physical or mental health of a person,⁴²⁸ could be processed by such systems. Health data are subject to specific protections due to their potential to reveal very intimate and private information about persons, which

⁴¹⁸ Häuselmann and others (n 17) 1.

⁴¹⁹ See: McStay and Urquhart (n 68) 2. McStay (n 17) 2.

⁴²⁰ Häuselmann and others (n 17) 3–4.

⁴²¹ Ludmila Georgieva and Christopher Kuner, ‘Article 9. Processing of special categories of personal data’ in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 373–374. Referring to WP29’s Advice Paper on Special Categories of Data and EDPB’s Guidelines 3/2019.

⁴²² Art. 3(34) AI Act, Art. 4(14) GDPR, Art. 3(13) LED, Art. 3(18) EUDPR.

⁴²³ Article 29 Data Protection Working Party’s Opinion 4/2007 (n 384) 8.

⁴²⁴ As McStay and Urquhart note, emotion recognition shifts the focus of identification-based harms (that occur for example with facial recognition) to intention-based harm, as they try to recognise the intentions of individuals. McStay and Urquhart (n 68) 7.

⁴²⁵ See: *ibid.*

⁴²⁶ For an analysis of biometric data under the GDPR, see: Bygrave and Tosoni (n 139) 207–216. See also: Häuselmann and others (n 17) 4.

⁴²⁷ Recital 51 GDPR. For an explanation of the process of specific technical processing, see: Bygrave and Tosoni (n 139) 212.

⁴²⁸ Art. 4(15) GDPR, Art. 3(14) LED, Art. 3(19) EUDPR.

could lead to stigma and discrimination if revealed.⁴²⁹ The concept of health data needs to be interpreted broadly, in line with Recital 35 of the GDPR, Recital 24 of the LED and Recital 31 of the EUDPR and the jurisprudence of the CJEU. The Court stated in *Lindqvist* that the notion of 'data concerning health' must cover all aspects of a person's physical and mental health.⁴³⁰ WP29 further clarified that in order for data to qualify as health data, it is not necessary that systems processing them are used or marketed as medical systems or that the data are reliable and accurate.⁴³¹

When it comes to data used by emotion recognition systems, these could amount to health data, as explained in Table 2 below. While Steindl noted that data about emotions as such does not amount to health data⁴³² and Häuselmann and others considered that only physiological data used to infer emotions amounts to health data,⁴³³ other input and output data could contain information about a person's physical or mental health too. For example, the lack of facial expressions could signal underlying medical conditions⁴³⁴ or written text could contain information about a person's health. Also vice versa, data showing the absence of any underlying medical conditions can be also considered health data.⁴³⁵

Even if data recorded seem to not lead to any conclusions about a person's health (for example a single recording of a person's alleged emotional stage), this can change subject to the processing modalities – WP29 clarified that raw sensor data that seems innocuous may also amount to health data if 'tracked over a period of time, combined with other data, or transferred to other data parties who have access to additional complementary datasets.'⁴³⁶ For example, health information (regardless of whether it is accurate or reliable) could be extracted from the data an emotion system processes, e.g. if a person is frequently labelled as being sad, which could lead to conclusions about underlying medical conditions.⁴³⁷

Third, emotion recognition systems could in some cases process other sensitive data, for example if processing text or speech that contain information about a person's political opinions, religious or philosophical beliefs, trade union membership or their sex life or sexual orientation, or if processing facial images that could reveal a person's racial or ethnic origin or religious beliefs. Physiological data, which would amount to health data, could indicate some other sensitive data too – research has been for example conducted on racial differences in ECG characteristics.⁴³⁸ Such sensitive data could be detected also from the context of deployment, for example if monitoring people's 'emotions' at political events.⁴³⁹

Ultimately, it should be also noted that in order for data to amount to sensitive data, they must in the first place constitute personal data, as described under Section 3.2.2.1.1. While this is

⁴²⁹ Lee A. Bygrave and Luca Tosoni, 'Article 4(15). Data concerning health' in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 218.

⁴³⁰ Case C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596, para 50. See: Bygrave and Tosoni (n 429) 221.

⁴³¹ Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (n 377) 2, 4.

⁴³² Steindl (n 30) 313.

⁴³³ Häuselmann and others (n 17) 3–4.

⁴³⁴ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 4.

⁴³⁵ Ienca and Malgieri (n 278) 9.

⁴³⁶ Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (n 377) 3, 5.

⁴³⁷ See also: EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 4.

⁴³⁸ Rajalakshmi Santhanakrishnan and others, 'Racial Differences in Electrocardiographic Characteristics and Prognostic Significance in Whites Versus Asians' (2016) *Journal of the American Heart Association*, 5(3).

⁴³⁹ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 4.

usually the case, there might be situations where data could be processed in a way that does not allow for the identification of a data subject through reasonable means.⁴⁴⁰ Importantly, the categorisation of personal data as sensitive data implies that there needs to be the aim to deduce such sensitive data from it.⁴⁴¹ This could limit the applicability of provisions concerning sensitive personal data in practice. As Ienca and Malgieri note, not all mental data amount to sensitive data – emotions amount to sensitive data only if related to other sensitive data such as a person’s health status, sexuality or beliefs, which might often not be the case, pointing to a gap in the data protection regime.⁴⁴²

Table 2 provides an overview of how different input and output data processed by emotion recognition systems could be classified under the EU data protection acquis and AI Act, in light of issues discussed above. Often, no clear-cut line can be drawn, as the classification would depend on the purpose and functioning of the system (including use of privacy preserving techniques) as well as specific context of use. The applicability of data protection law to the development and use of emotion recognition systems would therefore need to be examined on a case-by-case basis.

Table 2: The applicability of GDPR and AI Act provisions to data processed by emotion recognition systems⁴⁴³

Data processed by emotion recognition systems		EU data protection acquis					AI Act
		Personal data	Biometric data	Sensitive biometric data	Health data	Other sensitive data	Biometric data
Input	Facial expressions	Yes*	Potentially **	Potentially ***	Potentially ****	Potentially *****	Yes
	Speech	Yes*	Potentially **	Potentially ***	Potentially ****	Potentially *****	Yes
	Gestures/posture	Yes*	Potentially **	Potentially ***	Potentially ****	No	Yes
	Keystroke, mouse and touchscreen movements	Yes*	Potentially **	Potentially ***	Potentially ****	No	Yes
	Written text	Yes*	No	No	Potentially ****	Potentially *****	No

⁴⁴⁰ See regarding the issue of whether biometric data constitute personal data: Bygrave and Tosoni (n 139) 215.

⁴⁴¹ See: Georgieva and Kuner (n 421) 374.

⁴⁴² Ienca and Malgieri (n 278) 10–11, 14.

⁴⁴³ See Arts. 4(1), (14) and (15), 9 GDPR; Arts. 3(1), (13) and (14), 10 LED, Art. 3(1), (18) and (19), 10 EUDPR; Art. 3(34) AI Act and the analysis and the corresponding sources above.

	Different physiological data ⁴⁴⁴	Yes*	Potentially **	Potentially ***	Yes	Potentially *****	Yes
Output	Emotions	Yes*	No	No	Potentially ****	No	No (but can include behavioural and physiological elements)

Notes:

* If the data can be linked to a specific person, which is likely the case

** If the data is processed in a way that extracts biometric data allowing/confirming the unique identification of a person

*** If used in addition only for biometric identification purposes

**** If revealing information relating to the physical or mental health of a person and processed to deduce such data

***** If revealing other sensitive data, such as racial or ethnic origin or political opinions, and processed to deduce such data

3.2.2.2 Requirements under data protection law

As soon as emotion recognition systems process personal data, a number of data protection law requirements applies to the development and use of such systems – notably concerning the lawfulness, fairness and accuracy of processing.⁴⁴⁵ The compatibility with some of them is questionable, in light of the purpose and functioning of such systems.

3.2.2.2.1 The lawfulness of processing

When it comes to be the lawfulness of processing,⁴⁴⁶ the processing of personal data needs to be based on one or more exhaustively listed legal grounds under EU data protection law,⁴⁴⁷ with further restrictions applying to the processing of sensitive data.⁴⁴⁸ The AI Act does generally not provide for legal grounds for the processing personal data.⁴⁴⁹

When it comes to the processing of all personal data, including if these were initially collected for other purposes,⁴⁵⁰ Article 6 of the GDPR foresees that these can be processed on the basis of the consent of the data subject, for the performance of a contract, the compliance with a legal obligation, if there is a need to protect vital interests of natural persons, for the performance of public tasks or in cases of legitimate interests of the controller or a third party. These grounds are further limited under the LED⁴⁵¹ and EUDPR.⁴⁵²

⁴⁴⁴ This relates to different changes in bodily functions that are being measured by emotion recognition systems. It is noted that biological material in itself is not personal data, only the data derived from it. See: Recital 35 GDPR and Bygrave and Tosoni (n 429) 223.

⁴⁴⁵ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 3–4.

⁴⁴⁶ Art. 5 GDPR, Art. 4 LED, Art. 4 EUDPR.

⁴⁴⁷ Art. 6 GDPR, Art. 8 LED, Art. 5 EUDPR.

⁴⁴⁸ Art. 9 GDPR, Art. 10 LED, Art. 10 EUDPR.

⁴⁴⁹ Recital 63 and Art. 2(7) AI Act.

⁴⁵⁰ Art. 6(4) AI Act. McStay and Urquhart (n 68) 6.

⁴⁵¹ Art. 8 LED. Under the LED, the only permitted ground is the performance of law enforcement tasks.

⁴⁵² Art. 5 EUDPR. Under the EUDPR, the grounds are the same as under the GDPR, with the exception of the legitimate interests of the controller or a third party.

Moreover, data processed by emotion recognition systems could amount to sensitive data, as demonstrated under Sub-section 3.2.2.1.2. The processing of such data is generally prohibited, unless complying with exhaustively listed exceptions under data protection law, such as to protect the vital interests of natural persons or in cases where the data was made manifestly public by the data subject.⁴⁵³ Such data processing needs to, as a pre-requisite, comply also with the legal basis requirements in Article 6 of the GDPR, Article 8 of the LED and Article 5 of the EUDPR.⁴⁵⁴

In this context, it is important to distinguish the processing of emotional data by public and private bodies. In the case of *public bodies*, it may be argued that, subject to the purpose of deployment, the legal basis could be the performance of public tasks, albeit it is questionable whether this could be necessary and proportionate in light of the disputed scientific basis of those systems and their intrusiveness.⁴⁵⁵ In any case, such processing would require a legal basis in EU or national law.⁴⁵⁶ In addition, if a legal basis could be established, the processing of sensitive data would be possible only in limited cases, for example for substantial public interest cases or the provision of healthcare.⁴⁵⁷ Ienca and Malgieri considered for example that it is quite difficult to imagine how there could be a substantial public interest for the processing of mental data.⁴⁵⁸ The controller could also not rely on the ground of the data being made public by the data subject (e.g. by entering the premises of a public authority deploying such systems to spot aggressive behaviour), unless the data subject realised such processing would be used.⁴⁵⁹

In the case of *private bodies*, consent could be the most likely legal basis. In such situations, consent must be freely given, specific, informed and unambiguous, pursuant to Article 4(11) of the GDPR,⁴⁶⁰ which is a high threshold, especially for untargeted deployments of emotion recognition systems for purposes such as advertising.⁴⁶¹ However, consent is not a valid legal basis in situations of power imbalances between the data subject and controller,⁴⁶² which means that the permitted medical and safety exceptions for emotion recognition use in the workplace and education institutions would need to be based on another legal ground. Regardless of the ground, proving the necessity and proportionality would be again challenging.⁴⁶³ Overall, it is difficult to construe a legal basis apart from consent⁴⁶⁴ and potentially contract performance⁴⁶⁵ for the use of emotion recognition systems by private parties, such as for healthcare, entertainment, customer care or advertising. The fundamental

⁴⁵³ Art. 9 GDPR, Art. 10 LED, Art. 10 EUDPR.

⁴⁵⁴ See Recital 51 of the GDPR and Georgieva and Kuner (n 421) 376.

⁴⁵⁵ See also: Waltraut Kotschy, 'Article 6. Lawfulness of processing' in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 336. See also: Electronic Privacy Information Center (n 88) 24.

⁴⁵⁶ Art. 6(3) GDPR, Art. 8(2) LED, Art. 5(2) EUDPR.

⁴⁵⁷ Art. 6 GDPR, Art. 8 LED, Art. 5 EUDPR.

⁴⁵⁸ Ienca and Malgieri (n 278) 14.

⁴⁵⁹ See on the ground of data being made manifestly public: Georgieva and Kuner (n 421) 378. Referring also to EDPB's Guidelines 3/2019.

⁴⁶⁰ See also Arts. 7 and 8 GDPR and Kotschy (n 455) 329–330.

⁴⁶¹ See also: McStay and Urquhart (n 68) 7–8.

⁴⁶² Recital 43 GDPR.

⁴⁶³ As Kotschy notes, proportionality and the respect for the essence of the right to data protection have to be achieved even where consent was given. Kotschy (n 455) 340.

⁴⁶⁴ Fieldwork by Andrew McStay also identified a consensus on the need for privacy protection and 'opt-in' consent among interviewed industry and civil society representatives interviewed on emotional AI. McStay (n 17) 10.

⁴⁶⁵ See: Kotschy (n 455) 330–332. See also: Ienca and Malgieri (n 278) 14.

rights of data subjects and their reasonable expectations would clearly override the legitimate interests of the controller in such settings.⁴⁶⁶ If a legal basis could be established, further restrictions apply for the processing of sensitive data. To the extent emotion recognition systems process health data, the key, and likely only, legitimate basis for it would be the affected person's explicit consent. WP29 underlined the importance of user consent for data processing that can lead to conclusions about their health.⁴⁶⁷ Ienca and Malgieri also concluded that the commercial processing of sensitive data can be based only on explicit and free consent, which would be more likely if data subjects' express their interest in the processing, for example for self-monitoring purposes.⁴⁶⁸ However, they note that previous research has shown the limits of terms of service in such contexts, as they often remain unread, uninformative and based on presumed consent.⁴⁶⁹

3.2.2.2.2 *The fairness of processing*

Even if there is a basis for processing such data, the development and use of emotion recognition systems can be at odds with several other requirements under data protection law. For example, challenges can arise regarding the fairness of such processing due to the potential bias in such systems that could lead to discrimination (see Sub-section 3.2.1.2.6), and misclassification issues more broadly.⁴⁷⁰ The principle of fairness is further at stake if such systems are deployed in an untransparent manner, for manipulative purposes or in relationships of power asymmetry,⁴⁷¹ such as for example in a migration or law enforcement context. There were for example ideas to use emotion recognition for spotting persons posing a security risk at borders.⁴⁷² This seems questionable given the disputed scientific basis of such systems. As Durovic and Corno pose it, '[w]ould it be fair for people to be stopped and searched on the grounds of a particular detected emotion [...]?'⁴⁷³

3.2.2.2.3 *Accuracy requirements*

While data do not need to be true to be personal data,⁴⁷⁴ controllers and processors have an obligation of keeping data accurate and to erase or rectify inaccurate data without delay.⁴⁷⁵ According to technical experts, the accuracy of emotion recognition systems explored in studies so far has been quite high, reaching up to 100% in some cases.⁴⁷⁶ A review from 2022 acknowledged that, from a technical point of view, challenges exist if there is a 'partial occlusion or fake emotion expression' or if using physiological emotion recognition that is based on several complex signals.⁴⁷⁷ In this context, it has to be however underlined that

⁴⁶⁶ See Recital 47 GDPR. See also: Ienca and Malgieri (n 278) 14. Referring also to Article 29 Working Party and Irene Kamara and Paul De Hert.

⁴⁶⁷ Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (n 377) 4–5.

⁴⁶⁸ Ienca and Malgieri (n 278) 11.

⁴⁶⁹ Ibid, 12. Referring to Ienca, Haselager and Emanuel.

⁴⁷⁰ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 3.

⁴⁷¹ Häuselmann and others (n 17) 4–5.

⁴⁷² EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 1. See also: European Commission, 'Smart lie-detection system to tighten EU's busy borders' (n 39); Kate Crawford, 'Artificial Intelligence is Misreading Human Emotion' (n 55).

⁴⁷³ Durovic and Corno (n 53) 374.

⁴⁷⁴ See e.g. Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (n 377) 4.

⁴⁷⁵ Art. 5(1)(d) GDPR, Art. 4(1)(d) LED, Art. 4(1)(d) EUDPR.

⁴⁷⁶ Khare and others (n 17) 10–11.

⁴⁷⁷ Wang and others (n 13) 42.

accuracy will depend on the metrics used for its measurements. As explained in Sub-section 2.2.2, emotions are subjective phenomena that depend on the social and cultural context, therefore the whole concept of ‘correctly recognising them’ through AI systems is based on shaky scientific premises.⁴⁷⁸ This, coupled with technical limitations in the capturing of the data and its quality, can lead to wrong inferences about a person.⁴⁷⁹ Durovic and Corno also pointed out issues with determining what constitutes ‘accurate data’ under the GDPR in the context of emotion recognition systems, due to the premises on which such systems are designed (i.e. the output might be ‘accurate’ in terms of the theory on which the system is based and its design, but the theory itself might be flawed) and the inherent subjective nature of emotions.⁴⁸⁰ Similar issues and questions arise also under Article 15 of the AI Act, which contains requirements concerning system accuracy.⁴⁸¹

3.2.2.2.4 Other requirements

The development and use of emotion recognition systems would also need to comply with other data protection principles, including concerning transparency, purpose limitation, data minimisation, storage limitation and the confidentiality and integrity of the data,⁴⁸² and specific requirements contained in the GDPR, LED and EUDPR. For example, like with many other instances of personal data processing, also in such cases broader risks concerning the confidentiality and security of data exists, including due to a potential function creep. Providers and deployers therefore have to take appropriate safeguards.

3.2.2.2.5 Necessity and proportionality

Ultimately, as data protection law aims to further operationalise the right to data protection enshrined in Article 8 of the Charter and other fundamental rights,⁴⁸³ any interferences with this right need to be necessary and proportionate (see Sub-section 3.2.1.3). The EDPS underlined in its TechDispatch on facial emotion recognition the need for a careful assessment of whether the use of such technologies is necessary to achieve objectives pursued and whether there are less intrusive alternatives available, taking into account also the type of data collected, how the data are being retained and whether they could be further processed.⁴⁸⁴ Subsequently, the EDPS and EDPB considered that the use of emotion recognition systems is undesirable and called for their prohibition, unless used for health or research purposes where all data protection law requirements are met.⁴⁸⁵

3.2.2.3 Data protection in practice and the interplay with the AI Act

Data protection requirements can impact the development and use of emotion recognition systems in practice. The thesis will look more closely into three key aspects to this end: (1) the rights of data subjects that can enable them to challenge the use, (2) data protection impact assessments that providers and deployers of such system have to likely conduct as well as (3) the role of oversight and enforcement in upholding data protection safeguards.

⁴⁷⁸ See: McStay and Urquhart (n 68) 7.

⁴⁷⁹ EDPS, ‘TechDispatch #1/2021 - Facial Emotion Recognition’ (n 12) 3. See also: Häuselmann and others (n 17) 5.

⁴⁸⁰ Durovic and Corno (n 53) 378–379, 390, 394–395.

⁴⁸¹ Ibid, 390.

⁴⁸² Art. 5 GDPR; Art. 4 LED; Art. 4 EUDPR.

⁴⁸³ See Recitals 1 and 2 GDPR, Recitals 1 and 2 LED, Recital 1 EUDPR.

⁴⁸⁴ EDPS, ‘TechDispatch #1/2021 - Facial Emotion Recognition’ (n 12) 2–3.

⁴⁸⁵ EDPS - EDPB Joint Opinion on the AI Act proposal (n 56) 13.

3.2.2.3.1 Data subject rights

Under data protection law, personal data needs to be processed in a transparent manner. Data subjects have to be informed about the processing of their personal data in a clear manner. They also have certain rights to control the processing of their data, including by having a right to access their data and request their rectification and erasure.⁴⁸⁶ Some exceptions, as long as necessary and proportionate, apply in the field of law enforcement to not endanger on-going law enforcement work, protect public and national security as well as the rights and freedoms of others.⁴⁸⁷ With emotion recognition, issues arise if data subjects are not aware of such processing, including its duration, and therefore cannot exercise control over it.⁴⁸⁸ Deployers might diverge in their transparency and information provision practices. A recent survey by the Dutch Department for the Coordination of Algorithmic Oversight among approximately 30 customer service organisations showed that organisations using emotion recognition do not immediately disclose such use when interacting with customers and rather give general announcements or explain the use upon an explicit request.⁴⁸⁹ Häuselmann and others also raise concerns over the limited applicability of Articles 13 and 14 of the GDPR (as well as the AI Act's transparency provisions) with inferred data. In this context, the controller only needs to provide information about the purpose of the data processing and categories of data being inferred to the data subject, and not specific emotions inferred.⁴⁹⁰ Despite the information provision requirements being limited, informing data subjects about such data processing that aims at inferring their emotions in a clear manner can facilitate the exercise of their other rights under the data protection acquis and of further remedies.

Importantly, data subjects have also a right to not be subjected to automated individual decision-making, including profiling, unless authorised by national law with suitable safeguards in place, or in the case of the GDPR and EUDPR also where such processing is necessary for entering into or performing a contract or if it is based on the data subject's explicit consent.⁴⁹¹ Nevertheless, such decisions must not be based on sensitive data, unless processed on the basis of explicit consent or for reasons of substantial public interest, with suitable measures to protect the person's rights and legitimate interests in place.⁴⁹² The latter can be, as Durovic and Corno note, challenging, as the scientific basis of emotion recognition is being disputed, therefore also any kind of measures to ensure accurate and trustworthy results seem difficult.⁴⁹³ In cases of automated individual decision-making, data subjects have a right to receive relevant information which allows them to understand the decision in a

⁴⁸⁶ Recitals 58, 60, Art. 5(1)(a), Chapter III GDPR, Recitals 20, 35, Art. 4(1)(a), Chapter III EUDPR. See also: Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (n 377) 6. The WP29 underlined that when it comes to the processing of health data, the controller needs to inform the data subjects among others if the data collected in apps and devices will be combined with other data from the device or third parties and what are the consequences of it.

⁴⁸⁷ Recital 26, Art. 13 and the rest of Chapter III LED.

⁴⁸⁸ EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition' (n 12) 3.

⁴⁸⁹ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 46.

⁴⁹⁰ Häuselmann and others (n 17) 5–6. In reaching this conclusion, they refer also to: Sandra Wachter, Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019). *Columbia Business Law Review*, 2019(2) and WP29's Guidelines on transparency under Regulation 2016/679.

⁴⁹¹ Art. 22 GDPR, Art. 11 LED, Art. 24 EUDPR.

⁴⁹² Art. 22(4) GDPR, Art. 24(4) EUDPR. Under Art. 11 LED, which in any case further restricts the grounds for the automated individual decision-making, basing such processing on sensitive data is prohibited unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

⁴⁹³ Durovic and Corno (n 53) 381.

concise, transparent, intelligible and easily accessible form.⁴⁹⁴ This was affirmed by the CJEU in *Dun & Bradstreet Austria*,⁴⁹⁵ which brought some clarity on the matter.⁴⁹⁶ However, as is the case with emotion recognition, often no individual decision might be taken or such decisions might not be automated.⁴⁹⁷

3.2.2.3.2 *Data protection impact assessment*

Next to guaranteeing rights of data subjects, the data protection acquis includes a number of safeguards with which providers and deployers of emotion recognition systems have to comply. One of them is a data protection impact assessment (DPIA), which will be likely required if developing and using such systems.⁴⁹⁸ The DPIA is needed, based on the WP29's guidelines, when innovative technologies are used in combination with another criteria such as sensitive data processing (which is broader than the definition of sensitive data under Art. 9 of the GDPR), the evaluation or scoring of the data subject (including profiling and predicting), their systematic monitoring or if data of vulnerable data subjects is processed.⁴⁹⁹

This means that all providers and deployers of emotion recognition systems will have to conduct a DPIA to assess risks to the rights and freedoms of data subjects and ultimately necessity and proportionality of developing and using such systems.⁵⁰⁰ This would require a thorough reflection on issues discussed in this Sub-section as well as Sub-section 3.2.1.2. As Ienca and Malgieri note, the DPIA is an important accountability safeguard that applies regardless of whether the data processed are considered sensitive or not.⁵⁰¹ It also complements the FRIA under the AI Act (discussed in Sub-section 3.2.1.3.1) with its broader personal scope, as it applies to all controllers.

3.2.2.3.3 *The role of oversight and enforcement*

To ensure the effective protection of rights and freedoms of people affected by emotion recognition systems, external oversight of such systems is key. Under the EU data protection acquis, supervisory authorities can start investigations into such systems following a complaint by data subjects⁵⁰² or *ex officio*.⁵⁰³ They can issue administrative fines, which are higher for infringements of rules pertaining to the processing of sensitive data,⁵⁰⁴ and/or other applicable penalties.⁵⁰⁵

To date, there were a few cases where the use of emotion recognition was scrutinised by supervisory authorities. In 2022, the Hungarian Data Protection Authority issued a fine of

⁴⁹⁴ Art. 12 GDPR.

⁴⁹⁵ Case C-203/22 *Dun & Bradstreet Austria* [2025] ECLI:EU:C:2025:117, paras 49–50.

⁴⁹⁶ See Wachter, Mittelstadt, Floridi (n 6) 76–99. The paper argues that no such right to an ex-post explanation of automated decision making can be derived from the GDPR's notification duties (Articles 13 and 14 GDPR), access right (Article 15 GDPR) or safeguards against automated decision-making (Article 22 GDPR).

⁴⁹⁷ Ienca and Malgieri (n 278) 16.

⁴⁹⁸ Art. 35 GDPR, Art. 27 LED, Art. 39 EUDPR. See also: McStay and Urquhart (n 68) 6.

⁴⁹⁹ Article 29 Data Protection Working Party (2017), 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' WP 248 rev.01, 9–11. See also: Ienca and Malgieri (n 278) 17.

⁵⁰⁰ Art. 35 GDPR, Art. 27 LED, Art. 39 EUDPR. See: Article 29 Data Protection Working Party (2017), 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' WP 248 rev.01, 4.

⁵⁰¹ Ienca and Malgieri (n 278) 15.

⁵⁰² Art. 77 GDPR, Art. 52 LED, Art. 63 EUDPR.

⁵⁰³ Art. 57(1)(h) GDPR, Art. 46(1)(i) LED, Art. 57(1)(f) EUDPR.

⁵⁰⁴ Art. 83 GDPR, Art. 66 EUDPR.

⁵⁰⁵ Art. 84 GDPR, Art. 57 LED.

approximately 700,000 EUR to a bank that used an AI-based emotion analysis system for customer service calls to identify customers' dissatisfaction. In this *ex officio* investigation, it found that the bank did not establish a valid legal basis for the processing, as legitimate interest could not serve as a legal basis. It also considered that the controller did not adequately balance out interests at stake, inform data subjects as well as adopt adequate safeguards for the system's use.⁵⁰⁶ Another example comes from Italy, where the DPA imposed a temporary limitation on the AI companion app Replika due to its unclear legal basis.⁵⁰⁷ The DPA ultimately fined the company behind Replika with a 5 million EUR fine in 2025.⁵⁰⁸ In 2023, the DPA also fined a municipality which used an AI system to gain insights into museum visitors and their interactions with exhibited art, including through observing their emotions, without a proper legal basis.⁵⁰⁹

Ultimately, affected persons can also pursue judicial remedies, both against the decision of the supervisory authority and against the controller and/or processor directly.⁵¹⁰ No litigation on emotion recognition systems reported on internationally seems to have taken place so far.⁵¹¹

Despite limited oversight cases and litigation in practice, the EDPS and EDPB made it clear in their opinion on the AI Act that emotion recognition systems should be prohibited unless they are used for well-defined health or research purposes which comply with all data protection conditions and limits.⁵¹² It is therefore difficult to construe how the use of emotion recognition systems could generally meet requirements of lawfulness and necessity and proportionality under data protection law,⁵¹³ except for some narrowly defined and justified use cases.

⁵⁰⁶ GDPRhub, 'NAIH (Hungary) - NAIH-85-3/2022' 24 April 2022

<[https://gdprhub.eu/index.php?title=NAIH_\(Hungary\)_-_NAIH-85-3/2022](https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022)> last accessed 19 October 2025.

⁵⁰⁷ GDPRhub, 'Garante per la protezione dei dati personali (Italy) – 9852214' 3 February 2023

<[https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9852214](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214)> last accessed 19 October 2025.

⁵⁰⁸ EDPB, 'AI: the Italian Supervisory Authority fines company behind chatbot "Replika"' 21 May 2025

<www.edpb.europa.eu/news/national-news/2025/ai-italian-supervisory-authority-fines-company-behind-chatbot-replika_en> last accessed 19 October 2025.

⁵⁰⁹ GDPRhub, 'Garante per la protezione dei dati personali (Italy) – 9896808' 13 April 2023

<[https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9896808](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9896808)> last accessed 19 October 2025.

⁵¹⁰ Arts. 78, 79 GDPR; Arts. 53, 54 LED; Art. 64 EUDPR.

⁵¹¹ The research did not reveal any such cases, neither reported on in existing literature nor through targeted searches in relevant databases.

⁵¹² EDPS - EDPB Joint Opinion on the AI Act proposal (n 56) 13.

⁵¹³ See also: Electronic Privacy Information Center (n 88) 9.

4 Conclusions: Emotion recognition *de lege ferenda*

The development and use of emotion recognition systems, which aim to infer emotions of people based predominantly on their physiological and behavioural characteristics, are on the rise, leading to increased attention by legal scholars, civil society, oversight bodies and regulators, among others. These systems can be used for numerous purposes, ranging from entertainment and wellbeing to border control and law enforcement.⁵¹⁴ While their scientific basis, especially regarding inferences of emotions from facial expressions, is being heavily disputed, their development and prospect to achieve accurate models, allowing to infer the innermost states of persons, continue.⁵¹⁵ The strive for scientific robustness of such systems will however not solve the criticism they are facing – on the contrary, it will enhance concerns about their intrusiveness and impact on people's fundamental rights.⁵¹⁶

The AI Act recognises the risks that such systems can pose to fundamental rights. It generally prohibits their use in two settings typically marked by asymmetrical relationships, namely workplace and education institutions, unless used for medical or safety reasons.⁵¹⁷ In all other instances, emotion recognition systems are considered to be high-risk and require additional transparency measures.⁵¹⁸ The present thesis demonstrates, however, that the AI Act's application to emotion recognition systems is limited in practice, due to some rather restrictive definitions, including of the very notion of 'emotion recognition systems' itself, and exceptions from the AI Act's scope.

The AI Act does however not apply to emotion recognition systems in a vacuum. Other applicable EU and national law continue to apply to their development and use.⁵¹⁹ This raises the question of the extent to which emotion recognition systems, which are not prohibited by the AI Act, can be permitted under EU fundamental rights law and more specifically the EU data protection acquis. The thesis points out a number of challenges in this regard. While providers and (certain) deployers need to comply with fundamental rights obligations explicitly under the AI Act and also more broadly under other applicable law, the application of data protection law to emotion recognition systems is less clear. The thesis argues that, due to a broad notion of personal data processing, the development and use of such systems would likely fall under EU data protection law. However, as also noted by several scholars,⁵²⁰ the more restrictive rules concerning the processing of sensitive data would apply less frequently to such systems. Overall, the development and use of permitted emotion recognition systems under the AI Act might adversely impact many fundamental rights and be incompatible with several data protection principles and requirements. They may be often at odds with necessity and proportionality requirements under fundamental rights and data protection law.⁵²¹

Nevertheless, the assessments of whether the development and use of emotion recognition systems that are not prohibited under the AI Act is permitted under fundamental rights and data protection law leaves some room for interpretation. This interpretation is being further defined by oversight bodies, and ultimately courts. To uphold a high protection of fundamental

⁵¹⁴ See (n 30).

⁵¹⁵ See Sub-section 2.1 and in particular: Feldman Barrett and others (n 53) 1, 3, 48–49.

⁵¹⁶ See also: Durovic and Corno (n 53) 382.

⁵¹⁷ Art. 5(1)(f) AI Act.

⁵¹⁸ Art. 50 and Annex III AI Act.

⁵¹⁹ Recital 9 AI Act and (n 257).

⁵²⁰ See: Häuselmann and others (n 17) 3–4; Steindl (n 30) 313; Ienca and Malgieri (n 278) 10–11, 14.

⁵²¹ See the analysis and corresponding references in the relevant sub-section.

rights, which is also one of the objectives of the AI Act,⁵²² the following aspects of the current regulatory regime would therefore warrant further attention and consideration.

First, while it is to some extent understandable that the AI Act aims to draw a distinction between systems processing emotions and intentions on the one hand, and physical states and readily apparent expressions, gestures and movements on the other, this distinction may lead to loopholes in practice.⁵²³ The definition of emotion recognition systems under the AI Act should therefore be interpreted broadly, and not circumvented by narrow interpretations that focus solely on systems that aim at inferring the emotions and intentions of persons, but also on systems aimed at inferring other innermost states of persons.⁵²⁴ This could be done through a broad interpretation of ‘intentions’, which remain largely undefined. It should be also noted that several fundamental rights issues arise also with the processing of outward behaviours, without making conclusions about people’s innermost states, especially when used for profiling.⁵²⁵ A linked issue to that are LLMs which aim to emulate empathy, which might not fulfil the definition of emotion recognition systems under the AI Act as they do not label emotions.⁵²⁶ However, trying to decode someone’s inner world, especially through signals not noticeable to other humans as is the trend with (multimodal) emotion recognition system development, amounts to an even higher level of intrusion.⁵²⁷

Second, it is important to consider what can be the potential interests in emotion recognition – whether it happens in public interest, due to the private interests of affected persons or purely for commercial interests.⁵²⁸ Except for private interests of affected persons, under appropriate safeguards, it is difficult to conceive how the use of such scientifically disputed and intrusive technologies could be justified solely by public or commercial interests.⁵²⁹ Therefore, as already proposed to various degrees by several stakeholders,⁵³⁰ and indeed following arguments in Recital 44 of the AI Act,⁵³¹ it would be important to consider prohibiting the use of emotion recognition systems in relationships of power asymmetries, including for law enforcement,⁵³² asylum, migration, border control and public services purposes, where people could struggle to refuse such use.⁵³³ Exceptions in such relationships should be permitted solely for medical purposes, and based on the explicit consent of the person concerned or their legal representative, which needs to be free and informed,⁵³⁴ and be in full compliance with applicable law, including necessity and proportionality requirements under

⁵²² Art. 1(1) AI Act.

⁵²³ McStay and Bakir (n 46) 3–4.

⁵²⁴ See: Wendehorst and Duller (n 129) 21, 57, 71.

⁵²⁵ See: McStay and Bakir (n 46) 4.

⁵²⁶ See: *ibid.*, 4–5.

⁵²⁷ See: Durovic and Corno (n 53) 392.

⁵²⁸ Following the taxonomy of interests in data processing in Ienca and Malgieri (n 278) 8.

⁵²⁹ See also the discussion on the potential adverse impact on fundamental rights in Sub-section 3.2.1.2 and the lawfulness of processing under data protection law in Sub-section 3.2.2.2.1.

⁵³⁰ See Smuha and others (n 53) 56; Durovic and Corno (n 53) 400. See also civil society statements (n 83) and EDPS and EDPB (n 85).

⁵³¹ See also: Commission Guidelines on prohibited artificial intelligence practices (n 10) 81.

⁵³² In line with the old Roman law principle of *cogitationis poenam nemo patitur*, no one should be punished for their thoughts, and therefore, *mutatis mutandis*, emotions. See: Bublitz (n 288) 20.

⁵³³ See also: Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, ‘Report AI & Algorithms Netherlands’ (n 1) 37. As noted by the Dutch Department for the Coordination of Algorithmic Oversight, people could struggle refusing the use of emotion recognition systems in relationships marked by power imbalance, not only the workplace and education institutions, but also other areas ‘such as healthcare, public spaces or certain marketing contexts.’ See also: Bublitz (n 288) 24.

⁵³⁴ Article 3 Charter. See also Article 4(11) GDPR. See for more on this and rules governing instances of justified involuntary treatment e.g. Ligthart and others (n 128) 9–12. O’Callaghan and others (n 286) 10.

fundamental rights and data protection law. To this end, in line with suggestions by Ienca and Malgieri, it would be also beneficial if the data protection acquis would classify more explicitly emotions as sensitive personal data.⁵³⁵

The use of such systems in private (commercial) relationships, for example in the entertainment or wellbeing industry, might warrant some more flexibility when in the interest of the affected person in order to respect their autonomy. Nevertheless, the use in such contexts seems also potentially justifiable only when based on the person's explicit consent.⁵³⁶ It also requires strict compliance with other applicable law, including data protection rules,⁵³⁷ consumer law and transparency requirements under Article 50 of the AI Act. This is so especially as emotion recognition can be part of broader processes and an individual might not be aware of its role in outputs affecting them.⁵³⁸ Consequently, it would be important to consider to more explicitly spell out the prohibition of such use for purely commercial interests.

Overall, given the novel risks brought about by the advancement of emotion recognition systems, institutional regulation remains key.⁵³⁹ There is a need to ensure responsible innovation, including through institutional oversight and public scrutiny of such systems.⁵⁴⁰ Ultimately, emotions are part of our inner world, that we selectively, and often momentarily, choose to share with the outside world. And the law should help us to ensure that this remains our right also in the future.

⁵³⁵ Ienca and Malgieri (n 278) 11, 15.

⁵³⁶ The Dutch Department for the Coordination of Algorithmic Oversight e.g. also considered that consent is an important first step to ensure the responsible use of emotion recognition systems. Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 40. See Article 4(11) GDPR.

⁵³⁷ Due consideration needs to be given to all data protection principles contained in Article 5 of the GDPR, Article 4 of the LED and Article 4 of the EUDPR, as well as other applicable safeguards, including through the use of local storage and privacy preserving techniques. On the latter, see e.g.: Narula, Feng, Chaspari (n 393) 452. Ranya Aloufi, Hamed Haddadi, David Boyle, 'Emotionless: Privacy-Preserving Speech Analysis for Voice Assistants' (2019) arXiv:1908.03632 <<https://arxiv.org/abs/1908.03632>> last accessed 19 October 2025.

⁵³⁸ Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic oversight, 'Report AI & Algorithms Netherlands' (n 1) 37–38.

⁵³⁹ See: Durovic and Corno (n 53) 396–400.

⁵⁴⁰ See: *ibid.*, 400.

5 Annex I: Abstract in English and German

English:

In recent years, a growing trend of emotion recognition systems can be observed. At the same time, criticism about their scientific basis and reliability as well as intrusiveness is mounting. This led also to increased regulatory attention in such systems, resulting in the explicit regulation of AI-based emotion recognitions systems under the EU AI Act. The AI Act is, however, not the sole instrument regulating emotion recognition systems. Other applicable EU and national law continue to apply to their development and use. The master thesis examines the current state of development and use of emotion recognition systems and related criticism. It then analyses key pieces of the EU regulatory framework that govern emotion recognition systems – the EU AI Act, fundamental rights law, and data protection law. It explores three questions. First, it analyses the extent to which emotion recognition systems are covered by the AI Act and the different risk categories contained therein. It demonstrates that the AI Act's application to emotion recognition systems is limited in practice, due to some rather restrictive definitions and exceptions from the AI Act's scope. Second, the thesis explores the extent to which the development and use of emotion recognition systems can be permitted under EU fundamental rights law and more specifically the EU data protection acquis, whenever not prohibited by the AI Act. It shows that such development and use might adversely impact many fundamental rights and be incompatible with several data protection principles and requirements. They may be ultimately often at odds with necessity and proportionality requirements under both legal areas. Finally, the thesis sets forth some reflections and recommendations on the regulation of emotion recognition systems *de lege ferenda*, proposing their stricter regulation, including by prohibiting their use in asymmetrical power relationships and for purely commercial interests.

German:

In den letzten Jahren ist ein wachsender Trend von Emotionserkennungssystemen zu beobachten. Gleichzeitig nimmt die Kritik an ihrer wissenschaftlichen Grundlage und Zuverlässigkeit sowie ihrer Eingriffstiefe zu. Dies führte auch zu einer verstärkten regulatorischen Aufmerksamkeit gegenüber solchen Systemen, was zu einer ausdrücklichen Regulierung von KI-basierten Emotionserkennungssystemen im Rahmen der EU-Verordnung zur KI (KI-VO) führte. Die KI-VO ist jedoch nicht das einzige Instrument, das Emotionserkennungssysteme reguliert. Andere anwendbare EU- und nationale Rechtsvorschriften gelten weiterhin für das Anbieten oder Betreiben von solchen Systemen. Die Masterarbeit untersucht den aktuellen Stand der Entwicklung und Nutzung von Emotionserkennungssystemen und die damit verbundene Kritik. Anschließend analysiert sie die wichtigsten Elemente des EU-Rechtsrahmens, der Emotionserkennungssysteme regelt – die KI-VO sowie auch die grund- und datenschutzrechtlichen Anforderungen. Dabei werden drei Fragen untersucht. Zunächst wird analysiert, inwieweit Emotionserkennungssysteme unter der KI-VO und die darin enthaltenen verschiedenen Risikokategorien fallen. Die Arbeit zeigt, dass die Anwendung der KI-VO auf Emotionserkennungssysteme in der Praxis begrenzt ist aufgrund einiger recht restriktiver Definitionen und Ausnahmen von dem Anwendungsbereich der KI-VO. Zweitens untersucht die Arbeit inwieweit die Entwicklung und Nutzung von Emotionserkennungssystemen nach dem EU-Grundrecht und insbesondere nach dem EU-Datenschutzrecht zulässig ist, sofern dies nicht durch die KI-VO verboten ist. Sie zeigt, dass die Entwicklung und der Betrieb von solchen Systemen viele Grundrechte beeinträchtigen und mit mehreren Datenschutzgrundsätzen und -anforderungen unvereinbar sein könnten. Letztendlich stehen solche Systeme oft im Widerspruch zu den Anforderungen der Notwendigkeit und Verhältnismäßigkeit in beiden Rechtsbereichen. Abschließend enthält die Arbeit einige Überlegungen und Empfehlungen zur Regulierung von Emotionserkennungssystemen *de lege ferenda*. Eine strengere Regulierung, einschließlich eines Verbots der Verwendung von solchen Systemen in asymmetrischen Machtverhältnissen und für rein kommerzielle Interessen, ist vorgeschlagen.

6 Annex II: List of sources

6.1 Books

Martin Ebers and Karin Sein (eds.), *Privacy, Data Protection and Data-driven Technologies* (1st edition, Routledge 2024).

Lisa Feldman Barrett, Michael Lewis, Jeannette M. Haviland-Jones (eds.), *Handbook of Emotions* (4th edition, Guilford Press 2016).

Janneke Gerards (ed.), *Fundamental Rights, The European and International Dimension* (Cambridge University Press 2023).

Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

Daniel Moeckli, Sangeeta Shah, Sandesh Sivakumaran (eds.), *International Human Rights Law* (4th edition, Oxford University Press 2022).

Ceyhun Necati Pehlivan, Nikolaus Forgó, Peggy Valcke (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer 2024).

Steve Peers and others (eds.), *The EU Charter of Fundamental Rights: A Commentary* (2nd edition, Nomos 2022).

Nathalie A. Smuha (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press 2025).

6.2 Articles

Ranya Aloufi, Hamed Haddadi, David Boyle, 'Emotionless: Privacy-Preserving Speech Analysis for Voice Assistants' (2019) arXiv:1908.03632 <<https://arxiv.org/abs/1908.03632>> last accessed 19 October 2025.

Muhammad Anas Hasnul and others, 'Electrocardiogram-Based Emotion Recognition Systems and Their Applications in Healthcare—A Review' (2021) *Sensors* (Basel, Switzerland) vol. 21, 15 5015.

Mel Andrews, Andrew Smart, Abeba Birhane, 'The reanimation of pseudoscience in machine learning and its ethical repercussions' (2024) *Patterns*, Volume 5, Issue 9, 1–2.

Vian Bakir and others, 'On manipulation by emotional AI: UK adults' views and governance implications' (2024) *Frontiers in Sociology*, Volume 9.

Carmen Bisogni and others, 'Walk as you feel: Privacy preserving emotion recognition from gait patterns' (2024) *Engineering Applications of Artificial Intelligence*, Volume 128.

Jan Christoph Bublitz, 'Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right' (2014) *Archives for Philosophy of Law and Social Philosophy*, Volume 100, Number 1, 1–25.

Sze Chit Leong and others, 'Facial expression and body gesture emotion recognition: A systematic review on the use of visual data in affective computing' (2023) *Computer Science Review*, Volume 48, 100545.

Maarten den Heijer, Teun van Os van den Abeelen, Antanina Maslyka, 'On the Use and Misuse of Recitals in European Union Law' (2019) *Amsterdam Law School Research Paper* No. 2019-31.

Paul Ekman, 'An argument for basic emotions' (1992) *Cognition and Emotion*, 6(3–4), 169–200.

Lisa Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements' (2019) *Psychological Science in the Public Interest*, Volume 20, Number 1, 1–68.

Andrea Gadotti and others, 'Anonymization: The imperfect science of using data while preserving privacy' (2024) *Science Advances*, Volume 10 Issue 29.

Paul Graßl and others, 'Dark and Bright Patterns in Cookie Consent Requests' (2021) *Journal of Digital Social Research*, Volume 3, Number 1, 1–38.

Mélanie Gornet, Winston Maxwell, 'The European approach to regulating AI through technical standards' (2024) *Internet Policy Review*, Volume 13, Issue 3.

Atefeh Goshvarpour and Ateke Goshvarpour, 'The potential of photoplethysmogram and galvanic skin response in emotion recognition using nonlinear features' (2020) *Physical and Engineering Sciences in Medicine*, Volume 43, 119–134.

Eike Graef, Paul Nemitz, 'Addressing the Challenge of Protecting Fundamental Rights Through AI Regulation in the European Union' (2024) 71 *UCLA L. Rev. Disc.* 144.

Thomas Gremsl and Elisabeth Hödl, 'Emotional AI: legal and ethical challenges' (2022) *Information Polity* 27, 163–174.

Andreas Häuselmann and others, 'EU law and emotion data' (2023) *arXiv:2309.10776* <<https://arxiv.org/abs/2309.10776v1>> last accessed 19 October 2025.

Nora Hertz, 'Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought' (2023) *Neuroethics*, Volume 16, Article number 5.

Marcello Lenca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) *Life Sciences, Society and Policy*, Volume 13, Number 5.

Marcello Lenca and Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) *Journal of Law and the Biosciences*, Volume 9, Issue 1.

Agnes Jacob, 'Modelling speech emotion recognition using logistic regression and decision trees' (2017) *International Journal of Speech Technology*, Volume 20, 897–905.

Margot E. Kaminski and Gianclaudio Malgieri, 'The Right to Explanation in the AI Act' (2025) University of Colorado Law Legal Studies Research Paper No. 25-9, SSRN draft <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5194301> last accessed 19 October 2025.

Amelia Katirai, 'Ethical considerations in emotion recognition technologies: a review of the literature' (2023) *AI and Ethics*, Volume 4, 927–948.

Eugenia Kim and others, 'Age Bias in Emotion Detection: An Analysis of Facial Emotion Recognition Performance on Young, Middle-Aged, and Older Adults' (2021) AIES '21: AAAI/ACM Conference on AI, Ethics, and Society.

Smith K. Khare and others, 'Emotion Recognition and Artificial Intelligence: A Systematic Review (2014–2023) and Research Recommendations' (2024) *Information Fusion*, Volume 102, 102019.

Tadas Klimas, Jurate Vaiciukaite, 'The Law of Recitals in European Community Legislation' (2008) *ILSA Journal of International & Comparative Law*, Volume 15, Issue 1, 61–94.

Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) *German Law Journal*, Volume 20, Special Issue 6, 779–793.

Xiang Li and others, 'EEG Based Emotion Recognition: A Tutorial and Review' (2023) *ACM Computing Surveys*, Volume 55, Issue 4, 1–57.

Sjors Ligthart and others, 'Rethinking the Right to Freedom of Thought: A Multidisciplinary Analysis' (2022) *Human Rights Law Review*, Volume 22, Issue 4, December 2022, 1–14.

Taiba Majid Wani, 'A Comprehensive Review of Speech Emotion Recognition Systems' (2021) *IEEE Access*, Volume 9, 47795–47814.

Gianclaudio Malgieri and Marcello Ienca, 'The EU regulates AI but forgets to protect our mind', *European Law Blog*, 7 July 2021 <www.europeanlawblog.eu/pub/the-eu-regulates-ai-but-forgets-to-protect-our-mind/release/1> last accessed 19 October 2025.

Gianclaudio Malgieri and Cristiana Santos, 'Assessing the (Severity of) Impacts on Fundamental Rights' (2024) *Computer Law & Security Review*, 2025, forthcoming, SSRN version <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875937> last accessed 19 October 2025.

Kerry McInerney and Os Keyes, 'The Infopolitics of feeling: How race and disability are configured in Emotion Recognition Technology' (2024) *New Media & Society*, 27(7), 4246–4264.

Andrew McStay and Lachlan Urquhart, '“This time with feeling?” Assessing EU data governance implications of out of home appraisal based emotional AI' (2019) *First Monday*, Volume 24, Number 10.

Andrew McStay, 'Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy' (2020) *Big Data & Society*, Volume 7, Issue 1.

Andrew McStay and Vian Bakir, 'Soft law for unintentional empathy: addressing the governance gap in emotion-recognition AI technologies' (2025) *Journal of Responsible Technology*, Volume 23.

Ulises A. Mejias and Nick Couldry, 'Datafication' (2019) *Internet Policy Review*, Volume 8, Issue 4.

Vansh Narula, Kexin Feng, Theodora Chaspari, 'Preserving Privacy in Image-based Emotion Recognition through User Anonymization' (2020) *Proceedings of the 2020 International Conference on Multimodal Interaction (ICMI '20)*, 452–460.

Paul Nemitz and Eike Gräf, 'Artificial Intelligence Must Be Used According to the Law, or Not at All' *Verfassungsblog* 28 March 2022 <<https://verfassungsblog.de/roa-artificial-intelligence-must-be-used-according-to-the-law/>> last accessed 19 October 2025.

Patrick O'Callaghan and others, 'The right to freedom of thought: an interdisciplinary analysis of the UN special rapporteur's report on freedom of thought' (2023) *The International Journal of Human Rights*, Volume 28, Issue 1, 1–23.

OECD, 'Intellectual Property Issues in Artificial Intelligence Trained on Scraped Data' (2025) *OECD Artificial Intelligence Papers*, Number 33 <<https://doi.org/10.1787/d5241a23-en>> last accessed 19 October 2025.

Vagelis Papakonstantinou and Evangelos Zarkadoulas, 'Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement', *eu crim* issue 2/2023, 237–240 <<https://eucrim.eu/articles/remote-biometric-identification-and-emotion-recognition-in-the-context-of-law-enforcement/>> last accessed 19 October 2025.

Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) *Law, Innovation and Technology*, Volume 10, Issue 1, 40–81.

Mangesh Ramaji Kose, Mitul Kumar Ahirwal, Anil Kumar, 'A new approach for emotions recognition through EOG and EMG signals' (2021) *Signal, Image and Video Processing*, Volume 15, 1863–1871.

Lauren Rhue, 'Racial Influence on Automated Perceptions of Emotions' (2018) *SSRN* <<https://dx.doi.org/10.2139/ssrn.3281765>> last accessed 19 October 2025.

Javier Sánchez-Monedero and Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' (2022) *Information, Communication & Society*, Volume 25, Issue 3, 413–430.

Rajalakshmi Santhanakrishnan and others, 'Racial Differences in Electrocardiographic Characteristics and Prognostic Significance in Whites Versus Asians' (2016) *Journal of the American Heart Association*, 5(3).

Anvita Saxena, Ashish Khanna, Deepak Gupta, 'Emotion Recognition and Detection Methods: A Comprehensive Survey' (2020) *Journal of Artificial Intelligence and Systems* 2, 53–79 <<https://doi.org/10.33969/AIS.2020.21005>> last accessed 19 October 2025.

Nathalie A. Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (2021) SSRN <<http://dx.doi.org/10.2139/ssrn.3899991>> last accessed 19 October 2025.

Elisabeth Steindl, 'Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in Light of the Draft AI Act and its Interplay with the GDPR' (2022) *European Data Protection Law Review*, Volume 8, Number 2, 311–319.

Karim A. Tahboub, 'Intelligent Human-Machine Interaction Based on Dynamic Bayesian Networks Probabilistic Intention Recognition' (2006) *Journal of Intelligent and Robotic Systems* 45, 31–52.

Fatma M. Talaat, 'Real-time facial emotion recognition system among children with autism based on deep learning and IoT' (2023) *Neural Computing & Applications*, Volume 35, 12717–12728.

Vasileios Tsouvalas, Tanir Ozcelebi, Nirvana Meratnia, 'Privacy-preserving Speech Emotion Recognition through Semi-Supervised Federated Learning' (2022) arXiv:2202.02611 <<https://arxiv.org/abs/2202.02611>> last accessed 19 October 2025.

Sekar Vijayanthi, J. Arunnehru, 'Human Emotion Recognition from Body Posture with Machine Learning Techniques' in: Mayank Singh and others (eds.), *Advances in Computing and Data Sciences. ICACDS 2022* (Springer 2022).

Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) *Computer Law Review International*, Volume 22, Issue 4.

Sandra Wachter, Brent Mittelstadt, Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2019) *International Data Privacy Law*, Volume 7, Issue 2, 76–99.

Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) *Yale Journal of Law & Technology*, Volume 26, Issue 3.

Yan Wang and others, 'A systematic review on affective computing: emotion models, databases, and recent advances' (2022) *Information Fusion Volumes* 83–84, 19–52.

Liyang Yang, Sheng-Feng Qin, 'A Review of Emotion Recognition Methods From Keystroke, Mouse, and Touchscreen Dynamics' (2021) *IEEE Access*, Volume 9, 162197–162213.

Qiang Zhang and others, 'Respiration-based emotion recognition with deep learning' (2017) *Computers in Industry*, Volumes 92–93, 84–90.

Jia Zheng Lim, James Mountstephens, Jason Teo, 'Emotion Recognition Using Eye-Tracking: Taxonomy, Review and Current Challenges' (2020) *Sensors* (Basel, Switzerland), 20(8), 2384.

6.3 Legal sources

Charter of Fundamental Rights of the European Union, OJ C 326/391 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT>> last accessed 19 October 2025.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326/47 <https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng> last accessed 19 October 2025.

Convention for the protection of individuals with regard to the processing of personal data, as amended by Protocol CETS No. 223 (Convention 108+).

Council Directive of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC) (89/654/EEC), Consolidated text <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01989L0654-20190726>> last accessed 19 October 2025.

Council of the EU, Draft Regulation 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) (first reading) - Adoption of the legislative act = Statements, 2021/0106(COD) <<https://data.consilium.europa.eu/doc/document/ST-9645-2024-ADD-1-REV-2/en/pdf>> last accessed 19 October 2025.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>> last accessed 19 October 2025.

Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L <<https://eur-lex.europa.eu/eli/dir/2024/1760/oj>> last accessed 19 October 2025.

Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), OJ L 149/22 <<https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng>> last accessed 19 October 2025.

European Commission, Annex to the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final, 6.2.2025 <<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>> last accessed 19 October 2025.

European Commission, Annex to the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 6.2.2025 <<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>> last accessed 19 October 2025.

European Commission, Commission staff working document, Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, SWD(2021) 84 final, 21.4.2021 <<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>> last accessed 19 October 2025.

Explanations relating to the Charter of Fundamental Rights, OJ C 303/17 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2007_303_R_0017_01> last accessed 19 October 2025.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>> last accessed 19 October 2025.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021/0106(COD), DRAFT 20-06-2023 at 16h53 (AI Act trilogue mandates). Available at <www.kaizenner.eu/post/long-journey-towards-aiact> under 'Trilogue negotiations', last accessed 19 October 2025.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> last accessed 19 October 2025.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725>> last accessed 19 October 2025.

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169/1 <<https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng>> last accessed 19 October 2025.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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), OJ L, 2024/1689 <<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>> last accessed 19 October 2025.

United Nations, 'Guiding Principles on Business and Human Rights' (2011) HR/PUB/11/04 <www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> last accessed 19 October 2025.

6.4 Case law

Antović and Mirković v. Montenegro App. no. 70838/13 (ECtHR, 28 November 2017).

Case C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596.

Case C-203/22 *Dun & Bradstreet Austria* [2025] ECLI:EU:C:2025:117.

Case C-414/16 *Egenberger* [2018] ECLI:EU:C:2018:257.

Case C-434/16 *Nowak* [2016] ECLI:EU:C:2017:994.

Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779.

Denisov v. Ukraine App. no. 76639/11 (ECtHR, 25 September 2018).

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238.

Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECLI:EU:C:2010:662.

López Ribalda and Others v. Spain App. nos. 1874/13 and 8567/13 (ECtHR, 17 October 2019).

Tyrer v. The United Kingdom App no. 5856/72 (ECtHR, 25 April 1978).

6.5 Reports

Ahmed Shaheed, 'Interim report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed: Freedom of thought', A/76/380, 5 October 2021.

Article 29 Data Protection Working Party (2007), 'Opinion 4/2007 on the concept of personal data' 01248/07/EN.

Article 29 Data Protection Working Party (2014), 'Opinion 05/2014 on Anonymisation Techniques' 0829/14/EN.

Article 29 Data Protection Working Party (2017), 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' WP 248 rev.01.

Catalan Data Protection Authority, 'FRIA model: Guide and use cases' (2025) <www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_en_def.pdf> last accessed 19 October 2025.

Christiane Wendehorst and Yannic Duller, 'Biometric Recognition and Behavioural Detection' (2021) Study requested by the JURI and PETI committees, European Parliament <[www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf)> last accessed 19 October 2025.

Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, 'AI systems for emotion recognition in the areas of workplace or education institutions' (2025) <www.autoriteitpersoonsgegevens.nl/en/documents/summary-and-next-steps-call-for-input-on-prohibition-on-ai-systems-for-emotion-recognition-in-the-areas-of-workplace-or-education-institutions> last accessed 19 October 2025.

Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), Department for the Coordination of Algorithmic Oversight, 'Report AI & Algorithms Netherlands' (2025) Fifth edition <www.autoriteitpersoonsgegevens.nl/en/current/ap-recognising-emotions-using-ai-is-questionable-and-risky> last accessed 19 October 2025.

EDPS, 'TechDispatch #1/2021 - Facial Emotion Recognition', 26 May 2021 <www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf> last accessed 19 October 2025.

EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021 <www.edps.europa.eu/node/7140_en> last accessed 19 October 2025.

European Commission, 'Analysis of EU AI Office stakeholder consultations: defining AI systems and prohibited applications' (2025) Final study report, written by CEPS <<https://digital-strategy.ec.europa.eu/en/library/european-commission-releases-analysis-stakeholder-feedback-ai-definitions-and-prohibited-practices>> last accessed 19 October 2025.

European Union, 'The Joint practical guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation' (2015) Publications Office of the European Union <<https://op.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-en/format-PDF/source-341338175>> last accessed 19 October 2025.

European Union Agency for Fundamental Rights (FRA), 'Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level - Guidance' (2018) Publications Office of the European Union <<https://fra.europa.eu/en/publication/2018/applying-charter-fundamental-rights-european-union-law-and-policymaking-national>> last accessed 19 October 2025.

European Union Agency for Fundamental Rights (FRA) and Council of Europe, 'Handbook on European non-discrimination law' (2018) Publications Office of the European Union <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf> last accessed 19 October 2025.

European Union Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) Publications Office of the European Union <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> last accessed 19 October 2025.

European Union Agency for Fundamental Rights (FRA), 'Getting the future right – Artificial intelligence and fundamental rights' (2020) Publications Office of the European Union <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf> last accessed 19 October 2025.

European Union Agency for Fundamental Rights (FRA), 'Bias in algorithms - Artificial intelligence and discrimination' (2022) Publications Office of the European Union <<https://fra.europa.eu/en/publication/2022/bias-algorithm>> last accessed 19 October 2025.

Meredith Whittaker and others, 'AI Now Report 2018' (2018) <https://ainowinstitute.org/wp-content/uploads/2023/04/AI_Now_2018_Report.pdf> last accessed 19 October 2025.

Rania Wazir, 'The European Commission's guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Comment by the Advisory Committee on the Ethics of Artificial Intelligence of the Austrian Commission for UNESCO' (2025) <www.unesco.at/fileadmin/user_upload/Stellungnahme_zu_den_Leitlinien_der_EU-Kommission_zur_Definition_von_KI-Systemen__auf_Englisch__21._Maerz_2025.pdf> last accessed 19 October 2025.

Registry of the ECHR, 'Guide on Article 8 of the European Convention on Human Rights' (2024) <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng> last accessed 19 October 2025.

Registry of the ECHR, 'Guide on Article 9 of the European Convention on Human Rights' (2024) <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_9_eng> last accessed 19 October 2025.

Report of the Special Rapporteur on the rights of persons with disabilities, 'Rights of persons with disabilities', A/HRC/49/52, 28 December 2021.

UN High Commissioner for Human Rights, 'The right to privacy in the digital age' (2021) A/HRC/48/31.

6.6 Other online sources

A Civil Society Statement, 'An EU Artificial Intelligence Act for Fundamental Rights', 30 November 2021 <<https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf>> last accessed 19 October 2025.

Affectiva, 'Solutions' <www.affectiva.com/solutions/> last accessed 19 October 2025.

AI Superior, 'Best Emotion Recognition Companies', 9 July 2024 <<https://aisuperior.com/emotion-recognition-companies/>> last accessed 19 October 2025.

American Psychological Association, 'Emotion', updated on 19 April 2018 <<https://dictionary.apa.org/emotion>> last accessed 19 October 2025.

American Psychological Association, 'Intention', updated on 19 April 2018 <<https://dictionary.apa.org/intention>> last accessed 19 October 2025.

Article 29 Data Protection Working Party, 'Letter to the European Commission, Annex – health data in apps and devices' (2015) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> last accessed 19 October 2025.

AWS, 'Detecting and analyzing faces' <<https://docs.aws.amazon.com/rekognition/latest/dg/faces.html>> last accessed 19 October 2025.

Biometrics Institute, 'Physiological and Behavioural Biometrics' <www.biometricsinstitute.org/physiological-and-behavioural-biometrics/> last accessed 19 October 2025.

Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*), 'Rules for the Use of Biometrics' <www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics> last accessed 19 October 2025.

EDPB, 'AI: the Italian Supervisory Authority fines company behind chatbot "Replika"' 21 May 2025 <www.edpb.europa.eu/news/national-news/2025/ai-italian-supervisory-authority-fines-company-behind-chatbot-replika_en> last accessed 19 October 2025.

Electronic Privacy Information Center, 'AI Systems for Emotion Recognition in the Areas of Workplace or Education Institutions: Prohibition in EU Regulation 2024/1689 (AI Act)' (2024) <<https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/>> last accessed 19 October 2025.

EUR-Lex, EU hierarchy of norms <<https://eur-lex.europa.eu/EN/legal-content/glossary/eu-hierarchy-of-norms.html>> last accessed 19 October 2025.

European Commission, 'A novel and accurate emotion recognition system for real-time and continuous patient monitoring in psychiatry' <<https://cordis.europa.eu/project/id/190129251>> last accessed 19 October 2025.

European Commission, 'Market Surveillance Authorities under the AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act#1720699867912-2>> last accessed 19 October 2025.

European Commission, 'Multi-stakeholder consultation for Commission guidelines on the application of the definition of an AI system and the prohibited AI practices established in the AI Act' <<https://ec.europa.eu/eusurvey/runner/Prohibitions-and-Definition-Survey-2024#page3>> accessed 23 November 2024.

European Commission, 'Smart lie-detection system to tighten EU's busy borders', 24 October 2018 <<https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders>> last accessed 19 October 2025.

European Commission, Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, C(2023)3215, 22 May 2023 <[https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en)> last accessed 19 October 2025.

European Disability Forum, 'Resolution on the EU Artificial intelligence Act for the inclusion of persons with disabilities', adopted by the Board of Directors of the European Disability Forum on 1 April 2023 <www.edf-feph.org/publications/resolution-on-the-eu-artificial-intelligence-act-for-the-inclusion-of-persons-with-disabilities/> last accessed 19 October 2025.

Eurostat, 'Employed persons working from home as a percentage of the total employment, by sex, age and professional status (%)', last update 12 December 2024 <[https://ec.europa.eu/eurostat/databrowser/view/lfsa_ehomp\\$defaultview/default/table?lang=en](https://ec.europa.eu/eurostat/databrowser/view/lfsa_ehomp$defaultview/default/table?lang=en)> last accessed 19 October 2025.

Fora Soft, '7 Leading Real-Time AI Emotion Recognition Software Solutions', 29 August 2024 <www.forasoft.com/blog/article/real-time-ai-emotion-software> last accessed 19 October 2025.

FRA, 'What are fundamental rights?' <<https://fra.europa.eu/en/content/what-are-fundamental-rights>> last accessed 19 October 2025.

GDPRhub, 'Garante per la protezione dei dati personali (Italy) – 9896808' 13 April 2023 <[https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9896808](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9896808)> last accessed 19 October 2025.

GDPRhub, 'Garante per la protezione dei dati personali (Italy) – 9852214' 3 February 2023 <[https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-_9852214](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214)> last accessed 19 October 2025.

GDPRhub, 'NAIH (Hungary) - NAIH-85-3/2022' 24 April 2022 <[https://gdprhub.eu/index.php?title=NAIH_\(Hungary\)_-_NAIH-85-3/2022](https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022)> accessed 5 October 2025> last accessed 19 October 2025.

Google for Developers, 'Introducing PaliGemma 2: Powerful Vision-Language Models, Simple Fine-Tuning', 5 December 2024 <<https://developers.googleblog.com/en/introducing-paligemma-2-powerful-vision-language-models-simple-fine-tuning/>> last accessed 19 October 2025.

Google Patents, 'Emotion recognition for workforce analytics', US10496947B1 <<https://patents.google.com/patent/US10496947B1/en>> last accessed 19 October 2025.

Google Patents, 'Systems and methods for enhancing responsiveness to utterances having detectable emotion', US10566010B2 <<https://patents.google.com/patent/US10566010B2/en?q=US+10566010+B2>> last accessed 19 October 2025.

Google Patents, 'Voice-based determination of physical and emotional characteristics of users', US10096319B1 <<https://patents.google.com/patent/US10096319B1/en?q=US+10096319>> last accessed 19 October 2025.

Hannah Devlin, 'AI systems claiming to 'read' emotions pose discrimination risks' *The Guardian* (16 February 2020) <www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks> last accessed 19 October 2025.

Heike Anger, 'Gesichtsscan im Supermarkt ist unbedenklich', *Handelsblatt* (12 June 2017) <www.handelsblatt.com/politik/deutschland/datenschuetzer-zu-real-werbebildschirm-gesichtsscan-im-supermarkt-ist-unbedenklich/19921456.html> last accessed 19 October 2025.

Irish Council for Civil Liberties, 'AI system definition guidelines fail to provide clarity', 7 February 2025 <www.iccl.ie/news/ai-system-definition-guidelines-fail-to-provide-clarity> last accessed 19 October 2025.

James Vincent, 'AI 'emotion recognition' can't be trusted' *The Verge* (25 July 2019) <www.theverge.com/2019/7/25/8929793/emotion-recognition-analysis-ai-machine-learning-facial-expression-review> last accessed 19 October 2025.

Joint civil society amendments to the Artificial Intelligence Act, 'Prohibit emotion recognition in the Artificial Intelligence Act' <www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf> last accessed 19 October 2025.

Joint civil society statement, 'EU's AI Act fails to set gold standard for human rights', 3 April 2024 <www.amnesty.eu/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf> last accessed 19 October 2025.

Kate Crawford, 'Artificial Intelligence is Misreading Human Emotion' *The Atlantic* (27 April 2021) <www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/> last accessed 19 October 2025.

Kyle Wiggers, 'Google says its new AI models can identify emotions — and that has experts worried' *TechCrunch* (5 December 2024) <<https://techcrunch.com/2024/12/05/google-says-its-new-open-models-can-identify-emotions-and-that-has-experts-worried/>> last accessed 19 October 2025.

Maja Pantic, 'This is why emotional artificial intelligence matters', TEDxCERN, 2018
<https://youtu.be/4QjZDUaDxQU?si=g3g_BaR_DhW1qgxF> last accessed 19 October 2025.

MarketsandMarkets, 'Emotion AI Market', December 2024
<www.marketsandmarkets.com/Market-Reports/emotion-ai-market-134111673.html> last accessed 19 October 2025.

Marko Grobelnik, Karine Perset, Stuart Russell, 'What is AI? Can you make a clear distinction between AI and non-AI systems?' OECD.AI, 6 March 2024
<<https://oecd.ai/en/work/definition>> last accessed 19 October 2025.

NEC, 'NEC and Realeyes jointly develop emotion analysis service in support of video communications' 23 October 2020
<www.nec.com/en/press/202010/global_20201023_03.html> last accessed 19 October 2025.

NEC, 'NEC's Emotion Analysis Solution Supports Work Style Reform and Health Management', NEC Technical Journal, Vol.14 (2019)
<www.nec.com/en/global/techrep/journal/g19/n01/190109.html> last accessed 19 October 2025.

Paul Ekman Group, 'Facial action coding system' <www.paulekman.com/facial-action-coding-system/> last accessed 19 October 2025.

Plixavra Vogiatzoglou, 'The AI Act National Security Exception: Room for Manoeuvres?' Verfassungsblog, 9 December 2024 <<https://verfassungsblog.de/the-ai-act-national-security-exception/>> last accessed 19 October 2025.

Realeyes, 'Emotion' <www.realeyesit.com/technology/emotion/> last accessed 19 October 2025.

Reco 3.26, 'Emotion Recognition' <www.reco326.com/en/solutions/smart-recognition/emotion-recognition> last accessed 19 October 2025.

Sandra Wachter, "Every smile you fake' — an AI emotion-recognition system can assess how 'happy' China's workers are in the office' Berkman Klein Center (15 June 2021)
<<https://cyber.harvard.edu/story/2021-06/every-smile-you-fake-ai-emotion-recognition-system-can-assess-how-happy-chinas>> last accessed 19 October 2025.

Science Direct, 'Galvanic Skin Response' <www.sciencedirect.com/topics/computer-science/galvanic-skin-response> last accessed 19 October 2025.

Will Knight, 'Job Screening Service Halts Facial Analysis of Applicants' *Wired* (12 January 2021) <www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/> last accessed 19 October 2025.