EMOTIONAL AI AND DATA PROTECTION: RELEVANT IMPLICATIONS FOR OLDER ADULTS AND OTHER VULNERABLE SUBJECTS

SABRINA AKRAM IBRAHIM EL SABI[1]

ABSTRACT: By examining the legal framework that has recently emerged in Europe, the work focuses on the main problems caused by the proliferation of AI technologies used for the care and well-being of vulnerable subjects (especially older people) and aims to identify tools of protection that can be used by the subject-user in the event of discrimination and violations of fundamental rights.

One of the areas which has recently been most affected by AI is that concerning the use of emotion recognition systems for the health-care and well-being of these individuals, who are not offered secure protection for self-determination and privacy.

In light of an analysis of the rapid advancement of these systems, the article also examines, through a comparative perspective, the regulatory challenges and the issues faced by Europe and the US.

KEYWORDS: Artificial Intelligence; Emotion Recognition Systems; Vulnerable Subjects; Data Protection; Emotion Data; Transparency; Discrimination.

I. RECENT EVOLUTIONS OF AI TECHNOLOGY

The current society, characterized by the spread of technological innovations[2] that permeate every aspect of individual and social life[3], has led to a gradual development in

[1] Sabrina Akram Ibrahim El Sabi, research fellow at the University of Bari Aldo Moro. sabrina.elsabi@uniba.it
The researches for this paper were conducted as part of the project "AmICA – Holistic Intelligent Assistance for aCtive Aging in *Indoor* and *Outdoor* Ecosystems", University of Bari Aldo Moro. This paper represents the integration of a pending refereed article entitled: "AI and *Data Protection* in Electronic Devices: emotion recognition and protection perspectives for vulnerable individuals"
[2] See H. HYDEN, "AI, Norms, Big Data, and the Law", *Asian Journal of Law and Society*, 7, 3, 2020, pp. 409-436, 409.
[3] E. CALZOLAIO, "'I Dispositivi medici 'intelligenti': spunti di comparazione giuridica", *Il Foro Italiano*, 2, 2022, pp. 75-83, 75.

the use of artificial intelligence systems, causing new challenges and high risks that emerge[4] especially in the area of data protection[5].

In this regard, it seems appropriate to make assessments of the legal consequences (negative and positive) arising from the evolution of AI.

The area that has been mostly influenced recently is the one concerning the use of digital mobile services and applications for the care and well-being of specific groups of individuals (especially older persons[6]), which, while pursuing general interests aimed at improving the quality of life of different categories of individuals/users, do not offer secure protection for informational self-determination and privacy[7].

Indeed, digital technologies, employed mainly for research and innovation, would give rise to more and better protection of users' physical and psycho-emotional health, ensuring their high level of protection[8].

We are facing a real revolution[9] that presents risks and raises many questions about the privacy protection needs of the vulnerable subjects and the cognitive distortions that these individuals might suffer due to incorrect assumptions of the machine learning process[10].

In particular, one of the applications of AI also concerns the use of algorithms for the purpose of Active and Healthy Aging[11], which promises significant results for research

[4] S. WACHTER, "The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Anti-Discrimination", *Tulane Law Review*, 2022, 97, p. 9; H. STEEGE, "Algorithm-Based Discrimination by Using Artificial Intelligence: Comparative Legal Consideration and Relevant Areas of Application", *European Journal of Privacy Law & Technology*, 1, 2021, p. 57; K.A. CHAGAL-FEFERKORN, "The Reasonable Algorithm", *University of Illinois Journal of Law, Technology & Policy*, 2018, 1, p. 111.

[5] See G. CERRINA FERONI, "Intelligenza artificiale e ruolo della protezione dei dati personali", *Garante per la protezione dei dati personali*, 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742.

[6] For an overview of the topic, see C.M. CASCIONE, *Il lato grigio del diritto*, Torino, Giappichelli, 2022.

[7] R. CALO, "Privacy, Vulnerability and Affordance", *DePaul Law Review*, 66, 2017, p. 592.

[8] V. SALVATORE, "L'Unione europea disciplina l'impiego dell'intelligenza artificiale e dei processi di digitalizzazione anche al fine di promuovere la tutela della salute", in V. SALVATORE (ed), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, Giappichelli, 2023, p. 4.

[9] D. CHANG, "AI Regulation for the AI Revolution", *Singapore Comparative Law Review*, 2023, p. 130.

[10] W. NICHOLSON II PRICE, "Problematic Interactions between AI and Health Privacy", *Utah Law Review,* 4, 2021, p. 925.

[11] M. MCTEAR, K. JOKINEN, M.M. ALAM, Q. SALEEM, G. NAPOLITANO *et al*, "Interaction with a Virtual Coach for Active and Healthy Ageing", *Sensors*, 2023, 23, p. 2748, https://doi.org/10.3390/s23052748; A. BRUNZINI, M. CARAGIULI, C. MASSERA and M. MANDOLINI, "Healthy Aging: A Decision-Support Algorithm for the Patient-Specific Assignment of ICT Devices and Services", *Sensors* 2023, 23, p. 1836, https://doi.org/10.3390/s23041836; M. MENASSA, K. STRONKS, F. KHATAMI, Z. M. ROA DÍAZ, O. PANO ESPINOLA *et al.*, "Concepts and Definitions of Healthy Ageing: A Systematic Review and Synthesis of Theoretical Models", *eClinicalMedicine*, 2023, p. 56, https://doi.org/10. 1016/j.eclinm, 2022, p. 101821; A. PALIOTTA, "Successful, Active and Healthy Aging: differenze e similarità nell'approccio al tema dell'invecchiamento", *Vita e Pensiero*, 2022, p. 473; G. ÅGREN K., BERENSSON, "Healthy Ageing – A Challenge for Europe", 2006, p. 9, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ec.europa.eu/health/ph_projects/2003/action1/docs/2003_1_26_frep_en.pdf.; A. ROTA, "Invecchiamento attivo e solidarietà tra le generazioni nel dialogo sociale europeo", *Rivista del Diritto della Sicurezza Sociale*, 3, 2023, p. 593.

as well as for the development of tools capable to improve health and quality of life especially for those in advanced stages of age[12].

AI systems[13] are currently widely used as a preventive tool to aspire, for example, to healthy aging. This is done mainly through digital infrastructure and, more specifically, through wearable devices[14]. Such devices are certainly aimed at solving one of the most critical aspects, cause of frailty in older persons: the need to constantly monitor one's state of health and psycho-physical well-being by using, precisely, methods and devices that are as minimally invasive as possible[15]. However, at the same time, these applications engender in older adults (who often misunderstand the actual role of carebots or simple chatbots) an over-reliance or, even worse, a real dependence on AI with a relative loss of autonomy of the formers. For instance, the design of AI systems intended for the care and well-being of older people[16], recommends responsible development of the underlying technologies that takes into account the vulnerabilities of those involved and the sensitive issues related to their privacy[17].

Hence, the need to investigate the functioning, dynamics and the protection tools provided for those individuals placed in a special condition of vulnerability[18].

---

[12] EHDEN (European Health Data & Evidence Network), "Protecting People while Using their Health Data for Research, a Framework for Understanding Relative Responsibilities and Roles", 2022, https://www.ehden.eu/protecting-people/.

[13] These are automated systems that are designed to operate with varying levels of autonomy and that, for explicit or implicit purposes, could generate outputs, such as predictions, recommendations, or decisions that affect physical or virtual environments. See Art. 3(1), AI Act.

[14] Devices useful in the pursuit of active aging in one or more areas of the social or personal sphere, enabling the user to freely choose the activity or activities in which to engage according to his/her aspirations and motivations. See A. ZINZUWADIA, J.P. SINGH, "Wearable devices-Addressing Bias and Inequity", *The Lancet – Digital Health*, 2022, https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00194-7/fulltext; P. STANZIONE, "'Dispositivi indossabili: rischi per la privacy. Che fine fanno le informazioni raccolte?' – Intervista a Pasquale Stanzione", *Garante per la protezione dei dati digitali*, 2021, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9552323; L. TIRABENI, "I dispositivi indossabili per il benessere", *Il Mulino*, 3, 2022, pp. 119-120. On this point, see C. IRTI, "L'uso delle tecnologie mobili applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano", *Persona e Mercato*, 1, 2023, pp. 32-33.

[15] L. COLONNA, "Artificial Intelligence in the Internet of Health Things: Is the Solution to AI Privacy More AI?", *Boston University Journal of Science and Technology Law*, 27, 2, 2021, pp. 312-344.

[16] See A. SETHUMADHAVAN, G. BAIK, L. D'AMBROSIO *et al.* "World Economic Forum, Designing Artificial Intelligence Technologies for Older Adults" - Insight Report, 2021, pp. 2-10.

[17] D. AMRAM, "La transizione digitale delle vulnerabilità e il sistema delle responsabilità", *Rivista italiana di medicina legale*, 1, 2023, pp. 2-6;

[18] See C. IRTI, *supra*, nt. 12, p. 47. Meeting this need is the recently proposed Artificial Intelligence Regulation. In fact, the main purpose of the AI Act is to identify "complex vulnerability", for instance, "The proposed AI Regulation (see Art. 5(b), *AI Act*), takes note of this complexity taking into account the vulnerability of certain categories (groups) of individuals in relation to age or physical or mental disability as well as in relation to social or economic situation with a passage that testifies to an attitude of progressive attention to the issue of vulnerability and its multiple implications [...]. The idea that with respect to AI there is a condition of vulnerability common to all individuals, understood as dependence and trust, cannot obscure the fact that further conditions of vulnerability, dependent on the individual's own characteristics, such as age and disability, but also on changing and possibly transitory exogenous factors, may overlap with the first, even in a multiple form, determining the onset in the head of the individual or groups of individuals of a situation that we could define as one of complex vulnerability".

Specifically, this will reflect on emotional AI[19] applied to particular groups of vulnerable individuals, which characterizes the decision-making processes of some AI systems (especially those with "high risk[20]"), and the questions that the use of such devices currently raises.

AI technologies, especially those used for emotion recognition[21] (closely related to the field of so-called Affective computing[22]), are becoming increasingly prominent.

While such technologies take advantage of the digital transformation, they also result in significant drawbacks. These are practices aimed at profiting from the vulnerability of specific groups of individuals, in view of the need to protect their privacy.

Thus, Artificial Intelligence for emotion recognition, with related prediction of older person's state of mind, are designed to infer the individual's emotional state from the analysis of facial expressions, tone of voice, body movements (such as gait) as well as other biometric[23] and non-biometric data of the person. Indeed, it is now well known that technologies, using machine learning models[24] and so-called deep learning

Indeed, these considerations show the prominence given to the principle of non-discrimination, one of the fundamental principles of AI, which prevents the development or intensification of discrimination between persons or groups of persons (a notion that should be applied extensively to the older people group as well).

[19] Emotional AI is designed to infer an individual's emotional state from the analysis of his facial expressions, tone of voice, body movements (as well as his gait) and other biometric data, using machine learning tools (special techniques that, using algorithms, enable the rapid collection and processing *of* large datasets and information). See, D. RUGGIU, "L'emozione, nuovo territorio di conquista dell'intelligenza artificiale: applicazioni e rischi", *AgendaDigitale*, 2021, https://www.agendadigitale.eu/cultura-digitale/lemozione-nuovo-territorio-di-conquista-dellintelligenza-artificiale-applicazioni-e-rischi/; M. MARTORANA, "IA e riconoscimento delle emozioni: rischi e possibili vantaggi", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/sicurezza/privacy/ia-e-riconoscimento-delle-emozioni-rischi-e-possibili-vantaggi/.

[20] See Chapter III, Sec. 1 AI Act.

[21] That of emotions is an area of research that aims to develop algorithms and systems which can interpret human emotions using verbal and nonverbal communication signals such as facial expression, body language, or voice modulation. See European Data Protection Supervisor (EDPS), "TechDispatch on Facial Emotion Recognition", 1, 2021, p. 1; S.B. DAILY, M.T. JAMES, D. CHERRY, J.J. III PORTER, S.S. DARNELL, J. ISAAC and T. ROY, "Affective Computing Historical Foundations, Current Applications and Future Trends," in M. JEON (ed), *Emotions and Affect in Human Factors and Human-Computer Interaction*, Elsevier Academic Press, 2017, pp. 213-231.

[22] The process of analyzing human emotions has found its ultimate affirmation in Affective Computing. This phenomenon originates from the studies of Rosalind Picard and the group of researchers at the MIT Media Lab, the first to combine advances in computational and automated techniques with those obtained in the field of psychology on the analysis of human emotions. On this point see P. EKMAN and W.V. FRIESEN, "The Reportoire of Nonverbal Behaviour: Categories, Origins, Usage and Coding", *Semiotica*, 1, 1, 1969, pp. 49-98; *ID.*, "Constans Across Cultures in the Face and Emotion", *Journal of Personality and Social Psychology*, 17, 2, 1971, pp. 124-125. For a more thorough examination of the combination of human emotions-computational criteria for analyzing and designing systems aimed at improving people's quality of life, see R. PICARD, "Affective Computing", *MIT Media Laburatory Percetual Computing Section Technical Report*, 1995, *passim*.

[23] E. 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", *European Data Prtoection Law Review*, 8, 2, 2022, p. 312.

[24] A. ALSLAITY and R. ORJI, "Machine Learning Techniques for Emotion Detection and Sentiment Analysis: Current State, Challenges, and Future Directions", *Behaviour & Information Technology*, 43, 1, 2024, pp.

algorithms[25], feed their operations with a continuous and exponential input of data (health-related, biometric, etc.)[26], offering, on the one hand, revolutionary prospects for progress and, on the other hand, raising new questions[27].

Additional concerns arise from the processing of personal data and the risks posed by the manipulation of individuals' emotions, leading to the question of whether, in practice, the GDPR provisions[28] are sufficient[29] for the protection of this particular category of vulnerable individuals, or there will be a need for a reorganization of the discipline that adapts to new technologies and takes into account the issues associated with the use of such applications[30].

In such hypotheses, the identification of possible remedies and specific measures aimes at developing preventive control tools in full compliance with the principles of privacy by design and accountability of the GDPR, essential for the monitoring of such technologies. On this point, the appropriate regulation prepared at the EU level on the subject of AI should be equipped with targeted rules[31] aimed at regulating a conscious use of these emotion recognition devices, preferring less invasive approaches to privacy (for example, stricter transparency obligations, which must necessarily be guaranteed for this type of AI systems).

139-164; T. TELFORD, "'Emotion Detection' AI is a $20 Billion Industry. New Research Says it Can't Do What it Claims - Artificial Intelligence Advanced by Such Companies as IBM and Microsoft is Still no Match for Humans", *The Washington Post*, 2019, https://www.washingtonpost.com/business/2019/07/31/emotion-detection-ai-is-billion-industry-new-research-says-it-cant-do-what-it-claims/.

[25] It should be noted that, for 'effective functionality', machine learning models make use of neural networks and deep learning algorithms: models that are based on continuous and exponential processing of massive amounts of data, acquired and organized by the AI systems themselves. See G. MOSCA, "Deep learning: cos'è, come funziona e applicazioni", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/cultura-digitale/deep-learning-cose-come-funziona-e-applicazioni/.

[26] See M.C. CARROZZA, C. ODDO, S, ORVIETO, A. di MININ and G. MONTEMAGNI, "AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale", *BioLaw Journal*, 3, 2019, pp. 237-254.

[27] R. CARLEO, "Il trattamento dei dati sanitari digitalizzati tra tutele individuali e interessi comuni", in U. RUFFOLO and M. GABRIELLI (eds.), *Intelligenza artificiale, dispositivi medici e diritto*, Torino, Giappichelli, 2023; p. 153. According to the author, although "digitization fuels and accelerates the evolution and circulation of science, allowing old problems to be overcome, it has nevertheless imposed the need to balance such advances with individual protections of personal data processing".

[28] EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[29] L. COLONNA, "Artificial Intelligence in the Internet of Health Things: Is the Solution to AI Privacy More AI?", *Boston University Journal of Science and Technology Law*, 27, 2, 2021, pp. 312-344, 329; P. KROOT TUPAY, M. EBERS, J. JUKSAAR and K. KOHY, "Is European Data Protection Toxic for Innovative AI? An Estonia Perspective", *Juridica International,* 30, 2021, pp. 99-110; T.R. MOSLEY, "AI Isn't Great at Decoding Human Emotions. So Why are Regulators Targeting the Tech?", *MIT Technology Review,* 2023, https://www.technologyreview.com/2023/08/14/1077788/ai-decoding-human-emotions-target-for-regulators/.

[30] See, *supra*, nt. 25, p. 154.

[31] Consider the numerous European regulations in recent years – from the Data Governance Act (DGA) to the Digital Services Act (DSA); from the Digital Markets Act (DMA) to the Data Act (DA) – all adopted as part of the European Data Strategy, https://digital-strategy.ec.europa.eu/it/policies/strategy-data.

The purpose of these provisions would be to protect vulnerable individuals from potential harm by ensuring data security and informed user consent and by limiting the use of personal data collected to prevent abuse or discrimination[32].

One of the latest uses of AI is related to the transformation of the welfare and care sector that results in the gradual erosion of the individual's (in particular, older adults) autonomous decision-making spaces.

The profiles on which the research intends to focus legal consideration are the violation of the processing of special personal data, as well as the possible discrimination suffered by those groups of individuals placed in a special condition of vulnerability[33].

II. EMOTION RECOGNITION SYSTEMS IN THE DIGITAL AGE: RISKS AND BENEFITS FOR VULNERABLE (OLDER) PERSONS

Among the new phenomena increasingly resulting in forms of intrusion into people's real and digital lives – offering both perspectives of obvious criticality and significant possibilities for the advancement of the digital marketplace[34] - emotional AI systems[35]

[32] European Council, Report CAHAI(2020)23 Ad hoc Committee on Artificial Intelligence, 2020, 2-56, www.coe.int/cahai, "The prevention of harm is a fundamental principle that should be upheld, in both the individual and collective dimension, especially when such harm concerns the negative impact on human rights, democracy and the rule of law. The physical and mental integrity of human beings must be adequately protected, with additional safeguards for persons and groups who are more vulnerable. Particular attention must also be paid to situations where the use of AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens"; Parliamentary Assembly, *Preventing Discrimination Caused by the Use of Artificial Intelligence*, *Resolution* 2343/2020, https://pace.coe.int/en/files/28807/html. See A. PISAPIA, "What can we expect from European regulation on artificial intelligence?", *Cyberspace and Law*, 24, 1, 2023, p. 3.

[33] *Supra*, nt. 2, pp. 80-82.

[34] On this point see J.R. FLAHAUX, B.P. GREEN and A.G. SKEET, "Ethics in the Age of Disruptive Technologies: An Operational Roadmap", *Santa Clara University*, 2023, https://www.scu.edu/institute-for-technology-ethics-and-culture/itec-handbook/.

[35] For an overview of emotional AI systems see E.M. INCUTTI, "Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale", *Giustiziacivile*, 2022, p. 515; P. OTTOLINA, "AI Act, controllo biometrico a distanza e riconoscimento delle emozioni: i nodi dell'accordo Ue sull'intelligenza artificiale", *Corriere della Sera*, 2023, *https://www.corriere.it/tecnologia/23_dicembre_08/ai-act-controllo-biometrico-a-distanza-e-riconoscimento-delle-emozioni-dove-si-e-incagliato-l-accordo-ue-2ee5a84c-a930-45ea-8046-b595e368cxlk.shtml*; M. PURDY, J. ZEALLEY and O. MASELI, "The Risks of Using AI to Interpret Human Emotions," *Harvard Business Review*, 2019, https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions; H. DEVLIN, "AI Systems Claiming to 'Read' Emotions Pose Discrimination Risks - Expert Says Technology Deployed is Based on Outdated Science and therefore is Unreliable", *The Guardian*, 2020, https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks; M. DUROVIC and J. WATSON, "Nothing to Be Happy About: Consumer Emotions and AI", *Multidisciplinary Scientific Journal*, 2021, 4, p. 785.

are currently "regulated" within the European[36] AI Act[37], which raises ethical dilemmas[38] concerning privacy, the processing of personal data[39] as well as accountability in decisions made by algorithms.

Specifically, emotional AI – which seeks to enable machines to understand, interpret and respond to human emotions – is raising significant concerns, despite the lack of specific regulation[40]. One of the main questions raised by these technologies concerns whether or not automated AI-based systems can be able to infer and understand human emotions.

[36] The Explanatory Memorandum accompanying the proposed Regulation on Artificial Intelligence (formerly Regulation), specified that the term artificial intelligence refers to a rapidly evolving family of technologies capable of delivering a wide range of economic and societal benefits across the spectrum of industrial and social activities. In this sense, the use of artificial intelligence, by ensuring improved forecasting, optimization of operations and resource allocation as well as personalization of service delivery, may contribute to the achievement of socially and environmentally beneficial outcomes as well as provide key competitive advantages to European businesses and the economy. On the point, the final draft of the AI Act states that "AI system" means a designed automated system operate with varying levels of autonomy, capable of adapting after deployment, and which, for explicit or implicit purposes, can generate outputs, such as predictions, recommendations, or decisions that influence physical or virtual environments. As the first legislative proposal of its kind in the world, it can set a global standard for regulating AI in other jurisdictions, as has already been the case with GDPR (think of the U.S.), thereby promoting the European approach to regulating technology globally. This, therefore, binds the U.S. in many respects to comply with EU regulation of the processing of personal data. Currently, the Federal Privacy Act (American Data Privacy and Protection Act, https://www.congress.gov/bill/117th-congress/house-bill/8152/text) is still under discussion.

[37] See Corrigendum to the position of the European Parliament adopted at first reading on March 13rd 2024 with a view to the adoption of Regulation (EU) 2024/ ....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) P9_TA(2024)0138 (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)), adopted by the European Parliament on March 13rd, 2024, last version on April 17th, 2024, https://artificialintelligenceact.eu/the-act/. The reference assumes, in particular, the analysis of Recitals 1; 15; 44; 54; 69; 132; as well as Articles 1; 3(39); 10; 13; 50(3) of the AI Act.

[38] On "ethical dilemmas", remarkable is the speech by Professor G. CERRINA FERONI, "AI e diritto: 'L'umanesimo digitale diventa concreto solo con le regole", *Garante per la Protezione dei dati personali,* 2024, https://www.garanteprivacy.en/web/guest/home/docweb/-/docweb-display/docweb/9977187 (University of Florence, at the Conference: "Artificial Intelligence and Automated Decisions", January 22nd, 2024), in which perplexities are highlighted "about the preponderance of the ethical issue in the approach to the concept of artificial intelligence", says the vice president, "because I think it becomes very comfortable to hide behind ethical standards that big companies like a lot, soft law, codes of conduct that can become everything and nothing, even alibis to continue doing business without responsibility. It is much less comfortable to reason about legal rules that carry penalties. So we need law parameterized to what are the cornerstones of democratic systems, the heart of constitutionalism, separation of powers, fundamental rights and freedoms".

[39] G.M. RICCIO and G. GIANNONE CODIGLIONE, "La rilevanza delle basi giuridiche per il trattamento di dati personali mediante sistemi di intelligenza artificiale", in A. PAJNO, F. DONATI and A. PERRUCCI (eds.), *Intelligenza Artificiale e Diritto: una rivoluzione?*, Bologna, Il Mulino, 2022, pp. 281-311, p. 295; G. DE GREGORIO and F. PAOLUCCI, "Dati personali e AI Act", *MediaLaws, 2022*, https://www.medialaws.eu/dati-personali-e-ai-act/.

[40] See M. DI SALVO, "IA ed emozioni umane: definizione, regolamentazione e possibili implicazioni", *Diritto.it*, 2023, p. 3, who argues that "In the field of Artificial Intelligence (AI), the understanding of human emotions is central because they are able to shape the thoughts, decisions, and interactions of subjects".

In the field of "Emotion recognition systems" point of reference is the scientific field of Affective Computing, intended to be implemented or already used in various fields, making emotions machine-readable and offering the opportunity to automatically process a new type of data: emotional data (arising, in this sense, a "datafication" of human emotional life).

Machine learning algorithms have been trained on large data sets containing classified emotional responses to improve accuracy and advances in so-called computer vision; moreover, in natural language processing, they have paved the way for very sophisticated emotion recognition systems.

Indeed, emotional state analysis aims to pursue highly ethical and social ends, as the collection of the individual's emotional data is projected toward improving solutions to people's behaviors and lifestyles[41].

However, while it is true that the possibility of knowing the feelings and emotions of individuals may offer benefits, it is also true that, in certain cases, it jeopardizes the rights of the individual (who must be granted centrality, including consideration of his or her own needs)[42].

The fusion of emotions and technology presents intricate challenges, including those related to data privacy, emotional ambiguity, and the balance between personalization and generalization.

In this regard, it is useful to focus attention on the definition of emotional AI[43], which was integrated by the AI Act into "emotion recognition system"[44], on the risks associated with such technology as well as the serious doubts arising from their operation that have arisen under the theory that a complex element such as human emotions can be recognized in an automated way[45].

On this point, Recital 44 of the AI Act highlights in the final draft the "serious concerns about the scientific basis of AI systems aimed at detecting emotions" and acknowledges that "emotions or their expression and perception vary widely across cultures and situations and even in relation to the same person". Three fundamental shortcomings of these technologies are then listed: limited reliability, as emotions cannot be unequivocally associated with a set of movements or biological/biometric indicators;

[41] See, *supra*, nt. 34, pp. 516-517.

[42] D.U. GALETTA, "Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale", *federalismi.it*, 5, 2023, p. 4, https://www.federalismi.it/nv14/editoriale.cfm?eid=665.

[43] The first research project on the subject of emotions and personality of individuals dates back to the 1960s and was coordinated by Paul Ekman (University of California), taking the name "Facial Action Coding System (FACS)". It was, in essence, a system based on the reading and reprocessing of typical emotions, which combined with other physical-emotional elements (facial muscle movements) allowed the analysis of the study of human emotions, generating, thus, a universally applicable general paradigm. See P. EKMAN, J.R. DAVIDSON, *The Nature of Emotion: Fundamental Questions*, USA, Oxford University Press, 1994, *passim*; P. EKMAN, "Basic Emotion", in T. DALGLEISH and M.J. POWER (eds.), *Handbook of Cognition and Emotion*, England, John Wiley & Sons, 2000, pp. 45-47.

[44] Specifying that it is "an AI system aimed at identifying or inferring emotions or intentions of natural persons on the basis of their biometric data". See Art. 3(39), AI Act.

[45] This is better specified in M. MARTORANA, R. SAVELLA, *supra*, nt. 17.

lack of specificity, as physical or physiological expressions do not uniquely correspond to certain emotions; and finally, limited generalizability, as the expression of emotions is influenced by context and culture.

Among the many positive aspects arising from the use of such devices[46], first of all, the ones that could be used to monitor the state of health and well-being of a subject should be mentioned, i.e., in areas such as mental health, allowing a better understanding of patients' emotional conditions and facilitating the diagnosis of psychological disorders[47]. One of them may be some particularly innovative platforms related to wearable devices or about the specific applications deployed in the U.S.[48] (an example is SimSensei[49]), used to improve the emotional state of patients.

However, despite the many benefits brought about by emotional AI, there are considerable risk profiles arising from its use.

About artificial intelligence for older people care, for example, the natural decline of their cognitive faculties makes them more likely to develop a dependence on the "machine," the technology that assists and cares for them[50]. In some cases, it has been found that older adults, especially the loneliest and those without assistance from human caregivers, mystify carebots as real substitutes for human interaction[51].

[46] Despite the critical issues, there is no shortage of those who support the usefulness of AIs for emotion recognition, arguing that the limitations of these technologies are not inherent but stem from the complexity of the human soul, and that nonetheless identifying emotions (albeit in a necessarily imperfect way) has tremendous practical benefits. See in this regard, the report by D. CASTRO, (director of the Center for Data Innovation and Vice President of the Information Technology and Innovation Foundation), "The EU's AI Act Is Premature, Says ITIF", 2023, https://itif.org/publications/2023/12/08/the-eu-ai-act-is-premature/, according to which "Given how rapidly AI is developing, EU lawmakers should have hit pause on any legislation until they better understand what exactly it is they are regulating. There is likely an equal, if not greater risk of unintended consequences from poorly conceived legislation than there is from poorly conceived technology. And unfortunately, fixing technology is usually much easier than fixing bad laws"; G. SCORZA, "Scorza: AI Act è a rischio, ecco le regole che servono – Intervento di Guido Scorza", *Garante per la protezione della privacy*, 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9960565; see, *supra*, nt. 17.

[47] L. MONTALBANO, "Brain-Machine Interfaces and Ethics: A Transition from Wearable to Implantable", *Journal of Business and Technology Law*, 16, 2, 2021, pp. 191-222; C. BURR, N. CRISTIANINI, J. LADYMAN, "An Analysis of the Interaction Between Intelligent Software Agents and Human Users", *Minds and Machines*, 28, 2018, p. 735.

[48] N. SHEN, "AI Regulation in Health Care: How Washington State can Conquer the New Territory of AI Regulation", *Seattle Journal of Technology, Environmental & Innovation Law (SJTEIL)*, 13, 1, 2023, pp. 1-4; N. NI LOIDEAIN, R. ADAMS and D. CLIFFORD, "Gender as Emotional AI and the Case of 'Nadia': Regulation and Ethical Implications", *SSRN*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3858431.

[49] D. DEVAULT, R. ARTSTEIN, G. BENN, T. DEY *et al*, "SimSensei Kiosk: A Virtual Human Interviewer for Healthcare Decision Support", Conference: Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems, 2014, p. 1061.

[50] Consider, for example, the case where the AI system reproduces a human voice. In such hypotheses, in order not to raise misleading expectations in the older person regarding the interaction capabilities of the device, clarity and (preventive) transparency become crucial.

[51] As highlighted by the work done by the World Economic Forum in "It's Time We Embrace an Agile Approach to Regulating AI", 2023, https://www.weforum.org/agenda/2023/11/its-time-we-embrace-an-agile-approach-to-regulating-ai/.

Nevertheless, the collection and analysis of personal emotions may generate additional problems: violations of privacy, security[52] and data processing[53], loss of autonomy of individuals[54] (compounded by the difficulty, on the part of individuals, to clearly understand how such technologies work).

To mitigate such biases, it is necessary to take certain measures to pursue a balance of rights and interests[55]. Thus, it becomes crucial to develop control and accountability tools to monitor the implementation of such technologies and prevent privacy violations.

It was anticipated how specific reference is made in the AI Act to the use of emotion recognition devices, aimed at ensuring data security, informed user consent and restricting the processing of personal data collected. However, the mere reference to biometric data in the definition of emotion recognition systems[56] runs the risk of narrowing the scope of application of the article.

One of the issues being debated in the context of the adoption of the AI Act is the one related to the regulation of the design and the use of emotional AI systems (having the function of recognizing the emotions of individuals for a wide variety of purposes: education, professional sphere, and health and well-being of individuals). For several years, the application of such systems and, specifically, the risks that their use may pose to fundamental rights[57], have originated numerous criticisms, to the point that in certain cases (law enforcement; border management; workplaces and educational institutions[58]), a specific ban on the use of these technologies has been affixed.

In particular, the main questions have concerned whether or not this prohibition should be extended to all hypotheses of the use of emotional AI systems[59]. Hypothesis, the latter, not provided for in the final draft of the AI Act.

[52] See, *supra*, nt. 41, p. 4.

[53] That is why it is recommended – before the installation of any system – to address through timely information the concerns that older adults might have, for example, regarding the devices used in their homes, the data collected and processed by the data controllers, the purpose of the processing, the people who will have access to these data, their retention period and the security measures to protect them. See in this regard, *supra*, nt. 9.

[54] Those being monitored by AI-based systems may also experience them as intrusive, fearing a limitation of their independence and otherwise preferring human contact to digital. See J. STYPINSKA, "AI Ageism: A Critical Roadmap for Studying Age Discrimination and Exclusion in Digitalized Societies", *AI & Society*, 38, 2023, p. 669; B. HERRMANN, "The Perception of Artificial-Intelligence (AI) Based Synthesized Speech in Younger and Older Adults", *International Journal of Speech Technology*, 26, 2023, p. 395.

[55] Regarding possible discrimination of older adults, one example concerns AI-based tools that prioritize safety from falls over freedom of movement. In this sense, there would be an implicit tendency to marginalize the older person's desire for privacy and self-determination, preferring, in contrast, the needs of the children of such individuals. We refer, on this point, to P. KULURKAR, C.K. DIXIT, V.C. BHARATHI *et al*, "AI Based Elderly Fall Prediction System Using Wearable Sensors: A Smart Home-Care Technology with IOT", *Sensors*, 25, 2023, pp. 3-11.

[56] See art. 3, 39), AI Act.

[57] Consider that the AI Act does not apply to those AI systems developed and commissioned for scientific research and development purposes only (Art. 2(5a), AI Act*).*

[58] Art. 5 AI Act.

[59] Emotion recognition (especially the so-called Facial Emotion Recognition) qualifies as a new frontier of both the digital market and research and innovation, capable of offering constantly updated information

As a consequence, the need for a new normative approach, especially for the ethical use of AI, identified in the proposal for a technological humanism that can combine artificial intelligence and the fundamental rights of people (with special reference to the vulnerable).

Notably, for AI, the European Commission has proposed a risk-based approach, with four different levels for AI systems, as well as specific risk identification for general-purpose models.

Among the most relevant ethical and legal issues raised by Emotion Technologies, we could start from the risk of leading to an impairment of the fundamental rights of the individual[60], with possible violations of privacy and contextual issues related to the acquisition of data in the absence of the consent of the data subjects.

From the use of such applications, therefore, the need for their responsible development is noted. Emphasis is placed on information and transparency obligations for users of an emotion recognition system with respect to individuals exposed to such a technology.

These are applications that require certain elements from their production: compliance with the principles of privacy by design and by default[61]; protection of the processing of common and special personal data; consistency in the application of biometric data for emotion recognition; adequate transparency[62] to be provided to the user; special

through audience rendering systems and preparing predictive analysis codes capable of influencing the self-determination of individuals in the real world through conditionings occurring in virtual reality. See, in this regard, A. PIPITONE, "Empatia upmo-robot: il complesso rapporto tra l'AI e le emozioni", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/cultura-digitale/empatia-uomo-robot-il-complesso-rapporto-tra-lai-e-le-emozioni/; Y. CAI, X. LI and J. LI, "Emotion Recognition Using Different Sensors, Emotion Models, Methods and Datasets: A Comprehensive Review", *Sensors*, 23, 2023, p. 2455, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10007272/pdf/sensors-23-02455.pdf; J.S. BARD, "Developing Legal Framework for Regulating Emotion AI", *Boston University Journal of Science and Technology Law*, 27, 2, 2021, p. 272. See, also, C. JEE, "Emotion Recognition Technology Should Be Banned, Says an AI Research Institute", *MIT Technolgy Review,* 2019, https://www.technologyreview.com/2019/12/13/131585/emotion-recognition-technology-should-be-banned-says-ai-research-institute/; Article19, "Emotion Recognition Technology: A Threat to Free Speech, Equality and Privacy", 2021, https://www.article19.org/resources/emotion-recognition-technology/.

[60] See A. MANTELERO and V. TIANI, "Norma UE su AI 'appello urgente per una solida valutazione d'impatto sui diritti fondamentali'", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/sicurezza/privacy/norma-ue-su-ai-appello-urgente-per-una-solida-valutazione-dimpatto-sui-diritti-fondamentali/; A. ADINOLFI, "L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione", in A. PAJNO, F. DONATI and A. PERRUCCI (eds.), *Intelligenza Artificiale e diritto: una rivoluzione?*, Bologna, Il Mulino, 2022, p. 133; A. ODDENINO, "Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulle recente Proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica", in A. PAJNO, F. DONATI and A. PERRUCCI (eds.), *Intelligenza Artificiale e diritto: una rivoluzione?*, Bologna, Il Mulino, 2022, p. 111.

[61] Art. 10 AI Act.

[62] Section 13 of the AI Act provides for transparency and information obligations where it states, "High-risk AI systems shall be designed and developed to ensure that their operation is sufficiently transparent to enable deployers to interpret the output of the system and use it appropriately. An appropriate type

controls and a special mechanism related to prior impact assessment that can concretely verify the intelligibility of the AI system.

Indeed, any AI system (assistive robots, home automation devices, wearable devices[63]) aimed at interacting with vulnerable individuals is called upon to perform a rather delicate task, paying special attention to the cognitive abilities and psycho-emotional aspects of the individuals in question.

These are capabilities and aspects that must be taken into account during the development and design phase of such systems (obviously also during the training phase developed for operators).

This is made more explicit in Recital 69 of the AI Act, which specifies that "The right to privacy and protection of personal data must be guaranteed throughout the life cycle of the AI system. In this regard, the principles of minimization and data protection by design and by default - sanctioned by EU data protection law - are applied when personal data are processed. AI system providers and deployers should implement state-of-the-art technical and organizational measures in order to protect these rights [...]".

On this point, it is also fundamental to analyze Recital 132 where specific information and notification obligations are noted (since simple transparency notices may be ineffective[64]) to data subjects interacting with an AI system, especially when exposed to systems designed to identify or infer their emotions or intentions. In implementing this obligation, the characteristics of individuals belonging to vulnerable groups due to their age or disability should be taken into account to the extent that the AI system is intended to interact with such groups as well.

Under this perspective, it would be necessary to implement a prior, clear and effective[65] communication (depending on the type and risk of the system employed) in order for older people to understand their functioning and characteristics, enabling the

and level of transparency shall be ensured to achieve compliance with the relevant provider and deployer obligations in Section 3. High-risk AI systems shall be accompanied by instructions for use, in an appropriate digital or non-digital format, that include concise, complete, correct, and clear information that is relevant, accessible, and understandable to deployers". While there is no explicit provision for the intersection of these requirements with the GDPR, there is an implicit reference to the principle of transparency provided for in Article 5 of the GDPR, which requires Data Controllers to make data subjects aware of the management of the data in relation to the specific processing carried out, as well as the risks associated with it. This duty of transparency is also complemented by the provisions of Articles 13 and 14 of the GDPR, according to which data controllers are required to inform data subjects about how the data referred to them will be handled and about the rights that can be exercised in relation to data protection. On this subject, see also S. TROZZI, "Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy", *federalismi.it*, 1, 2024, p. 197.

[63] Z. MA, Q. GAO and M. YANG, "Adoption of Wearable Devices by Older People: Changes in Use Behaviors and User Experiences", *International Journal of Human-Computer Interaction*, 39, 2023, pp. 964-966.

[64] See G. MALGIERI and M. IENCA, "Artificial Intelligence Act: l'UE regola l'AI ma dimentica di proteggere la mente", *AgendaDigitale*, 2021, https://www.agendadigitale.eu/cittadinanza-digitale/artificial-intelligence-act-lue-regola-lai-ma-dimentica-di-proteggere-la-mente/.

[65] See Art. 1(d), AI Act according to which this regulation provides for "harmonized transparency rules for certain AI systems" (regarding AI systems intended to interact with natural persons, emotion recognition systems, biometric categorization systems as well as AI systems used to generate or manipulate images or audio or video content).

vulnerable not to adhere to conditions detrimental to them. In this regard, specific transparency requirements are prescribed in order to prevent risks and remove the negative effects that the manipulation of certain AI systems might entail[66].

Furthermore, the analysis of the AI Act[67] does not reveal any new tools that the person, individually or even collectively organized, may use to make protection faster or more effective. In fact, since emotions in the proposed regulation are equated with particularly sensitive data[68], emotional AI would be subject to the same requirements already in the GDPR for the processing of personal data, *ex* Article 6[69]. This gives rise to the main difficulties in implementing the AI Act, which lie on dealing with certain challenges related to GDPR compliance; more specifically: transparency, providing people with clear information about the processing of their personal data using AI, as well as assessing the potential impact this may have on their privacy[70].

As an outcome, emotional AI, being often built on discriminatory and pseudo-scientific foundations, is likely, for a long time to come, to remain scientifically questionable and legally opaque[71].

III. EMOTION DATA, GDPR AND LEGAL IMPLICATIONS

It is necessary, at this point, to shed light on the legal consequences and challenges that emotional AI and the processing of emotional data may bring about in the EU regulatory framework.

"Big data and AI allow for the collection and processing of huge amounts of data. One of the new data-driven technologies gaining attention is emotion technology. Emotion tech promises to make emotions machine readable and usable. Emotions provide a primary filter for all our thoughts and impressions; they are important for our ability to make decisions and they drive us to act and engage. Knowledge about people's emotional state can turn into a powerful tool to influence healthcare, education, labor,

[66] See on this point the Explanatory Memorandum to the proposed Artificial Intelligence Regulation, par. 5.2.4. under the heading "Transparency requirements for certain AI systems (Title IV)", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206; as well as the final draft of April 17th, 2024, https://artificialintelligenceact.eu/ai-act-explorer/, where the updated version of AI Act can be analized.

[67] B. CALDERINI, "AI Act, il punto su risultati raggiunti e i dubbi sul futuro", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/sicurezza/privacy/ai-act-raggiunto-un-equilibrio-instabile-ecco-perche/; G. RESTA, "Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?", *Diritto dell'Informazione e dell'Informatica*, 2, 2022, pp. 323-342.

[68] V. Recital 2 AI Act.

[69] See Art. 50, par.3, AI Act.

[70] Some emotional AI systems use software that detects the user's emotions not based on biometric detections, but through written text, thus generating results through analysis of the user's chosen words and text setting.

[71] V. MARDA and E. JAKUBOWSKA, "Emotion (Mis)Recognition: is the EU missing the point?", *EDRi*, 2023, https://edri.org/our-work/emotion-misrecognition/.

politics, security and markets. At the same time, knowledge about the inner state of mind makes people vulnerable and exposed to manipulation[72]".

Indeed, the AI technologies used for emotion recognition are closely related to the issue of personal data protection – and the related discipline of consent to their use – relevant in particular, in the context of artificial intelligence systems used to assist the vulnerable, particularly older people (subjects placed in a particular condition of vulnerability, that should be made more aware of the collection, processing of their personal data and, in particular, of the controls put in place to ensure the proper functioning of the devices).

Consequently, questions arise whether prevailing and upcoming laws adequately respond to emotion tech[73] .

Indeed, the objective is to investigate the scope of the concept of emotion data so as to embrace the limits that the Union legislation on the subject prepares, wondering whether there is adequate protection for the individuals to whom such emotions belong.

Through the application of machine learning algorithms and statistical analysis, emotional AI could generate inferences about human emotions, bringing with it both benefits and concerns. On the one hand, it has been ascertained how the use of these technologies could contribute to improving the well-being of specific vulnerable groups by being able to identify situations of stress or dissatisfaction, use the acquisition of such information to improve the quality of users' experience by adapting their interactions with the outside world based on their emotions; on the other hand, their use raises important ethical and privacy issues[74]. Moreover, it is critical to ensure that emotion monitoring is done transparently and with respect for the privacy of these individuals.

The use of emotional AI also raises concerns about the possibility of manipulating emotions themselves[75]. Despite the progress that has been made, therefore, there are several challenges to be faced, and above all, it is good to consider that emotions are highly subjective and influenced by cultural, social and personal factors: accurately interpreting emotions requires understanding the context in which they arise.

In this regard, it is necessary to start with the assumption that emotion is sometimes not just a simple feeling, but also a particularly sensitive type of information. "The decision to share one's emotions should be an individual choice, so teaching machines to recognize and interpret these signals accurately is a complicate challenge, (e.g. cases where emotions often exhibit ambiguity and complexity, making it difficult to classify them into distinct labels)"[76]. Indeed, emotional states can evolve rapidly and manifest themselves in subtle variations that may be difficult to identify accurately.

---

[72] E. 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", *European Data Protection Law Review*, 8, 2, 2022, pp. 311-319.
[73] *Ibidem.*
[74] See, *supra*, nt. 39.
[75] M. FRANKLIN, H. ASHTON, R. GORMAN and S. ARMSTRONG, "The EU's AI Act Needs to Address Critical Manipulation Methods", *OECD.AI*, 2023, https://oecd.ai/en/wonk/ai-act-manipulation-methods.
[76] See again, *supra*, nt. 39.

The use of these technologies has presented significant critical issues related to the framing of emotional data collected by the algorithm within the group of biometric data.

In fact, one of the main problems is precisely qualifying: the Regulation, in its definition of emotion recognition systems[77], focuses on the use of biometric data; however, these are not the only elements used in emotion scanning activity.

Under this definition, emotional data would be equated with biometric data. However, the reference to biometric data alone would make the discipline incomplete, limiting it, as it has been possible to note how these systems can also be based on non-biometric data (for instance, there are numerous cases of technologies used to recognize emotions based on a written text). The AI Act, regarding the protection of personal data, frames emotions among "information/data with sensitive characteristics" (Recital 54), such as other particularly relevant personal data.

Specifically, in Recital 14 it provides that "Biometric data may enable authentication, identification or categorization of natural persons and recognition of the emotions of natural persons".

On this point, different authors appear to be divided: a part[78] of them believes that emotional data is comparable to biometric data and, as such, the regulations prepared by the GDPR, as well as Article 9, which identifies biometric data as particularly sensitive data, should be extended to them by analogy. The other part[79] , on the other hand, believes that the notion should be broadened to include non-biometric data and that it needs ad hoc regulation, as emotional data cannot essentially qualify as sensitive data, since it is not present within the exhaustive listing in Article 9 of the GDPR. Ultimately, the approach taken in Affective Computing systems determines whether processing personal data used to detect or derive emotion data falls under the scope of Article 9 GDPR.

"According to the wording of Article 9(1) GDPR, biometric data is only protected as special personal data if it is used for the purpose of uniquely identifying an individual. This means "processed through a specific technical means allowing the unique identification or authentication of a natural person (recital 51 GDPR)"[80].

Hence, reducing emotions on the qualifying level to biometric data alone would *de facto* exclude similar systems.

Moreover, under the GDPR, emotion AI would seem to be subject to the same requirements for processing personal data as any other form of data processing. In this

[77] See art. 3., 39) AI Act: "emotion recognition system" means an AI system aimed at identifying or inferring emotions or intentions of individuals based on their biometric data.
[78] A. McSTAY, "Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy", *Big Data & Society*, 7, 1, 2020, pp. 3-4; N. PURTOVA, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", *Law, Innovation and Technology*, 10, 1, 2018, pp. 74-75.
[79] A. HÄUSELMANN, "Fit for purpose? Affective Computing Meets EU Data Protection Law", *International Data Privacy Law,*11, 3, 2021, pp. 245-251, 2021.
[80] A. HÄUSELMANN, E. FOSCH-VILLARONGA, A.M. SEARS and L. ZARD, "EU Law and Emotion Data", 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII), 2023, pp. 1-8.

sense, according to Article 6 of the GDPR, processing can take place, in addition to predetermined purposes, only if there are suitable legal bases, that are conditions under which processing is considered lawful. Moreover, any processing of personal data can only be carried out within the limits of specific and predetermined purposes.

It is necessary to provide clear and transparent information about the processing of personal data, including the purposes of processing and the categories of data processed[81].

A high influx of data raises a number of questions about the dissemination and control of information descending from the use of such devices.

From a regulatory perspective, data protection is essentially delegated to compliance with the GDPR by treating emotional data in the same way as any personal data.

As a consequence, it is outlined that emotion data is not protected as 'special data' according to Art. 9 of the GDPR despite its sensitive nature and the related impacts processing such data may have on people. For that reason, it is also tricky for the affective computing community to consider the applicable legal requirements when developing Affective Computing systems that involve study participants in the EU or intended for the EU market. For instance, processing special data is prohibited under the GDPR unless an exception applies. Whether processing of personal data used to detect or derive emotion data falls under the framework applicable to special personal data (Art. 9 GDPR) depends on the approach taken in Affective Computing[82].

This leads to a significant gap in legal protection. It could be argued that emotions should be regulated like human speech or text because both somehow define humanity. In this way, the inherently highly sensitive nature of emotion data and the close link with one's personhood merits specific protection.

"It seems that the GDPR fails to keep up with technological developments, which leads to a gap of protection".

In light of these considerations, it is clear that the rapid progression of AI systems in its ability to understand human emotions necessitates the implementation of safeguards to protect the processing of this category of data, prevent emotional manipulation, and address the biases that may emerge from emotion recognition algorithms.

Although regulatory impulses are entailed by existing dispositions, a more explicit regulation addressing the management and the protection of such data and technologies is – perhaps – needed at this point.

4. AI'S ISSUES IN THE AMERICAN LEGAL SYSTEM

[81] *Ibidem*.

[82] Approaches that process physiological information fall under the scope of Article 9 GDPR, whereas visual approaches relying on the processing of facial expressions do not.

"The relationship between the EU and the U.S., major players in the race for AI leadership, can be named paradoxical in several respects[83]". On the one hand, the U.S. has prepared a patchwork of regulatory acts on the subject of AI, leading up to the most recent presidential directive (Executive Order 14110[84]) aimed at setting binding guidelines and fostering research and innovation; on the other hand, the EU, with the AI Act, aims to define a regulatory framework capable of coping with the negative consequences that derive from their systematic use in certain areas (e.g., health and individual well-being)[85]. At the same time, despite the diversity of approaches[86] just outlined, which is linked to historical, economic and social reasons, there is a gradual convergence between the EU and the U.S., evidenced in particular by two phenomena: the "Act-ification" process[87] which places the EU alongside the U.S. regulatory model, and the Brussels effect[88], which describes the opposite process. This phenomenon is particularly evident in the area of personal data protection, where the high levels of protection posed by the GDPR prevent the U.S. from setting a level of protection that is not substantially equivalent[89], running the risk of not being allowed to enjoy the gains from the European market.

This prompts the U.S. to avoid the provision of an organic body of regulation, preferring more fragmentation[90], in order to prevent excessive and stringent regulation from limiting systems development and competitiveness.

---

[83] V. SALVATORE (ed), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, Giappichelli 2023, p. 126.

[84] G. AMADEO, "L'AI ACT e l'Executive Order a confronto – I differenti approcci regolamentari dell'Europa e degli Stati Uniti per affrontare i rischi comuni dell'intelligenza artificiale", *Altalex*, 2023, https://www.altalex.com/documents/news/2023/12/23/ai-act-executive-order-a-confronto. Reference is also made to the work of M. BASSINI, "La corsa globale per regolamentare l'intelligenza artificiale: effetti di ricaduta dell'ordine esecutivo di Biden sulla legge UE sull'intelligenza artificiale", *MediaLaws*, 2024, who argues that "After the adoption of the Blueprint for an AI Bill of Rights in October 2022, the U.S. administration seems to have adopted a more pragmatic approach, despite the predominantly programmatic nature of the Executive Order, which nevertheless embodies a clear agenda-setting ambition", full text of the article available at the following link https://iep.unibocconi.eu/global-race-regulate-ai-bidens-executive-order-spillover-effects-eu-ai-act.

[85] *Supra*, nt. 104, p. 127-129.

[86] E. MAZZA, "Regole su intelligenza artificiale, ecco le differenze tra Ue e Usa", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/mercati-digitali/tutela-dei-diritti-dai-rischi-dellai-approcci-ue-e-usa-a-confronto/.

[87] See V. PAPAKONSTANTINOU, "The Act-ification of EU Law: The (Long-Overdue) Move toward 'Eponymous' EU Legislation", *European Law Blog*, 2021, https://europeanlawblog.eu/2021/01/26/the-act-ification-of-eu-law-the-long-overdue-move-towards-eponymous-eu-legislation/; V. PAPAKONSTANTINOU and P. DE HERT, "The Regulation of Digital Technologies in the EU: The Lw-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'", *Technology and Regulation Journal,* 2022, p. 49.

[88] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020, p. 299; V. E. CHITI and B. MARCHETTI, "Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale", *Rivista della regolazione dei mercati*, 2020, p. 30.

[89] G. CAPUZZO, "A(I) Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina", *Rivista Critica del Diritto Privato*, 4, 2022, p. 479.

[90] The so-called "fragmented approach." See, again, *supra*, nt. 104, p. 131, where it is pointed out that "At the European level, the push for digitization, inspired in some ways by the American model, nevertheless seems not to take sufficient account of the implications of a strategy to promote the development of innovative technologies".

In fact, there is no comprehensive and organic federal legislation in the United States that specifically addresses AI[91]. Instead, AI systems are governed by a set of federal (and state[92]) laws and regulations that apply to specific areas[93].

Among the early regulatory initiatives that have emerged at the federal level, particular mention should be made of: the American AI Initiative[94], established in 2019 by the Trump administration through Executive Order 13859, which enunciates a set of key goals that can ensure standardized, secure and reliable AI systems; the National Artificial Intelligence Initiative Act of 2020[95], enacted to strengthen U.S. technology leadership globally; the Algorithmic Accountability Act of 2022[96] aimed at ensuring the transparency and oversight of software, algorithms and other automated systems; the Biden administration's Blueprint for an AI Bill of Rights[97], released in January 2023 by the White House Office of Science and Technology Policy, whose guidelines identify five principles aimed at regulating the design, use and implementation of AI-based automated systems to protect the rights of U.S. citizens.

Most recently, the Biden administration, after the adoption of AIBoR, would take a more pragmatic approach through the U.S. policy and strategic position on the creation, deployment, and use of AI models, outlined in the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, signed by Biden on October 30th, 2023. In contrast to the European human-centric view, the U.S. prefers a business-friendly approach, aimed at fostering business and the development of AI systems.

As for the state law level, on the subject of AI, the notable regulatory initiatives by state legislators with respect to the federal Congress are noteworthy: in addition to the introduction of numerous bills with a wide variety of contents, there has been the establishment of new administrative authorities with AI competencies and advisory

[91] From a careful analysis of the U.S. system, it is possible to see that over the past few years there have been a great number of legislative interventions on the subject of AI, both at the state and federal levels, to such an extent that the legislative framework characterizing the U.S. is considered to be largely heterogeneous. The *Executive Order* itself has practical purposes limited to the level of principles, without having any major legal impact, except for a few provisions D.J. FELZ *et al.*, "Privacy, Cyber & Data Strategy Advisory: AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023", *ALSTON & BIRD*, 2022, https://www.alston.com/en/insights/publications/2022/12/ai-regulation-in-the-us.

[92] As for state initiatives, however, this is not the place to fully analyze the taxonomy of protective measures and individual regulatory initiatives.

[93] See P. CIHON, M.M. MAAS and L. KEMP, "Should Artificial Intelligence Governance be Centralised? Six Design Lessons from History", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, New York, 2020, pp. 228-234. (defining "fragmentation or decentralization" as a "patchwork of international organizations and institutions which focus on a particular issue area [like A.I.] but differ in scope, membership and often rules"). An example of this is the multitude of different international environmental agreements and treaties.

[94] See Trump White House, "Artificial Intelligence for the American People", 2019, https://trumpwhitehouse.archives.gov/ai/.

[95] 116th Congress, National Artificial Intelligence Initiative Act (H.R.6216), 2020, https://www.congress.gov/bill/116th-congress/house-bill/6216.

[96] 117th Congress, Algorithmic Accountability Act (S.3572), 2022, https://www.congress.gov/bill/117th-congress/senate-bill/3572.

[97] V. The White House, "Blueprint for an AI Bill of Rights - Making Automated Systems Work for the American People", 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

functions[98], thus finding confirmation of the choice by political institutions – already emerged at the federal level – to rely on technical bodies at the state level as well[99].

A comparison of the two models shows that while the proposed AI bill takes a risk-based approach, defining high-risk AI systems more narrowly; in contrast, the U.S. approach appears more flexible, encompassing a wide range of technologies and leaving out high-risk AI systems.

The different *modus operandi* in the preparation of regulatory models by the EU and the U.S.[100], moreover, is relevant to an assessment of Emotion Tech.

Although AI systems based on emotional recognition[101] have been yet introduced into the market for some time, there is currently no regulation of such systems in the US.

On the issue, it was noted[102] the need to introduce targeted provisions highlighting the risks associated with emotion detection and considering the EU's choice to act against the misuse of such technologies exemplary.

One area on which, on the other hand, the two levels would seem to converge is that related to privacy and the processing of personal data[103]: while European law focuses on safeguarding fundamental rights, establishing specific and clear prohibitions on intrusive and discriminatory AI practices, relying on their compliance with the principles enshrined in the GDPR, the U.S. approach[104] focuses on safeguarding the privacy of U.S.

[98] See Colorado Department of Regulatory Agencies - Insurance Division, "Protecting Consumers from Unfair Discrimination in Insurance Practices (SB21-169)", 2021, https://doi.colorado.gov/for-consumers/sb21-169-protecting-consumers-from-unfair-discrimination-in-insurance-practices. On this issue, see B. MARCHETTI and L. PARONA, "La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio", *DPCE online*, 1, 2022, p. 244, esp. nt. 26-27.

[99] For example, some states, such as Colorado, have long since completed the legislative process by introducing a ban on the use of certain predictive algorithms in the insurance industry. This is further detailed in E. STRADELLA, "Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)", *DPCE online*, 51, 1, 2022, p. 219, https://www.dpceonline.it/index.php/dpceonline/article/view/1569/1551. At the state level, most AI-focused bills fall into different categories: the first includes bills aimed at ensuring greater transparency, relative to the design, development and use of AI technologies. Consider, for example, California, where Senate Bill No. 1047, aimed at requiring safety testing of AI products before their release, was introduced last February; the second category, on the other hand, focuses on specific areas, particularly on the use of AI systems to determine or assist in decisions related to personnel selection, housing allocation, and other important issues, which, however, have shown significant shortcomings.

[100] E. MAZZA, "Regole su intelligenza artificiale, ecco le differenze tra Ue e Usa", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/mercati-digitali/tutela-dei-diritti-dai-rischi-dellai-approcci-ue-e-usa-a-confronto/.

[101] As for the European framework, regulation of emotion recognition systems is indeed emerging, but it is far from being sufficient and effective.

[102] See Senator Ron Wyden's webpage, press releases, "EU Restrictions on AI Emotion Detection Products", 2023, https://www.wyden.senate.gov/news/press-releases/eu-restrictions-on-ai-emotion-detection-products.

[103] A. MANTELERO, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", *Computer Law & Security Review*, 34, 2018, p. 754; see, *supra*, nt. 110.

[104] Sec. 2 and Sec. 9 Executive Order. Also, on the comparison between the AI Act and Executive Order, see, *supra*, nt. 111, M. BASSINI, which states that "the Executive Order clarifies the federal government's commitment to ensuring that 'the collection, use, and storage of data are legal, secure, and mitigate risks

citizens, recognizing the increasing risk of exploitation-abuse of personal data that AI has resulted in over time[105].

Also, with regard to the principle of transparency, both the AI Act and the Executive Order recognize that users should be made aware by providers of their interaction with AI systems, so as to ensure that privacy and self-determination are respected.

This distinguishes, indeed, the European "human-centered[106]" view, based on the risk-based classification of AI systems and the provision of a set of horizontal obligations and related penalty provisions, from the more business-friendly U.S. approach, which prefers fragmented and broader regulation without resorting to rigid regulations that could make technological progress unduly burdensome.

The main difference that distinguishes the U.S. on AI from the EU is that, while the centralized European model allows for more effective oversight, implementation, and adaptability capable of encouraging the participation of members of society, presenting numerous advantages (including the elimination of conflicting or overlapping laws; the reduction of forum shopping perpetrated by fragmented legislation); on the other hand, the U.S. fragmented approach introduces guidelines that are too broad and non-binding, not caring about the risks AI poses with respect to fundamental rights or identifying possible means of protection[107].

Despite the points highlighted/outlined, a centralized approach cannot be considered inherently better than a fragmented one, not lacking significant risks, such as slow and fragile legislation. In addition, a centralized regulatory framework risks, with its excessive rigidity, holding back European innovation[108].

Hence, it emerges the need to build connecting bridges to fill the respective gaps.

5. CONCLUDING REMARKS

The analysis leads to some brief considerations.

AI has now become an integral part of the individual's daily life (not always with the same awareness), conditioning their choices and opportunities and, above all, individual freedoms. This poses the need to address in the most appropriate way the challenges

related to privacy and confidentiality. Interestingly, among the technical tools available, the Executive Order encourages the use of privacy-enhancing technologies".

[105] With all the misgivings arising from the fact that the United States has yet to have a federal privacy framework.

[106] See R. PANETTA, "AI Act, Panetta: 'Ecco la via per una tecnologia al servizio dell'umanità'", *AgendaDigitale*, 2023, https://www.agendadigitale.eu/cultura-digitale/ai-act-panettaue-sulla-strada-giusta-ma-ancora-non-basta/.

[107] This, however, occurred during Biden administration through the drafting of the AIBoR to protect individual rights and democratic principles.

[108] V. ZENO-ZENCOVICH, "Artificial Intelligence, Natural Stupidity and Other Legal Idiocies", *MediaLaws*, 2024, https://www.medialaws.eu/rivista/artificial-intelligence-natural-stupidity-and-other-legal-idiocies/.

and risks inherent in the digital society, putting the individual at the center of legal consideration[109].

The several initiatives and the various acts adopted by EU[110] in recent years have led to the establishment of a regulatory framework aimed at regulating the prerequisites, limits and methods of use of AI systems, as well as the spread of digitization processes, to ensure greater protection for individuals/users.

The above-mentioned hypotheses also raise questions inherent in the coordination between the legal regime of personal data and that of AI. What is problematic is not so much the identification of principles and rules of conduct, but their concrete application to AI systems[111].

Giving a look to devices for detecting the emotional state of the user[112], one of the most recently debated issues by European institutions (and not only[113]) has been to develop an appropriate and transparent framework on the design and subsequent use of AI systems, having the function of recognizing the emotions of individuals[114].

Among the critical issues concerning the operation of these systems and the various risks associated with their use, a first aspect concerns the possible forms of discrimination (of race, gender, and, above all, age) that the devices in question would

[109] E. BATTELLI, "Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona", *Diritto di Famiglia e delle Persone*, 3, 2022, p. 1096; European Parliament, "EU AI Act: First Regulation on Artificial Intelligence", 2023, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[110] M. EBERS, "Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act", in L.A. DI MATTEO, N. CANNARSA and C. PONCIBÒ (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge, Cambridge University Press, 2022, *passim*; A. RENDA, A. ENGLER, "What's the Name? Getting the Definition of Artificial Intelligence Right in the EU's AI Act", *CEPS Explainer*, 2023, https://www.ceps.eu/ceps-publications/whats-in-a-name/.

[111] On the subject of fundamental rights and freedoms in the digital realm see, again, *supra*, nt. 4, "It is necessary, therefore, to understand how this legislation will go about incorporating these principles and rules, wondering, for example, about the role that the 'fundamental-rights oriented' rules of the GDPR should play in cases of interpretive doubt".

[112] T.R. MOSLEY, "AI Isn't Great at Decoding Human Emotions. So Why are Regulators Targeting the Tech?", *MIT Technology Review*, 2023, https://www.technologyreview.com/2023/08/14/1077788/ai-decoding-human-emotions-target-for-regulators/.

[113] The White House, "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/; Congressional Research Service, L. A. HARRIS and C. JAIKARAN, "Highlights of the 2023 Executive Order on Artificial Intelligence for Congress - (R47843)", 2023, https://crsreports.congress.gov., chrome-extension://efaidnbmnibpcajpcglclefindmkaj/https://crsreports.congress.gov/product/pdf/R/R47843.

[114] On transparency, see, again, D. DELLA ROSA and F. CRISCUOLI, "AI Act, pratiche vietate e regole per i sistemi ad alto rischio nel segno della trasparenza e sicurezza", *NT+Diritto – Il Sole 24ore*, 2023, https://ntplusdiritto.ilsole24ore.com/art/ai-act-pratiche-vietate-e-regole-i-sistemi-ad-alto-rischio-segno-trasparenza-e-sicurezza-AFH5Quv.

determine[115]. Under such an assumption, there would be a risk of unreliability of those AI systems made on the basis of emotion recognition modalities.

A second problematic aspect determined by these technologies concerns the individual's inability to refute the result produced by the algorithm: it would, in fact, be particularly complex to prove the error made by the algorithm when analyzing facial expressions or collecting the user's biometric data.

Finally, the use of AI systems also raise certain concerns, relating to the protection of vulnerable persons' privacy and the processing of personal data (for instance, older persons may not always understand how the technology works or how their data is being used).

This is because the operation of such technologies requires the processing of a large amount of special data (especially biometric and health data), which, when combined, can easily lead to user identification[116].

For these reasons, on the one hand, the main concern is that AI systems – especially those of future design – may be regulated on the basis of a regulation that is still considered sufficiently generic, risking, moreover, a failure in adapting to developments in this field; on the other hand, the principles of the GDPR cannot be disregarded, given that artificial intelligence itself feeds on data and, in particular, precisely on data of a personal nature.

Therefore, it is crucial to make sure that the applicable laws at each stage of the life cycle of an AI system are in place to ensure the compliant and ethical processing of personal data, pursuing a clear, legitimate, and well-defined purpose at the beginning of the project.

Indeed, in recent years, interventions in the field of AI have been characterized by a proactive approach, aimed at extracting from this technology the positive effects for citizens and businesses while mitigating the harmful ones[117]. However, to date, several concerns remain unsettled (also in view of the fact that new systems not yet envisaged under the AI Act and the creation of new methods aimed at implementing artificial intelligences – changing their level of risk – will result from the digitization process).

The provisions on AI, in fact, would represent, especially in the view of the European legislator, an expression of a "new" protection of the rights of the individual, related to the processing of personal data, affected by new technologies. Nevertheless, on this point some critical issues have been raised inherent in the compliance of these rules with the GDPR and the concrete effectiveness of transparency obligations, which is expressed in the remedy of notification to the data subject at the time of interaction

[115] M. HILDEBRANDT, "Discrimination, Data-Driven AI Systems and Practical Reason", *European Data Protection Law Review* (EDPL), 7, 3, 2021, p. 358.

[116] G. D'ACQUISTO, "Intelligenza artificiale, obiettivo regole privacy per renderla 'umana'", *AgendaDigitale*, 2021, https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-e-protezione-dati-le-regole-per-comprendere-il-senso-della-tecnologia/.

[117] G. FINOCCHIARO, "La regolazione dell'intelligenza artificiale", *Rivista Trimestrale di Diritto Pubblico*, 4, 2022, p. 108.

with an AI system for emotion recognition[118]. Hence, the reference in the AI Act to the Data Protection Regulation would seem in some respects insufficient in the face of the more complex phenomenon of AI, and may, as a result, fail to ensure effective protections. The text of the AI Act itself appears particularly deficient, ambiguous and contradictory.

It is difficult at present to make predictions about future prospects, partly because the debate does not propose clear outcomes and the issue is not yet well defined, given the lack of practical application of AI provisions.

To pursue these aims, therefore, it seems desirable to identify a balance between the technical aspects related to the development of new AI solutions and an optimal use of the same[119], aimed solely at the elaboration of concrete safeguard tools[120] necessary for the production of enhanced protection in the hands of those subjects placed in a condition of particular vulnerability[121] (such as, precisely, older adults).

[118] See, *supra*, nt. 60, S. TROZZI.
[119] By placing itself in dialogue with the other sciences and prospecting, at the same time as the algorithms that apply AI are conceived and designed, the legal issues that come to the fore through their use.
[120] Aimed at protecting privacy, preventing emotional manipulation and addressing biases that may arise in emotion recognition algorithms.
[121] C. EQUIZI, "Il limite delle risorse disponibili nella tutela dei diritti delle persone vulnerabili", *Dirittifondamentali.it*, 2, 2023, p. 690; V. LORUBBIO, "La tutela dei soggetti vulnerabili", *DPCE online*, 1, 2020, p. 661.