RICONOSCIMENTO DELLE EMOZIONI E MARKETING PERSONALIZZATO

Di Roberta Montinaro

SOMMARIO: ***Premessa - 1. Il riconoscimento delle emozioni alla luce della regolamentazione in materia di protezione dei dati personali - 1.1. La qualificazione giuridica dei dati analizzati dagli ERS: quando si ha trattamento di dati biometrici ai sensi del GDPR? – 1.2. Pratiche di mera rilevazione di bio-caratteristiche di persone fisiche per desumerne le emozioni: si applica il GDPR? – 1.3. Se le emozioni possano considerarsi dati 'particolari' ai sensi dell'articolo 9 (1) GDPR – 1.4. Il riconoscimento delle emozioni come forma di trattamento automatizzato ai sensi del GDPR – 2. Il riconoscimento delle emozioni per fini di pubblicità personalizzata secondo le disposizioni europee in tema di pratiche commerciali sleali e sui servizi digitali – 3. Le disposizioni del Regolamento europeo sull'IA in materia di riconoscimento delle emozioni e di categorizzazione biometrica.***

ABSTRACT. L'articolo esamina i sistemi di riconoscimento delle emozioni e il loro utilizzo nel campo della pubblicità personalizzata adottando la prospettiva del diritto dell'Unione europea. L'identificazione delle emozioni di un individuo attraverso l'uso di tali sistemi consiste in una forma di profilazione basata sull'analisi di dati relativi a caratteristiche biologiche umane, da cui è possibile estrarre informazioni personali, comprese informazioni 'sensibili'. Forme di trattamento di questo tipo mettono in crisi il concetto di 'identità' e 'identificazione', in particolare quando si adottano tecniche che appaiono lontane da quelle in uso nelle tecnologie di identificazione biometrica. L'intera gamma di disposizioni e principi desumibili dal GDPR attinenti ai c.d. trattamenti automatizzati, compresi i principi di trasparenza, accuratezza e correttezza, si applicano al riconoscimento delle emozioni. L'analisi prende in considerazione anche il punto di vista della direttiva 2005/29/CE e delle disposizioni sulla pubblicità online introdotte dal Regolamento europeo sui servizi digitali. L'articolo analizza infine la portata della definizione di sistemi di riconoscimento delle emozioni nel Regolamento europeo sulla commercializzazione, immissione in servizio e uso di sistemi di intelligenza artificiale, che considera questa tecnologia come parte della 'seconda generazione' di tecnologie biometriche volte a caratterizzare gli individui piuttosto che a identificarli. Il suddetto regolamento classifica i sistemi in oggetto come sistemi di IA ad alto rischio. Inoltre, stabilisce una forma di coordinamento tra le autorità incaricate della supervisione delle pratiche di utilizzo di tali sistemi di IA e le altre autorità di controllo nazionali e dell'UE, contribuendo così a migliorare i meccanismi di enforcement previsti in altre aree del diritto dell'UE.

This article examines emotion recognition systems and their use in the field of personalised advertising from the perspective of EU law. The identification of an individual's emotions through the use of an emotion recognition system is a form of

ISSN 2239-8570

profiling based on the analysis of data on human biological characteristics, from which personal information, including 'sensitive' information, can be extracted. Forms of processing of this kind undermine the concept of 'identity' and 'identification' established by the GDPR, particularly when adopting techniques that appear far removed from those in use in biometric identification technologies. The full range of provisions and principles laid down by the GDPR for automated processing, including the principles of transparency, accuracy and fairness, apply to emotion recognition. The analysis also considers the point of view of Directive 2005/29/EC and the provisions on online advertising in the Digital Services Regulation. Finally, the article analyses the scope of the definition of emotion recognition systems in the EU Regulation laying down armonised rules on the placing on the market, putting into service and use of artificial intelligence systems, which considers this technology as part of the 'second generation' of biometric technologies aimed at characterizing individuals rather than identifying them. This regulation classifies these systems as high-risk AI systems. Moreover, it establishes a form of coordination between the authorities in charge of supervising the practices of using such AI systems and other national and EU supervisory authorities, thus helping to improve the enforcement mechanisms provided for in other areas of EU law.

ISSN 2239-8570

Premessa.

Molteplici campi di ricerca, tra cui le neuroscienze, ambiscono a definire e interpretare le emozioni umane, nonché a misurarne l'incidenza sul comportamento umano[1]. Le conoscenze conseguite in tali campi sono utilizzate per sviluppare i c.d. sistemi di riconoscimento delle emozioni ('emotion recognition systems', d'ora in poi "riconoscimento delle emozioni' o 'ERS'), un tipo di intelligenza artificiale (di seguito 'IA') che impiega svariate tecniche (come l'analisi dei tratti del viso[2], del corpo, della voce[3], del linguaggio[4] , l'esame EEG, etc.) per rilevare le caratteristiche fisiche, fisiologiche o comportamentali delle persone fisiche (d'ora in poi, per brevità, 'bio-caratteristiche') e identificarne le emozioni[5].

Più in dettaglio, tali sistemi si basano su una specifica 'teoria delle emozioni': innanzitutto presumono che le emozioni umane siano desumibili da determinate bio-caratteristiche 'sintomatiche'[6] (ad esempio, che il sorriso significhi felicità, che digitare nervosamente sulla tastiera di un computer indichi rabbia, ecc.) ed universali (non variabili a seconda degli individui o delle culture); essi poi presuppongono che dalle rilevate emozioni possano dedursi informazioni sugli individui. Pertanto, il riconoscimento automatizzato delle emozioni, da un lato, comporta un processo di 'datificazione' delle emozioni umane, dall'altro, implica una forma di categorizzazione delle persone fisiche sulla base delle loro emozioni[7] .

[1] Si vedano J.S. LERNER, Y. LI, P. VALDESOLO, K.S. KASSAM, *Emotion and Decision-Making*, in *Annu. Rev. Psychol.*, 2015, 66, 799 ss. D. CLIFFORD, *Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?*, in, *Future Law: Emerging Technology, Regulation and Ethics* a cura di L. Edwards e altri, Edinburgh, 2020.

[2] Per avere un'idea di questo tipo di tecnologia e dei suoi utilizzi, si può consultare https://www.morphcast.com/. Una demo è disponibile all'indirizzo https://demo.morphcast.com/sdk-features/index.html?video=&sv=false&emotionBalancer=true&features=DCE5CC6B7.

[3] P. FILIPPI, *Emotion communication through voice modulation: Insights on biological and evolutionary underpinnings of language. Theoria et Historia Scientiarum*, 2019, 16, 83 ss.

[4] T. WANI ET AL, *A comprehensive review of speech emotion recognition systems*, in *IEEE Access*, 2021, 9, 47795 ss, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9383000.

[5] S. PAL, S. MUKHOPADHYAY, N. SURYADEVARA, *Development and progress in sensors and technologies for human emotion recognition*, in *Sensors*, 2021, 21(16), 5554 ss. Si vedano anche R. GILL, J. SINGH, *A Review of Neuromarketing Techniques and Emotion Analysis Classifiers for Visual-Emotion Mining*, in *2020 9th International Conference System Modeling and Advancement in Research Trends* (SMART), 2020, 103 ss.

[6] L. STARK, J. HOEY, *The Ethics of Emotion in Artificial Intelligence Systems*, 1 ss, in FAccT '21: 2021 *ACM Conference on Fairness, Accountability, and Transparency*, 2021, DOI:10.1145/3442188.3445939.

[7] Il termine è stato coniato da K. CUCKIER, V. MAYER-SCHÖNBERGER, *The Rise of Big Data: How It's Changing the Way We Think About the World*, in *Foreign Affairs*, 2013, 92, 28 ss. Si veda anche H. RUSCHEMEIER, *Data Broker and European Digital Legislation*, in EDPL - *European Data Protection Legislation*, 2023, 9, 27-38, nonché il Gruppo di lavoro "Articolo 29", istituito dalla direttiva 95/46/CE (d'ora in poi, nelle note e nel corpo del documento 'Gruppo di Lavoro art. 29'), Opinion n. 3/2013, WP 80 (01.08.2003), 4:

Sino a tempi recenti, l'impiego di questa tecnologia per scopi commerciali è stato trascurato dalla letteratura giuridica[8]. Eppure, gli ERS sono incorporati in molti beni di consumo[9] e vengono utilizzati nel contesto del cosiddetto 'neuromarketing', un campo della ricerca di marketing il quale mira a conseguire una conoscenza approfondita su gusti, preferenze, etc., dei consumatori, grazie all'analisi dei processi decisionali inconsci di tali soggetti[10]. Le emozioni sono infatti considerate alla stregua di una 'finestra' per l'osservazione dei tratti psicologici dei consumatori[11] e quindi per determinarne la personalità e, in ultima analisi, l'identità, molto spesso con l'obiettivo ultimo di costruire profili dei consumatori e di prevederne il comportamento (dal comportamento di acquisto alla decisione di voto)[12]. Ne

"Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use".

[8] Tuttavia, si vedano P. VALCKE, D. CLIFFORD, V. K. DESSERS, *Constitutional Challenges in the Emotional AI Era, in Constitutional Challenges in the Algorithmic Society*, a cura di Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor e Giovanni De Gregorio, 2021, Cambridge, 57 ss.; M. DUROVIC, J. WATSON, *Nothing to Be Happy about: Consumer Emotions and AI*, in *J Multidisciplinary Scientific Journal* 2021, 4, 784 ss, https://doi.org/10.3390/j4040053; D. CLIFFORD, *The Legal Limits to the Monetisation of Online Emotions*. Tesi di dottorato, KU, Leuven, Belgio, 2019; A. MCSTAY, V. BAKIR, L. URQUHART, *Briefing Paper: All Party Parliamentary Group on Artificial Intelligence-Emotion Recognition: Trends, Social Feeling, Policy; Emotional AI*, Londra, 2020, https://www.researchgate.net/publication/344433149_EMOTION_RECOGNITION_TRENDS_SOCIAL_FEELING_POLICY_Briefing_paper_All_Party_Parliamentary_Group_on_Artificial_Intelligence. Per la dottrina italiana, tra i primi contributi spicca il saggio di E.M. INCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale*, in *Giustizia civile*, 2022, 2, 515 ss.

[9] Cfr. Gruppo di lavoro art. 29, Opinion 02/2012 sul riconoscimento facciale nei servizi online, WP192, 4.1, in ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf: "A games console uses a gesture control system where movements of the user are detected in order to provide controls to the game. The camera(s) used for the gesture control system share images of individuals with a facial recognition system which predicts the likely age, gender and mood of the game players. Data, including that from other multimodal factors, may then alter the game play to enhance the user experience or to change the environment to reflect the user's predicted profile. In a similar manner, a system could classify users to allow/deny access to age-related content or to display in-game targeted advertising".

[10] M. ALIMARDANI, M. KABA, *Deep Learning for Neuromarketing; Classification of User Preference using EEG Signals*, 2021, 1 ss, https://doi.org/10.1145/3460881.3460930. Gli esperti di neuromarketing sono interessati a identificare i meccanismi cognitivi dei consumatori e a misurare le risposte implicite. Per un'ampia panoramica degli usi dell'IA nel marketing, si veda MING-HUI HUANG, ROLAND T. RUST, *A strategic framework for artificial intelligence in marketing*, in *Journal of the Academy of Marketing Science*, 2021, 49, 30 ss, https://doi.org/10.1007/s11747-020-00749-9. Cfr. altresì L. TAFARO, *Some reflections on neurosciences and civil law*, in *Neurosciences and Law: complicated crossings and new perspectives*, a cura di Antonio D'Aloia e Maria Chiara Errigo, Springer 2020, 113 ss., nonché E. TUCCARI, Neuromarketing*: un'asistematica disciplina…oltre il consenso?*, in Persona e mercato, 2024, 2, 511 ss.

[11] Cfr. S. C. MATZ, O. NETZER, *Using big data as a window into consumer's psychology*, in *Current Opinion in Behavioral Sciences*, 2017, 7 ss., https://doi.org/10.1016/j.cobeha.2017.05.009.

[12] Cfr. M. RAMIREZ, S. KAHEH, K. GEORGE, *Neuromarketing Study Using Machine Learning for Predicting Purchase Decision*, in 2021 *IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference* (UEMCON), 2021, 560 ss.,

ISSN 2239-8570

discendono rischi di lesione del diritto alla protezione dei dati personali e della vita privata, nonché del diritto a non essere discriminati né rappresentati in modo inaccurato. Inoltre, le conoscenze acquisite grazie a tale metodologia possono essere utilizzare per distorcere il processo decisionale dei consumatori facendo leva sulle vulnerabilità associabili a determinate emozioni – comprese emozioni e stati d'animo 'negativi'[13] (quali rabbia, paura o disgusto, etc.).

Il riconoscimento delle emozioni si differenzia dall'analisi dei 'sentimenti' (*sentiment analysis*), che viceversa consiste in un'analisi computazionale dei lemmi linguistici presenti in un testo scritto, ad es. i c.d. post di utenti di social networks o le recensioni degli utenti di un servizio digitale, per determinarne la generale inclinazione (ad es. nei confronti di beni o servizi, ma anche di opinioni espresse da imprese ed enti, uomini politici etc.). Di norma, questa forma di analisi non mira a riconoscere emozioni specifiche e i suoi usi sono più limitati rispetto all'analisi delle emozioni[14]. I dati testuali utilizzati sono spesso anonimizzati ed elaborati in forma aggregata[15], con la conseguenza che questa metodologia non comporta rischi paragonabili a quelli insiti nell'analisi delle emozioni. Tuttavia, i due tipi di analisi possono essere eseguite congiuntamente per ottenere una più approfondita comprensione delle emozioni, degli atteggiamenti e persino della personalità di un individuo[16] .

Il presente articolo intende prendere in analisi i sistemi di riconoscimento automatizzato delle emozioni ed il loro impiego nel campo del marketing e della pubblicità personalizzati, adottando il punto di vista del diritto dell'Unione europea. La personalizzazione del marketing e della pubblicità costituisce una pratica commerciale che utilizza tecniche di apprendimento automatico, per adattare informazioni commerciali o di altro tipo (ad esempio di contenuto politico[17]) alle caratteristiche e ai tratti della personalità dei destinatari delle informazioni. In questo caso, le persone fisiche vengono prima '*categorizzate*' (vale a dire segmentate in gruppi) e

---

E. MOSES, K.R. CLARK, *The Neuromarketing Revolution: Bringing Science and Technology to Marketing Insight*, in *Anthropological Approaches to Understanding Consumption Patterns and Consumer Behavior*, IGI Global, 2020, 449 ss.

[13] A. MC STAY, *Empathic media and advertising: industry, policy, legal and citizen perspectives (the case for intimacy)* in *Big Data & Society*, 2016, 1-11, 6 ss.

[14] M. RAMBOCAS, B.G. PACHECO, *Online Sentiment Analysis in Marketing Research: A Review*, in *Journal of Research in Interactive Marketing*, 2018, 12(2) 146 ss, 147. Cfr., altresì, https://www.morphcast.com/blog/sentiment-analysis-vs-emotion-ai-understanding-the-differences/.

[15] Cfr. https://www.private-ai.com/2024/03/21/sentiment-analysis-anonymization/. Si vedano anche F. VOGE, L. LANGE, *Privacy-Preserving Sentiment Analysis on Twitter*, in *Gesellschaft für Informatik (Hrsg.): SKILL* 2023, *Lecture Notes in Informatics (LNI)*, Gesellschaft für Informatik, Bonn, 2023, 1, 1 ss.

[16] P. CHAKRISWARAN, D. R. VINCENT, K. SRINIVASAN, V. SHARMA, CHUAN-YU CHANG, D. GUTIÉRREZ REINA, *Emotion AI-Driven Sentiment Analysis: A Survey, Future Research Directions, and Open Issues*, in *Appl. Sci.* 2019, 9, 5462 ss, https://www.researchgate.net/publication/337827890_Emotion_AI-Driven_Sentiment_Analysis_A_Survey_Future_Research_Directions_and_Open_Issues.

[17] J. CHESTER, K.C. MONTGOMERY, *The role of digital marketing in political campaigns*, in *Internet Policy Review*, 2017, *6*(4), 6 ss. https://doi.org/10.14763/2017.4.773.

poi '*individuate*', perché fatte oggetto di specifica attenzione (ad es., vengono 'valutate') e/o di trattamento differenziato (ricevono informazioni, appunto, 'personalizzate') rispetto alla generalità delle persone fisiche. Quando si utilizzano ERS, la categorizzazione e il *targeting* avvengono alla luce delle rilevate emozioni di un individuo. La comprensione del modo in cui questa pratica viene attuata appare indispensabile al fine di determinarne le conseguenze giuridiche.

Nel paragrafo 1 il riconoscimento automatizzato delle emozioni viene considerato alla luce del complesso sistema di norme e principi stabiliti nel Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati, di seguito 'GDPR')[18], risultante dalla interpretazione avanzata dalla Corte di giustizia dell'Unione europea e dalle pertinenti fonti di *soft law*. Si noterà come quest'ultimo sia chiamato a regolare non solo la raccolta dei dati personali necessari per i sistemi di IA e di apprendimento automatico, ma anche i processi di estrazione di 'conoscenza' a partire dai dati[19] e l'incidenza dell'impiego di tale conoscenza su un'ampia gamma di interessi giuridicamente protetti, ivi inclusi i diritti fondamentali.

Il paragrafo 2, invece, analizza le pratiche commerciali implicanti impiego di ERS dal punto di vista della direttiva 2005/29/CE[20]. Si vedrà che tale disciplina si applica, al ricorrere di date condizioni, a quelle pratiche commerciali basate sul riconoscimento automatico delle emozioni, tese a (o comunque aventi l'effetto di) distorcere il processo decisionale umano. Tale paragrafo prende poi in considerazione le disposizioni sulla pubblicità online contenute nel Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali[21] (di seguito 'Regolamento sui servizi digitali'), per giungere alla conclusione che questo ultimo *corpus* normativo, a causa del suo ridotto ambito di applicazione, contempla solo un numero limitato di simili pratiche.

Infine, il paragrafo 3 esamina le disposizioni del Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sull'intelligenza artificiale (Regolamento sull'intelligenza artificiale, di seguito 'Regolamento su IA'[22]). Il Regolamento su IA, da un lato, vieta

[18] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (L 119/1).

[19] Sui dati come conoscenza costruita si veda N. IRTI, *Il tessitore di Goethe (per la decisione robotica)*, in *Decisione robotica*, a cura di A. Carleo, Bologna, 2019, 19 ss. Per un esame critico del concetto di dato e informazione nel contesto della c.d. data economy, cfr. S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, in *Nuovo dir. civ*., 2022, 14 ss., 41.

[20] Direttiva 2005/29/CE relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE e il regolamento (CE) n. 2006/2004 [2005] GU L 149.

[21] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (legge sui servizi digitali), GU L 277 del 27 ottobre 2022.

[22] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828

ISSN 2239-8570

alcune pratiche che impiegano tali sistemi in settori specifici e, dall'altro, include gli ERS nella categoria dei sistemi di intelligenza artificiale ad alto rischio. Inoltre, talune previsioni concernenti le c.d. tecnologie di categorizzazione biometrica, contenute nel Regolamento su IA, si applicano anche agli ERS utilizzati per la pubblicità personalizzata. Come si dirà, tale Regolamento, nel disciplinare le tecnologie biometriche, mira alla 'responsabilizzazione' tanto dei fornitori dei suddetti sistemi quanto di coloro che li utilizzano (i c.d. 'deployer'[23], i quali assumono doveri autonomi e distinti da quelli desumibili dalla disciplina sulla protezione dei dati personali); esso stabilisce altresì un coordinamento tra le autorità incaricate della sorveglianza degli ERS e le autorità competenti in materia di protezione dei dati personali[24] .

1. Il riconoscimento delle emozioni alla luce della regolamentazione in materia di protezione dei dati personali

Come già osservato in premessa, i sistemi di riconoscimento automatizzato delle emozioni raccolgono e utilizzano dati relativi a bio-caratteristiche umane per dedurre le emozioni delle persone fisiche e compierne una categorizzazione. In linea di principio, il GDPR si applica a entrambe tali attività, nella misura in cui esse comportano un trattamento di dati personali.

L'analisi che sarà condotta in questo paragrafo mira innanzitutto a indagare la qualificazione dei dati analizzati dagli ERS e, in particolare, le condizioni in presenza delle quali ricorre un trattamento di dati biometrici ai sensi degli articoli 4 (14) e 9 (1) GDPR (para. 1.1.). Talvolta le tecniche adottate per il riconoscimento delle emozioni rendono arduo accertare se sussista un trattamento dei dati personali ai sensi dell'art. 4 (1) GDPR (para. 1.2.). Inoltre, le emozioni dedotte grazie all'impiego di ERS possono essere utilizzate per ottenere informazioni 'sensibili' sulle persone fisiche, il che solleva la questione dell'applicazione dell'articolo 9 (1) GDPR (para. 1.3). Oltre a ciò, si analizzerà in quale misura la normativa sulla protezione dei dati stabilisca limiti e divieti per le pratiche di pubblicità personalizzata basate sul riconoscimento delle emozioni e in che modo consenta un'efficace supervisione per il caso di violazione di tali limiti o divieti, aprendo la strada a rimedi di c.d. *private enforcement* (para. 1.4).

(regolamento sull'intelligenza artificiale), disponibili in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ%3AL_202401689#d1e39-1-1.

[23] Cfr. l'art. 3 (4) Regolamento su IA: "«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

[24] Sulle interazioni tra Regolamento su IA e GDPR si veda il Parere congiunto EDPB-EDPS Joint Opinion on the AI Act Proposal, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf .

1.1. La qualificazione giuridica dei dati analizzati dagli ERS: quando si ha trattamento di dati biometrici ai sensi del GDPR?

La nozione di dati biometrici desumibile dal GDPR è tributaria dell'avvento della cosiddetta 'prima generazione' di tecnologie biometriche, comprendenti tecnologie che utilizzano principalmente bio-caratteristiche umane a fini di identificazione e autenticazione biometrica[25]. Ai sensi di tale Regolamento, solo i dati risultanti "da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici" costituiscono dati biometrici (cfr. art. 4 (14) e considerando 51 GDPR[26]). Mentre la gamma di caratteristiche coperte da questa definizione è molto ampia e generica (comprendendo "caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica"), al contrario, i due requisiti della presenza di un 'trattamento tecnico specifico' e della 'identificazione univoca' hanno lo scopo di limitarne la portata. Infatti, il primo requisito implica che le bio-caratteristiche rappresentate da questo tipo di dati presentino un elevato livello di 'unicità' e invariabilità nel tempo per poter essere utilizzate nel contesto dell'identificazione biometrica (ad es. le impronte digitali o i tratti del viso); il secondo, invece, è volto a escludere dall'ambito dei dati biometrici i 'dati grezzi', vale a dire, dati che, pur rappresentando bio-caratteristiche (ad esempio una foto o un video che ritraggono i tratti del viso o le impronte digitali di un individuo), non appaiono adatti all'identificazione biometrica in quanto non sono stati sottoposti alle metodologie tecniche in uso a tale scopo.

Alla luce di quanto sopra, una lettura dell'art. 4 (14) GDPR coerente con il suo tenore letterale induce a concludere che i dati biometrici sono dati relativi a una persona fisica identificata (anziché meramente identificabile), in quanto presuppongono la preventiva estrazione delle caratteristiche biometriche della stessa, la loro trasformazione in dati leggibili dalla macchina e la successiva registrazione in banche di dati[27]. Solo a seguito di queste attività tali dati possono essere utilizzati per identificare un individuo in modo univoco confrontando le sue caratteristiche biometriche con i dati

[25] C. WENDEHORST, Y. DULLER, *Biometric Recognition and Behavioural Detection, Policy Department for Citizens' Rights and Constitutional Affairs IT Directorate-General for Internal Policies*, 12-15 (PE 696.968 - August 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf. Cfr. Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Clearview AI, 10 febbraio 2022, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362.

[26] Considerando 51 GDPR: "Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica (...)".

[27] LEE A BYGRAVE, LUCA TOSONI, Articolo 4(14). *Biometric Data*, in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di Christopher Kuner e altri, Oxford, 2020, 213 ss.

ISSN 2239-8570

biometrici conservati[28]. Se tale condizione non è soddisfatta, i dati contenenti informazioni biometriche (ossia informazioni relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica) possono comunque considerarsi relativi a una persona fisica ai sensi dell'articolo 4 (1) GDPR, purché si tratti di un individuo identificato o identificabile (cfr., a questo proposito, il paragrafo 1.2.). Pertanto, il legislatore europeo del GDPR ha inteso fare riferimento alla applicazione di specifiche operazioni tecniche (c.d. 'identificazione biometrica')[29] ai dati contenenti informazioni su bio-caratteristiche umane.

Inoltre, ai sensi dell'articolo 9 (1) del GDPR, i dati biometrici conseguono lo status di dati particolari solo quando sono trattati a fini di identificazione univoca. In altri termini, a tal fine, ciò che conta non è la natura intrinseca di questi dati, ma piuttosto lo scopo per cui vengono utilizzati, con la conseguenza che le pratiche di utilizzo di dati biometrici per scopi diversi dall'identificazione biometrica sfuggono al trattamento giuridico riservato dal GDPR alle categorie speciali di dati[30] .

Ciò giova a comprendere la esigenza di ampliare in via di interpretazione la portata dei dati biometrici rilevanti ai sensi dell'articolo 9 (1) del GDPR, avvertita da dottrina e giurisprudenza. A questo proposito, vale la pena menzionare una recente decisione della Corte di Cassazione secondo cui questa disposizione si applica anche rispetto a dati biometrici trattati per 'valutare' il comportamento una persona fisica nel contesto di una forma di c.d. profilazione biometrica[31] (il caso deciso verteva su un sistema di c.d. *e-proctoring* utilizzato per elaborare bio-caratteristiche di studenti nel contesto di prove d'esame svolte 'a distanza'[32], quali movimenti oculari o

[28] C. JASSERAND, *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*, in *Social Science Research Network Electronic Paper Collection*, 15 ss., https://ssrn.com/abstract=3230342, 10.

[29] Viceversa, il regime giuridico dei diritti fondamentali offre protezione più rigorosa alle informazioni biometriche. Infatti, secondo la giurisprudenza della Corte europea dei diritti dell'uomo, la mappatura facciale e la mera memorizzazione dei dati da essa risultanti in una banca dati comportano un'interferenza con il diritto alla privacy ai sensi dell'articolo 8 CEDU, indipendentemente dal fatto che tali dati possano essere o vengano utilizzati a fini di identificazione. Si veda E. J. KINDT, *Having Yes, Using No? About the new legal regime for biometric data*, in *Computer Law & Security Review*, 2018, 34 (3), 523 ss., https://doi.org/10.1016/j.clsr.2017.11.004.

[30] *Linee guida EDPB 3/2019 sul trattamento dei dati personali mediante dispositivi video* del 29 gennaio 2020, par. 5, punto 80: "quando lo scopo del trattamento è ad esempio distinguere una categoria di persone da un'altra ma non identificare in modo univoco nessuno, il trattamento non rientra nell'articolo 9" (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf).

[31] Corte di Cassazione, Cassazione civile sez. I - 13/05/2024, n. 12967. La Corte, da un lato, ha ritenuto che nel caso in questione si sia trattato di una forma di autenticazione biometrica degli studenti (sebbene ciò sia controverso da un punto di vista tecnico), dall'altro, ha stabilito che l'autenticazione biometrica può essere abbinata ad altre operazioni di trattamento aventi una finalità diversa (ad esempio, la profilazione degli studenti al fine di rilevare e segnalare eventuali anomalie nel loro comportamento).

[32] Si veda Garante per la protezione dei dati personali, Garante privacy - Ordinanza 9703988 - 16 settembre 2021. Cfr. G. BINCOLETTO, *Italy - E-Proctoring During Students' Exams: Emergency Remote Teaching at Stake*, in *European Data Protection Law Review*, 2021, 7(4), 586 ss., nonché A. GIANNOPOULOU, R. DUCATO, C. ANGIOLINI, G. SCHNEIDER,

facciali, la voce, il modo di utilizzo della tastiera del dispositivo elettronico, etc.).

Ciò detto, occorre aggiungere che gli ERS non sempre impiegano dati che rappresentano bio-caratteristiche connotate da un elevato grado di unicità, tali da poter essere collegate a uno specifico individuo in modo univoco, secondo quanto richiesto dall'articolo 4 (14) GDPR. Infatti, gli ERS appartengono alla c.d. 'seconda generazione' di tecnologie biometriche, vale a dire quelle tecnologie aventi il fine di valutare e/o categorizzare gli individui per prevederne la personalità, il comportamento etc.[33]. Da qui il termine 'biometria comportamentale'[34]. Per perseguire un simile scopo, è possibile utilizzare un'ampia gamma di dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che vengono definiti 'bio-identificatori deboli' (o 'soft'), in quanto presentano un minor grado di unicità (come l'andatura e in generale i movimenti del corpo delle persone fisiche)[35]. Di conseguenza, questi dati difficilmente possono qualificarsi come dati che consentono o confermano l'identificazione univoca di una persona fisica secondo quanto richiesto dall'articolo 4 (14) GDPR.

Inoltre, tale nuova generazione di tecnologie biometriche non elabora bio-caratteristiche esclusivamente a fini di identificazione delle persone fisiche e, pertanto, il requisito di cui all'art. 9 (1) GDPR necessario per conseguire lo status di dati sensibili non è sempre soddisfatto. Appare evidente, tuttavia, che le suddette tecnologie mirano a "generare descrizioni semantiche di un individuo" (in altri termini, a definirne le qualità e quindi l'identità)[36] attraverso processi tecnici di categorizzazione biometrica[37]. Alla

---

From data subjects to data suspects: challenging e-proctoring systems as a university practice, in JIPITEC, 2023, 278 ss.

[33] Cfr. Gruppo di lavoro art. 29, *Opinion n. 3/2012 on recent developments in biometrics*, cit., 4: "Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use".

[34] La seconda generazione di tecnologie biometriche è caratterizzata dai seguenti aspetti: mira ad analizzare tratti comportamentali e psicologici; utilizza dati sulle caratteristiche biometriche che possono essere raccolti a distanza, senza bisogno di collaborazione da parte degli individui a cui si riferiscono. Si vedano a questo proposito M. SUTROP, K. LAAS-MIKKO, *From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics*, 2012, 21 ss, 23, DOI: 10.1111/j.1541-1338.2011.00536.x.

[35] D. A. REID, M. S. NIXON, S. V. STEVENAGE, *Soft Biometrics. Human identification using comparative descriptions*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2013, 6, 1216 ss., https://doi.org/10.1109/TPAMI.2013.219. Nella letteratura tecnica il termine "biometria soft" definisce il processo di "categorizzazione delle informazioni sui tratti corporei in cui una persona può non essere identificata nel processo". Si veda anche A. DANTCHEVA, *What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics*, in *IEEE Transactions on Information Forensics and Security* 11, 2016, 3, 441 ss., https://doi.org/10.1109/TIFS.2015.2480381.

[36] Cfr. G. M. RIVA, *Metadata, Semantic data and their protection: legal nature and issues under the GDPR and the E-Privacy draft Regulation*, 2018, Amsterdam Privacy Conference, academia.edu/41506888/Metadata_Semantic_data_and_their_protection_legal_nature_and_issues_under_the_GDPR_and_the_E_Privacy_draft_Regulation.

ISSN 2239-8570

luce di ciò, una parte nutrita della letteratura giuridica persegue la via della interpretazione estensiva del concetto di 'identificazione', al fine di includervi qualsiasi forma di attribuzione di identità, non solo quella 'civile', ma anche quella derivante da indici quali l'appartenenza a un gruppo sociale (ad esempio, 'donna' o 'bianco'), un tratto del comportamento (ad esempio, la qualifica di 'fumatore') o un'emozione (ad esempio, 'soggetto triste o adirato')[38]. In questa prospettiva, l''univocità' di questo tipo di dati risiede nella loro idoneità a individuare una persona rivelando informazioni su di essa (sulla sua personalità, salute, sessualità, etc.) (cfr. paragrafo 1.2). Simili informazioni, dedotte in via di inferenza[39], possono a loro volta influenzare il modo in cui tale persona viene rappresentata o trattata[40].

Un'analisi giuridica approfondita sull'evoluzione delle tecnologie biometriche si ricava dai documenti del Gruppo di lavoro Articolo 29 sul concetto di dati biometrici, redatti prima dell'entrata in vigore del GDPR[41]. I dati biometrici sono ivi descritti come dati personali relativi a caratteristiche fisiche, fisiologiche e comportamentali uniche per ciascun individuo e misurabili[42]. La trasformazione di queste ultime in dati leggibili da una macchina, ne rende possibile lo sfruttamento anche a fini commerciali. Inoltre, questo tipo di dati, pur non essendo necessariamente dati sensibili di per sé, possono rivelare informazioni sensibili[43] . Pertanto, è necessario un elevato livello di protezione dei diritti fondamentali coinvolti nel loro trattamento, da garantirsi applicando i principi in materia di protezione dei dati. Come verrà dimostrato nel presente studio, simili rilievi rimangono pertinenti ed attuali anche dopo l'adozione del GDPR, contribuendo a fare

[37] Si veda Gruppo di lavoro art. 29, Opinion 3/2012 on developments in biometric technologies (2012), (27.04.2012), WP 193, 6: "The categorisation/segregation of an individual by a biometric system is typically the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, it is not important to identify or verify the individual but to assign him/her automatically to a certain category. For instance, an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender".

[38] S. MIGLIORINI, *Biometric harm*, in *Law, technology and Humans*, 2023, 5(2), 238 ss.. 239, https://doi.org/10.5204/lthj.2830.

[39] D. IMBRUGLIA, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ*., 2023, 3, 922 ss.

[40] D. J. SOLOVE, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, in *Northwestern University Law Review*, 2024, 118, 1081 ss., https://ssrn.com/abstract=4322198 o http://dx.doi.org/10.2139/ssrn.4322198.

[41] Gruppo di lavoro art. 29, *Working Document on Biometrics* (2003), (01.08.2003), WP 80, e Id., Opinion 3/2012 on developments in biometric technologies (2012), (27.04.2012), WP 193.

[42] Secondo il Gruppo di lavoro art. 29, *Opinion n. 4/2007 on the concept of personal data*, WP136, (20.06.2007), 8, i dati biometrici sono: "biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability".

[43] Gruppo di lavoro art. 29, *Opinion 3/2012 on developments in biometric technologies*, cit., 15: "Some biometric data could be considered sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health".

luce sulle principali questioni legate alle tecnologie biometriche (ad esempio, sui rischi di danno inerenti al loro trattamento) e sulle relative conseguenze giuridiche (cfr. para. 1.3 e 1.4)).

1.2. Pratiche di mera rilevazione di bio-caratteristiche di persone fisiche per desumerne le emozioni: si applica il GDPR?

Come già accennato, è alquanto controverso se la regolamentazione in tema di dati personali possa applicarsi ad alcune pratiche peculiari di riconoscimento delle emozioni, come ad esempio quando i tratti del viso delle persone non vengono memorizzati in una banca di dati, perché semplicemente rilevati ('scansionati') in tempo reale, per scopi di pubblicità personalizzata[44], e poi cancellati.

Ciò può riscontrarsi nel contesto del c.d. *outdoor advertising* che avviene in luoghi pubblici o aperti al pubblico per mezzo di cartelloni pubblicitari 'intelligenti' e simili dispositivi, che analizzano volti di passanti[45].

Forme analoghe di trattamento di dati si rinvengono nel caso di analisi automatizzata di movimenti del corpo[46] (ad es., movimenti degli occhi o il modo di camminare) o del tono di voce, del modo di parlare, etc., di persone fisiche. Si pensi a pratiche poste in essere per scopi di profilazione e personalizzazione in tempo reale nel contesto della vendita al dettaglio[47], in cui vengono elaborati dati sul modo in cui "a consumer drives a shopping trolley in a supermarket" da parte di un consumatore[48]. In un simile caso, i dati sono utilizzati "as a means of inferring the type of customer at stake (e.g. hurried, with higher purchasing power)"[49].

---

[44] Si veda A. MC STAY, *Empathic media and advertising: industry, policy, legal and citizen perspectives (the case for intimacy)* in *Big Data & Society*, 2016, 1 ss., 3 e 7-8. Cfr. anche M. GALIČ, R. GELLERT, *Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab*, in *Computer Law & Society Review*, 2021, 40, 14, in https://ssrn.com/abstract=3699900), nonché J. CHEN, L. MIOTTO, *Manipulation, Real-Time Profling, and their Wrongs*, in 2022, *The Philosophy of Online Manipulation*, a cura di Fleur Jongepier and Michael Klenk, Rutledge, 2022, 392 ss.

[45] P. DAVIS, *Facial Detection and Smart Billboards: Analysing the "Identified" Criterion of Personal Data in the GDPR*, in *University of Oslo Faculty of Law Legal Studies Research Paper Series*, 2020, 1, 1 ss. e D. GEORGE, K. REUTIMANN, A. TAMÒ-LARRIEUX, *GDPR Bypass by Design? Transient Processing of Data under the GDPR*, in *International Data Privacy Law*, 2019, 9 (4), 285 ss.

[46] M. RAJA, S. SIGG, *RFexpress! - Exploiting the Wireless Network Edge for RF-Based Emotion Sensing*, 2016, https://doi.org/10.48550/arXiv.1612.06189.

[47] Si veda ACI INFOTECH, *How Does Emotion AI Redefine Retail Interaction and Sales?* https://www.linkedin.com/pulse/how-does-emotion-ai-redefine-retail-interaction-sales-aciinfotech-eraac.

[48] Cfr. W. SCHREURS, M. HILDEBRANDT, E. KINDT, M. VANFLETEREN, *Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector*, in *Profiling the European Citizen*, a cura di Mireille Hildebrandt, Serge Gutwirth, Springer, 2008, 241 ss., 246.

[49] B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, in *Philos. Technol*., 2017, 30, 475 ss., 478, il quale ritiene che, in un simile caso, i dati "non

ISSN 2239-8570

Innanzitutto, occorre premettere che le peculiarità di simili pratiche si spiegano alla luce dei relativi scopi: poiché quel che conta è individuare un segmento di mercato a cui indirizzare una pubblicità personalizzata, è sufficiente classificare le persone fisiche per stabilirne le caratteristiche (e stimare quanto esse siano suscettibili di subire l'influenza del messaggio personalizzato), senza che occorra accertarne l'identità[50], né conservare le informazioni usate a tal fine.

La pertinente letteratura riscontra l'impiego di una terminologia tecnica atta a distinguere l'operazione consistente nel 'riconoscere' un volto umano da quella implicante la sua mera 'rilevazione' (ad es., '*facial detection*', anziché '*facial recognition*'). Il primo tipo di attività si ha quando si utilizzano sensori che catturano dati (ad es. immagini di un volto) elaborati da un *software*, che vengono subito dopo cancellati o anonimizzati. Senza entrare nel dettaglio tecnico, si riscontra, in una simile ipotesi, una serie di operazioni: innanzitutto, l'analisi della forma e delle fattezze di volti di persone fisiche rilevati da tali tecnologie e la loro riduzione ad un numero ristretto di elementi 'salienti'; infine i dati così ottenuti vengono messi a confronto con un *ideal-tipo* di volto (c.d. 'comparazione'), consistente in un'ipotesi frutto della correlazione statistica tra centinaia di migliaia di immagini (ad es., immagini di volti 'felici' o 'adirati')[51]. Tali dati sono 'effimeri' quando non vi sia conservazione degli stessi in un luogo virtuale. Ciò non toglie però che, per effetto delle descritte operazioni, venga a crearsi una rappresentazione digitale di informazioni e, dunque, si ottengano dei dati[52]. Il punto è dunque stabilire se essi possano considerarsi personali.

In merito, appare rilevante la casistica in materia di telecamere a circuito chiuso che rilevano le immagini facciali dei passanti, desumibile dalle decisioni di alcune autorità nazionali per la protezione dei dati personali, casistica che restituisce una condizione di incertezza[53]: secondo alcune decisioni, queste tecnologie individuano persone fisiche anche quando non ha luogo alcuna operazione per verificare la corrispondenza dei dati dei soggetti sottoposti ad osservazione con dati previamente memorizzati

consentono di identificare gli individui che spingono il carrello". Come si dirà nel testo, tale aspetto merita invece una più accorta analisi giuridica.

[50] B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, op. cit., 478.

[51] Cfr. P. DAVIS, *Facial Detection and Smart Billboards: Analysing the "Identified" Criterion of Personal Data in the GDPR*, op. cit., 4. Di tutta evidenza appare la differenza esistente, da un lato, tra la identificazione biometrica (la quale presuppone la previa creazione di un calco digitale del viso di un individuo specifico) o non biometrica (compiuta usando cioè dati non biometrici, ad es. comparando una fotografia di quell'individuo con una registrazione video che lo rappresenta) e la rilevazione dei tratti del volto per fini di analisi delle emozioni. In quest'ultimo caso infatti certe bio-caratteristiche ritenute salienti di un determinato individuo (ad es., un passante le cui fattezze siano captate dai sensori) sono messe a confronto con un modello digitale di un volto (che rappresenta un tipo ideale, non quello specifico individuo).

[52] Cfr. S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, op. cit., 51-52.

[53] Offrono una risposta negativa a tale interrogativo S. WACHTER, *Affinity profiling and discrimination by association in online bahavioural advertising*, in *Berkley Technology Law Journal*, 2020, 35, 367 ss. (secondo cui i dati devono essere conservati per categorizzare gli individui, al fine di qualificarsi come dati personali) e D. GEORGE, K. REUTIMANN, A. TAMÒ-LARRIEUX, *GDPR Bypass by Design? Transient Processing of Data under the GDPR*, op. cit., 286.

ISSN 2239-8570

relativi ai medesimi soggetti[54]; mentre altre autorità hanno espresso parere contrario[55] .

Senza entrare nel dettaglio di una simile casistica, è possibile notare come ivi si dibatta soprattutto sulla possibilità di indentificare le persone fisiche 'in futuro' (vale a dire una volta cessato il tipo di trattamento oggetto di scrutinio). Da qui l'attenzione all'elemento della conservazione dei dati, della sua durata, etc. Orbene, come osservato poco sopra, la conservazione dei dati appare superflua nel caso di categorizzazione di persone fisiche in base alle emozioni, con la conseguenza che, una volta che tale trattamento sia cessato, la persona fisica non è più individuabile. Ciò che, piuttosto, occorre valutare è se il requisito della identificazione sia soddisfatto quando tale trattamento è ancora in corso.

Più di recente, l'Autorità Garante per la protezione dei dati personali (d'ora in poi 'Garante privacy') ha affermato che "l'acquisizione e la conservazione temporanea di dati personali, come le immagini del volto riprese da dispositivi video, anche per un breve periodo di tempo, costituisce un trattamento di dati personali"[56]; e ciò in linea con un precedente del 2018, in cui il Garante privacy aveva ritenuto esservi trattamento di dati personali quando i sensori di una telecamera a circuito chiuso sono in grado di conservare le immagini di passanti solo per poche frazioni di secondo[57]. Tale ultimo provvedimento è di particolare interesse perché, con motivazione succinta, concerne specificamente la pubblicità personalizzata tramite 'cartelloni *smart'*.

Al fine di stabilire se si abbia trattamento di dati personali, occorre considerare - alla luce della giurisprudenza, della *soft law* e della dottrina - il significato giuridico dell'attributo 'personale' riferito al dato, avendo

[54] Si veda N. PURTOVA, *From Knowing by name to targeting: the meaning of identification under the GDPR*, in *International Data Privacy Law* 2022, 12 (3), 163 ss. L'autrice cita la giurisprudenza delle autorità nazionali per la protezione dei dati personali (*R (on the application of Edward Bridges) v The Chief Constable of South Wales Police and Secretary of State for the Home Department* [2019] EWHC 2341 (Admin), 122-125 e *R (on the Application of Bridges) v South Wales Police [2020] EWCA Civ* 1058, 46), https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[55] Si veda l'Irish Data Protection Commissioner, *Press Release on the Use of Facial Detection Technology in Advertising* (15 maggio 2017) citato nella relazione annuale del 2017, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Annual%20Report%202017.pdf.

[56] Cfr. Autorità Garante per la protezione dei dati personali 11 gennaio 2024 doc. web n. 9977020, disponibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020: tale decisione riguarda dati relativi a bio-caratteristiche, acquisiti e conservati, anche se per un tempo molto breve, e resi anonimi. Una delle principali questioni giuridiche considerate è l'adeguatezza delle tecniche di anonimizzazione utilizzate nel caso in questione.

[57] Cfr. Garante privacy, Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria' (Decisione n. 551, 11 dicembre 2017), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252.

ISSN 2239-8570

riguardo, in particolare, all'elemento per cui deve trattarsi di una persona fisica 'individuata' o 'individuabile', secondo l'articolo 4 (1) GDPR[58].

Per accertare se i dati siano personali, non è rilevante solo il loro contenuto (le informazioni desumibili dai dati), ma contano anche le finalità perseguire e l'incidenza del trattamento, il fatto che il trattamento implichi l'individuazione di una determinata persona fisica e che per effetto di esso tale persona sia resa oggetto di valutazione e attenzione (in quanto ne vengono indagate qualità, comportamenti, tratti della personalità etc.). Siffatta interpretazione è stata, prima, avanzata dal Gruppo di lavoro art. 29[59] e, poi, fatta propria dalla Corte di giustizia dell'Unione europea. Quest'ultima, nel caso *Novak*, ha ritenuto che l'espressione 'qualsiasi informazione' nella definizione di dati personali includa informazioni "non solo oggettive ma anche soggettive, sotto forma di opinioni e valutazioni, a condizione che 'si riferiscano' all'interessato"[60].

Quando si ricorre a sistemi di IA e apprendimento automatico si ottengono, per inferenza, informazioni su una persona fisica, consistenti in valutazioni o opinioni. Per stabilire se esse si riferiscono ad una persona fisica identificata o identificabile, il criterio della c.d. identità civile (per il quale il dato non è personale se non consente di risalire a tale specie di identità) appare insoddisfacente, nella misura in cui non tutela da usi impropri delle caratteristiche ed attributi della persona[61].

[58] Gruppo di lavoro art. 29, *Opinion n. 4/2007 on the concept of personal data*, WP136, (20.06.2007), 10. Si vedano M. FINCK, F. PALLAS, *They who must not be identified-distinguishing personal from non-personal data under the GDPR*, in *International Data Privacy Law*, 2020, vol. 10, Issue 1, pp. 11-36; M. VON GRAFENSTEIN, *Refining the Concept of the Right to Data Protection in Article 8, - Part I*, in *European Data Protection Law Review*, 2020, 6, 509 ss., 513.

[59] Gruppo di lavoro art. 29, *Opinion n. 4/2007 on the concept of personal data*, WP136, (20.06.2007), 14: "Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name".

[60] Cfr. Corte di giustizia dell'Unione europea Causa C-434/16 Peter Nowak c. Commissario per la protezione dei dati, ECLI:EU:C:2017:994, punto 34. Si veda da ultimo Corte di giustizia dell'Unione europea, sentenza (Quarta Sezione) del 7 marzo 2024 (domanda di pronuncia pregiudiziale proposta dallo Hof van beroep te Brussel - Belgio) – IAB Europe / Gegevensbeschermingsautoriteit (Causa C-604/22): "L'uso dell'espressione «qualsiasi informazione» nella definizione della nozione di «dato personale», che figura in tale disposizione, riflette l'obiettivo del legislatore dell'Unione di attribuire un'accezione estesa a tale nozione, che comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse «riguardino» la persona interessata (sentenza del 4 maggio 2023, Österreichische Datenschutzbehörde e CRIF, C-487/21, EU:C:2023:369, punto 23 nonché giurisprudenza ivi citata)". "37 La Corte ha dichiarato, in proposito, che un'informazione riguarda una persona fisica identificata o identificabile qualora, in ragione del suo contenuto, della sua finalità o del suo effetto, essa sia connessa a una persona identificabile (sentenza del 4 maggio 2023, Österreichische Datenschutzbehörde e CRIF, C-487/21, EU:C:2023:369, punto 24, nonché giurisprudenza ivi citata)".

[61] L. DALLA CORTE, *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law*, in *European Journal of Law and Technology*, 2019, 10, 1 ss., 9: secondo cui "data protection law does not aim at protecting individuals

ISSN 2239-8570

Al di là di tale, seppur importante, notazione, occorre però stabilire come debba intendersi *de lege lata* il requisito della identificazione. A tal fine, soccorrono i vari criteri di interpretazione utilizzabili, innanzitutto, la lettera dell'art. 4 (1) GDPR e poi il criterio teleologico.

In primo luogo, si può notare che, nel testo della disposizione in parola, l'aggettivo 'identificata', riferito alla persona fisica a cui i dati pertengono, assume il significato di 'distinta' o isolata da una moltitudine, grazie ad elementi identificanti, alcuni dei quali sono elencati dallo stesso art. 4 (1) a titolo esemplificativo. Nessuno di tali elementi, tuttavia, singolarmente considerato, giova a identificare con certezza una persona fisica (nemmeno il nome, in assenza di una sua contestualizzazione alla luce di altri dati, quali, ad es., la data di nascita, etc.). In ragione di ciò, la pertinente *soft law*, a seconda della natura e del contesto del trattamento, considera adeguato qualsivoglia criterio che giovi ad individuare una persona fisica, ancorché inidoneo a stabilirne la identità civile[62].

Ciò è quanto si verifica nella profilazione ai sensi dell'art. 4 (4) GDPR[63] la quale implica, sì, in un primo momento, l'assimilazione di un individuo ad un gruppo, o classe, di persone fisiche; ma comporta, poi, la sua individuazione, giacché questa operazione logica consente di acquisire conoscenza (più o meno accurata[64]) circa caratteristiche o elementi che concernono la sua persona e, quindi, di sapere 'come ella/egli sia'. Ed invero, "[...] l'*applicazione del* profilo a individui specifici comporta *di per sé* che tali individui siano identificabili[65]", nel senso appena detto[66]. In

only from the misuse of their identities, but from the misuse of their attributes – their characteristics and defining traits – too. From this perspective, the fact that any data can become personal data is a regulatory 'feature', rather than a 'bug', necessary to provide the flexible, contextual protection in context EU data protection".

[62] In merito, cfr. Gruppo di lavoro art. 29, *Opinion n. 4/2007 on the concept of personal data*, WP136, (20.06.2007): 'in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group; "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light".

[63] Cfr. art. 4 (4) GDPR: «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. Cfr., per un esame approfondito, R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano, Milano, 2019, 167 ss.

[64] S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2019, 2, 494, 585.

[65] Cfr. M. GALIČ, R. GELLERT, *Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab*, op. cit., 14.

[66] V. RUPP, M. VON GRAFENSTEIN, *Clarifying "personal data" and the role of anonymization in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection*, in *Computer Law & Security Review*, 2024, 52, 4 ss., in https://doi.org/10.1016/j.clsr.2023.105932. Secondo gli aa., ai fini della qualificazione rileva la presenza di un rischio specifico: "there might already be a specific risk if the data subject is affected as a nameless part of a group, for example, in the case of personalized advertising, where a specific risk of manipulation

ISSN 2239-8570

sintesi, quando il trattamento ha lo scopo di valutare aspetti della personalità di un individuo, il requisito dell'identificazione è soddisfatto poiché tale individuo viene in rilievo nella sua 'singolarità' ed è dunque distinto da una indefinita moltitudine[67].

Anche il riconoscimento delle emozioni di una persona fisica è una forma di profilazione, giacché esso implica l'uso di dati personali "per valutare determinati aspetti personali relativi a una persona fisica" (art. 4 (4) GDPR). Ed infatti, il riconoscimento delle emozioni si basa sulla comparazione tra dati concernenti bio-caratteristiche di una specifica persona ed una ipotesi astratta, frutto della correlazione statistica tra innumerevoli informazioni relative a persone fisiche[68]. Una simile operazione è atta poi a valutare tale persona fisica in base ai suoi stati emozionali e, eventualmente, a desumere tratti della sua personalità.

A fortiori, adottando questa chiave di lettura, si riscontra una forma di identificazione riconducibile all'art. 4 (1) GDPR, ogni qual volta le caratteristiche rilevate - e tra esse gli stati emozionali e i tratti della personalità - siano trattate per scopi di personalizzazione del messaggio pubblicitario[69], giacché la persona fisica viene fatta oggetto di specifica attenzione (ad es., 'valutata') e di trattamento differenziato (riceve informazioni, appunto, 'personalizzate')[70].

Tenendo conto di questo elemento, il Gruppo di lavoro art. 29 ha ritenuto che, viceversa, dati concernenti bio-caratteristiche di persone fisiche utilizzati per categorizzare queste ultime in forma aggregata (ad esempio, per ottenere informazioni sul numero di individui di sesso maschile o femminile in un gruppo, o sulla loro età) non costituiscono dati personali[71]. In un simile caso, infatti, il trattamento concerne delle 'persone', anziché una persona individuata.

L'interpretazione qui accolta[72] appare preferibile anche alla luce di un criterio teleologico, e, in particolare, sulla scorta del principio della 'tutela

---

exists even if the advertisers recognize the data subject only as belonging to a group of people with certain purchase interests " (cfr. ibidem, p 5). Contra, B. WOOLSEY, *Emotion Recognition Technology Could Transform Retail Advertising*, in *Handelsblatt Today* (24 January 2018), 190, https://www.handelsblatt.com/today/companies/data-privacy-emotion-recognition- technology-could-transform-retail-advertising/23580844.html?ticket=ST-7740357-Ki75S6Jdw0bSvWEhtQIW- ap6.

[67] Infatti, la profilazione rappresenta un modo "per conoscere gli individui attraverso la conoscenza dei gruppi a cui sono assegnati" (così B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, op. cit., 481).

[68] Cfr. W. SCHREURS, M. HILDEBRANDT, E. KINDT, M. VANFLETEREN, *Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector*, op. cit., 241.

[69] Cfr. C. JASSERAND, *Biometric Data, Within and Beyond Data Protection. The Boundaries of Data* (AUP, 2024), in University of Groningen Faculty of Law Research Paper, 2023, 18, 6 ss., https://ssrn.com/abstract=4483962.

[70] N. PURTOVA, *From Knowing by name to targeting: the meaning of identification under the GDPR*, op. cit., 172.

[71] Gruppo di lavoro art. 29, Parere 02/2012 sul riconoscimento facciale nei servizi online e mobili (WP192, adottato il 22 marzo 2012).

[72] Né appare di ostacolo a tale conclusione altra giurisprudenza della Corte di giustizia e, in particolare, la decisione della Corte di giustizia dell'Unione europea nel caso *Breyer* (Seconda sezione 19 ottobre 2016, causa C-582/14, *Patrick Breyer contro Bundesrepublik*

effettiva' dei diritti fondamentali degli interessati, di cui la Corte di giustizia ha mostrato di fare largo uso nelle pronunce più recenti[73]. Se si propende infatti per il criterio restrittivo della individuazione come attribuzione di un'identità civile, si limita oltremodo il campo di applicazione della regolamentazione in materia di protezione dei dati personali[74].

Si consideri, in merito, che gli esempi di pratiche sopra citati corrispondono a forme di monitoraggio sistematico e automatizzato di luoghi pubblici o aperti al pubblico, suscettibili di interferire con i diritti fondamentali delle persone fisiche interessate, le quali potrebbero non essere consapevoli del fatto che si sta svolgendo un trattamento di questo tipo. Al riguardo, le Linee guida 3/2019 del Comitato europeo per la protezione dei dati personali (d'ora in poi 'EDPB') sul trattamento di dati personali attraverso dispositivi video (di seguito, 'Linee guida EDPB su dispositivi video') sono illuminanti, giacché chiariscono che le persone fisiche ivi presenti non si aspettano di essere sottoposte a monitoraggio[75]. Per giunta, nel tipo di pratica qui in esame, l'interferenza concerne la dimensione privata del corpo e finanche la sfera cognitiva delle persone fisiche, entrambe protette dall'articolo 8 della CEDU[76] attinente alla

Deutschland, punti 38-49), in cui la Corte si è interrogata circa il significato del requisito della identificabilità della persona fisica nella definizione di dato personale rispetto al trattamento di indirizzi IP dinamici - che quindi non permettono una identificazione diretta di un visitatore di un sito web una volta che sia cessata la sessione di visita. Si è ivi concluso che tali dati, conservati dopo tale momento e in assenza di altri dati, non consentono di risalire alla identità delle persone fisiche cui essi si riferiscono e dunque non sono personali nell'accezione di cui al GDPR. Viceversa, nella pratica che costituisce qui oggetto di analisi, non si ha conservazione dei dati, con la conseguenza che le argomentazioni alla base di tale sentenza non possono ad essa pedissequamente applicarsi.

[73] Cfr. causa C-634/21, ECLI:EU:C:2023:957, avente ad oggetto la domanda di pronuncia pregiudiziale proposta ai sensi dell'articolo 267 TFUE, dal Verwaltungsgericht Wiesbaden (tribunale amministrativo di Wiesbaden, Germania), con decisione del 1° ottobre 2021, nel procedimento tra OQ contro il Land Hessen, con l'intervento di SCHUFA Holding AG, cit., punto 60.

[74] Cfr. altresì Corte di giustizia dell'Unione europea, sentenza (Quarta Sezione) del 7 marzo 2024 (domanda di pronuncia pregiudiziale proposta dallo Hof van beroep te Brussel - Belgio) – IAB Europe / Gegevensbeschermingsautoriteit (Causa C-604/22), punto 34: "…, per giurisprudenza costante, l'interpretazione di una disposizione del diritto dell'Unione richiede di tener conto non soltanto della sua formulazione, ma anche del contesto in cui essa si inserisce nonché degli obiettivi e delle finalità che persegue l'atto di cui fa parte (sentenza del 22 giugno 2023, Pankki S, C-579/21, EU:C:2023:501, punto 38 nonché giurisprudenza ivi citata)". La sentenza in questione verte sulla interpretazione dell'elemento della identificazione indiretta di una persona fisica al fine di accertare se una stringa composta da una combinazione di lettere e di caratteri, come la TC String (Transparency and Consent String), contenente le preferenze di un utente di Internet o di un'applicazione relative al consenso di tale utente al trattamento dei dati personali che lo riguardano, possa considerarsi un dato personale.

[75] Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali mediante dispositivi video del 29 gennaio 2020)(https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf), che rinviano alle Linee guida del Gruppo di lavoro art. 29 sulla trasparenza ai sensi del Regolamento 2016/679 (WP260), par. 38.

[76] A. MCSTAY, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society*, 2020, 1 ss., 10; S. WACHTER, *Affinity*

ISSN 2239-8570

salvaguardia del diritto alla vita privata. Questo diritto comprende l'intimità della persona fisica (la sua integrità mentale e corporea), ma attiene altresì alla protezione della sua identità (ha dunque anche una dimensione relazionale, oltre a servire ad escludere terzi da intromissioni in tale sfera) ed è distinto dal diritto alla protezione dei dati personali, venendo in rilievo anche nei casi di uso di informazioni non qualificabili come dati personali[77] .

Senza addentrarsi nell'analisi di tale aspetto, sia sufficiente qui osservare che la prospettiva appena menzionata ha il merito di far luce sui molteplici interessi coinvolti nel tipo di trattamento qui in parola[78] (cfr. para. 1.4).

Occorre, infine, notare che il Regolamento su IA ha optato per una definizione di ERS comprendente la semplice rilevazione di bio-caratteristiche umane (cfr. para. 3).

1.3. Se le emozioni possano considerarsi dati 'particolari' ai sensi dell'articolo 9 (1) GDPR

Come già osservato, l'ambito della definizione dei dati biometrici è piuttosto angusto e, inoltre, i dati biometrici sono dati particolari ai sensi dell'articolo 9 (1) del GDPR solo quando vengono trattati allo scopo di identificare in modo univoco una persona fisica. Alcuni tipi di dati personali astrattamente utilizzabili per il riconoscimento delle emozioni possono considerarsi di per sé dati particolari perché concernenti lo stato di salute dell'interessato, come, ad esempio, la frequenza cardiaca, la pressione sanguigna etc.[79]. Tuttavia, questo tipo di dati è raramente impiegato nel contesto del marketing personalizzato, dove si preferisce utilizzare dati la cui raccolta non richiede la collaborazione degli interessati.

È notorio che, grazie alle tecnologie di IA e all'uso dei c.d. *big data*, l'analisi di dati non appartenenti alle categorie particolari elencate nell'articolo 9 (1) GDPR può condurre a ricavare, per inferenza,

---

profiling, op. cit., 55; S.MIGLIORINI, *Biometric Harm, Law, Technology and Humans*, 2023, 5 (2), 238 ss., 244-246, https://doi.org/10.5204/lthj.2830.

[77] Cfr. R. GELLERT, S. GUTWIRTH, *The legal construction of privacy and data protection*, in *Computer Law & Security Review*, 2013, 29 (5), 522 ss., 524-527, https://doi.org/10.1016/j.clsr.2013.07.005.

[78] Per una panoramica generale, B. VAN DER SLOOT, *Legal fundamentalism: Is data protection really a fundamental right*, in *Data protection and privacy: (In)visibilities and infrastructure*. *Law, Governance and Technology Series*, a cura di R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert, in *Issues in Privacy and Data Protection*, Springer 2017, 37, 3 ss., 15, https://doi.org/10.1007/978-3-319-50796-5_1.

[79] Si vedano A. HAUSELMANN, A. M. SEARS, L. ZARD, E. FOSCH-VILLARONGA, *EU Law and Emotion Data*, in *11th International Conference on Affective Computing and Intelligent Interaction* (ACII), 2023,
https://doi.org/10.48550/arXiv.2309.10776
(secondo cui i dati sulla salute non riguardano solo la salute fisica o mentale, ma anche "qualsiasi informazione (...) sullo stato fisiologico o biomedico dell'interessato, indipendentemente dalla sua fonte", secondo il Considerando 35GDPR).

informazioni sensibili relative a persone fisiche identificate o identificabili[80].

Alla luce di ciò, la pertinente *soft law* ritiene che un trattamento automatizzato di dati che dia origine a informazioni di tal genere rientri nell'ambito di applicazione della citata disposizione[81]. Ad esempio, nel parere reso dal Gruppo di lavoro art. 29 sulla evoluzione delle tecnologie biometriche, si sostiene che i dati biometrici *possono* rivelare informazioni sensibili. Le argomentazioni alla base di questa constatazione sono sintetizzabili come segue: i sistemi biometrici sono in grado di raccogliere "informazioni relative agli stati emotivi o alle caratteristiche corporee" dell'interessato, e ciò può portare a ottenere informazioni, ad esempio, sulla salute dell'interessato[82]. Conclusioni simili si rinvengono nelle Linee guida 3/2019 dell'EDPB sui dispositivi video[83], dove però si precisa altresì che, per valutare se, in uno specifico caso, si abbia trattamento di dati sensibili, occorre accertare se la *finalità* di esso consista nell'ottenere informazioni di questo tipo. La *ratio* alla base di tale interpretazione è impedire che il perimetro dell'articolo 9 del GDPR divenga eccessivamente ampio, fino ad includere qualsiasi dato suscettibile di rivelare accidentalmente informazioni sensibili (ad es., si pensi a un dispositivo di videosorveglianza che riprende gli avventori di una chiesa)[84].

È quindi necessario prendere in considerazione, caso per caso, la finalità del trattamento[85] , da individuare in base al tipo di trattamento effettuato, in

[80] O. TENE, J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in 11 *NW. J. TECH. & INTELL. PROP.*, 2013, 239 ss.

[81] Gruppo di lavoro art. 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, (WP 251, 3/10/2017), 15. Si veda anche Id., *Advice paper on special categories of data* (Ref- Ares (2011) 444105), 20/04/2011, 6: "The term "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded".

[82] Gruppo di lavoro art. 29, *Opinion n. 3/2012*, cit., 17: "some systems can secretly collect information related to emotional states or body characteristics and reveal health information resulting in a non-proportional data processing as well as in the processing of sensitive data in the meaning of article 8 of the Directive 95/46/EC".

[83] Si vedano le Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali mediante dispositivi video, cit., p. 5, punto 62: (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf): "Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data". Cfr., inoltre, "Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9" (ivi, p. 5, punto 64). Infine, si veda Ibidem: "if the video footage is processed to deduce special categories of data, Article 9 applies".

[84] Ibidem, p. 5, punto 64.

[85] Sulla questione se debba adottarsi un criterio oggettivo consistente nella possibilità di ottenere per inferenza informazioni sensibili, o, piuttosto, se debba aversi riguardo alle finalità dichiarate dal titolare del trattamento, si veda P. QUINN, G. MALGIERI, *The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework*, in *German Law Journal* (2021), 22, pp. 1583-1612, p. 1584, doi:10.1017/glj.2021.79. Si veda anche della Corte di giustizia dell'Unione europea, causa

ISSN 2239-8570

considerazione dei dati e delle tecnologie impiegate e, soprattutto, alla luce dell'*uso* previsto delle conoscenze acquisite a seguito del trattamento[86]. Così, nel contesto del citato provvedimento del Garante privacy sulle telecamere a circuito chiuso, il trattamento in esame consisteva anche nell'effettuare una *sentiment analysis* di *post* di utenti di social media, con l'obiettivo di sviluppare un sistema di intelligenza artificiale in grado di prevedere i 'crimini d'odio' a sfondo religioso. Il Garante ha rilevato che "il Comune [il titolare del trattamento nel caso di specie] ha trattato anche dati personali appartenenti a categorie particolari (cfr. art. 9 del Regolamento [GDPR] e art. 2-sexies del Codice della privacy)", poiché i "messaggi/commenti acquisiti dai social network riguardano la sfera religiosa e *possono* rivelare le convinzioni religiose dei loro autori o di terzi citati in tali messaggi"[87]. La stessa conclusione vale quando l'esame delle emozioni e dei sentimenti vengano combinate, per misurare le reazioni a 'claims' resi pubblici da imprese, vertenti su iniziative di 'sostenibilità sociale' (ad es. assumere immigrati come forza lavoro presso l'impresa), con il risultato di ottenere informazioni idonee a rivelare l'opinione politica di persone fisiche[88]. Infine, nel noto caso Cambridge Analytica, l'EDPB ha attribuito lo status di dati sensibili ai dati di utenti di social media trattati per identificare le loro emozioni e costruire profili a fini di pubblicità politica personalizzata[89] .

In base a quanto sopra, sembra ragionevole concludere che l'art. 9 (1) GDPR viene in applicazione allorché il riconoscimento delle emozioni basato sulle caratteristiche fisiche, fisiologiche e comportamentali delle persone fisiche abbia la finalità di conseguire per inferenza informazioni 'sensibili' relative a un individuo identificabile o identificato. Al tempo stesso, come sopra ricordato, l'accertamento della esistenza di una simile finalità va compiuta sulla base di una serie di elementi oggettivi, non rilevando la presenza o meno di un intento in tal senso del titolare del trattamento.

Di conseguenza, porsi la domanda se le emozioni possano essere considerate di per sé dati appartenenti a categorie speciali è fuorviante.

C-184/20, *Vyriausioji tarnybinės etikos komisija* [2022] ECLI:EU:C:2022:601, paragrafo 128.

[86] Per quanto riguarda il dibattito se alcuni (o tutti) i dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica siano da considerarsi sensibili e la rilevanza attribuita al modo in cui i dati vengono utilizzati, si veda E. J. KINDT, *Having Yes, Using No? About the new legal regime for biometric data*, in *Computer Law & Security Review*, Volume 34, Issue 3, 2018, pp. 523-538, https://doi.org/10.1016/j.clsr.2017.11.004.

[87] Cfr. Cfr. Autorità Garante per la protezione dei dati personali 11 gennaio 2024 doc. web n. 9977020, disponibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020, punto 3.1.

[88] A. CARVALHO, A. LEVITT, S LEVITT, E. KHADDAM, J. BENAMATI, *Off-The-Shelf Artificial Intelligence Technologies for Sentiment and Emotion Analysis: A Tutorial on Using IBM Natural Language Processing*, in *Communications of the Association for Information Systems*, (2019) 44, pp. 918 – 943, pp. https://doi.org/10.17705/1CAIS.04443.

[89] European Data Protection Board, Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns (Mar. 13, 2019), https://edpb.europa.eusites/edpb/files/files/file 1/edpb-2019-03- 13- statement-on-elections_en.pdf [https://perma.cc/5BS2-4VJE].

Piuttosto, il riconoscimento delle emozioni (come trattamento di dati personali) può produrre come risultato informazioni sensibili cui si applica il regime speciale per i dati sensibili, alle condizioni sopra menzionate.

Detto questo, è anche degno di nota il fatto che, in linea di principio, l'accertamento della sussistenza di un trattamento di dati particolari è rilevante per la produzione di una serie di conseguenze giuridiche, quali: *i)* identificare la base giuridica del trattamento ai sensi dell'articolo 6 GDPR e *ii)* determinare se si incorra nel divieto di cui all'art. 22 GDPR.

Il prosieguo dell'analisi, tuttavia, è volto a dimostrare che, ai fini della individuazione della disciplina applicabile al tipo di pratica di cui qui si discute, la distinzione tra dati speciali e dati ordinari assume rilevanza limitata. Mentre la prima questione viene trattata in questo paragrafo, l'incidenza di tale distinzione sul divieto appena menzionato sarà analizzato nel paragrafo 1.4.

Per quanto riguarda la base giuridica del trattamento, secondo le Linee Guida dell'EDPB sugli assistenti vocali virtuali, l'analisi della voce per fini di pubblicità personalizzata[90] è un tipo di trattamento che non può qualificarsi strettamente "necessario per l'esecuzione di un contratto" ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR, nemmeno nel contesto di un contratto per la fornitura di un contenuto o di un servizio digitale; allo stesso tempo, la pubblicità personalizzata non può essere "[...] considerata come un servizio esplicitamente richiesto dall'utente finale". Pertanto, in caso di trattamento svolto per un simile scopo, il consenso degli utenti dovrebbe essere sistematicamente raccolto"[91]. Una conclusione analoga si può trarre dalle Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali mediante dispositivi video, secondo cui il titolare del

[90] K. T. SMITH, *Marketing via smart speakers: what should Alexa say?*, in *Journal of Strategic Marketing*, 2020, 28(4), pp. 350-365.

[91] Linee guida 02/2021 dell'EDPB sugli assistenti vocali virtuali. Versione 2.0, adottata il 7 luglio 2021, punto 80, disponibile su https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en. Sul tema del consenso alla raccolta di dati personali la letteratura è sterminata. Cfr. qui, senza pretesa di completezza e rinviando alla bibliografia ivi citata, C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; G. RESTA, V. ZENO- ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo regolamento europeo*, in *Oss. Dir. civ. comm.*, 2018, p. 67 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consent to the processing of personal data: a legal and behavioural analysis. Some Insights into the Effectiveness of Data Protection Law*, in EJPLT, 2018, p. 1-15; ID., *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Pol. Dir.*, 2017, p. 363 ss. Per la dottrina anteriore al GDPR, si vedano le autorevolissime voci di V. CUFFARO, *Il consenso* dell'interessato, in *La disciplina del trattamento dei dati personali*, a cura di V. Cuffaro e V. Ricciuto, Torino, 1997, p. 201 ss.; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 339 ss. V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno resp.*, 1998, p. 23 ss.; S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, p. 621 ss. Con specifico riguardo al tema del consenso nel contesto del neuromarketing, cfr. E. TUCCARI, Neuromarketing*: un'asistematica disciplina…oltre il consenso?*, cit., p. 6 manoscritto.

ISSN 2239-8570

trattamento, per valutare se il legittimo interesse possa costituire idonea base giuridica, deve tenere conto, oltre che del tipo di dati in questione (personali, biometrici o particolari), delle aspettative degli interessati[92], nonché dei rischi di pregiudizio per i diritti fondamentali coinvolti. Questi fattori devono poi essere soppesati rispetto agli scopi di lucro del titolare del trattamento. Inoltre, l'EDPB, nel contesto della serie di 'decisioni vincolanti' emesse nel 2023 in tema di pubblicità comportamentale[93], ha chiarito che questo tipo di trattamento richiede il consenso dell'interessato[94]. Cosa ancora più importante, tale conclusione è stata confermata da una recente decisione della Corte di giustizia dell'Unione europea[95] .

Il tipo di dati trattati è rilevante altresì per stabilire se il consenso specifico costituisca idonea base giuridica per il trattamento in parola, al posto del consenso esplicito richiesto per il trattamento di dati particolari. Il GDPR ha reso meno netta la linea di demarcazione tra consenso specifico e consenso esplicito, stabilendo requisiti rigorosi anche per quanto riguarda il primo tipo di consenso[96] . Infatti, il consenso specifico è valido se, tra l'altro, è *informato*. Il che implica, però, che si individui l'oggetto del dovere di trasparenza di cui agli articoli 12 e 13 del GDPR[97]: indiscusso essendo che il titolare del trattamento è tenuto rendere note le finalità del trattamento (cfr. considerando 42 e art. 58 GDPR)[98], le opinioni appaiono discordanti in merito al grado di specificità richiesto per tali informazioni.

---

[92] Nel caso di monitoraggio sistematico di un luogo specifico, è rilevante il tipo di luogo monitorato, ad es., che si tratti di un luogo pubblico destinato al tempo libero, all'interazione con altre persone, ecc.)

[93] *European Data Protection Board* – Binding Decisions n. 2/2022, 3/2022 e 4/2023, https://edpb.europa.eu/our-work-tools/ consistency-findings/register-for-decisions_en.

[94] Di diverso avviso C. WENDEHORST, Y. DULLER, *Biometric Recognition and Behavioral Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, Policy Department for Citizens' Rights and Constitutional Affairs, PE 696.968 - August 2021, p. 81: secondo cui, nella maggior parte dei casi, il trattamento dei dati personali ai fini del riconoscimento delle emozioni o della categorizzazione biometrica è subordinato al semplice consenso ai sensi dell'art. 6, paragrafo 1, lettera a) GDPR. Tali aa., tuttavia, non considerano in modo specifico la pratica qui in esame.

[95] Corte di giustizia dell'Unione europea, (Case C-252/21, Meta Platforms and Others (General terms of use of a social network), Judgment of the Court (Grand Chamber) of 4 July 2023 (request for a preliminary ruling from the Oberlandesgericht Düsseldorf — Germany) — Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd, Facebook Deutschland GmbH v Bundeskartellamt (C 296/3).

[96] Si veda P. QUINN, G. MALGIERI, *The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework*, cit., 1584 e 1601.

[97] A. MANTELERO, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law & Security Review*, vol. 30, Issue 6, Dicembre 2014, pp. 643-660. Si veda anche H. RUSCHEMEIER, *Data Brokers and European Digital Legislation*, op. cit., 37.

[98] Si veda, per una panoramica, G. SARTOR, F. LAGIOIA, F. GALLI, *Regulating targeted and behavioural advertising in digital services. How to ensure users' informed consent*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, PE 694.680, 59, http://www.europarl.europa.eu/supporting-analyses.

Tuttavia, se si accoglie la conclusione qui proposta, vale a dire che lìidentificazione delle emozioni di un individuo per fini di pubblicità personalizzata comporta una forma di profilazione (cfr. paragrafo 1.2)[99], ai sensi degli articoli 13 (2) (f) e 14 (2) (g) GDPR, i titolari del trattamento devono ottenere il consenso esplicito degli interessati e informarli del trattamento, rendendo note non solo le finalità per le quali la profilazione ha luogo, ma anche i criteri sottostanti[100]. Queste disposizioni e la Linee guida del Gruppo di lavoro art. 29 in tema di decisioni automatizzate e profilazione fanno riferimento alla 'logica' coinvolta nell'attività di profilazione, il che comporta che "all'interessato dovrebbero essere fornite anche informazioni sul suo profilo, ad esempio in quali 'segmenti' o 'categorie' è collocato"[101]. Di recente, inoltre, la Cassazione italiana ha rilevato che il dovere di informare, inter alia, circa le *modalità* del trattamento (stabilito dall'art. 13 del d.lgs 196 del 2003, applicabile *ratione temporis*) riguarda i 'parametri' utilizzati dal sistema di IA per pervenire ad un dato *output*[102]. Applicando quanto sopra al riconoscimento delle emozioni, si ha che le persone fisiche che vi sono sottoposte debbono essere informate del fatto di essere oggetto di profilazione sulla base delle proprie emozioni[103]. Si noti, infine, che un obbligo di 'rivelare' i principali parametri impiegati per personalizzare le informazioni fornite ai destinatari del marketing online è stabilito dal Regolamento sui servizi digitali[104], nonché da talune specifiche disposizioni del diritto dei consumatori (cfr. para. 2).

Pertanto, per quanto riguarda l'uso di ERS per valutare le emozioni e caratterizzare le persone per fini di pubblicità personalizzata, le informazioni da comunicare agli interessati dovrebbero avere la funzione di 'segnalare' una pratica socialmente e giuridicamente discutibile, facilitando l'esercizio dei diritti dei soggetti interessati nonché la supervisione di eventuali violazioni della normativa sulla protezione dei dati. Le informazioni fornite sotto forma di avvertimento conciso e chiaro sono particolarmente adatte a tal fine[105], anche in considerazione del contesto in

[99] Questo tipo di trattamento può rientrare nell'ambito di applicazione dell'articolo 22 del GDPR (cfr. paragrafo 1.4). Si noti che, in questo caso, è necessario un consenso esplicito ai sensi dell'articolo 22 del GDPR, indipendentemente dal tipo di dati utilizzati.

[100] Circa i doveri di informazione da fornirsi ai soggetti interessati, per il caso in cui siano ottenute, per inferenza, informazioni che li riguardano, si vedano S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2019, 2, 494 ss., 543 e 545.

[101] Gruppo di lavoro articolo 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 16.

[102] Cass. civ., 10 ottobre 2023, n. 28358, in *Nuova giur. civ. comm.*, 2024, 2, 402 ss., con nota di N. BRUTTI, *Mito del consenso e rating reputazionale*. Cfr., inoltre, F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. Il caso "Mevaluate"*, nota a Cass. Civ. 25.5.2021, n. 14381, in *Dir. inf.*, 2021, 1005 ss.

[103] Si veda A. HAUSELMANN, A. M. SEARS, L. ZARD, E. FOSCH-VILLARONGA, *Eu Law and Emotion Data*, op. cit., 5, secondo i quali un'adeguata trasparenza dovrebbe comportare l'obbligo per il titolare del trattamento dei dati di rivelare alle persone fisiche interessate l'emozione specifica rilevata da questa tecnologia.

[104] Si veda in merito il paragrafo 2.

[105] A. KAK, *Regulating Biometrics: Global Approaches and Urgent Questions. AI Now Institute, The State of Play and Open Questions in the Future*, a cura di A. Kak, 2020, 16

ISSN 2239-8570

cui il trattamento si svolge (il quale comporta interazioni transitorie ed effimere tra titolari del trattamento e interessati).

Considerazioni simili sono apertamente articolate dalle già citate Linee guida dell'EDPB sugli assistenti virtuali: ai sensi dell'art. 5, paragrafo 1, lettera a), dell'art. 12 e dell'art.13 GDPR (il cui significato è chiarito dal considerando 58), "Data controllers are obliged to inform users of the processing of their personal data in a concise, transparent, intelligible form, and in an easily accessible way". Ivi si aggiunge che: "Complying with the transparency requirement […] serves as a control mechanism over the data processing and allows users to exercise their rights. Informing users properly on how their personal data is being used makes more difficult for data controllers to misuse the VVA for purposes that go far beyond user expectations. For example, patented technologies *aim to infer health status and emotional states* from a user's voice and adapt the services provided accordingly"[106].

1.4. Il riconoscimento delle emozioni come forma di trattamento automatizzato ai sensi del GDPR

Il GDPR non trascura di regolare le tecnologie, come i sistemi di IA e di apprendimento automatico[107], che 'producono' conoscenza sulle caratteristiche e sul comportamento delle persone fisiche. Esso contiene, infatti, disposizioni che stabiliscono divieti o limiti circa il modo in cui gli *output* di tali sistemi sono ottenuti e utilizzati[108] .

Poiché una di tali disposizioni è contenuta nell'art. 22 GDPR[109], il presente paragrafo intende innanzitutto stabilire a quali condizioni essa si applichi all'uso di ERS per lo scopo oggetto di analisi. Successivamente, si

---

ss., 25-26, https://ainowinstitute.org/regulatingbiometrics.html. Cfr. punto 25: "il diritto dell'individuo di rifiutare o revocare il consenso alla raccolta o all'uso dei propri dati è uno strumento importante per contrastare l'uso di sistemi biometrici" (traduzione nostra).

[106] Cfr. ibidem, punto 48.

[107] È molto discusso se le tecnologie che "apprendono dai dati" per produrre conoscenza siano considerate dal GDPR. Si veda R. GELLERT, *Comparing definitions of data and information*, in *Regulation & Governance* (2020, 16, 156 ss. In merito, cfr. Gruppo di lavoro art. 29, Opinion n. 3/2012 on developments in biometric technologies, cit., 14: "Data subjects have a right to obtain from the data controller access to their data, in general including their biometric data. Data subjects also have a right to access possible profiles based on these biometric data".

[108] A. TAMÒ-LARRIEUX, *Decision-making by machines: is the "Law of Everything" enough?*, in *Computer & Security Review*, 2021, 41, 1 ss., 8-13.

[109] Sul tema si vedano, per riferimenti bibliografici, L. EDWARDS, M. VEALE, *Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"'*, in *IEEE Security and Privacy*, 2018, 16(3), 46 ss.; E. PALMERINI, *Algoritmi e decisioni automatizzate. Tutele esistenti e linee evolutive della regolazione*, in *I diritti fondamentali nell'era della digital mass surveillance*, a cura di *L. Efrén Ríos Vega, L. Scaffardi, I. Spigno*, Napoli, 2021, 209 ss.; D. IMBRUGLIA, *Diritti fondamentali e ambienti digitali: prime note di una ricerca sul diritto a non essere sottoposto a una decisione interamente automatizzata*, in *Annuario OGID 2022- Yearbook JODI 2022*, a cura di S. Orlando e G. Capaldo, Roma, 2022, 113 ss.

ISSN 2239-8570

prenderanno in considerazione altri pertinenti principi in materia di protezione dei dati personali.

Come noto, in una recente sentenza emessa nella causa OQ vs Land Hessen e SCHUFA Holding[110], la Corte di giustizia dell'Unione europea ha optato per un'accezione ampia del termine 'decisione', sulla base di un'interpretazione sistematica e teleologica dell'articolo in questione[111], con l'obiettivo di garantire effettiva protezione dei diritti fondamentali degli interessati. Secondo la Corte, il considerando 71 GDPR fa riferimento a 'qualsiasi misura' basata su un trattamento automatizzato di dati personali (che comprende "una serie di atti in grado di incidere sull'interessato in molti modi"[112]). Ciò che conta è il carattere 'significativo' dell'incidenza della decisione sui diritti dell'interessato ("la gravità degli effetti sullo status giuridico, economico e sociale dell'interessato"[113]), da valutarsi caso per caso.

A questo proposito, il citato considerando chiarisce che il requisito dell'incidenza significativa comprende non solo i pregiudizi di carattere patrimoniale, ma anche la discriminazione delle persone fisiche[114]. Ad esempio, l'assegnazione di una persona fisica a una data categoria sulla base delle di lei rilevate emozioni può comportare una valutazione delle caratteristiche fisiche, fisiologiche o comportamentali di detta persona, che la esponga ad effetti pregiudizievoli. Ad es., sulla base della previsione di una sua più elevata propensione a spendere, le viene offerto, per un dato prodotto, un prezzo personalizzato svantaggioso[115]; o le viene 'raccomandato' un farmaco, perché considerata affetta da una data patologia. Si consideri inoltre l'eventualità che la caratterizzazione e conseguente valutazione della persona fisica siano inaccurate. Ad es., tale persona viene ritenuta affetta da una data patologia ("Tizia prova spesso rabbia acuta, quindi soffre di una malattia mentale") o rappresentata come avente certi tratti psicologici ("Tizia presenta indolenza, mancanza di

[110] Corte di giustizia dell'Unione europea (Prima Sezione), 7 dicembre 2023, OQ contro Land Hessen. (ECLI:EU:C:2023:957), in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0634.

[111] P. A. EARLS DAVIS, S. F. SCHWEMER, *Rethinking Decisions under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making*, in *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023), held in conjunction with ICAIL 2023*, June 19, 2023, Braga, http://dx.doi.org/10.2139/ssrn.4478107.

[112] Cfr. Conclusioni emesse dall'Avvocato generale Pikämae nella causa C-634/21, OQ vs Land Hessen con l'intervento di SHUFFA Holding, della Corte di Giustizia dell'Unione europea, 7 dicembre 2023, https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=2468721).

[113] Cfr. loc. ult. cit., punto 39.

[114] Cfr. G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Persona e mercato*, 2023, 4, 638 ss.

[115] Cfr. S. PAGLIANTINI, *Alla ricerca di una direttiva 93/13 rimasterizzata*, in *Le clausole abusive nei contratti dei consumatori. Trent'anni di direttiva 93/13*, a cura di S. Pagliantini, Torino, 2024, 2 ss., 199-201, nonché R. MONTINARO, *I sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)*, in *Persona e mercato*, 2022, 3, 346 ss.

ISSN 2239-8570

concentrazione, etc."), e quindi giudicata inadatta a svolgere una certa attività; etc.

Inoltre, in considerazione del fatto che il quadro normativo in materia di protezione dei dati mira a tutelare i diritti fondamentali delle persone interessate (art. 1 GDPR), alcuni studiosi sostengono l'art. 22 GDPR proibisca qualsiasi interferenza significativa con tali diritti[116], compresa la manipolazione. Con tale ultimo termine si intende un'ampia gamma di pratiche lesive dell'autonomia[117] e finanche della dignità della persona fisica[118]. Così, per quanto riguarda la pubblicità online, le Linee guida del Gruppo di lavoro art. 29 sui processi decisionali automatizzati spiegano che, sebbene questo tipo di pratica non comporti di per sé un'incidenza di questo tipo, una pubblicità online, rivolta a soggetti particolarmente vulnerabili e svolta con modalità particolarmente manipolative, fa entrare in gioco l'articolo 22 GDPR[119]. Ciò può verificarsi, secondo le suddette Linee guida, quando i responsabili del trattamento adottano tecnologie che consentano loro di acquisire conoscenza delle "*vulnerabilità* delle persone interessate" e di fare leva tale conoscenza.

Come già osservato, il riconoscimento e la categorizzazione delle emozioni implicano una forma di profilazione ai sensi dell'art. 4 (4)

[116] G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7 (3), 15 ss., https://ssrn.com/abstract=3088976. Contra I. MENDOZA, L. A. BYGRAVE, *The Right Not to Be Subject to Automated Decision Based on Profiling*, in *EU Internet Law: Regulation and Enforcement* 2, a cura di Tatiany Synodinou, Springer, 2017, 12 ss.

[117] T.Z. ZARSKY, *Privacy and Manipulation in the Digital Age*, in *Theoretical Inquiries in Law*, 2019, 20 (1), 157 ss. Si veda anche G. MALGIERI, *In/Acceptable Marketing and Consumers' Privacy Expectations: Four Tests from EU Data Protection Law*, in *Journal of Consumer Marketing*, 2021, 40 (2), 209 ss., https://doi.org/10.1108/JCM-03-2021-4571, nonché K. GRISSE, *Recommender Systems, Manipulation and Private Autonomy: How European Civil Law Regulates and Should Regulate Recommender Systems for the Benefit of Private Autonomy*, in *Recommender Systems: Legal and Ethical Issues*, a cura di S. Genovesi, K. Kaesling, S. Robbins. *The International Library of Ethics, Law and Technology*, vol. 40, 2023, Springer, 101 ss., https://doi.org/10.1007/978-3-031-34804-4_6). Per la dottrina italiana, cfr. V. RICCIUTO, *La persona e la vulnerabilità tecnologica: il diritto della tecnologia sostenibile*, in *Rivista dir. impr*., 2023, 3, 487 ss.

[118] P. STANZIONE, *Relazione introduttiva. Privacy e neurodiritti. La persona al tempo delle neuroscienze*, in *Atti del Convegno – 28 gennaio 2021*, *GPDP*, 16; A. MOLLO, *La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici*, in *European Journal of Privacy Law & Technologies*, 2021, 200 ss., 207.

[119] Si veda M. E. KAMINSKY, *The Right to Explanation, Explained*, op. cit., 202, a commento di Gruppo di lavoro art. 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, adottato il 3 ottobre 2017, da ultimo rivisto e adottato il 6 febbraio 2018, 21-22, secondo la quale il requisito degli "effetti giuridici o effetti altrettanto significativi" dovrebbe essere interpretato in senso ampio: anche il marketing online o la discriminazione dei prezzi, in alcune condizioni, potrebbero essere considerati effetti significativi rilevanti ai sensi dell'articolo 22. A tal proposito, vengono proposti alcuni criteri per valutare l'importanza della pratica: l'intrusività del processo di profilazione, le aspettative degli interessati, il modo in cui la pubblicità viene diffusa o le particolari vulnerabilità di tali soggetti.

GDPR[120], grazie alla quale il titolare del trattamento può determinare gli stati emotivi e le caratteristiche psicologiche dell'interessato[121] e dunque apprendere in quale misura il di lui processo decisionale sia 'suscettibile' (nel senso letterale del termine, cioè passibile di risentire degli effetti di un elemento esterno) di venire influenzato dalla pratica di marketing adottata. Questa tecnologia, infatti, può essere utilizzata, anche involontariamente[122], per orientare i processi decisionali delle persone fisiche, distorcendone le scelte[123].

Le argomentazioni qui riportate attengono ad un terreno di riflessione relativamente nuovo - sul quale non è dato soffermarsi - concernente la individuazione del raggio d'azione della regolamentazione sui dati personali: si tratta di stabilire se in esso ricadano pratiche che incidono negativamente sull'autonomia della persona fisica, anziché sulla semplice autodeterminazione informativa; e, in ultima istanza, di comprendere se stiamo assistendo alla "fine" del diritto alla protezione dei dati, come tradizionalmente inteso e applicato, o, piuttosto, ad un sua nuova "epifania"[124], grazie alla quale tale sistema si fa accorto custode anche del modo in cui le informazioni concernenti le persone fisiche vengono impiegate e delle relative ricadute sui diritti degli interessati. Molteplici indici normativi inducono ad accogliere una simile conclusione.

È appena il caso di ricordare che altri campi del diritto sono tradizionalmente votati alla protezione dell'autonomia decisionale, per finalità e/o contesti circoscritti. Si pensi al diritto dei consumatori e in particolare alla regolamentazione in tema di pratiche commerciali sleali (cfr. para. 2), i quali proteggono l'autonomia dei consumatori in vista della

[120] Si tratta di un tipo di trattamento da intendere in un'ampia accezione, secondo la lettera e lo spirito della relativa definizione. Si vedano, in merito, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., 7.

[121] Si veda S.C. MATZ, M. KOSINSKI, G. NAVE, D.J. STILLWELL, *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, in *Proceedings of the National Academy of Sciences of the United States of America*, 2017, 114, 12714 ss., https://api.semanticscholar.org/CorpusID:9309185, su come l'efficacia dei messaggi di marketing aumenti quando vengano adattati ai profili psicologici degli individui. Cfr. anche N. WILDMAN, N. RIETDIJK, A. ARCHER, *Online affective manipulation*, in *The Philosophy of Online Manipulation*, a cura di F. Jongepier, M. Klenk, Routledge, 2022, 311 ss., che descrive le forme di manipolazione basate sulle emozioni.

[122] Una pratica di marketing che preveda il *targeting* degli individui sulla base delle informazioni elaborate dagli ERS è per definizione connotata da una più intensa efficacia condizionante delle scelte di coloro che vi sono esposti, rappresentando così un rischio per la loro autodeterminazione e dignità.

[123] T. CASARETO DAL VERME, *Artificial Intelligence, Neuroscience and Emotional Data. What Role for Private Autonomy in the Digital Market?*, in *Erasmus Law Review*, 2024, 3, doi: 10.5553/ELR.000257.

[124] Sul tema, si veda già I. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 2013, e in *NYU School of Law, Public Law Research Paper No. 12-56*, 1 ss., 5, in http://dx.doi.org/10.2139/ssrn.2157659. K. GRISSE, *Recommender Systems, Manipulation and Private Autonomy: How European Civil Law Regulates and Should Regulate Recommender Systems for the Benefit of Private Autonomy*, op. cit., 106 ss. Cfr. anche T.Z. ZARSKY, *Privacy and Manipulation in the Digital Age*, op. cit., 161 ss.

ISSN 2239-8570

esigenza di prevenire fallimenti del mercato[125]. Ivi le pratiche che distorcono la scelta dei consumatori costituiscono oggetto di specifiche fattispecie. Le disposizioni in materia di protezione dei dati personali si candidano, invece, a tutelare la persona fisica in quanto tale, a prescindere da un rapporto di consumo.Infine, si noterà più oltre che, nel Regolamento su IA, le pratiche implicanti tecnologie atte a manipolare le persone fisiche sono proibite, a certe condizioni ivi indicate (cfr. para. 3).

In sintesi, si può affermare che la valutazione dello stato emotivo di una persona per i fini di cui si discute costituisce un trattamento automatizzato riconducibile all'art. 22 GDPR, quando implica una incidenza significativa sui suoi diritti (compresi i diritti fondamentali) dell'interessato[126] .

Una critica che si suole comunemente sollevare a questo proposito è che il divieto di cui all'art. 22 (1) GDPR può essere derogato da una semplice manifestazione di consenso esplicito dell'interessato (cfr. art. 22 (2) (c)) offrendo dunque una protezione soltanto nominale per i diritti dell'interessato[127]. Analoga critica viene rivolta anche al divieto di trattare categorie particolari di dati, che viene meno quando l'interessato dia il proprio consenso al trattamento per una o più finalità specifiche (ai sensi dell'art. 22 (4) e dell'art. 9 (2) (a) GDPR). Secondo la lettura avanzata poco sopra (si veda il para. 1.3), questo divieto (e la relativa deroga) include il caso in cui le informazioni sensibili siano elaborate come risultato di un trattamento che ha lo scopo di ottenere tale tipo di informazioni mediante la combinazione di dati che, di per sé isolatamente considerati, non rivestono la qualifica di dati particolari (ad es. dati su bio-caratteristiche o su emozioni desunte sulla scorta dell'analisi di tali ultime caratteristiche).

A tali critiche è tuttavia possibile obiettare che la 'fallacia' del principio del consenso[128] appare mitigata dal complesso sistema normativo in materia di protezione dei dati, nel quale si rintraccia il principio di trasparenza[129]

[125] Cfr. T.Z. ZARSKY, op. cit., 172, il quale individua tre differenti ragioni per proibire pratiche manipolative, una *market-oriented*, una seconda *autonomy-based* e, infine, una terza basata sulla considerazione della dignità della persona (giacché simili pratiche degradano l'individuo a oggetto di sperimentazione). Si veda, per considerazioni di ampio respiro sulle funzioni della regolamentazione consumeristica, G. GRISI, *Rapporto di consumo e pratiche commerciali*, in *Eur. dir. priv*., 2013, 1, 6 ss.

[126] J. CHEN, L. MIOTTO, *Manipulation, Real-Time Profling, and their Wrongs*, in *The Philosophy of Online Manipulation*, op. cit., 392-409.

[127] S. BAROCAS, H. NISSENBAUM, *Big Data's End Run around Anonymity and Consent*, in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, a cura di Helen Nissenbaum e Victoria Stodden, Cambridge 2014, 46.

[128] A. MANTELERO, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law and Security Review*, 2014, 30, 643 ss., ssrn.com/abstract=2529245.

[129] Cfr. M. E. KAMINSKY, *The Right to Explanation, Explained*, op. cit., 189 ss., 196, https://doi.org/10.15779/Z38TD9N83H, in cui si osserva che "the right to object, the right to rectification (correction), data protection by design and by default, and the requirement of data protection impact assessments, likely apply to most or even all algorithmic decision-making".

unitamente ad altri principi, quali accuratezza, correttezza[130] e 'responsabilizzazione'.

Ai fini della presente analisi e senza pretesa di completezza, sia sufficiente qui ricordare come il GDPR prescriva l'accuratezza delle informazioni relative ad una persona fisica (cfr. art. 5 GDPR), affinché quest'ultima non debba subire pregiudizi di sorta per via di una rappresentazione non accurata di tratti attinenti alla propria personalità. Le tecnologie di IA e di apprendimento automatico sono in grado di elaborare dati personali per compiere valutazioni su persone fisiche identificate o identificabili, le quali equivalgono a informazioni che le concernono (cfr. paragrafo 1.2). La questione se il requisito di accuratezza valga anche rispetto alle informazioni ottenute per inferenza è dibattuta in dottrina[131]. La soluzione affermativa pare potersi desumere dalla giurisprudenza della Corte di giustizia dell'Unione europea[132], in considerazione, da ultimo, della decisione sul caso OQ vs Land Hessen e SHUFA Holding, già richiamata: qui l'accuratezza è richiesta rispetto ai dati elaborati dai sistemi di IA, in quanto costituisce uno dei fattori da cui dipende la qualità dei relativi *output*. Spetta dunque al titolare del trattamento assicurarla, adottando adeguate misure tecniche o organizzative[133].

La trasparenza ai sensi del GDPR è un principio ampio[134] che comprende, sì, ma non si esaurisce nell'obbligo per il titolare del trattamento di rendere note le finalità e la logica alla base del trattamento automatizzato e le relative conseguenze (come previsto dall'articolo 15 (1) (h)[135]). Lo stesso diritto di accesso ai dati svolge in primo luogo una

[130] D. CLIFFORD, J. AUSLOOS, *Data Protection and the Role of Fairness*, in *Yearbook of European Law*, 2018, 37, 130 ss.

[131] Si veda D. HALLINAN, F. ZUIDERVEEN BORGESIUS, *Opinions can be Incorrect! In our Opinion. On the accuracy principle in data protection law*, in *International Data Privacy Law* 2020, 4, 1 ss., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540737.

[132] Cfr. CGUE, Google Spain SL e Google Inc. contro Agencia Espanola de Proteccion de Datos (AEPD) e Mario Costeja Gonzalez, C-131/12, 13 maggio 2014, ECLI:EU:C:2014:317, par. 88. Si veda anche Corte di giustizia del 16 gennaio 2019, C-496/17 (Deutsche Post AG), par. 57. Per ulteriori riferimenti cfr. A. TAMÒ-LARRIEUX, *Decision-making by machines. Is the "Law of Everything enough?"*, in *Law & Security Review*, 2021, 41, 1 ss., 10.

[133] Cfr. causa C-634/21, ECLI:EU:C:2023:957, avente ad oggetto la domanda di pronuncia pregiudiziale proposta ai sensi dell'articolo 267 TFUE, dal Verwaltungsgericht Wiesbaden (tribunale amministrativo di Wiesbaden, Germania), con decisione del 1° ottobre 2021, nel procedimento tra OQ contro il Land Hessen, con l'intervento di SCHUFA Holding AG, in https://curia.europa.eu/juris/document/document.jsf;jsessionid=33FDD0B33B2ACB3A4A0D257BFA64DD8F?text=&docid=280426&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=3404418. La decisione, oltre a richiamare l'art. 5 GDPR, rinvia altresì al Considerando 71, secondo cui "[…] è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati […]".

[134] Si veda M. E. KAMINSKY, *The Right to Explanation, Explained*, in *Berkeley Technology Law Journal*, 2019, 34, 189 ss., 210, https://doi.org/10.15779/Z38TD9N83H, secondo cui il GDPR ha istituito un regime di "trasparenza qualificata".

[135] Si vedano le conclusioni dell'Avvocato generale Pikamäe del 16 marzo 2023 sulla causa Shufa (causa C-634/21), par. 58. Ai sensi del GDPR, la protezione dei segreti commerciali

ISSN 2239-8570

funzione di controllo dei processi automatizzati (oltre che di stimolo alla relativa supervisione)[136]. Soprattutto, la trasparenza è affiancata dai principi di responsabilizzazione e correttezza, che hanno acquisito crescente rilievo, in particolare a seguito dell'avvento di tecnologie come l'IA e il *machine learning*[137] .

Un trattamento automatizzato è contrario al principio di correttezza quando dia luogo a relazioni squilibrate tra titolare del trattamento e soggetto interessato e/o implichi gravi rischi per quest'ultimo[138], nel qual caso esso è vietato anche in presenza di una legittima base giuridica[139]. Una simile condizione ricorre, come già rilevato, allorché il titolare faccia leva su (o dia origine a) una condizione di vulnerabilità dell'interessato sfruttando le informazioni sui di lui stati emotivi e tratti della personalità, acquisite grazie al riconoscimento delle emozioni[140].

Come per ogni altro principio generale del trattamento, spetta al titolare dare ad esso attuazione (secondo la logica propria dell'*accountability* di cui all'art. 5 (2) GDPR)[141], innanzitutto nel contesto della valutazione della

---

e della proprietà intellettuale non giustifica il rifiuto di fornire informazioni agli interessati (Considerando 63), ad esempio sulla logica dello specifico trattamento automatizzato che li riguarda (cfr. G. MALGIERI, *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights* in *International Data Privacy Law*, 2016, 6 (2), 102 ss., https://ssrn.com/abstract=3002685.

[136] M. E. KAMINSKY, *The Right to Explanation, Explained*, op. cit., 204-217, per cui la trasparenza ai sensi del GDPR comprende il principio "human in the loop", il dovere di adottare garanzie adeguate e tutti i diritti procedurali concessi all'interessato ai sensi dell'articolo 22 del GDPR. Si veda anche G. MALGIERI, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7 (3), https://ssrn.com/abstract=3088976, 25-26.

[137] LEE A. BYGRAVE, *Data Protection Law, Approaching Its Rationale, Logic and Limits, in Information Law Series*, vol. 10, The Hague, 2002, https://api.semanticscholar.org/CorpusID:153406054. Si vedano European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Adopted on 20 October 2020), 1.

[138] G. MALGIERI, *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation*, in *Proceedings of FAT* '20*, January 27–30, 2020. ACM, New York, NY, USA, 1 ss., 6, https://ssrn.com/abstract=3517264; D. CLIFFORD, J. AUSLOOS, *Data Protection and the Role of Fairness*, in *Yearbook of European Law*, 2018, 37, 130 ss., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139; M. BUTTERWORTH, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law & Security Review*, 2018, 34 (2), 257 ss.

[139] S. ORLANDO, *Per un sindacato della liceità del consenso privacy*, in *Persona e mercato*, 2022, 4, 527 ss., 533-538.

[140] J. Chen, L. Miotto, *Manipulation, Real-Time Profiling, and their Wrongs*, in *The Philosophy of Online Manipulation*, a cura di F. Jongepier, M. Klenk, Rutledge, 2022, 392 ss., 404.

[141] Si veda EDPB's Response to the MEP Sophie in't Veld's letter on unfair algorithms, in https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mep-sophie-int-velds-letter-unfair-algorithms_en, p. 3, il GDPR mira a garantire che "data subjects are not adversely impacted, including by unintentional consequences of automated decision-making".

'incidenza' del trattamento sui diritti dell'interessato[142]. Quest'ultima, come noto, è da compiersi (*ex* art. 35 GDPR) quando siano soddisfatte alcune condizioni specifiche[143] o allorché il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della sua natura, portata, contesto e finalità. Simili condizioni sono soddisfatte nella pratica in analisi, in considerazione del tipo di dati utilizzati (dati ottenuti dall'analisi della sfera più intima delle persone), del tipo (trattamento automatizzato) e contesto in cui viene condotto il trattamento, della metodologia di analisi dei dati utilizzata e, soprattutto, della sua incidenza. Si tratta invero di fattori che comportano la probabilità di un rischio elevato per i diritti fondamentali delle persone esposte a questa pratica.

La pertinente dottrina sottolinea come, lungi dal consistere in un mero esercizio di *compliance* per individui e organizzazioni titolari del trattamento, l'istituto in parola valga a proteggere diritti e libertà dell'interessato da tali rischi in via preventiva[144]. La valutazione dei rischi effettuata e le misure di mitigazione individuate - da adottare *by design*[145] - devono essere inserite dai titolari del trattamento nei registri delle attività di trattamento a cui le autorità di protezione dei dati possono accedere ai sensi degli art. 24 e 58 GDPR[146], in modo da consentire una supervisione più efficace.

---

[142] A. KASIRZADEH, D. CLIFFORD, *Fairness and Data Protection Impact Assessments*, in *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (AIES '21), May 19–21, 2021, 1 ss., 2, https://doi.org/10.1145/3461702.3462528, p. 2.

[143] Alcune di queste condizioni possono verificarsi quando gli ERS vengono utilizzati per scopi di pubblicità personalizzata. Ad esempio, una forma di valutazione sistematica ed estesa degli aspetti personali delle persone ai sensi dell'articolo 35 (3) (a) del GDPR può riscontrarsi quando essi siano utilizzati nel contesto della pubblicità personalizzata sui social media o veicolata da "assistenti virtuali". Un monitoraggio sistematico di un'area accessibile al pubblico su larga scala può aversi poi nel caso di cartelloni pubblicitari intelligenti e pubblicità personalizzata nelle vendite al dettaglio (si veda il para. 1.2).

[144] A questo proposito, un aspetto rilevante consiste nello stabilire se l'istituto possa essere interpretato come avente la funzione di valutare i rischi per i diritti fondamentali coinvolti nel trattamento, come suggerisce il tenore normativo dell'art. 35 GDPR e come sostenuto da diversi studiosi. Per una panoramica della letteratura giuridica in materia, si veda G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford, 2023. Sulla questione, si vedano N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right? Beyond Data Protection Risk Assessments*, in *Computer Law & Security Review*, 2016, 32, 286 ss., https://doi.org/ 10.1016/j.clsr.2015.12.017. Cfr., inoltre, Gruppo di lavoro art. 29, *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* [Art. 29 WP 248 (4 Apr. 2017)]. Si veda anche EDPB's *Response to the MEP Sophie in't Veld's letter on unfair algorithms*, cit., 4, secondo cui "The outcome of the assessment can also be that the controller will have to refrain from using a specific algorithm, or parts of it, if the risks to the rights of data subjects and other persons cannot be sufficiently mitigated".

[145] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, adottate il 20 ottobre 2020, punto 69. Cfr., per riferimenti, M. RATTI, *Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, in *Codice della Privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, Milano, 2021, 410 ss.

[146] Cfr. A. TAMÒ-LARRIEUX, *Designing for Privacy and its Legal Framework: Data Protection by design and Default for the Internet of Things*, in *Law, Governance and Technology Series*, Springer, 2018, 182 ss.

ISSN 2239-8570

In sintesi, il GDPR regola non solamente la raccolta dei dati personali necessari per i sistemi di IA e di apprendimento automatico, ma, al verificarsi delle condizioni e sulla scorta dei principi sopra indicati, anche i processi di estrazione di conoscenza da tali dati[147] e la loro incidenza su un'ampia gamma di interessi giuridicamente protetti[148] come l'auto-determinazione, la non discriminazione e la dignità[149] .

Tali considerazioni appaiono di particolare importanza per la pratica oggetto di analisi nel presente studio, la quale, come già ricordato, può comportare manipolazione e discriminazione delle persone fisiche, il loro monitoraggio con il fine di identificarne le emozioni (eventualmente in assenza di consenso informato) e/o una loro inaccurata caratterizzazione[150] .

Da ultimo, merita fare cenno al fatto che l'insieme delle tutele di diritto privato desumibili dal regime giuridico dell'Unione europea sulla protezione dei dati personali è stato fatto oggetto di pronunce e innesti legislativi. Più in dettaglio, quanto al primo aspetto, basti pensare agli

[147] Corte di giustizia dell'Unione europea, Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez, C-131/12, 13 May 2014, ECLI:EU:C:2014:317, punto 68: "the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter". Si veda anche Judgment of the Court (First Chamber) of 7 December 2023. OQ v Land Hessen (ECLI:EU:C:2023:957), in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0634, che adotta una interpretazione teleologica dell'art. 22 GDPR al fine di assicurare tutela ai diritti fondamentali dell'interessato. Cfr., negli stessi termini, N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, 10, 40 ss.

[148] A. KASIRZADEH, D. CLIFFORD, *Fairness and Data Protection Impact Assessments*, cit., p. 6. Si veda anche L. DALLA CORTE, *On proportionality in the data protection jurisprudence of the CJEU*, in *International Data Privacy Law*, 2022, 12 (4), 259 ss., https://doi.org/10.1093/idpl/ipac014, pp. 262-266.

[149] B. VAN DER SLOOT, *Legal fundamentalism: Is data protection really a fundamental right*, in *Data protection and privacy: (In)visibilities and infrastructure*, a cura di R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert, Law, Governance and Technology Series, Issues in Privacy and Data Protection, Springer, 2017, 36, 3 ss., https://doi.org/10.1007/978-3-319-50796-5_1.

[150] P. VALCKE, D. CLIFFORD, V. K. DESSERS, *Constitutional Challenges in the Emotional AI Era*, in *Constitutional Challenges in the Algorithmic Society*, a cura di Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor, and Giovanni De Gregorio, 2021, Cambridge University Press, 57 ss., 65-67. Sul tema della inaccurata rappresentazione della persona fisica, dovuta a forme di caratterizzazione algoritmica, si vedano le riflessioni sul c.d. "representational harm", rispetto a single persone fisiche o gruppi. Cfr. J. KATZMAN, A. WANG, M. SCHEUERMAN, S. LIN BLODGETT, K. LAIRD, H. WALLACH, S. BAROCAS, *Taxonomizing and Measuring Representational Harms: A Look at Image Tagging*, 4-5, in arXiv:2305.01776v1, nonché C. VÉLIZ, *Self-Presentation and Privacy Online*, in *Journal of Practical Ethics*, 2022, 9 (2), doi: https://doi.org/10.3998/jpe.2379, sul rapporto tra auto-rappresentazione e diritto alla privacy. Si veda, infine, B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, in *Philos. Technol*., 2017, 30, 475 ss., 482, in 10.1007/s13347-017-0253-7.

articoli 80 e 82 del GDPR[151]. In base a tali ultime disposizioni, le tutele di *private enforcement*, ivi incluse l'inibitoria e il risarcimento del danno (patrimoniale e non, ad esempio sotto forma di stress emotivo[152]), possono essere azionate dai soggetti interessati e, altresì, dalle associazioni rappresentative, indipendentemente dalla dimostrazione della violazione dei diritti di specifici interessati[153].

Analogamente, la direttiva (UE) 2020/1828, contempla gli interessi collettivi dei consumatori (intesi come interessi generali dei consumatori e/o come interessi di un gruppo di consumatori)[154] , lesi da violazioni delle disposizioni del GDPR (oltre che del Regolamento su IA). In tal modo, essa vincola gli stati membri a riconoscere ai suddetti interessi una tutela effettiva, anche attraverso l'alleggerimento dell'onere di dimostrare un danno derivante da tali violazioni (cfr. articolo 18 della direttiva (UE) 2020/1828)[155] .

---

[151] E. PALMERINI, *AI systems and liability in the European and national regulatory strategies*, in *Tort Liability and Autonomous Systems Accidents, in Common and Civil Law Perspectives*, *a cura di* Phillip Morgan, Cheltenham, 2023, 63 ss., 91-92.

[152] Si veda la sentenza della Corte di giustizia dell'Unione europea (Terza Sezione) del 25 gennaio 2024, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, EU:C:2024:72: "…the wording of Article 82(1) of the GDPR, read in the light of recitals 85 and 146 of that regulation, which encourage the acceptance of a broad interpretation of the concept of 'non-material damage' within the meaning of that first provision, but also the objective of ensuring a high level of protection of natural persons with regard to the processing of their personal data, … that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage', within the meaning of Article 82(1) (see, to that effect, judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, paragraphs 79 to 86)".

[153] Cfr. Meta Platforms Ireland Limited contro Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV., sentenza della Corte (Terza Sezione) del 28 aprile 2022 (causa C-319/20), secondo cui un trattamento di dati non conforme all'articolo 5 GDPR comporta un rischio di danno per il diritto alla protezione dei dati personali e la possibilità di accedere alle azioni collettive ex art. 80 GDPR. L'assunto alla base di questa decisione è che le disposizioni che concernono la protezione e la circolazione di dati personali riguardano sia la sfera pubblica che quella privata e che la loro violazione incide su interessi sia collettivi che individuali. Si veda anche G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. Dir*., 2019, 236 ss.; F. CASAROSA, *La tutela aggregata dei dati personali nel Regolamento 2016/679: una base per l'introduzione di rimedi collettivi?*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di A. Mantelero. D. Poletti, Pisa, 2018, 237 ss.; A. MANTELERO, From group privacy to collective privacy: towards a new dimension of privacy and data protection in the era of big data, in *Group privacy. New challenges of data technologies*, a cura di L. Floridi, L. Taylor, B. van der Sloot, Dordrecht, 2017, 179.

[154] Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative per la tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (L 409/1). Si veda M. FEDERICO, *European Collective Redress and Data Protection Challenges and Opportunities*, in *Media Laws*, 2023, 1, nonché A. GIANNOPOULOU, R. DUCATO, C. ANGIOLINI, G. SCHNEIDER, *From data subjects to data suspects: challenging e-proctoring systems as a university practice*, op. cit., 293-294.

[155] Cfr. E. CAMILLERI, *L'azione rappresentativa e il raccordo imperfetto con il diritto privato regolatorio. Le decisioni delle Autorità tra libero apprezzamento e presunzioni*

ISSN 2239-8570

2. Il riconoscimento delle emozioni per fini di pubblicità personalizzata secondo le disposizioni in tema di pratiche commerciali sleali e sui servizi digitali

La direttiva 2005/29/CE in materia di pratiche commerciali sleali[156] intende prevenire la distorsione del processo decisionale – più esattamente, del comportamento economico[157] – di un consumatore medio[158], anche tenendo conto della esistenza di categorie di consumatori vulnerabili (cfr. Considerando 18 e art. 20 cod. cons.). Sulla scorta di tale *ratio legis*, le Linee Guida della Commissione Europea sull'interpretazione e l'applicazione della direttiva 2005/29/CE (di seguito 'Linee Guida della Commissione Europea'[159]) hanno preso in esame le pratiche di personalizzazione della comunicazione commerciale nelle interazioni tra professionisti e consumatori, giungendo alla conclusione che simili pratiche sono sleali e dunque vietate quando comportino uno sfruttamento dello stato di vulnerabilità dei consumatori[160], falsandone o essendo idonee a falsarne il

giurisprudenziali: spunti dall'arrêt Repsol, in *Nuove leggi civili commentate*, 2024, 2, 437 ss., 457.

[156] Cfr., senza pretesa di completezza, G. DE CRISTOFARO, *Le pratiche commerciali scorrette nei rapporti fra professionisti e consumatori*, in *Nuove leggi civ. comm.*, 2008, pp. 1102-1103, nonché M. LIBERTINI, *Clausola generale e disposizioni particolari nella disciplina delle pratiche commerciali scorrette*, in *Contr. impr.*, 2009, 112 ss., nonché M. NUZZO, *Pratiche commerciali sleali ed effetti sul contratto: nullità di protezione o annullabilità per vizi del consenso?*, in *Le pratiche commerciali sleali*, a cura di E. Minervini, L. Rossi Carleo, Milano, 2007, 235 e L. ROSSI CARLEO, *Dalla comunicazione commerciale alle pratiche commerciali scorrette*, ivi, 15 ss. Sul rapporto tra regolamentazione in parola e neuroscienze, si veda R. CATERINA, *Psicologia della decisione e tutela del consumatore*, in *Analisi giuridica dell'economia*, 2012, 1, 1 ss., 8, in particolare, sul tema della influenza dispiegata dal professionista sui processi decisionali dei consumatori.
Per una analisi completa della disciplina in oggetto e della sua evoluzione, cfr. L. GUFFANTI PESENTI, *Scorrettezza delle pratiche commerciali e rapporto di consumo*, Napoli, 2020, passim.

[157] Il concetto di comportamento economico deve essere interpretato in senso ampio, in modo da comprendere anche la decisione di entrare in un negozio o di visitare un sito web (cfr. Corte di giustizia europea, Trento Sviluppo srl, Centrale Adriatica Soc. Coop. Arl contro Autorità Garante della Concorrenza e del Mercato, 19 dicembre 2013, causa C-281/12, punti 35, 36 e 38).

[158] A. SACCOMANNI, *Le nozioni di consumatore e di consumatore medio nella direttiva 2005/29/CE* in *Le pratiche commerciali sleali. Direttiva comunitaria e ordinamento italiano*, a cura di E. Minervini e L. Rossi Carleo, Milano, 2007, 141 ss.

[159] Guida all'interpretazione e all'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno (2021/C - 526/01). Si veda M. NARCISO, *The Unfair Commercial Practice Directive - Fit for the Digital Challenges?*, in *EuCML*, 2022, 4, 147 ss.

[160] Si vedano le Linee guida della Commissione europea, paragrafo 4.2.7: "l'ambiente digitale consente ai professionisti di impiegare più efficacemente le loro pratiche sulla base dei dati dei consumatori, con un'elevata scalabilità e persino dinamicamente in tempo reale. I professionisti possono sviluppare pratiche di persuasione personalizzate perché si avvalgono di conoscenze superiori basate su dati aggregati riguardanti il comportamento e le preferenze dei consumatori, per esempio collegando dati provenienti da fonti differenti. I

ISSN 2239-8570

processo decisionale, in contrasto con il requisito della diligenza professionale.

La diligenza professionale ai sensi dell'art. 5 direttiva 2005/29/CE è una clausola generale che riassume i doveri di diligenza di un professionista derivanti da una serie di fattori, quali il tipo di pratica e le tecnologie utilizzate. Pertanto, una pratica commerciale - che non sia né ingannevole (artt. 6 e 7 direttiva 2005/29/CE) né aggressiva (artt. 8 e 9 direttiva 2005/29/CE) o inserita nella c.d. lista nera (art. 5 (5) direttiva 2005/29/CE) - può comunque dirsi scorretta se contrasta con la diligenza professionale[161] .

L'ulteriore requisito che la pratica distorca materialmente (o sia suscettibile di distorcere) il comportamento economico dei consumatori (cfr. art. 6, paragrafo 1, lettera b), e art. 7, paragrafo 4, direttiva 2005/29/CE) deve essere valutato alla luce del parametro di riferimento costituito dal consumatore medio che, tuttavia, non è un paradigma realistico[162], come suggeriscono ricerche nel campo delle neuroscienze e dell'economia comportamentale. Alla luce di ciò, le Linee Guida della Commissione Europea[163] elencano esplicitamente tra le forme di vulnerabilità che si possono incontrare nell'ambiente digitale, oltre a quelle derivanti da fattori quali età, infermità e ingenuità, altre forme 'dinamiche' e 'situazionali', presenti nel contesto delle interazioni tra professionisti e consumatori nei mercati digitali. Queste forme di vulnerabilità derivano da vari fattori che portano i consumatori a essere più inclini a essere influenzati da una determinata pratica.

I professionisti che utilizzano le emozioni come "finestra" per ottenere informazioni sugli stati psicologici e sulla personalità dei consumatori

professionisti hanno anche la possibilità di apportare modifiche per migliorare l'efficacia delle loro pratiche, poiché testano continuamente gli effetti delle loro pratiche sui consumatori e in tal modo ne conoscono meglio il comportamento (per es. tramite test A/B). Inoltre, tali pratiche potrebbero spesso essere utilizzate senza che il consumatore ne sia pienamente a conoscenza. È la presenza di tali fattori e la loro opacità a distinguere tecniche di vendita o pubblicità estremamente persuasive, da un lato, da pratiche commerciali che possono essere manipolatorie e di conseguenza sleali ai sensi del diritto dei consumatori, dall'altro lato. Inoltre, esse potrebbero violare gli obblighi di trasparenza ai sensi del GDPR o della direttiva relativa alla vita privata e alle comunicazioni elettroniche".

[161] Cfr. 2021 Linee guida della Commissione europea, punto 2.7. Si veda anche S. ORLANDO, *The Use of Unfair Contractual Terms as an Unfair Commercial Practice*, in *European Review of Contract La*, 2011, 1, 26 ss., 38; contra P. HACKER, *Manipulation by algorithms. Exploring the triangle of Unfair Commercial Practice, Data Protection, and Privacy Law*, *European Law Journal*, 2021, 1, 20, in https://onlinelibrary.wiley.com/doi/full/10.1111/eulj.12389. Si vedano J. LAUX, S. WACHTER, B. MITTELSTADT, *Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice*, in *Common Market Law Review*, 2021, 58(3), 22 ss., SSRN: https://ssrn.com/abstract=3822962.

[162] Si veda, a tal proposito, N. HELBERGER, F. ZUIDERVEEN BORGESIUS, A. REYNA, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, in *Common Market Law Review*, 2017, 54, 1466 ss., nonché G. HELLERINGER, A.L. SIBONY, *European Consumer Protection Through the Behavioral Lens*, in *Columbia Journal of European Law*, 2017, 607 ss. Si vedano poi le notazioni di F. TRUBIANI, *Le incerte sorti del "consumatore medio" tra condizionamenti cognitivi e nuove aperture della giurisprudenza*, in *Accademia*, 2023, 101 ss., sul dibattito in dottrina e soprattutto nella giurisprudenza recente.

[163] Cfr. Linee guida della Commissione UE 2021, punto 2.6.

ISSN 2239-8570

possono acquisire conoscenze su caratteristiche che rendono i consumatori particolarmente suscettibili agli effetti della pubblicità personalizzata[164]. Adottare tecniche con cui si faccia leva su tali conoscenze per distorcere il processo decisionale dei consumatori non è in linea con lo standard di diligenza professionale[165].

Per giunta, secondo le suddette Linee Guida, le pratiche di personalizzazione, per definizione, individuano un gruppo di persone fisiche o una specifica persona fisica sulla base dei loro stati emotivi o della loro personalità, come identificati e dedotti dall'impiego di ERS. L'effetto distorsivo di simili pratiche sul processo decisionale deve essere, quindi, valutato prendendo in considerazione non il generico consumatore medio, ma il consumatore medio del gruppo preso di mira[166] o addirittura lo specifico individuo a cui è rivolta la pubblicità[167] .

Si consideri altresì che le probabilità di sfruttamento di caratteristiche che rendono i consumatori particolarmente vulnerabili aumentano allorché questi ultimi non siano consapevoli di essere esposti a simili pratiche[168]. Ciò trova conferma in una serie di obblighi specifici di informazione stabiliti di recente da diverse disposizioni del diritto dei consumatori[169].

---

[164] Cfr. A. SACCOMANNI, *Le vendite di beni e servizi – Pratiche commerciali scorrette*, op. cit., 417 ss., secondo cui occorre che il professionista possa prefigurarsi gli effetti della pratica sui consumatori vulnerabili.

[165] P. HACKER, *Manipulation by algorithms. Exploring the triangle of Unfair Commercial Practice, Data Protection, and Privacy Law*, in *European Law Journal*, 2021, 17 ss. Si veda anche J. TRZASKOWSKI, *Behavioural Innovations in Marketing Law*, in *Copenhagen Business School, CBS LAW Research Paper* 2018, 19 ss., 21, in *Research Methods in Consumer Law* a cura di Hans-W Micklitz, Anne-Lise Sibony, Fabrizio Esposito, Elgar, 2018, https://ssrn.com/abstract=3398471.

[166] Cfr. R. CATERINA, *Psicologia della decisione e tutela del consumatore*, op. cit., 17: "diventa importante valorizzare il riferimento, contenuto nella direttiva sulle pratiche commerciali sleali e nell'art. 20 del Codice del Consumo italiano, alla possibilità che la pratica sia rivolta a gruppi particolarmente vulnerabili di consumatori. La segmentazione della clientela è uno degli strumenti fondamentali del marketing; oggi le pratiche commerciali possono essere specificamente mirate agli adolescenti, agli anziani, alle donne in gravidanza, ai consumatori con una alta avversione al rischio, agli one stop shoppers, etc. Nelle sue valutazioni, il diritto deve essere altrettanto duttile: se di fatto una pratica è idonea a trarre in inganno o a condizionare una fascia anche ridotta di consumatori, dovrebbe essere disincentivata, senza parametrare il giudizio alle reazioni di un consumatore ideale o anche solo medio". Si vedano anche ID., *Paternalismo e antipaternalismo nel diritto privato*, in *Riv. dir. civ*., 2005, II, 771 ss.; ID., *Processi cognitivi e regole giuridiche*, in *Sistemi intelligenti*, 2007, III, 381 ss.

[167] Cfr. Linee guida della Commissione UE, par. 4.2.7.: "Ai fini di questa valutazione, il parametro di riferimento di un consumatore medio o vulnerabile può essere modulato sul gruppo target e, se la pratica è altamente personalizzata, anche formulato dal punto di vista di una singola persona che è stata oggetto della specifica personalizzazione". Cfr. anche J. LAUX, S. WACHTER, B. MITTELSTADT, *Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice*, op. cit., 21-26.

[168] Cfr. Linee guida della Commissione, 4.2.7. Riflessioni critiche sul punto si rinvengono in T. KIM, K. BARASZ, L.K. JOHN, *Why am I seeing this ad? the effect of ad transparency on ad effectiveness*, in *J. Consum. Res*., 2018, 45, 906 ss.

[169] M. DUROVIC, J. WATSON, *Nothing to Be Happy about: Consumer Emotions and AI*, in *J Multidisciplinary Scientific Journal* 2021, 4, 784 ss., 791, https://doi.org/10.3390/j4040053:

L'inosservanza di tali obblighi può assumere rilevanza allorché si tratti di valutare se una pratica sia ingannevole ai sensi della direttiva 2005/29/CE[170].

In sintesi, l'analisi svolta tocca anche il tema, di più ampio respiro, del rapporto tra la direttiva 2005/29/CE e la regolamentazione in materia di protezione dei dati. In merito, le indagini compiute dalla dottrina e i provvedimenti delle autorità competenti nei due campi restituiscono il quadro di un ordine giuridico, in cui i diversi livelli normativi interagiscono secondo un rapporto, non di reciproca esclusione, ma anzi di interazione, con l'obiettivo di catturare fenomeni (almeno all'apparenza) 'sfuggenti'. Ad esempio, rispetto a talune pratiche riscontrabili in concreto, l'uno, il diritto dei consumatori, può apparire più 'attrezzato', come avviene nel caso di pratiche di manipolazione[171] (perché distorsive della decisione economica dei consumatori) o di pratiche nelle quali è dubbio se la regolamentazione in materia di dati personali sia applicabile. Viceversa, rispetto agli altri rischi insiti nel riconoscimento automatizzato delle emozioni (quali, ad es., la inaccurata rappresentazione della personalità delle persone fisiche categorizzate in base alle emozioni, il monitoraggio sistematico delle emozioni in forme e modi inattesi per i soggetti che vi siano sottoposti, etc.) istituti e principi desumibili dal GDPR ed il relativo apparato di *enforcement* possono vantare maggiore agio[172].

Infine, non può non farsi riferimento al Regolamento sui servizi digitali, il quale reca tra i propri dichiarati obiettivi la tutela dei diritti fondamentali dei destinatari dei servizi di intermediazione, ivi incluse le piattaforme digitali (cfr. art. 1, paragrafo 1; art. 2 (1); art. 3, lett. (g) e lett. (i) Regolamento sui servizi digitali).

---

quando gli ERS sono incorporati nei prodotti di consumo, si applicano i doveri di trasparenza stabiliti dalle relative legislazioni di tutela dei consumatori.

[170] Cfr. i molteplici doveri di informazione introdotti con riferimento alla ricerca online di prodotti, la cui violazione è rilevante ai fini dell'accertamento della esistenza di una pratica commerciale ingannevole: cfr., a titolo di esempio, l'art. 22, 4 bis, d. lgs. 6 settembre 2005 n. 206 (c.d. Codice del consumo), introdotto dando attuazione all'art. 7 paragrafo 4a, direttiva 2005/29/CE. Per una rassegna completa delle pertinenti disposizioni, si veda K. GRISSE, *Recommender Systems, Manipulation and Private Autonomy: How European Civil Law Regulates and Should Regulate Recommender Systems for the Benefit of Private Autonomy*, cit., 119, nonché M. ĐUROVIĆ, *Adaptation of Consumer Law to the Digital Age: EU Directive 2019/2161 on Modernisation and Better Enforcement of Consumer Law*, in *Anali Pravnog fakulteta u Beogradu*, LXVIII, 2020, II, 62 ss.; G. VERSACI, *Le tutele a favore del consumatore digitale nella "Direttiva Omnibus"*, in Persona e mercato, 2021, 3, 189 ss. Si veda, soprattutto, C. CAMARDI, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Juscivile*, 2021, 4, 902 ss.

[171] Cfr. A. GAMBINO, *IA e pratiche commerciali scorrette*, in *La via europea per l'intelligenza artificiale. Atti Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche* - Venezia, 25-26 novembre 2021, a cura di C. Camardi, Milano, 2022, 381 ss.

[172] J. TRZASKOWSKI, *Manipulation by design*, in *Electronic Markets*, 2024, 34, 14, https://doi.org/10.1007/s12525-024-00699-y: "It remains fair to say that data protection law provides for a much tighter, more coherent and more robust framework to further its aims compared to the field of consumer law. The UCPD shares the principles of empowerment, proportionality and transparency with the GDPR, but the UCPD does not contain similar requirements for legitimacy, accountability and security".

ISSN 2239-8570

Ai fini della presente analisi, sono pertinenti alcune disposizioni contenute in tale Regolamento, relative alla pubblicità online. Tra esse, innanzitutto, vi è l'art. 26 che vieta la pubblicità online basata sulla profilazione effettuata utilizzando (dati particolari e tra l'altro) dati biometrici, quali definiti dall'art. 9(1) GDPR. Pertanto, a differenza del GDPR, il Regolamento sui servizi digitali regola esplicitamente l'uso di dati biometrici allo scopo di valutare e/o prevedere le caratteristiche personali degli individui. Inoltre, questo divieto pare comprendere non solo l'impiego di dati particolari per scopi di pubblicitari mirata, ma anche la creazione di "categorie speciali di profilazione"[173]. Sembrerebbe da ciò potersi argomentare che tale articolo vieta altresì la creazione di classi o gruppi (astratti) di individui sulla base di attributi sensibili per scopi di pubblicità comportamentale[174].

Inoltre, il Regolamento sui servizi digitali stabilisce requisiti di trasparenza in base ai quali è obbligatorio comunicare al destinatario della pubblicità, tra l'altro, "i principali parametri utilizzati per determinare il destinatario a cui viene presentata la pubblicità" (articolo 26, paragrafo 1, lettera d))[175]. Ne deriva che, quando un messaggio pubblicitario viene personalizzato sulla base del rilevamento delle emozioni, questo tipo di parametro deve essere comunicato al destinatario del servizio[176] .

Sia, poi, sufficiente fare cenno agli ulteriori doveri di trasparenza in materia di pubblicità online (art. 39 (2) (e) Regolamento sui servizi digitali [177]) e di valutazione del rischio[178], nonché ai doveri di ricorrere a *auditors*

[173] Infatti, secondo il Considerando 69 Regolamento sui servizi digitali, "... i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione, come definite all'articolo 4, punto 4), del regolamento (UE) 2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, dello stesso regolamento, anche utilizzando categorie di profilazione basate su tali categorie speciali".

[174] Se applicata alla pubblicità personalizzata effettuata da ERS, questa disposizione può portare al divieto di utilizzare i dati biometrici di un individuo per valutare la sua salute mentale, nonché di costruire profili di individui sulla base di caratteristiche protette (ad esempio, 'individui tristi' o 'individui depressi', ecc.). Pertanto, il Regolamento sui servizi digitali sembra aver stabilito un meccanismo di controllo su 'come' vengono profilati i destinatari di un servizio di intermediazione online.

[175] S. TOMMASI, *Verso il Digital Services Act: la Proposta di Regolamento sul "mercato unico dei servizi digitali" del 15.12.2020*, in *Persona e mercato*, 2021, 1, 215 ss.

[176] Cfr. Considerando 68 Regolamento sui servizi digitali: "[...] i destinatari del servizio dovrebbero disporre di informazioni direttamente accessibili dall'interfaccia online in cui viene presentato il messaggio pubblicitario, sui principali parametri utilizzati per determinare che venga loro presentato un determinato messaggio pubblicitario, fornendo spiegazioni significative della logica utilizzata a tal fine, anche quando questa è basata sulla profilazione. Tali spiegazioni dovrebbero includere informazioni sul metodo utilizzato per presentare la pubblicità, ad esempio se si tratta di pubblicità contestuale o di altro tipo, e, se del caso, i principali criteri di profilazione utilizzati [...]".

[177] Si veda l'articolo 39 (2) (e) Regolamento sui servizi digitali: "se la pubblicità fosse destinata a essere presentata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine, compresi, se del caso, i principali parametri utilizzati per escludere uno o più di tali particolari gruppi".

[178] Cfr. l'articolo 34 (2) (a), sull'obbligo di effettuare un'autovalutazione del rischio sistemico, e l'articolo 34, paragrafo 2, lettera b), sulle misure appropriate necessarie per attenuare questo tipo di rischi, il cui elenco deve essere redatto e presentato alle autorità di

indipendenti (art. 37 (1) (a) Regolamento sui servizi digitali), e di concedere l'accesso ai dati necessari per accertare l'adempimento delle disposizioni in materia di identificazione e attenuazione dei rischi sistemici (art. 40 (3) Regolamento sui servizi digitali).

Il complesso delle disposizioni sopra descritte, pur presentando tratti di indubbia novità, si applica solo alle informazioni rese disponibili "da una piattaforma online sulla relativa interfaccia online a fronte di un corrispettivo versato specificamente per la promozione di tali informazioni" (secondo la definizione contenuta nell'articolo 3 (r) Regolamento sui servizi digitali). Ciò implica che la pubblicità personalizzata per gli utenti di piattaforme di social media basata sulla rilevazione e la categorizzazione delle emozioni è destinataria dei divieti e nelle prescrizioni sopra citati. Al contrario, pratiche quali l'acquisizione di immagini facciali di individui in luoghi pubblici per fornire pubblicità mirata basata su profili costruiti a partire da tali dati[179] o la pubblicità personalizzata veicolata da assistenti vocali, non rientrano nell'ambito di applicazione del Regolamento sui servizi digitali.

3. Le disposizioni del Regolamento europeo sull'IA in materia di riconoscimento delle emozioni e di categorizzazione biometrica

Il Regolamento su IA persegue l'obiettivo di promuovere l'adozione di un'intelligenza artificiale 'antropocentrica' e 'affidabile'[180], riducendo i rischi di danni alla salute, ai diritti fondamentali e ad altri valori tutelati dal diritto dell'UE, derivanti dall'immissione sul mercato, dalla messa in servizio e dall'uso di sistemi di intelligenza artificiale (art. 1 Regolamento su IA)[181] .

---

vigilanza Si veda C. CAUFFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, 2021, 12 (4), 758 ss.

[179] Cfr. A. MCSTAY, *Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)*, in *Big Data & Society*, 2016, 3 (2), 1 ss., https://journals.sagepub.com/doi/epub/10.1177/2053951716666868.

[180] N. SMUHA, E. AHMED-RENGERSB, A. HARKENS, W. LI, J. MACLAREN, R. PISTELLI, K. YEUNG, *How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, 5 agosto 2021, 14 ss., ssrn.com/abstract=3899991. Si veda anche Commissione europea, *Commission Report on Safety and Liability implications of AI, the Internet of Things and Robotics*, COM(2020)64, February 19th 2020, ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-aiinternet-things-and-robotics-0_en; nonché High-Level Expert Group on Artificial Intelligence, Ethical Guidelines for Trustworthy AI (Deliverable 1), in https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Si veda altresì G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 2022, 1097 ss.

[181] M. EBERS, V.R.S. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER, B. STEINROTTER, *The European Commission's Proposal for an Artificial Intelligence Act-A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J 2021, 4, 589 ss., https://doi.org/10.3390/j4040043. Cfr., altresì, G. MAZZINI, S. SCALZO, *The Proposal for the Artificial Intelligence Act: considerations around some key concepts*, in *La via europea per l'intelligenza artificiale. Atti Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche*, op. cit., 22-52.

ISSN 2239-8570

Ciò fa, senza introdurre deroghe alla normativa in materia di protezione dei dati personali[182]. Più in particolare, mentre il GDPR regola la raccolta e il trattamento dei dati personali da parte di tali sistemi stabilendo requisiti e obblighi per i responsabili e gli incaricati del trattamento, il Regolamento su IA 'responsabilizza' sia i fornitori[183] (compresi altri partecipanti alle catene di valore dell'IA) che i c.d. 'deployer'[184], secondo una metodologia di regolazione basata sul rischio[185]. Di conseguenza, sono ivi introdotte regole e principi in materia di progettazione, sviluppo e uso di questi sistemi.

Un sistema di riconoscimento delle emozioni è ivi definito come "un sistema di IA avente lo scopo di identificare o dedurre emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici" (art. 3 (39) Regolamento su IA).

Il significato del lemma 'dati biometrici' assume, nell'economia di tale definizione, rilievo primario: si tratta di dati personali[186] risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, come le immagini facciali o i dati dattiloscopici (art. 3 (34) Regolamento su IA).

Si può notare che, mentre nella parte iniziale della fattispecie si ricalca la nozione di dato biometrico di cui dall'art. 4 (14) GDPR, a differenza che in quest'ultimo, non è richiesto nel Regolamento su IA che i dati siano tali da consentire o confermare l'identificazione univoca di una persona fisica. A questo proposito, il considerando 14 Regolamento su IA, da un lato, afferma che la nozione di dati biometrici "dovrebbe essere interpretata *alla luce della* nozione di dati biometrici quale definita all'articolo 4, paragrafo 14, del regolamento (UE) 2016/679 [...]", dall'altro, chiarisce che i dati biometrici sono utilizzati non solo per l'identificazione biometrica, ma anche per scopi di categorizzazione biometrica e di riconoscimento delle

[182] Si veda il considerando 9 e l'articolo 1 (7) Regolamento su IA, secondo cui qualsiasi trattamento di dati personali rimane soggetto alla legislazione dell'UE in materia di dati personali, *privacy* e riservatezza delle comunicazioni. Cfr. A. MANTELERO, *Beyond Data Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022, 165-173, doi.org/10.1007/978-94-6265-531-7.

[183] Cfr. l'art. 3 (3) Regolamento su IA: «fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito.

[184] Cfr. l'art. 3 (4) Regolamento su IA: "«deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

[185] T. MAHLER, *Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal*, in *Nordic Yearbook of Law and Informatics*, 2021.

[186] Il Regolamento su IA fa riferimento al GDPR per la definizione di dati personali (articolo 3 (50), Regolamento su IA) e di categorie particolari di dati personali (articolo 3 (37) Regolamento su IA). Ciò implica che l'analisi teorica e la giurisprudenza derivante dall'applicazione del quadro giuridico sulla protezione dei dati in relazione a queste due ultime definizioni sono rilevanti anche per l'interpretazione del Regolamento su IA (cfr. paragrafi 1.2 e 1.3).

emozioni[187]. Quindi, i dati che rivelano informazioni biometriche su una persona fisica (ad es. una foto che ritrae i tratti del viso di un individuo) non costituiscono dati biometrici ai sensi del Regolamento su IA, a meno che non vengano sottoposti a uno specifico trattamento tecnico (proprio come nel GDPR, e questo può spiegare il riferimento, nel considerando 14, all'interpretazione delle disposizioni sulla protezione dei dati relative ai dati biometrici). Tuttavia, il trattamento tecnico specifico richiesto dal Regolamento su IA non coincide con l'identificazione biometrica, potendo essere di altra natura.

Inoltre, il considerando 18 Regolamento su IA, al fine di stabilire i confini della nozione di emozioni, esclude, da un lato, gli stati fisici (come il dolore o la fatica) e, dall'altro, "la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, *a meno che non siano utilizzati per identificare o inferire emozioni*"[188]. In merito, il suddetto considerando utilizza i seguenti esempi: "espressioni facciali di base quali un aggrottamento delle sopracciglia o un sorriso, gesti quali il movimento di mani, braccia o testa, o caratteristiche della voce di una persona, ad esempio una voce alta o un sussurro". Pertanto, sebbene occorra che gli ERS utilizzino dati personali ai sensi del GDPR, il significato dell'aggettivo 'biometrico' che perimetra la categoria rilevante di dati personali sembra includere la mera rilevazione di bio-caratteristiche c.d. 'soft' (cfr. *retro*, para. 1.2 e 1.3).

La formulazione dell'articolo 3 (39) Regolamento su IA usa l'espressione 'persone fisiche', perendo riferirsi quindi al riconoscimento delle emozioni tanto di gruppi, quanto di individui specifici[189].

Si pensi, per un esempio del primo tipo, ad un ERS che elabora in via aggregata il tono di voce dei clienti di un esercizio commerciale, al fine analizzarne le emozioni e regolare di conseguenza luci e musica dell'ambiente. Il secondo tipo di ERS è invece quello che, sulla base dei movimenti corporei di un determinato individuo, ne indovina le emozioni

[187]Si veda il considerando 14 Regolamento su IA: "I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione di persone fisiche e il riconoscimento di emozioni di persone fisiche".

[188] Considerando 18 Regolamento su IA: "La nozione di "sistema di riconoscimento delle emozioni" di cui al presente regolamento dovrebbe essere definita come un sistema di IA allo scopo di identificare o dedurre emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici. Il concetto si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. [...]. Questo non include anche il semplice rilevamento di espressioni, gesti o movimenti facilmente visibili, *a meno che non siano utilizzati per identificare o dedurre le emozioni*. Tali espressioni possono essere espressioni facciali di base, come un cipiglio o un sorriso, o gesti come il movimento delle mani, delle braccia o della testa, o caratteristiche della voce di una persona, come una voce alzata o un sussurro".

[189] Si veda però European Parliament, Artificial Intelligence Act. 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. Ivi l'articolo 3 (1) (34) definiva: "sistema di riconoscimento delle emozioni": un sistema di intelligenza artificiale allo scopo di identificare o dedurre emozioni, pensieri, stati d'animo o intenzioni di individui o gruppi sulla base dei loro dati biometrici o a base biometrica" (traduzione nostra).

ISSN 2239-8570

per personalizzare la comunicazione commerciale a lui destinata. Nel secondo esempio, si produce un *output* costituito da informazioni su 'una persona', anziché da informazioni su delle 'persone'[190]. Il grado di interferenza con la sfera dei diritti dell'interessato (e dunque di rischio di lesione) è più elevato, specialmente quando le informazioni in tal modo ottenute siano analizzate in combinazione con altri dati relativi alla medesima persona fisica (ad esempio, dati relativi al suo comportamento attuale o passato).

In ordine al trattamento giuridico, l'articolo 50 (3) Regolamento su IA obbliga i *deployer* di ERS, oltre che ad osservare la disciplina in materia di trattamento di dati personali, a "informare le persone fisiche che vi sono esposte in merito al funzionamento del sistema", e ciò al fine di scongiurare che il riconoscimento delle emozioni avvenga all'insaputa delle persone esposte a tali sistemi di IA (ad es., sul presupposto che non ricorra un trattamento di dati personali). La citata disposizione non identifica esplicitamente la portata di tale obbligo. Il considerando 132 del Regolamento, tuttavia, sembra indicare che tali persone debbano ricevere una 'notifica' concernente il fatto che avviene un trattamento dei loro dati biometrici e che tali sistemi di IA possono "identificare o inferire le emozioni o intenzioni di tali persone"; e aggiunge altresì che tali informazioni vanno rese in "formati accessibili per le persone con disabilità"[191]. Lasciando intendere dunque che il tipo di dati e le finalità perseguite vadano resi noti[192].

Inoltre, alla luce della limitata affidabilità nonché della carenza di specificità e 'generalizzabilità' del rilevamento delle emozioni (cfr. considerando 44)[193], il Regolamento su IA, da un lato, vieta l'immissione

[190] Cfr. L. DALLA CORTE, *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law*, in *European Journal of Law and Technology*, 2019, 10, 1 ss., 9.

[191] Considerando 132 Regolamento su IA: "È inoltre opportuno che le persone fisiche ricevano una notifica quando sono esposte a sistemi di IA che, nel trattamento dei loro dati biometrici, possono identificare o inferire le emozioni o intenzioni di tali persone o assegnarle a categorie specifiche. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti personali, l'origine etnica, le preferenze e gli interessi personali. Tali informazioni e notifiche dovrebbero essere fornite in formati accessibili alle persone con disabilità".

[192] Cfr. ANDREAS HAUSELMANN, ALAN M. SEARS, LEX ZARD, EDUARD FOSCH-VILLARONGA, *Eu Law and Emotion Data*, op. cit., 6.

[193] Considerando 44 Regolamento su IA: " Sussistono serie preoccupazioni in merito alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare perché l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona. Tra le principali carenze di tali sistemi figurano la limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità. Pertanto, i sistemi di IA che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate".
Cfr. S. PRETO, *Emotion-reading algorithms cannot predict intentions via facial expressions* in USC News. 2016, https://news.usc.edu/160360/algorithms-emotions-facial-expressions-predict-intentions/. L.FELDMAN BARRETT, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 2019, 1 (20), 46 ss. Si vedano anche L. STARK, J. HOEY, *The Ethics of Emotion in Artificial Intelligence Systems*, in *FAccT '21: 2021 ACM Conference*

sul mercato, la messa in servizio e l'utilizzo di ERS nei luoghi di lavoro e negli istituti di istruzione[194], dall'altro, classifica tali sistemi, indipendentemente dal contesto in cui vengono utilizzati, come sistemi di IA ad alto rischio ai sensi dell'art. 6 (2) e Allegato III (1) (c). · Come noto, l'articolo 6 (2) Regolamento su IA dà vita ad un peculiare regime giuridico, per il quale i fornitori dei sistemi di cui all'Allegato III del Regolamento possono sottrarsi alla rigorosa disciplina dei sistemi di IA ad alto rischio dimostrando che talune condizioni elencate nell'art. 6 (3), sono soddisfatte nel caso concreto. Tuttavia, è altresì previsto che i sistemi di IA elencati nell'allegato III "*sono sempre considerati ad alto rischio*" se effettuano la profilazione di persone fisiche. Come già osservato, il riconoscimento delle emozioni implica una forma di profilazione ed è quindi da ritenersi sempre sottoposto alla regolamentazione dei sistemi ad alto rischio.

Al fine di promuovere l'accuratezza degli output prodotti dagli ERS[195], nonché di prevenire la lesione dei diritti delle persone che vi sono esposte, viene introdotto l'obbligo di istituire un sistema di gestione del rischio, nonché vengono prescritti requisiti relativi a *governance* dei dati, trasparenza e documentazione.

Infatti, il sistema di gestione del rischio mira a: *i)* "identificare e analizzare i rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può comportare per la salute, la sicurezza o i diritti fondamentali..." e *ii)* adottare "misure di gestione del rischio opportune e mirate tese ad affrontare i rischi individuati" (rispettivamente, artt. 9 (2) (a) e b) Regolamento su IA), "attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate (art. 9 (3) Regolamento su IA)".

Invece, gli obblighi di trasparenza e documentazione (cfr. art. 11 e allegato IV Regolamento su IA) hanno come oggetto, tra l'altro, il livello di accuratezza dei sistemi di IA ad alto rischio e la descrizione del sistema di gestione del rischio ai sensi dell'art. 9 del Regolamento. Inoltre: *i)* l'articolo 49 della legge sull'IA stabilisce un obbligo di registrazione che si applica ai fornitori di sistemi di IA elencati nell'allegato III[196] e *ii)* è richiesto il

---

on Fairness, Accountability, and Transparency, 2021, 1 ss., 9, doi:10.1145/3442188.3445939.

[194] Cfr. art. 5 (1) (f), Regolamento su IA, secondo il quale è vietata: "l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza". Si veda anche il considerando 44.

[195] Cfr. ANDREAS HAUSELMANN, ALAN M. SEARS, LEX ZARD, EDUARD FOSCH-VILLARONGA, *Eu Law and Emotion Data*, op. cit., 5, in cui si osserva che, ai sensi dell'art. 5 (1) (d) GDPR, "il principio di accuratezza protegge l'individuo interessato dall'essere trattato in modo irrazionale o ingiusto sulla base di rappresentazioni errate e inaccurate".

[196] Si veda art. 49 (1) Regolamento su AI: "Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, il fornitore o, ove applicabile, il rappresentante autorizzato si registra e registra il suo sistema nella banca dati dell'UE di cui all'articolo 71".

ISSN 2239-8570

coinvolgimento di un organismo notificato nella valutazione di conformità da effettuare prima dell'immissione sul mercato degli ERS[197] .

I requisiti di cui si è detto servono a garantire un efficace *enforcement* pubblico e privato[198], incluso il diritto di presentare un reclamo alle autorità di vigilanza del mercato competenti, spettante a "*qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni" del* Regolamento (cfr. art. 85 Regolamento su IA). Infatti, in vista di tale obiettivo, viene disposto un coordinamento a livello nazionale tra le autorità di vigilanza del mercato designate a norma del Regolamento e "altre autorità o organismi nazionali pertinenti che controllano l'applicazione [..] di altre disposizioni del diritto dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III" (cfr. art. 74 (10) Regolamento su IA). Oltre a tale coordinamento, per quanto riguarda i sistemi ad alto rischio, come gli ERS, inclusi nell'Allegato III, è previsto che tali autorità abbiano accesso alla documentazione tecnica richiesta dal Regolamento su IA (cfr. art. 77 (1)[199]). Tali autorità e organismi comprendono anche le autorità nazionali di protezione dei dati[200].

Si vorrebbe in tal modo perseguire un livello più elevato di trasparenza qualificata[201] e quindi un più efficace controllo, ovviando al noto problema della opacità (anche solo di mero fatto, perché dovuta alla carenza di disposizioni che prevedano un'adeguata supervisione) dei sistemi di IA ad alto rischio.

Infine, alcune pratiche di riconoscimento delle emozioni possono incorrere nei divieti di cui all'art. 5 Regolamento su IA[202], in presenza di date condizioni.

---

[197] Si veda il considerando 125 Regolamento su IA: è "opportuno che la valutazione della conformità di tali sistemi sia generalmente effettuata dal fornitore sotto la propria responsabilità, con la sola eccezione dei sistemi di IA destinati a essere utilizzati per la biometrica".

[198] G. MAZZINI, S. SCALZO, *The Proposal for the Artificial Intelligence Act: considerations around some key concepts*, op. cit., 37: "considering the peculiarities of AI (opacity, complexity, etc.), the AI Act complements data protection legislation with some provisions aimed at ensuring that the rights, obligations and principles of the GDPR can be effectively enforced by the data protection authorities".

[199] Cfr. art. 77 (1) Regolamento su IA: "Le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, in relazione all'uso dei sistemi di IA ad alto rischio di cui all'allegato III hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati".

[200] Cfr. il considerando 157 che cita esplicitamente le autorità di protezione dei dati.

[201] Si veda M. WIERINGA, *What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability*, 20 Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, January 2020, 1 ss., doi.org/10.1145/3351095.3372833. Si veda anche M. MARTINI, *Regulating Artificial Intelligence - How to De-Mystify the Alchemy of Code?*, *Algorithms and Law*, a cura di M. Ebers, S.N. Navarro, 2019, Cambridge, doi.org/10.2139/ssrn.3458261.

[202] S. ORLANDO, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di Artificial Intelligence Act*, in *Persona e mercato*, 2022, 3, 346 ss.

Come già ricordato, il rilevamento delle emozioni può essere strumentale alla categorizzazione, quando costituisca un primo passo per assegnare persone fisiche a categorie predefinite, con l'obiettivo di valutarle e/o prevederne il comportamento. Il Regolamento su IA prende in considerazione i sistemi di categorizzazione biometrica all'art. 3 (40), da intendersi come quei sistemi aventi lo "scopo di assegnare persone fisiche a categorie specifiche sulla base dei loro dati biometrici [...]". Il considerando 16 chiarisce che "Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico". Si tratta di un chiaro riferimento al concetto di inferenze biometriche, quanto mai ampio giacché concerne anche il comportamento o la personalità degli individui (ad es. categorizzare un individuo come pigro o di scarsa intelligenza sulla scorta dell'analisi della sua voce). Gli ERS sono riconducibili a tale definizione, allorché siano progettati per conseguire informazioni attinenti al comportamento e alla personalità di persone fisiche, a partire dal rilevamento delle loro emozioni.

A ben vedere, i sistemi di categorizzazione biometrica sono assoggettati nel contesto del Regolamento su IA ad una disciplina che varia a seconda del grado di rischio, alto o inaccettabile, in essi insito.

Ed infatti, secondo l'art. 6 (2) e allegato III (1) (c) Regolamento su IA, i sistemi di IA progettati per essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili o protetti o in base alla deduzione di tali attributi o caratteristiche[203] costituiscono sistemi di IA ad alto rischio. Come già rammentato, informazioni sensibili relative alle persone fisiche possono essere dedotte anche dall'analisi delle loro emozioni. Ad es., secondo alcune ricerche, l'analisi dell'andatura di una persona può rivelare uno stato di depressione e quindi sfociare nella categorizzazione di quell'individuo come soggetto affetto da malattia mentale[204] .

Invece, l'art. 5 (1) (g), Regolamento su IA vieta *"l'immissione sul mercato, la messa in servizio a questo scopo specifico o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per dedurne o dedurne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale [...]*"[205]. L'uso dell'avverbio 'individualmente' in questa disposizione serve a distinguere tale pratica, che è fatta oggetto di divieto perché implicante un rischio inaccettabile, dalla categorizzazione biometrica basata su informazioni

[203] Il testo dell'Allegato III (1) (2) nella versione in lingua italiana contiene in realtà dei refusi, giacché così recita: "i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche". Cfr., invece, la versione ufficiale in lingua inglese: "AI systems intended to be used for biometric categorisation, according to sensitive *or* protected attributes *or* characteristics based on the inference of those attributes or characteristics".

[204] Cfr. Enisa, *Behavioural Biometrics*, Enisa Briefing 10, 1 ss., 4.

[205] Cfr. considerando 30 Regolamento su IA.

ISSN 2239-8570

sensibili, che invece costituisce semplicemente una pratica ad alto rischio ai sensi dell'art. 6 (2) e dell'Allegato III, la quale – come si ricava adottando l'argomento *a contrario* – include anche la categorizzazione di gruppi di persone fisiche sulla base dei suddetti attributi[206]. Quindi, ad es., ai sensi dell'art. 5 (1) (g), sono vietati sistemi che deducano le opinioni politiche di una specifica persona fisica sulla base dell'analisi delle sue emozioni.

Il riconoscimento delle emozioni può anche rientrare nell'ambito di applicazione dell'art. 5 (1) (a) Regolamento su IA, che vieta l'immissione sul mercato, la messa in servizio o l'impiego di un sistema di IA che utilizzi tecniche subliminali o deliberatamente manipolative o ingannevoli, laddove si verifichino alcune condizioni: *i)* che la pratica abbia l'obiettivo o l'effetto di distorcere significativamente il comportamento di una persona fisica o di un gruppo di persone fisiche, inducendole a prendere una decisione che non avrebbero altrimenti preso; *ii)* che sia stato causato o che sia ragionevolmente probabile un danno significativo a tale persona o a un'altra o a gruppi di persone[207] .

Pertanto, tale divieto entra in gioco quando sussiste (o è probabile che vi sia) un'incidenza significativa sull'autonomia, sul processo decisionale e sulla libera scelta delle persone fisiche[208]. Il requisito del danno, ivi previsto, da un lato, è di ampia interpretazione, in quanto comprende casi in cui viene colpita un'altra persona o un gruppo di persone; per altro verso, esso sembra essere soddisfatto solo quando il danno sia significativo. In merito, il considerando 29 cita, tra i criteri da prendere in considerazione, la probabilità di "*effetti negativi sufficientemente importanti sulla salute fisica, psicologica o sugli interessi finanziari*" delle persone fisiche[209], con il

[206] Si ha quindi che l'art. 5 (1) (g) Regolamento su IA non si applica ai sistemi di IA che elaborano dati biometrici allo scopo di categorizzare gruppi di persone fisiche (ad esempio, per ottenere informazioni sul numero di individui di una certa razza o orientamento sessuale all'interno di una moltitudine di persone fisiche), presupponendo invece che essi siano volti a categorizzare uno specifico individui. Inoltre, l'elenco delle caratteristiche deducibili da tali sistemi sembrerebbe costituire un numero chiuso, al contrario di quanto avviene nel III (1) (c) Regolamento su IA.

[207] Cfr. art. 5 (1) (a) Regolamento su IA: "l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo". Si veda M. LEISER, *Psychological Patterns and Article 5 of the AI Act AI-Powered Deceptive Design in the System Architecture and the User Interface*, in *Journal of AI Law and Regulation*, 1/2024, pp. 1-19, p. 12.

[208] Si veda il considerando 29, che fa riferimento a tecniche basate su IA usate " per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la libera scelta".

[209] Considerando 29 Regolamento su IA: "L'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA *con l'obiettivo o l'effetto di distorcere materialmente il* comportamento umano, per cui è probabile che si verifichino *danni significativi, in particolare con impatti negativi sufficientemente importanti sulla salute* fisica, *psicologica*

risultato di rendere ardua la dimostrazione che si sia verificato un danno siffatto in un caso specifico[210].

o sugli interessi finanziari, sono particolarmente pericolosi e dovrebbero *pertanto* essere vietati".

[210] S. ORLANDO, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di Artificial Intelligence Act*, op. cit., 354. Si veda il parere congiunto EDPB-EDPS sulla proposta di legge sull'intelligenza artificiale, 10, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf. Pertanto, questo tipo di danno è interpretato in modo restrittivo, se confrontato con il danno di cui all'art. 82 GDPR, che è interpretato dalla Corte di giustizia europea come comprendente qualsiasi tipo di danno non patrimoniale derivante dall'inosservanza delle disposizioni in materia di protezione dei dati. Cfr., infine, M. FRANKLIN, *Missing Mechanisms of Manipulation in the EU AI Act*, in *The International FLAIRS Conference Proceedings*, 2022, 35 ss.

ISSN 2239-8570