ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

20 NOVEMBRE 2024

Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale

di Francesca Mollo
Ricercatrice di Diritto privato
Alma mater Studiorum - Università di Bologna

Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*

di Francesca Mollo
Ricercatrice di Diritto privato
Alma mater Sudiorum - Università di Bologna

Abstract [It]: Il contributo ricostruisce il tema dell'Intelligenza artificiale, disciplinato oggi dal Regolamento UE 1689/2024, intrecciato con la tutela dei dati personali. Da qui si procede a indagare i profili critici connessi al trattamento di alcune particolari categorie di dati, in particolare i dati biometrici, il cui trattamento – soprattutto sistematico e su larga scala – è idoneo a definire nuovi modelli di sorveglianza e ad incidere sui diritti fondamentali.

Title: The processing of biometric data in the AI Act: intersections between data protection legislation and the new European regulation of artificial intelligence
Abstract [En]: The contribution reconstructs the topic of Artificial Intelligence, now regulated by EU Regulation 1689/2024, intertwined with the protection of personal data. From here we start to investigate the critical profiles connected to the processing of some particular categories of data, in particular biometric data, whose processing - especially systematic and on a large scale - is suitable for defining new surveillance models and impacting fundamental rights.

Parole chiave: intelligenza artificiale, Reg. UE 1689/2024, dati biometrici, categorie particolari di dati
Keywords: Artificial Intelligence, *IA Act*, Reg. UE 1689/2024, biometric data, particular categories of data, data protection

1. Introduzione

Il recente Regolamento UE 2024/1689 del 13 giugno 2024 (*IA Act*) [1] che stabilisce regole armonizzate sull'intelligenza artificiale nasce e si colloca in un quadro quantomai complesso e sfidante.

* Articolo sottoposto a referaggio.

[1] Regolamento UE 1689/2024 del 13 giugno 2024, "PECONS 24/1/24 REV 1, Regolamento del Parlamento europeo e del Consiglio 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", pubblicato in. Gazzetta Ufficiale dell'Unione Europea il 12 luglio 2024. La procedura europea è iniziata con la Proposta di Regolamento del Parlamento Europeo e del Consiglio, che ha stabilito

«In misura crescente conduciamo le nostre vite *onlife*» [2], neologismo coniato per sottolineare la natura ormai ibrida dell'esistenza, che si svolge tra essere connesso e non, in quello spazio denominato infosfera; quasi una società delle mangrovie, dove analogico e digitale si mischiano e si confondono l'uno nell'altro. A ciò si aggiunge che, come è stato efficacemente sottolineato [3], la società odierna è caratterizzata da «poteri nuovi, privati, penetranti, opachi», per cui «il potere è un gioco complesso, a più voci, sempre meno decifrabile, stabile e riconoscibile (...). Numerosi nuovi attori, non solo poteri finanziari ed economici, ma anche tecnologici e padroni dell'intelligenza artificiale, muovendosi disinvoltamente tra politica ed economia, forgiano le nuove fondamenta del nostro mondo». «Ormai la sicurezza è al di sopra delle leggi», si è affermato [4]. L'odierna società dell'informazione si atteggia così sempre più spesso a società della sorveglianza [5] e del controllo, da un lato, e società del rischio [6], che tutto conosce del cittadino, anch'esso globale, immerso nella sua solitudine [7] attraverso la conoscenza e nel trattamento

regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) 2021/0106(COD), 21/4/21, cui sono seguiti l'Orientamento generale del Consiglio dell'Unione Europea, 6/12/22 e poi gli emendamenti del Parlamento Europeo, 14/6/23. Si è raggiunto un accordo su un testo comune il 9 dicembre 2023, approvato poi dal Comitato dei Rappresentanti Permanenti il 2 febbraio 2024 e definitivamente dal Parlamento europeo il 13 marzo 2024. Il Regolamento prevede un periodo di adeguamento piuttosto lungo: sarà pienamente applicabile solo a partire da agosto 2026, anche se alcune specifiche disposizioni saranno efficaci già in periodi antecedenti, come quelle sulle "pratiche vietate" e quelle sui sistemi di IA con finalità generali. Tra i primi commenti C. CASONATO – B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal -Rivista di BioDiritto*, 3, 2021; A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO – F. DONATI – A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. I, Il Mulino, Bologna, 2022, p. 168; R. PETRUSO G. SMORTO, *Il regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *Nuova giur. civ. comm.*, 4, 2024, p. 989.

[2] L. FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli, Torino, 2009; ID., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina editore, Milano, 2017, p. 47. Con la quarta rivoluzione (il cui padre è Alan Turing), che segue la prima e nota rivoluzione copernicana, la seconda darwiniana, e la terza freudiana, gli uomini sono «organismi informazionali (*inforg*), reciprocamente connessi e parte di un ambiente informazionale (l'infosfera), che condividiamo con altri agenti informazionali, naturali e artificiali, che processano informazioni in modo logico e autonomo»; nella precedente edizione in lingua inglese *The Fourth Revolution. How the Infosphere Is Reshaping Human, Reality*, Oxford, 2014, p. 219, «*the task is to formulate an ethical framework that can treat the infosphere as a new environment worthy of the moral attention and care of the human inforgs inhabiting it. Such an ethical framework must address and solve the unprecedented challenges arising in the new environment. It must be an environmental ethics for the whole infosphere. This sort of synthetic (both in the sense of holistic or inclusive, and in the sense of artificial) environmentalism will require a change in how we perceive ourselves and our roles with respect to reality, what we consider worth our respect and care, and how we might negotiate a new alliance between the natural and the artificial*»; ID., *Pensare l'infosfera. La filosofia come design concettuale,* Milano, 2020; nonché ID., *Soft Ethics and the Governance of the Digital*, in *Phil. & Tech.*, 2018, 4, 1, *«today, in any mature information society, we no longer live online or offline but onlife, that is, we increasingly live in that special space, or infosphere, that is seamlessly analogue and digital, offline and online*».

[3] M. R. FERRARESE, *Poteri nuovi. Privati, penetranti, opachi*, Il Mulino, Bologna, 2022.

[4] M. FOUCAULT, *Ormai la sicurezza al di sopra delle leggi*, in ID., *La strategia dell'accerchiamento. Conversazioni interventi 1975-1984*, a cura di S. VACCARO, Palermo, 2009, p. 63. Cfr. anche D. LYON, *La cultura della sorveglianza*, trad. it. di C. Veltri, Luiss University Press, Roma, 2020.

[5] Cfr. S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 2004, p. 174 s.

[6] U. BECK, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2004, p. 63 ss.

[7] Z. BAUMAN, *La solitudine del cittadino globale*, Feltrinelli, Milano, 2003, p. 24. Cfr. anche R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003, p. 13.; nonché M. FOUCAULT, *Sécurité, territoire, population*, Paris, 2004: ID., *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1976. Cfr., altresì, S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici,* in *Quale libertà. Dizionario minimo contro i falsi liberali*, a cura di BOVERO, Laterza, Roma-Bari, 2004, p. 54.

massivo dei dati che caratterizza il nostro tempo, incardinato su una struttura circolare del trasferimento di informazioni e sul principio «*make data by data*», che pone sempre più le basi per una vera e propria «sorveglianza liquida» [8], orientata sempre più in senso predittivo [9]. In questa «società dell'accesso» [10] la persona è sempre più digitalizzata, profilata e trasparente; delineandosi così una società dell'integrale trasparenza che rievoca la metafora dell'«uomo di vetro» [11], e che legittima la pretesa di altri di richiedere e ottenere ogni informazione e che implica la classificazione (*id est*, la divisione in classi) come «sospetto, cattivo cittadino, nemico dello Stato» di chiunque rivendichi di mantenere spazi di intimità [12]. In effetti, il binomio accesso-segretezza è strettamente correlato con il potere [13] ed il suo esercizio, laddove «i nuovi poteri sono quelli che riducono la persona a oggetto».[14].

Le interferenze tra l'evolversi incessante della tecnologia e la *privacy* sono ineludibili: il valore attribuito delle informazioni cresce esponenzialmente per i grandi attori economici e politici a livello globale [15] che di tale tecnologia dispongono, mentre pare pericolosamente decrescere in misura pressoché proporzionale per i titolari di dette informazioni [16], che sembrano non avvedersi adeguatamente del fatto che «nella società digitale noi siamo i nostri dati» [17], che nella c.d. «dittatura dell'algoritmo» [18], costituiscono una traccia della persona, frammenti della stessa che ne rivelano caratteristiche e peculiarità, anche attinenti alla vita privata. Già nella Comunicazione del 2018 "L'intelligenza artificiale per l'Europa" [19], la Commissione aveva sottolineato come la «strada da seguire» per «incrementare la capacità industriale e

[8] Z. BAUMAN, D. LYON, *La sorveglianza nella modernità liquida*, Laterza, Roma-Bari, 2015.
[9] Cfr. Garante per la protezione dei dati personali, provvedimento del 24 novembre 2016 n. 488, doc. web n. 5796783, che ha bloccato un progetto di banca dati privata per la misura del «rating reputazionale».
[10] J. RIFKIN, *L'era dell'accesso*, Milano, 2001, p. 17.
[11] Per un'analisi della figura dell'«uomo di vetro» in relazione ai totalitarismi e al rispetto della vita privata si veda S. NIGER, *Le nuove dimensioni della privacy*, Cedam, Padova, 2006, p. 33.
[12] S. RODOTÀ, *Tecnopolitica*, cit., 175. Nello stesso senso, ID., *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006, p. 104.
[13] Cfr. N. BOBBIO, *Il futuro della democrazia*, Einaudi, Torino, 1995, p. 215 ss.
[14] S. RODOTÀ, *Il mondo nella rete, Quali i diritti, quali i vincoli,* Laterza, Roma-Bari, 2014, p. 27.
[15] JOINSON, MCKENNA E POSTMES (a cura di), *Oxford Handbook of Internet Psychology*, Ulf-Dietrich Reips.
[16] Cfr. R. D'ORAZIO, *Protezione dei dati by default e by design, in La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO e G.M. RICCIO, Cedam-WKI, Milano, 2016, p. 88.
[17] Si vedano, in questo senso, le parole del *Presidente dell'Autorità Garante dell'Autorità per la Protezione dei Dati Personali, Antonello Soro, in occasione della Giornata europea della protezione dei dati del 28 gennaio 2015.*
[18] S. RODOTÀ, *Il mondo della rete*, Laterza, Roma-Bari, 2014, p. 37.
[19] Comunicazione della commissione comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "L'intelligenza artificiale per l'Europa», {SWD(2018) 137 *final*}del 25 aprile 2018, in cui, fra il resto, si legge che« Sono necessari ingenti volumi di dati per sviluppare l'IA. L'apprendimento automatico, un tipo di IA, opera mediante l'individuazione di modelli a partire dai dati disponibili e la successiva applicazione di questa conoscenza ai dati nuovi35. Quanto più è grande il set di dati, tanto più accurata sarà l'individuazione delle relazioni anche impercettibili tra i dati. Quando si tratta di utilizzare l'IA, gli ambienti ad alto contenuto di dati offrono anche le maggiori opportunità, perché i dati sono il mezzo attraverso il quale l'algoritmo apprende e interagisce con il suo ambiente», sottolineando già allora come «Le decisioni politiche pubbliche dovrebbero anche incoraggiare la più ampia disponibilità di dati detenuti a titolo privato, assicurando al contempo il pieno rispetto della legislazione sulla protezione dei dati di carattere personale».

tecnologica dell'UE e l'adozione dell'IA in tutti i settori economici» fosse quella di «mettere a disposizione più dati», assumendo tutte le necessarie iniziative per incrementare lo spazio dei dati europeo.

D'altra parte, come si legge nel recente "Rapporto Draghi" di settembre 2024 [20], «con il mondo che si trova sull'orlo di una rivoluzione AI, l'Europa non può permettersi di rimanere bloccata nelle "tecnologie e industrie di mezzo" del secolo precedente. Dobbiamo sbloccare il nostro potenziale innovativo. Questo sarà fondamentale non solo per essere leader nelle nuove tecnologie, ma anche per integrare l'AI nelle nostre industrie esistenti, in modo che possano rimanere all'avanguardia». Di fronte alle grandi trasformazioni che l'Europa deve gestire, essa in primo luogo «deve porre rimedio al rallentamento della crescita della produttività colmando il divario di innovazione. Questo obiettivo comporterà un'accelerazione significativa dell'innovazione tecnologica e scientifica, il miglioramento del passaggio dall'innovazione alla commercializzazione, l'eliminazione degli ostacoli che impediscono alle imprese innovative di crescere e di attrarre finanziamenti».

Oltre a garantire che la sua politica di coesione rimanga coerente con la spinta verso l'aumento dell'innovazione e il completamento del mercato unico, l'Europa dovrebbe così imparare dagli errori commessi nella fase di "iperglobalizzazione" e prepararsi a un futuro in rapida evoluzione, salvaguardando l'inclusione sociale «la trasformazione può portare alla prosperità per tutti solo se accompagnata da un forte contratto sociale» [21]. Punto nodale della strategia allora è proprio quella di colmare il divario tecnologico, dal momento che «il fattore chiave dell'aumento del divario di produttività tra l'UE e gli Stati Uniti è stata la tecnologia digitale, e attualmente l'Europa sembra destinata a rimanere ancora più indietro» [22].

L'integrazione dell'IA "verticale" nell'industria europea sarà un fattore critico per sbloccare una maggiore produttività: anche se le stime quantitative degli effetti dell'IA sulla produttività aggregata sono ancora incerti, ci sono già segnali evidenti che l'IA rivoluzionerà diversi settori in cui l'Europa è specializzata e sarà fondamentale per la capacità delle aziende dell'UE di rimanere leader nel loro settore. Con importanti ricadute, in particolare, nei settori farmaceutico, automobilistico, trasporto merci e passeggeri, ed energetico. Tutte sfide poste dall'IA e che l'Europa dovrà essere in grado di cogliere.

Si segnala anche che il 5 settembre 2024 la Commissione europea ha firmato la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale [23], il primo accordo internazionale giuridicamente

[20] Report "Il futuro della competitività Europea", settembre 2024.
[21] *Ibid.*, p. 17.
[22] *Ibid.*, p. 21.
[23] *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Vilnius, 5 settembre 2024. La firma è avvenuta in occasione della conferenza informale dei ministri della Giustizia del Consiglio d'Europa a Vilnius, Lituania. Tra le parti negoziali figuravano l'UE, altri Stati membri del Consiglio d'Europa, la Santa Sede, Stati Uniti, Canada, Messico, Giappone, Israele, Australia, Argentina, Perù, Uruguay e Costa Rica. Il contributo di 68 rappresentanti internazionali della società civile, del mondo accademico, dell'industria e di altre organizzazioni

vincolante sull'IA, in linea con il Regolamento (UE) 2024/1689, e che prevede un approccio comune per garantire che i sistemi di IA siano compatibili con i diritti umani, la democrazia e lo Stato di diritto, consentendo al contempo innovazione e fiducia.

Essa include una serie di concetti chiave contenuti nell'*AI Act*, come l'approccio basato sul rischio, la trasparenza lungo la catena del valore dei sistemi di IA e dei contenuti generati dall'IA, gli obblighi di documentazione dettagliata per i sistemi di IA identificati come ad alto rischio e gli obblighi di gestione del rischio con la possibilità di introdurre divieti per i sistemi di IA considerati una chiara minaccia ai diritti fondamentali.

Le disposizioni della Convenzione mirano a garantire che le attività all'interno del ciclo di vita dei sistemi di intelligenza artificiale siano pienamente coerenti con i diritti umani, la democrazia e lo Stato di diritto. Al fine di dare attuazione alle disposizioni della Convenzione.

ciascuna Parte della stessa dovrà adottare o mantenere in vigore le opportune misure legislative, amministrative, che dovranno essere graduate e differenziate in funzione della gravità e della probabilità che si verifichino impatti negativi sui diritti umani, sulla democrazia e sullo Stato di diritto, durante il ciclo di vita dei sistemi di intelligenza artificiale, istituendo altresì la Convenzione un meccanismo di *follow-up* e di cooperazione internazionale.

D'altra parte, come precisato pure nel recente report Europol "*Ai And Policing The Benefits And Challenges Of Artificial Intelligence For Law Enforcement*"[24], l'intelligenza artificiale è destinata a «offrire strumenti senza precedenti per migliorare la capacità di salvaguardare la sicurezza pubblica» anche a livello europeo, «*profoundly reshap[ing] the law enforcement landscape*».

Questo, sinteticamente, il quadro di riferimento in cui si inseriscono queste riflessioni, incentrate sul trattamento di categorie particolari di dati, in specie i dati biometrici, nel nuovo Regolamento europeo in tema di intelligenza artificiale, in quanto suscettibili di presentare criticità sotto il profilo dell'impatto sui diritti fondamentali delle persone cui tali dati si riferiscono.

internazionali ha inoltre garantito un approccio globale e inclusivo. La convenzione del Consiglio d'Europa firmata fa parte dei più ampi sforzi dell'UE in materia di IA a livello internazionale, che comprendono discussioni in sede di G7, OCSE, G20 e Nazioni Unite.

[24] «*Ai And Policing The Benefits And Challenges Of Artificial Intelligence For Law Enforcement. An Observatory Report from the Europol Innovation Lab,* per cui «*Artificial intelligence will profoundly reshape the law enforcement landscape, offering unprecedented tools to enhance our ability to safeguard public safety. Europol is committed to staying at the forefront of these technological advancements. This report from the Innovation Lab not only reflects our dedication to the responsible adoption of AI, but also serves as a guide for the broader European law enforcement community as we navigate this new era of digital policing*».

2. Il Regolamento UE 1689/2024 quale strumento volto a promuovere la diffusione di un'intelligenza artificiale «antropocentrica e affidabile»

In prima battuta, è bene ricordare che il Regolamento in tema di intelligenza artificiale pone tra i propri obiettivi, esplicitati all'art. 1, quello di «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione» [25]. In proposito, si ripropone il bilanciamento tra benessere e mercato, che rievoca quella che è stata definita «doppia anima» [26] già del Regolamento UE 679/2016 in tema di protezione dei dati personali (GDPR), e in cui resta latente la dialettica tra persona e mercato [27], che ha nel tempo segnato il passaggio «dall'Europa dei mercati all'Europa dei diritti» [28], in cui i diritti sono stati via via sempre più «presi sul serio» [29] dalla giurisprudenza, divenuto poi «solido cemento edificato» [30] su cui poggia la stessa Carta dei diritti fondamentali, proprio valorizzando quella centralità della persona, divenuta la cifra del processo di integrazione europea [31].

---

[25] Cfr. anche considerando 1 e considerando 176.

[26] La suggestiva espressione è di N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in *Persona e mercato dei dati*, a cura di N. ZORZI GALGANO, Wolters Kluwer Italia, Milano, 2019, p. 35.

[27] Sul rapporto tra persona e mercato, con particolare riferimento all'ordinamento italiano anche in relazione al processo di integrazione europea, cfr. L. MENGONI, *Persona e iniziativa economica privata nella Costituzione*, in *Persona e mercato. Lezioni*, a cura di Vettori, Padova, 1996, p. 34 ss., che sottolinea in particolare il mutamento di prospettiva a partire dagli anni Ottanta, portando al «riconoscimento del mercato come centrale dell'ordinamento dell'economia e la riqualificazione dell'intervento pubblico diretto principalmente a dettare regole», nonché il riconoscimento al mercato stesso del «compito di determinare, sia pure con margini di flessibilità, i limiti di compatibilità economica entro i quali l'azione politica deve contenere, selezionandoli, il soddisfacimento dei bisogni e delle domande espresse dalla società civile», richiamato anche da G. VETTORI, *Diritti fondamentali e diritti sociali. Una riflessione fra due crisi*, in *Contratto e impresa*, 4-5, 2011, p. 906. Si veda altresì N. LIPARI, *Persona e mercato*, in *Riv. trim. dir. e proc. civ.*, 2010, p. 766, secondo cui la sensibilità dei giuristi ha a lungo collocato il terreno dei diritti fondamentali e quello dello scambio mercantile su piani del tutto paralleli. Più in generale, sempre attuale N. IRTI, *L'ordine giuridico del mercato*, Bari 1998, p. 67,

[28] Sul punto, si veda G. ALPA e M. ANDENAS, *L'Europa dei diritti e i diritti fondamentali*, in G. ALPA E M. ANDENAS, *Fondamenti del diritto privato europeo*, Milano, 2005, p. 53 ss. Proprio grazie all'attività svolta dalla Corte di Giustizia in materia si è quindi progressivamente passati da concezioni comunitarie che privilegiavano i valori mercantili, legati in sostanza alla creazione del mercato unico, a una concezione comunitaria che privilegia i diritti della persona, tanto da far osservare quel passaggio «dall'Europa dei mercati all'Europa dei diritti». Per questa via, i diritti fondamentali hanno fatto breccia nell'ordinamento dell'Unione, di modo che, «come per la circolazione dei cittadini europei, anche per i diritti individuali le frontiere nazionali sono state gradualmente smantellate». Cfr. M. CARTABIA, *I diritti fondamentali in Europa dopo Lisbona: verso nuovi equilibri*, in *Il trattato di Lisbona, 13 dicembre 2007, ratificato con legge 2 agosto 2008 numero 130*, in *Giorn. dir. amm.*, 2010, p. 21.

[29] Il riferimento è al volume di R. DWORKIN*, I diritti presi sul serio*, Bologna, 2010.

[30] R. COSIO e R. FOGLIA (a cura di) *Il diritto europeo nel dialogo delle Corti*, Giuffrè, Milano, 2013, p. 116.

[31] Cfr. J. RIFKIN, *Il sogno europeo. Come l'Europa ha creato una nuova visione del futuro che sta lentamente eclissando il sogno americano*, Milano, 2004, p. 283, in cui si legge che «il nuovo sogno europeo si compone di una miscela composita fatta di diritti umani universali, reti e forme di governo multilivello: i diritti umani sono la norma che governa l'attività del *network*; l'Unione europea, per parte sua, è il meccanismo regolatore, la cui autorità direttiva e legittimità morale rende possibile il dialogo continuo tra le parti, teso a far progredire il sogno di una consapevolezza globale». Andando più indietro nel

Sotto questo profilo, il Regolamento persegue il duplice obiettivo del Libro bianco sull'intelligenza artificiale [32] di promuovere l'adozione dell'IA ed affrontare i rischi associati all'utilizzo di tale tecnologia, allo scopo di sviluppare un ecosistema di fiducia attraverso un quadro giuridico per un'IA affidabile.

Come pure sottolineato dalla Commissione [33], per evitare di «diventare un consumatore di soluzioni (...) sviluppate altrove» e invece «accelerare il processo di sviluppo e immissione sul mercato dei sistemi di IA» (considerando 141), è essenziale che il cambiamento sia accettato dai singoli e dal mondo imprenditoriale, per cui «sia i cittadini sia le imprese» devono poter avere fiducia nella tecnologia con cui interagiscono, disporre di un contesto normativo prevedibile e contare su efficaci misure di salvaguardia che proteggano i loro diritti e le loro libertà fondamentali». Ciò che presuppone che l'IA sia progettata, sviluppata e distribuita in Europa secondo «le proprie modalità e i propri valori», dando luogo ad un'IA «sicura, affidabile ed etica» [34], incentrata sul rispetto dei valori di base dell'Unione e sui diritti fondamentali dei singoli. In tema giova anche richiamare il documento *Orientamenti etici per un'IA affidabile* [35], ivi già definita come «inclusiva» e «antropocentrica», con un approccio poi confermato fin dal considerando 1 del Regolamento (oltre che dall'art. 1 stesso, come detto), diretto a porre le persone al centro dello sviluppo dell'IA, presentato come il grande vantaggio dell'Unione europea rispetto agli altri attori internazionali nella competizione globale. Tale documento già esplicitava i principi sui quali si fonda

tempo, e in generale, si vedano le parole sempre attuali di N. BOBBIO, *L'età dei diritti, introduzione*, Torino, 1990, in cui si legge che «il riconoscimento e la protezione dei diritti dell'uomo stanno alla base delle costituzioni democratiche moderne. La pace è, sua volta, il presupposto necessario per il riconoscimento e l'effettiva protezione dei diritti dell'uomo nei singoli Stati e nel sistema internazionale. Nello stesso tempo il processo di democratizzazione del sistema internazionale, che è la via obbligata per il perseguimento dell'ideale della pace perpetua, nel senso kantiano della parola, non può andare innanzi senza una graduale estensione del riconoscimento e della protezione dei diritti dell'uomo al di sopra dei singoli Stati», per cui «Diritti dell'uomo, democrazia e pace sono tre momenti necessari dello stesso movimento storico». Cfr. L. FERRAJOLI, *L' itinerario di Norberto Bobbio: dalla teoria generale del diritto alla teoria della democrazia*, in *Teoria politica democrazia. Dal passato al futuro*, a cura di BONANATE, Milano, 2011.

[32] Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65), 19 febbraio 2020.

[33] Comunicazione della Commissione «L'intelligenza artificiale per l'Europa», 25.4.2018 COM(2018) 237 final, 15, nonché «Piano coordinato sull'intelligenza artificiale», COM(2018) 795 final, 4.

[34] Considerando 8.

[35] Il documento, pubblicato l'8 aprile 2019, è stato elaborato dal gruppo di esperti di alto livello sull'intelligenza artificiale: un organismo indipendente istituito dalla Commissione europea nel giugno 2018. Esso individua altresì sette requisiti fondamentali che i sistemi di IA devono soddisfare per essere affidabili: 1) intervento e sorveglianza umani, 2) robustezza tecnica e sicurezza, 3) riservatezza e *governance* dei dati, 4) trasparenza, 5) diversità, non discriminazione ed equità, 6) benessere sociale e ambientale e 7) *accountability*. Anche la comunicazione *Creare fiducia nell'intelligenza artificiale antropocentrica indica*, cit., a p. 4 indica tre elementi per ottenere una IA affidabile: rispetto della legge, osservanza dei principi etici, robustezza, e richiama i suddetti requisiti.

un'IA *reliable*: rispetto dell'autonomia umana [36], prevenzione dei danni [37], equità [38], ed esplicabilità [39]. Vengono in rilievo altresì i profili di sicurezza [40], trasparenza correlata all'esplicabilità [41], oltre che di affidabilità nel senso previsto dal sopra richiamato art. 1.

[36] *Ibid.,* p. 13: «gli esseri umani che interagiscono con i sistemi di IA devono poter mantenere la propria piena ed effettiva autodeterminazione e devono poter essere partecipi del processo democratico. I sistemi di IA non devono subordinare, costringere, ingannare, manipolare, condizionare o aggregare in modo ingiustificato gli esseri umani. Al contrario, devono essere progettati per aumentare, integrare e potenziare le abilità cognitive, sociali e culturali umane».

[37] *Ibid.,* p. 14: «i sistemi di IA non devono causare danni né aggravarli e neppure influenzare negativamente gli esseri umani (…). I sistemi di IA e gli ambienti in cui operano devono essere sicuri e protetti. Devono essere tecnicamente robusti e si deve garantire che non siano esposti ad usi malevoli. Le persone vulnerabili dovrebbero ricevere maggiore attenzione ed essere incluse nello sviluppo e nella distribuzione dei sistemi di IA. Occorre prestare particolare attenzione anche alle situazioni in cui i sistemi di IA possono causare o aggravare gli effetti negativi dovuti ad asimmetrie di potere o di informazione, come ad esempio tra datori di lavoro e dipendenti, imprese e consumatori o governi e cittadini. La prevenzione dei danni implica anche il rispetto dell'ambiente naturale e di tutti gli esseri viventi».

[38] *Ibid.*, p. 14: la dimensione sostanziale dell'equità «implica un impegno a garantire una distribuzione giusta ed equa di costi e di benefici e a garantire che gli individui e i gruppi siano liberi da distorsioni inique, discriminazioni e stigmatizzazioni. Riuscendo a evitare distorsioni inique, i sistemi di IA potrebbero persino aumentare l'equità sociale. Occorre inoltre promuovere le pari opportunità in termini di accesso all'istruzione, ai beni, ai servizi e alla tecnologia. L'utilizzo dei sistemi di IA, inoltre, non deve mai ingannare gli utenti (finali) né ostacolarne la libertà di scelta. Inoltre, l'equità implica che gli operatori del settore dell'IA rispettino il principio di proporzionalità tra mezzi e fini, e valutino attentamente come bilanciare interessi e obiettivi concorrenti. La dimensione procedurale dell'equità implica la capacità di impugnare le decisioni elaborate dai sistemi di IA e dagli esseri umani che li gestiscono e la possibilità di presentare un ricorso efficace contro di esse. A tal fine, l'organismo responsabile della decisione deve essere identificabile e i processi decisionali devono essere spiegabili».

[39] *Ibid.*, il quarto principio, p. 14 e 15, «è fondamentale per creare e mantenere la fiducia degli utenti nei sistemi di IA. Tale principio implica che i processi devono essere trasparenti, le capacità e lo scopo dei sistemi di IA devono essere comunicati apertamente e le decisioni, per quanto possibile, devono poter essere spiegate a coloro che ne sono direttamente o indirettamente interessati (…). Non sempre è possibile spiegare, tuttavia, perché un modello ha generato un particolare risultato o decisione (e quale combinazione di fattori di input vi ha contribuito). È il cosiddetto caso della "scatola nera" i cui algoritmi richiedono un'attenzione particolare. In tali circostanze, possono essere necessarie altre misure per garantire l'esplicabilità (ad esempio, la tracciabilità, la verificabilità e la comunicazione trasparente sulle capacità del sistema), posto che il sistema nel suo complesso rispetti i diritti fondamentali. Il grado di esplicabilità necessario dipende in larga misura dal contesto e dalla gravità delle conseguenze nel caso in cui il risultato sia errato o comunque impreciso».

[40] In argomento, M. COSTANZA, *L'Intelligenza Artificiale e gli stilemi della responsabilità civile*, in *Intelligenza Artificiale e diritto*, a cura di E. GABRIELLI e U. RUFFOLO, in *Giur. it.*, 7, 2019, p. 1688, afferma: «alla intelligenza artificiale si demandano prestazioni che la più incerta mano umana non sarebbe in grado d'eseguire con migliore esattezza. La intelligenza artificiale come mezzo correttivo o integrativo delle umane carenze non tollererebbe alcun attributo che la qualifichi come rischiosa; anzi, la intelligenza artificiale sarebbe un ente non pericoloso perché capace di evitare gli inconvenienti che senza il suo intervento possono generarsi con lo svolgimento di certe attività. Le perfezioni che s'attribuiscono all'A.I. stridono con la qualificazione di pericolose. Esiste tuttavia un limite negativo della perfezione: il riconoscimento delle imperfezioni, delle anomalie della realtà, di quelle zone d'ombra che esulano dai paradigmi conosciuti e riconoscibili dalla intelligenza artificiale. (…). Il margine dell'imperscrutabile riporta per certi aspetti alle rischiosità intrinseche alle tecnologie, che pur se sofisticate non sono esenti da falle, che anche se ridotte, non sembrano evitabili neppure attraverso le esperienze che l'A.I. è proiettata a formarsi».

[41] Sul principio di trasparenza, cfr. F. BRAVO, Software *di intelligenza artificiale e istituzione del registro per il deposito del codice sorgente*, in *Contr. e impr.*, 4, 2020, p. 1412, «il principio di trasparenza pervade il nostro ordinamento a tutela di interessi individuali e generali, è baluardo della democrazia così come di insopprimibili esigenze di tutela della persona, nei suoi diritti e nelle sue libertà fondamentali (…), ha un'importanza strategica con riguardo alla tecnologie di intelligenza artificiale, là dove impiegate per assumere decisioni automatizzate capaci di incidere in maniera significativa sulla sfera giuridica degli individui o, comunque, suscettibili di avere effetti di portata fattuale direttamente incidenti sulla persona, che di fronte all'intelligenza artificiale potrebbe incontrare limitazioni o, come già avvenuto nella circolazione in via sperimentale di auto a guida autonoma, danni irreparabili alla salute o ad altri diritti fondamentali».

Sotto il profilo delle ineludibili intersezioni con il tema della protezione dei dati personali, va detto che il Regolamento si colloca si colloca nell'ambito di un preciso quadro normativo europeo, che prende le mosse dalla c.d. Strategia europea sui dati 2030, varata dalla Commissione europea nel 2020 [42] con l'intento di realizzare un unico sistema normativo applicabile in tutta Europa, atto a disciplinare l'economia dei dati, nonché a prevenire rischi e abusi derivanti dalla posizione dominante delle grandi piattaforme online.

Come si evince dalla lettura della relazione introduttiva al Regolamento, l'interesse primario dell'Ue è quello di «tutelare la sovranità digitale dell'Unione e sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale», volendosi l'UE imporre come leader nella regolazione e produzione normativa in tema [43], con l'intento di rendere il modello europeo un riferimento globale atto ad essere adottato implementato in tutto il resto del mondo [44], sulla scorta di quanto già accaduto con la normativa sulla protezione dei dati contenuta nel Regolamento (UE) n. 2016/679 ("GDPR").

Per tracciare un primo quadro, appare interessante soffermarsi un momento su alcuni aspetti definitori di rilievo. La definizione di sistema di IA contenuta all' art. 3 del Regolamento come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali», in linea peraltro con quella proposta in ambito OCSE [45]– appare volutamente generica ed ampia, proprio per risultare quanto più possibile neutrale e così ridurre il pericolo di una rapida obsolescenza della normativa.

Si tenga qui presente la diversa definizione che era contenuta nella Proposta di Reg., COM (2021) 206 final, 21.04.2021, che all'art. 3, par. 1, punto 1) faceva riferimento a «un software sviluppato con una o

[42] Commissione europea, «Una strategia europea per i dati», COM (2020)66, 19 febbraio 2020. Questo obiettivo – ancora oggi al centro dell'impegno delle istituzioni europee – viene perseguito attraverso un pacchetto di norme che regolano il fenomeno del mercato unico dei dati sotto diversi aspetti, tra di loro interconnessi: *Data Governance Act*, volto ad individuare processi e strutture per favorire la disponibilità dei dati (personali e non) tramite il riutilizzo dei dati della PA e la condivisione dei dati tra imprese attraverso gli *European Data Spaces*; *Data Act*, volto ad integrare il Data Governance Act, chiarendo chi e a quali condizioni possa creare valore dai dati; *Digital Services Act*, volto a proteggere lo spazio digitale dalla diffusione di beni, contenuti e servizi illegali e garantire la protezione dei diritti fondamentali degli utenti; *Digital Markets Act*, volto a contrastare gli abusi di mercato delle grandi piattaforme digitali in Europa e finalizzato a limitare gli squilibri economici e le pratiche commerciali sleali dei *Gatekeeper.*

[43] E.C. RAFFIOTTA, *Dalla self-regulation alla over-regulation in ambito digitale: come (e perché) di un necessario cambio di prospettiva,* in *Osservatorio sulle Fonti, 2,* 2023.

[44] G. RESTA, *Cosa c'è di "europeo" nella proposta di regolamento UE sull'intelligenza artificiale?,* in *Il Diritto dell'informazione e dell'informatica,* 2022, 2, p. 328.

[45] *«Machinebased system that can, for a given set of humandefined objectives, make predictions, recommendations or decisions influencing real or virtual environments. It uses machine and/or humanbased inputs to perceive real and/or virtual environments; abstract such perceptions into models (in an automated manner e.g. with ML or manually); and use model inference to formulate options for information or action. AI systems are designed to operate with varying levels of autonomy»,* in OECD 2019.

più delle tecniche e degli approcci elencati nell'allegato 1, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Il considerando n. 12 fornisce alcune indicazioni sul punto, precisando, fra il resto, che «Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati». E ancora, le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione. Il termine «automatizzato» si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine. La definizione di sistemi di IA è ampia, al fine di fronteggiare i rischi di obsolescenza, oltre che di guadagnare in termini di flessibilità. Allo stesso modo, la nozione di fornitori comprende, siano persone fisiche o giuridiche, coloro che sviluppano o fanno sviluppare un sistema di IA e che lo immettono poi sul mercato o in servizio (art. 3 n. 3), mentre gli utilizzatori sono coloro che utilizzano i sistemi di intelligenza artificiale, inteso ampiamente quale «persona fisica o giuridica, autorità pubblica, agenzia o 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» (art. 3 n. 4).

Un ulteriore aspetto significativo disciplinato dall'*AI Act* riguarda gli obblighi di trasparenza che i fornitori e *deployer* dei sistemi di AI devono garantire, dovendo assicurare che le persone

fisiche che interagiscono con questi sistemi siano pienamente consapevoli di stare interagendo con esso e non con un essere umano [46]. Coloro che producono contenuti audio, immagini, video o di testo devono dichiarare che questi sono stati manipolati artificialmente, specie laddove questo abbia generato un *deep fake*. Ed è proprio correlata soprattutto a questa imperativa necessità di trasparenza l'enfatizzazione, all'articolo 56, dell'adozione di codici di buone pratiche per garantire una corretta attuazione del Regolamento. Inoltre, i sistemi ad alto rischio devono sempre essere corredati da informazioni che siano accessibili e chiare, per cui le istruzioni devono includere l'identità e i dati di contatto del fornitore e, se

[46] Tale informazione non è però necessaria laddove i sistemi in questione siano impiegati per accertare, prevenire o perseguire reati.

applicabile, del suo rappresentante autorizzato, nonché le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, compresa la finalità prevista e il livello di accuratezza atteso. Più in generale, il Regolamento si ispira al c.d. *risk-based approach* [47] per classificare i principali sistemi di IA secondo una struttura piramidale a rischio crescente fondata su quattro distinti livelli di rischio determinati dall'uso di un dato sistema: rischio inaccettabile; rischio alto; rischio basso o minimo e rischio specifico per la trasparenza, introducendo restrizioni ed obblighi graduati a seconda del tasso di rischio che una determinata applicazione può presentare. Quindi, l'*IA Act* adotta un approccio fondato sul rischio, come già era avvenuto con il GDPR: mentre là, però, il legislatore europeo aveva scelto il modello dell'*accountability*, qui la classificazione viene effettuata direttamente dal legislatore, che distingue tra rischi di diverso tipo come sopra precisato, in modo però calibrato alla tecnologia di oggi, il che rischia già di prestare il fianco a critiche di rigidità e intrinseca obsolescenza.

In proposito, e con particolare riferimento ai sistemi di IA «ad alto rischio» la «gestione dei rischi» andrebbe realizzata, ai sensi dell'art. 10 *IA Act*, proprio garantendo un'elevata qualità dei dati di addestramento, convalida e prova del sistema di IA, imponendo, a tal fine, l'adozione di pratiche di *governance* e gestione dei set di dati di addestramento, convalida e prova adeguate alla finalità prevista del sistema di IA. Tali pratiche riguardano la progettazione, la raccolta, il trattamento (annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione dei dati), e l' individuazione dei rischi legati a distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, e la predisposizione di misure adeguate al fine di individuare, prevenire e attenuare tali possibili distorsioni. A tal fine i dati sono considerati di elevata qualità dal Regolamento se sufficientemente rappresentativi e, «nella misura del possibile», esenti da errori e completi, tenuto conto della finalità del sistema di IA, delle sue caratteristiche, e dello specifico contesto geografico, comportamentale o funzionale in cui il sistema di IA ad alto rischio è destinato ad essere usato. Proprio per garantire tale qualità dei dati il fornitore deve adottare misure appropriate per il monitoraggio, il rilevamento e la correzione delle distorsioni ed evitare i rischi di discriminazioni, adottando pratiche adeguate già a partire dalla progettazione dei processi di raccolta, trattamento e gestione dei dati. Proprio in quest'ottica sono previste misure aggiuntive per categorie particolari di dati personali ex art. 10 par. 5, come si dirà *infra*, nel paragrafo seguente.

[47] Più in generale, sull'approccio incentrato sulla *risk regulation*, cfr. G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, p. 303; G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel Regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Il Foro it.*, 2024, V, p. 208 ss.; M. U. SCHERER, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in *29 Harv. J.L & Tech.*, 2016, p. 353; J. CHAMBERLAIN, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *European Journal of Risk Regulation,* 1, 2023, p. 8.

3. Il trattamento dei dati biometrici nel Regolamento UE 1689/2024

Sotto il profilo del trattamento dei dati, di cui i sistemi di IA si "nutrono", risultano, quindi, ineludibili le intersezioni con la normativa di protezione dei dati personali, segnatamente i Regolamenti UE 2016/679 (GDPR) e 2018/1725, che costituiscono la base per un trattamento sostenibile e responsabile dei dati, anche nei casi in cui insiemi degli stessi comprendano una combinazione di dati personali e non personali, per cui il regolamento in tema di IA non pregiudica l'applicazione del diritto vigente dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo [48] competenti a monitorare la conformità con tali strumenti *ex* art. 51 GDPR [49].

Nel quadro di tali premesse, un aspetto peculiare e che presenta aspetti di criticità è (e sarà) sicuramente rappresentato dal trattamento delle categorie personali di dati *ex* art. 9 GDPR. Ed in particolare, dei dati biometrici, cui il nuovo regolamento dedica ampio spazio.

Sul punto, va qui subito detto che l'*IA Act* fornisce sì una definizione di dati biometrici all'articolo 3 n. 34 quali «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici», che va interpretata così esplicita già il considerando 14 «alla luce dei dati biometrici di cui all'art. 4 punto 14 GDPR» [50], laddove il n. 37 dello stesso articolo 4, quanto alle categorie particolari di dati, rinvia *tout court* alla nozione contenuta nell'art. 9 GDPR. Lo stesso GDPR all'articolo 4 par. 1 n. 4, definisce i dati biometrici come i «dati personali ottenuti 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».

Essi, nell'impianto sistematico disegnato dal GDPR, rientrano in quella categoria particolare di dati cui il Regolamento pone una specifica attenzione, vietando o limitandone il trattamento, tranne che in alcune particolari situazioni, indicate dall'art. 9 par. 2, solo se tramite il loro trattamento si può giungere all'identificazione univoca o all'autenticazione di una persona fisica [51]. Il GDPR per tali dati, che consentono o confermano l'identificazione univoca dell'individuo, crea cioè una sotto-categoria all'interno della più ampia categoria dei dati particolari disciplinati dall'art. 9, per i quali la liceità del trattamento è ancorata al requisito alternativo del consenso esplicito oppure della necessità, consentendo agli Stati membri di introdurre garanzie supplementari (art. 9, par. 4). Il consenso è quindi alternativo ad altre condizioni – indicate dallo stesso art. 9, tra cui l'ipotesi in cui il trattamento sia necessario per motivi di interesse pubblico o per ragioni correlate alla sanità pubblica, quali la protezione da gravi minacce per

[48] Sulle cui decisioni in tema, cfr. *infra*, par. 6.
[49] Considerando 10.
[50] Oltre che all'art. 3 punto 18 del regolamento UE 2018/172 e dell'articolo 3, punto 13 della direttiva UE 2016/680.
[51] In tema di riconoscimento facciale, cfr. considerando 51 GDPR.

la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi; ovvero il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; o ancora sia necessario in relazione all'esercizio del diritto di difesa o per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e protezione sociale [52].

In ambito nazionale, l'art. 2 *septies* del D.lgs. 101/2018 attua l'art. 9, par. 4 del Regolamento, prevedendo che il trattamento dei dati biometrici, genetici e relativi alla salute sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica, tenendo in particolare considerazione, oltre alle linee guida, raccomandazioni e migliori prassi pubblicate dal Comitato europeo per la protezione dei dati, anche l'evoluzione tecnologica e scientifica del settore a cui tali misure sono rivolte, nonché l'interesse alla libera circolazione dei dati nel territorio europeo [53].

Sempre tra le definizioni dell'*IA Act*, al n. 35 dello stesso articolo 3 è poi contenuta quella di «identificazione biometrica», quale «il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati» [54], con esclusione dei sistemi di IA destinati a essere utilizzati per la verifica biometrica con la sola finalità di confermare l'identità di una persona fisica (autenticazione) [55], nonché di «categorizzazione biometrica» quale sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive (art. 3 n. 40). In punto a quest'ultimo, in particolare, l'art. 5 par. 1 lett. g)

[52] Sebbene non si riscontrino indicazioni in tal senso all'interno del Regolamento l'Autorità garante ha escluso esplicitamente che i dati biometrici possano essere trattati sulla base del legittimo interesse del titolare. Cfr. Garante, provvedimento 22 febbraio 2018, recante "Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679)".

[53] Con specifico riferimento ai dati biometrici, già oggetto di particolare attenzione del Garante per la protezione dei dati personali vigente la normativa precedente (Garante per la protezione dei dati personali, provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 e relativo allegato A recante Linee guida in materia di riconoscimento biometrico e firma grafometrica.), occorre qui sottolineare come siano necessarie misure di garanzia specifiche. *Medio tempore*, l'art. 22 co. 11 del D.lgs. 101/2018 sembra suggerire la possibilità di continuare ad utilizzare i dati biometrici in conformità alle Linee guida sulla biometria adottate nel 2014, adattando la base giuridica a quella indicata dal Regolamento. L'articolo sopra richiamato, infatti, prevede espressamente che per il trattamento dei dati biometrici e genetici, le norme esistenti continuano a trovare applicazione in quanto compatibili, sino all'adozione delle misure di garanzia da parte del Garante. Si tenga altresì presente che, più in generale sul punto, sebbene non si riscontrino indicazioni in tal senso all'interno del Regolamento, l'Autorità italiana ha escluso esplicitamente che i dati biometrici possano essere trattati sulla base del legittimo interesse del titolare. Cfr. Provvedimento 22 febbraio 2018, recante Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679.

[54] Ad esempio, il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti.

[55] Considerando 15.

prevede il divieto di immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale [56].

Infine, fornisce una definizione di «sistema di riconoscimento delle emozioni» quale sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici (art. 3 n. 39) [57]. Sul punto, attese le manifestate preoccupazioni delle Istituzioni europee [58] in relazione alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare sotto il profilo della loro «limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità», si vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in alcuni contesti sensibili, quali situazioni relative al luogo di lavoro e all'istruzione», per i possibili effetti discriminatori o comunque invasivi dei diritti e delle libertà delle persone interessate (art. 5, par. 1, lett. f).

Attenzione particolare viene posta ai sistemi di identificazione biometrica remota, in ragione del loro potenziale significativo impatto sui diritti fondamentali in ragione del dato quantitativo sotto il profilo dell'elevato numero di persone i cui dati biometrici possono essere trattati e, d'altro lato, dell'assenza di un coinvolgimento attivo degli interessati [59]. In particolare, i sistemi di identificazione biometrica remota in spazi accessibili al pubblico [60], in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione (art. 3 n. 42). Questi si rivelano

[56] Precisando che tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto.

[57] La nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento, non comprendendo stati fisici, quali dolore o affaticamento, né la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni. Tali espressioni possono essere 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. Cfr. considerando 18.

[58] Cfr. considerando 44.

[59] Che il criterio selettivo sia proprio l'impatto sui diritti fondamentali delle persone fisiche si ricava anche dal considerando 17, laddove si escludono i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali, adducendo esplicitamente a giustificazione di tale esclusione il fatto che «detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone senza il loro coinvolgimento attivo».

[60] Inteso quale qualsiasi luogo fisico accessibile a un numero indeterminato di persone fisiche e a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata, indipendentemente dall'attività per la quale il luogo può essere utilizzato. Si veda sul punto il considerando 19, con la precisazione, altresì, che «Non sono del pari contemplati gli spazi online, dato che non sono luoghi fisici. L'accessibilità di un determinato spazio al pubblico dovrebbe tuttavia essere determinata caso per caso, tenendo conto delle specificità della singola situazione presa in esame».

particolarmente invasivi dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbero avere ripercussioni sulla vita privata di un'ampia parte della popolazione, inducendo la sensazione di essere costantemente sotto sorveglianza, come a più riprese sottolineato dalla giurisprudenza (si veda *infra*, par. 5), scoraggiando, d'altra parte, in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali, come precisato anche dall'*European Data Protection Board* (come pure si vedrà *infra*, par. successivo).

Non solo, ma le inesattezze di carattere tecnico di tali sistemi potrebbero determinare risultati distorti e comportare effetti discriminatori, particolarmente sotto il profilo dell'età, etnia, razza, sesso o disabilità. D'altra parte, l'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi che operano «in tempo reale» comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone interessate.

Per questo si impone un divieto di utilizzo di tali sistemi salvo ipotesi specifici, «elencate in modo esaustivo e definite rigorosamente» [61], in cui esso è strettamente necessario al fine di perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi. In tali ipotesi, si rende necessario che siano rispettate le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che lo autorizza, in particolare per quanto riguarda le limitazioni temporali [62], geografiche e personali.

A garanzia di un utilizzo «responsabile e proporzionato» di tali sistemi, si prevedono poi alcune specifiche condizioni cui è subordinato l'uso: predisposizione di valutazione d'impatto sui diritti fondamentali ex art. 26 *IA Act* (con le ricadute e gli ineludibili collegamenti con la valutazione d'impatto sulla protezione dei dati di cui all'art. 35 GDPR [63]), autorizzazione esplicita e specifica da parte di autorità giudiziaria o

[61] Considerando 33.

[62] Sul delicato aspetto della durata della conservazione, si veda *infra*, nella giurisprudenza, par. 5.

[63] Nel quadro degli obblighi generali incombenti sul titolare del trattamento *ex* art. 24, e delle misure di sicurezza adottabili *ex* art. 32 del Regolamento – letti in un'ottica di responsabilizzazione (o accountability) dello stesso, oltre che in funzione di protezione dei dati personali – il livello di misure dovrà essere in questi casi molto elevato, trattandosi di trattamento che riguarda dati personali «particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali» (Cfr. considerando 51). Cfr. F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali,* in *Persona e mercato dei dati. Riflessioni sul GDPR,* a cura di N. ZORZI GALGANO, Wolters Kluwer Italia, Milano, 2019, p. 255.
Posto che nell'odierna società dell'informazione basata sui Big Data emerge una sostanziale difficoltà nell'individuare l'*an*, il quando e il *quomodo* (inteso in termini di finalità) dei singoli concreti trattamenti cui i dati vengono sottoposti, il legislatore europeo della privacy mostra ampia consapevolezza delle proporzioni massive assunte negli ultimi decenni dal fenomeno circolatorio dei dati, avendo ben presente che «la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo», e ha reso «disponibili al pubblico su scala mondiale informazioni personali» (Considerando 6), che consentono di effettuare «trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato (…) per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti». (Considerando 91), con particolare riferimento al monitoraggio del comportamento dell'interessato attraverso tecniche di trattamento che ne consentano l'analisi, anche in termini predittivi, sotto il profilo delle preferenze, usi comportamentali o posizioni

amministrativa indipendente, meccanismi di notifica all'autorità di vigilanza, pubblicazione di relazioni annuali sull'uso di tali sistemi, come specificato dall'art. 5 lett. h) [64].

Sul punto, va detto che è lo stesso *IA Act* a precisare come le regole in esso contenuto, fatte salve alcune eccezioni, vietano tale uso, sulla base dell'articolo 16 TFUE, dovendosi applicare come *lex specialis* rispetto alle regole sul trattamento dei dati biometrici di cui all'articolo 10 della direttiva (UE) 2016/680, non essendo esso inteso a fornire la base giuridica per il trattamento dei dati personali a norma dell'articolo 8 della direttiva (UE) 2016/680, e precisando altresì come nell'applicazione dell'art. 9, par. 1 del GDPR, l'uso dell'identificazione biometrica remota a fini diversi dalle attività di contrasto è già stato oggetto di decisioni di divieto da parte delle autorità nazionali per la protezione dei dati (su cui *infra*, par. 6).

Posto che qualsiasi trattamento di dati biometrici interessati dall'uso di sistemi di IA a fini di identificazione biometrica a scopo di contrasto deve essere conforme all'art. 10 della direttiva (UE) 2016/680, che consente tale trattamento solo laddove strettamente necessario, fatte salve le tutele adeguate per i diritti e le libertà dell'interessato, e se autorizzato dal diritto dell'Unione o degli Stati membri, esso deve rispettare i principi di liceità, correttezza e trasparenza, determinazione delle finalità, esattezza e limitazione della conservazione [65].

I sistemi di identificazione biometrica remota a posteriori, invece, in ragione della loro «natura invasiva» [66],devono sempre essere utilizzati in modo proporzionato, legittimo e strettamente necessario e quindi mirato, per quanto riguarda le persone da identificare, il luogo e l'ambito temporale e sulla base di un set di dati chiuso di filmati acquisiti legalmente. In ogni caso, essi «non dovrebbero essere utilizzati nel quadro delle attività di contrasto per condurre una sorveglianza indiscriminata» (il tema della sorveglianza è ricorrente nella giurisprudenza multilivello, come si vedrà *infra*, nel par. 5).

Ciò detto, il Regolamento all'art. 5 elenca, accanto ai sistemi di identificazione biometrica remota in tempo reale di cui si è anzidetto e cui tanto spazio dedica il Regolamento, una serie di partiche di IA vietate.

Tra le pratiche considerate dal Regolamento suscettibili di accrescere il senso di sorveglianza di massa portando «a gravi violazioni dei diritti fondamentali, compreso il diritto alla vita privata» [67] oggetto di

personali (considerando 24 e 71). In tale contesto, assumono centrale rilevanza e maggiore complessità, in particolare, i profili di tutela dei diritti e delle libertà degli interessati sotto il profilo del trattamento di dati su larga scala di categorie di dati personali, tra cui i dati qui in commento. Ad essi si riferisce la previsione che rende obbligatoria la valutazione d'impatto [63] sulla protezione dei dati contenuta nella lett. b) dell'art. 35 del Regolamento, con formulazione peraltro speculare rispetto a quella adottata dalla dir. UE 2016/680, e ulteriormente specificata dal provvedimento adottato dal Garante per la protezione dei dati nell'ottobre 2018. Sulla valutazione di impatto si veda R. TORINO, *La valutazione d'impatto,* in *I dati personali nel diritto europeo,* a cura di V. CUFFARO, R. D'ORAZIO E V. RICCIUTO, Giappichelli, Torino, 2019, p. 855 ss.

[64] Art. 5 lett. h) par. 3-8.

[65] Cfr. articolo 4, paragrafo 1, della direttiva (UE) 2016/680.

[66] Cfr. considerando 95.

[67] Considerando 43.

divieto, rientra, in particolare, l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso (art. 5, par. 1, lett e).

Parimenti, e per lo stesso motivo correlato al grave impatto sui diritti e le libertà fondamentali, sono vietate le pratiche di *scoring* [68] di persone fisiche o gruppi di persone fisiche. Per cui l'art. 5 par. 1 lett. c) vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. Nel quadro degli obblighi di trasparenza previsti dal Regolamento per i sistemi di IA destinati all'interazione con persone fisiche o alla generazione di contenuti, le persone fisiche ricevono 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, inclusi il sesso, l'età, il

[68] Sul punto, cfr. anche Garante per la protezione dei dati personali, provvedimento del 24 novembre 2016 n. 488, [doc. *web* n. 5796783], consultabile al sito istituzionale *www.garanteprivacy.it*, che ha bloccato un progetto di banca dati privata per la misura del «*rating* reputazionale» tramite incrocio di dati immessi volontariamente sulla piattaforma e dati recuperati dalla rete mediante operazioni di *webcrawling*. Elaborato da un'associazione e da una società preposta alla gestione dell'iniziativa, il progetto consisteva in una piattaforma *web* e un archivio informatico che raccoglie grande quantità informazioni personali su diversi tipi di individui (candidati, imprenditori, liberi professionisti ma anche privati cittadini) caricate dagli utenti o provenienti dal *web*. Attraverso un algoritmo, il sistema sarebbe poi in grado di misurare in modo oggettivo l'affidabilità delle persone in campo economico e professionale, attribuendo un punteggio (*rating*) alla loro reputazione online. Il Garante ha rilevato che il sistema comporta rilevanti problematiche per la *privacy* a causa della delicatezza delle informazioni**,** del pervasivo impatto sugli interessati e delle modalità di trattamento. Infatti, il progetto presuppone una raccolta massiva, anche on line, di informazioni suscettibili di incidere significativamente sulla rappresentazione economica e sociale di migliaia di cittadini. Il «*rating* reputazionale» elaborato potrebbe ripercuotersi sulla vita delle persone censite, influenzando le scelte altrui e condizionando l'ammissione degli interessati a prestazioni, servizi o benefici. L'Autorità ha espresso dubbi anche in merito all'asserita oggettività delle valutazioni, sottolineando che la società non è stata in grado di dimostrare l'efficacia dell'algoritmo che regolerebbe la determinazione dei «*rating*» al quale dovrebbe essere rimessa, senza possibilità di contestazione, la valutazione dei soggetti censiti. Vista la difficoltà di misurare situazioni e variabili non facilmente classificabili, la valutazione potrebbe basarsi su documenti e certificati incompleti o viziati, con il rischio di creare profili inesatti e non rispondenti alla identità sociale delle persone censite. Da un punto di vista generale, il Garante ha inoltre manifestato perplessità sull'opportunità di rimettere ad un sistema automatizzato ogni decisione su aspetti così delicati e complessi come quelli connessi alla reputazione. Anche le misure di sicurezza del sistema, basate, prevalentemente, su sistemi di autenticazione «debole» (*user*, *id* e *password*) e su meccanismi di cifratura dei soli dati giudiziari, sono state definite «davvero inadeguate» dall'Autorità. Ulteriori criticità, infine, sono state ravvisate nei tempi di conservazione dei dati e nell'informativa da rendere agli interessati. Il Garante ha pertanto disposto il divieto di qualunque operazione di trattamento presente e futura per il progetto di rating reputazionale.

colore dei capelli, il colore degli occhi, i tatuaggi, i tratti personali, l'origine etnica, le preferenze e gli interessi personali [69].

A monte, il Regolamento classifica come «ad alto rischio», diversi casi di uso critico di sistemi biometrici [70], proprio «perché i dati biometrici costituiscono una categoria particolare di dati personali» [71], nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale. Allo stesso modo, sono così classificati i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti a norma dell'art. 9, par. 1, del GDPR sulla base di dati biometrici, e i sistemi di riconoscimento delle emozioni che non sono vietati a norma del regolamento stesso. Non sono invece considerati ad alto rischio i sistemi biometrici destinati a essere utilizzati al solo scopo di consentire la cibersicurezza e le misure di protezione dei dati personali. D'altra parte, è il Regolamento stesso a prendere in considerazione il rischio che le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possano determinare risultati distorti e comportare effetti discriminatori («particolarmente con riferimento a età, etnia, razza, sesso o disabilità» [72]), derivando la classificazione di tali sistemi come ad alto rischio proprio in considerazione dei rischi che comportano.

Va qui precisato che il fatto che un sistema di IA sia classificato come sistema di IA ad alto rischio a norma del Regolamento non deve essere però interpretato come un'indicazione del fatto che l'utilizzo del sistema sia lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità dei requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale.

Nel Regolamento si precisa, altresì, che esso non dovrebbe essere in alcun modo inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali, salvo quando diversamente disposto in modo specifico dallo stesso [73]. Precisa altresì il Regolamento, infatti, che l'art. 5 par. 1 lett h) («uso di sistemi di identificazione biometrica remota in tempo reale») lascia impregiudicato l'art. 9 del GDPR per quanto riguarda il trattamento dei dati biometrici a fini diversi dall'attività di contrasto.

Quanto poi, in particolare, al trattamento di categorie particolari di dati, atteso che «il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante l'intero ciclo di vita del sistema

[69] Cfr. considerando 132.
[70] Cfr. art. 27.
[71] Considerando 54.
[72] Cfr. Considerando 54.
[73] Considerando 63.

di IA» avuto riguardo anche ai principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione e per impostazione predefinita, esso è previsto solo in casi peculiari. Nello specifico, al fine di proteggere i diritti altrui contro la discriminazione che potrebbe derivare dalla distorsione nei sistemi di IA, i fornitori in via eccezionale e nella misura strettamente necessaria al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche e previa attuazione di tutte le condizioni applicabili previste dalla normativa di protezione dei dati, possono eccezionalmente trattare anche categorie particolari di dati personali, come questione di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lettera g), del Regolamento (UE) 2016/679 e dell'art. 10, par. 2, lettera g), del Regolamento (UE) 2018/1725 [74].

L' *IA Act* prevede poi, all'art. 10 par. 5, che oltre alle condizioni previste dalla normativa in materia di protezione dei dati, siano soddisfatte anche condizioni ulteriori: in primo luogo, il rilevamento e la correzione delle distorsioni non possono essere realizzati efficacemente mediante il trattamento di altri dati, compresi i dati sintetici o anonimizzati; le categorie particolari di dati personali sono soggette a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione; tali categorie sono soggette a misure tese a garantire che i dati personali trattati siano resi sicuri e protetti nonché soggetti a garanzie adeguate, ivi compresi controlli e documentazione rigorosi dell'accesso; le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi e devono essere cancellate dopo che la distorsione è stata corretta oppure i dati personali hanno raggiunto la fine del loro periodo di conservazione, a seconda di quale delle due condizioni si verifica per prima; infine, i registri delle attività di trattamento a norma dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 comprendono i motivi per cui il trattamento delle categorie particolari di dati personali era strettamente necessario per rilevare e correggere distorsioni e i motivi per cui tale obiettivo non poteva essere raggiunto mediante il trattamento di altri dati.

4. La posizione assunta dalle Istituzioni europee in punto al trattamento dei dati biometrici in quanto suscettibili di definire nuovi modelli di sorveglianza

Per inquadrare la questione delle intersezioni tra la nuova disciplina europea dell'IA e il trattamento di categorie particolari di dati, in specie dati biometrici, vanno prese in considerazione le posizioni assunte in tema dalle Istituzioni europee, gli orientamenti della giurisprudenza delle Corti di Lussemburgo e Strasburgo, oltre che delle Autorità di controllo competenti in materia.

[74] Cfr. considerando 70.

La questione, in primo luogo, è stata a più riprese al centro dell'attenzione delle Istituzioni europee, in ragione del potenziale significativo impatto sui diritti fondamentali.

L'*European Data Protection Board*, da ultimo nel 2023 nelle linee guida in tema di uso di tecnologia di riconoscimento facciale [75], atteso che l'applicazione delle normative aventi ad oggetto il trattamento di dati biometrici è suscettibile di per sé di incidere su molti diritti fondamentali, ha fornito una lettura alla luce della Carta dei diritti fondamentali dell'Unione europea. Come efficacemente sottolineato, infatti, l'applicazione delle normative aventi ad oggetto il trattamento di dati biometrici è suscettibile di per sè di incidere su molti diritti fondamentali, per cui la Carta dei diritti fondamentali dell'Unione europea è essenziale per l'interpretazione di dette normative, venendo in rilievo in particolare il diritto alla protezione dei dati di carattere personale di cui all'articolo 8 della Carta di Nizza [76], ma anche il diritto al rispetto della vita privata di cui all'articolo 7 della Carta [77].

[75] Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, adottate il 26 aprile 2023, consultabili sul sito web istituzionale dell'EDPB.

[76] La bibliografia sull'art. 8 CDFUE è quantomai ampia e variegata. Cfr. A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974; DONATI, *sub art. 8. Protezione dei dati di carattere personale*, in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione Europea*, a cura di R. BIFULCO, M. CARTABIA e A. CELOTTO, Bologna, 2001, p. 83 ss.; G. F. FERRARI (a cura di), *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, 2001; V. ZENO ZENCOVICH, *sub art. 8*, in *Commentario alla convenzione europea per la tutela dei diritti dell'uomo e delle libertá fondamentali*, a cura di S. BARTOLE, B. CONFORTI e G. RAIMONDI, Padova, 2001, 307 ss.; A. DI MARTINO, *La protezione dei dati personali: aspetti comparatastici e sviluppo di un modello europeo di tutela*, in *I diritti fondamentali e le corti in Europa*, a cura di S. PANUNZIO, Napoli, 2005, p. 65 ss.; B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *DUE*, 2013, 313 ss.; M. BASSINI, *Il diritto all'oblio ai tempi di Internet: la Corte di giustizia sui motori di ricerca*, in *QC*, 3, 2014, p. 730 ss.; T. E. FROSINI, *Diritto all'oblio e Internet*, in *DPCE*, 2014; p. 1 ss.; O. POLLICINO e M. BASSINI, *The Luxembourg Sense of the Internet: Towards a Right to Digital Privacy*?, *The Global Community Yearbook of International Law and Jurisprudence*, 2014, p. 223 ss.; G. BUTTARELLI, *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche,* in *federalismi.it*, 2015, p. 1 ss.; F. FABBRINI, *Human Rights in the Digital Age. The European Court of justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights J.*, 2015, 28, p. 65; G. RESTA e V. ZENO ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015; G. RESTA e V. ZENO ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali, Roma*, 2016.

[77] La bibliografia sull'art 7 CDFUE è particolarmente ampia. Si vedano, in proposito: GRUPPI, *sub art. 7*, in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione Europea*, a cura di R. BIFULCO, M. CARTABIA e A. CELOTTO, Bologna, 2001, 76 ss.; A. PIZZORUSSO, *Il patrimonio costituzionale europeo*, Bologna, 2002; KILKELLY, *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, *Council of Europe*, 2003; A. PIZZORUSSO, R. ROMBOLI, A. RUGGERI, SAITTA e G. SILVESTRI (a cura di), *Riflessi della Carta europea dei diritti sulla giustizia e la giurisprudenza costituzionale*: *Italia e Spagna a confronto*, Torino, 2003; A. CELOTTO e G. PISTORIO, *L'efficacia giuridica della Carta dei diritti fondamentali dell'Unione europea* (*rassegna giurisprudenziale 2001-2004*), in *GI*, 2004, p. 112 ss.; O. POLLICINO (et. al.), *Discriminazione sulla base del sesso e trattamento preferenziale nel diritto comunitario. Un profilo giurisprudenziale alla ricerca del nucleo duro del new legal order*, Milano, 2005; V. SCIARABBA, *Le "spiegazioni" della Carta dei diritti fondamentali dell 'Unione*, in *DPCE*, 2005, p. 59 ss.; O. DE SCHUTTER, *Commentary on the Charter of Fundamental Rights of the European Union*, in *E.U. Network of Independent Experts on Fundamental Rights/ Le Réseau UE d'Experts independants en matière de droits fondamentaux*, 2006, p. 78 ss.; N. LIPARI, *Riflessioni su famiglia e sistema comunitario*, in *FA*, 2006, 1 ss.; CHOUDHRY e HERRING, *European Human Rights and Family Law*, Oxford, 2010; G. DI FEDERICO (a cura di), *The EU Charter of Fundamental Rights: from declaration to binding instrument*, Dordrecht, 2011; G. MARTINICO, *Chasing the European Court of justice: On Some (Political) Attempts to Hijack the European Integration Process*, *International Community Law Review*, 2012, p. 243 ss.; CHOUDHRY, *sub art. 7 (Family Life)*, in *The EU Charter of Fundamental Rights, a commentary*, edited by Peers, Hervey, Kenner e Ward, Oxford, 2014, p. 183.

Ancora, le misure legislative che fungono da base giuridica per il trattamento dei dati personali interferiscono direttamente con i diritti garantiti dagli articoli 7 e 8 della Carta, e in tutte le circostanze il trattamento dei dati biometrici costituisce di per sé una grave ingerenza, indipendentemente dal risultato, sicché eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà.

Tali dati devono quindi essere trattati in modo da garantire l'applicabilità e l'efficacia delle norme e dei principi di protezione dei dati dell'UE, dovendo la valutazione della necessità e della proporzionalità individuare e considerare tutte le possibili implicazioni per altri diritti fondamentali in base al caso concreto. In particolare, l'*EDPB* sottolinea a più riprese che se i dati vengono trattati sistematicamente all'insaputa degli interessati, è probabile che si generi un senso generale di sorveglianza costante, che può comportare effetti inibitori per quanto concerne alcuni i diritti fondamentali interessati, come la dignità umana *ex* art. 1 della Carta, la libertà di pensiero, di coscienza e di religione *ex* art. 10, la libertà di espressione *ex* art. 11 e la libertà di riunione e di associazione *ex* art. 12 [78].

Il trattamento di categorie particolari di dati, quali ad esempio i dati biometrici, si può considerare «strettamente necessario» solo se l'ingerenza nella protezione dei dati personali e le sue limitazioni non eccedono la misura assolutamente necessaria, ossia indispensabile, escludendo qualsiasi trattamento di carattere generale o sistematico.

Nello specifico, il *Board* prende astrattamente in considerazione una gamma di potenziali utilizzi a seconda del grado di controllo esercitato dalle persone sui propri dati personali, dei mezzi efficaci di cui dispongono per esercitarlo e del loro diritto di iniziativa per attivare e impiegare tale tecnologia, delle conseguenze per loro (in caso di riconoscimento o di mancato riconoscimento) e dell'entità del trattamento effettuato. Perciò, ad esempio, il riconoscimento facciale basato su un modello memorizzato su un dispositivo personale, come una smart card o uno smartphone che appartiene alla persona, utilizzato a fini di autenticazione e per scopi strettamente personali attraverso un'interfaccia dedicata, non comporterebbe gli stessi rischi dell'uso a fini di identificazione in un ambiente non controllato, senza il coinvolgimento attivo degli interessati, in cui il modello di ogni volto che entra nell'area di monitoraggio viene confrontato con i modelli di un'ampia sezione trasversale della popolazione, memorizzati in una banca dati. Ed è tra questi estremi che si colloca una gamma molto variegata di utilizzi e questioni correlate attinenti alla protezione dei dati personali [79].

[78] Secondo l'EDPB dovrebbero poi considerarsi con attenzione anche i potenziali rischi generati dal ricorso alle tecnologie di riconoscimento facciale da parte delle forze dell'ordine per quanto riguarda il diritto a un giudice imparziale e la presunzione di innocenza ai sensi degli articoli 47 e 48 della Carta. Cfr. punto 41 delle linee guida.

[79] Punto 17 delle linee guida.

In particolare, il trattamento tecnico dei dati afferenti al volto di una persona fisica in relazione al tempo e al luogo consente di trarre conclusioni sulla vita privata delle persone interessate, che possono riguardare l'origine razziale o etnica, la salute, la religione, le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali che frequentano.

In tali circostanze, inoltre, non è inconcepibile che la raccolta, l'analisi e l'ulteriore elaborazione dei dati biometrici in questione possano incidere sul modo in cui le persone si sentono libere di agire, anche se il loro agire sarebbe pienamente conforme a una società libera e aperta, con le anzidette gravi ripercussioni sull'esercizio dei loro diritti fondamentali. Ma secondo il *Board*, un trattamento di questo tipo comporta anche altri rischi, come quello di abuso delle informazioni personali raccolte dalle autorità competenti in seguito all'accesso e all'uso illeciti dei dati personali, alla violazione della sicurezza, ecc. I rischi dipendono spesso dal trattamento e dalle circostanze in cui avviene, come ad esempio il rischio di accesso e utilizzo illeciti per mano di agenti di polizia o di altre parti non autorizzate [80].

Posto che, come detto, «in tutte le circostanze il trattamento dei dati biometrici costituisce di per sé una grave ingerenza indipendentemente dal risultato» e anche se il modello biometrico viene immediatamente cancellato dopo il riscontro positivo, viene qui in rilievo il profilo delle limitazioni all'esercizio dei diritti e delle libertà, siccome previsto dall'art. 52 CDFUE [81]. Quanto alla giustificazione dell'ingerenza, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui.

[80] Cfr. punto 35 delle linee guida, dove si precisa anche che «Tuttavia, alcuni rischi sono semplicemente intrinseci alla natura univoca dei dati biometrici; a differenza di un indirizzo o di un numero di telefono, è impossibile che un interessato modifichi le proprie caratteristiche uniche, come il volto o l'iride. In caso di accesso non autorizzato o di pubblicazione accidentale di dati biometrici, il loro utilizzo come password o chiavi crittografiche sarebbe compromesso o i suddetti dati potrebbero essere impiegati per ulteriori attività di sorveglianza non autorizzata a danno dell'interessato».

[81] Sull'art. 52 CDFUE. Cfr. N. LAZZERINI, *Sub. Art 52 CDFUE*, in *Carta dei diritti fondamentali dell'Unione europea*, a cura di R. MASTROIANNI, Milano, 2017; ROPPI, *sub art. 52. Portata dei diritti garantiti*, in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione europea*, a cura di R. BIFULCO, M. CARTABIA e A. CELOTTO, Bologna, 2001, p. 351 ss.; B. CONFORTI, *La Carta dei diritti fondamentali dell'Unione europea e la Convenzione europea dei diritti umani*, in *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, a cura di ROSSI, Milano, 2002, p. 3 ss.; P. MANZINI, *La portata dei diritti garantiti dalla Carta dell'Unione europea, problemi interpretativi posti dall'art. 52*, in *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, a cura di ROSSI, Milano, 2002, 127 ss.; A. RUGGERI, *Il bilanciamento degli interessi nella Carta dei diritti fondamentali dell'Unione europea: osservazioni di diritto comparato a margine dell'art. 52*, Padova, 2004; L. TRUCCO, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Torino, 2013, 128 ss.; F. POCAR, *sub art. 52*, in *Commentario breve ai Trattati dell'Unione europea*, a cura di F. POCAR e BARUFFI, 2ª ed., Padova, 2014, 1792 ss.; V. ZAGREBELSKY, *L'UE e il controllo esterno della protezione dei diritti e delle libertà fondamentali in Europa. La barriera elevata dalla Corte di Giustizia*, in *DUDI*, 2015, 1 ss.

L'articolo 52, paragrafo 1, della Carta stabilisce il requisito di una base giuridica specifica, che deve essere sufficientemente chiara nella sua formulazione per fornire ai cittadini un'indicazione adeguata in merito alle condizioni e alle circostanze in cui le autorità possono ricorrere a qualsiasi misura di raccolta di dati e di sorveglianza segreta. Tale base giuridica deve indicare con ragionevole chiarezza l'ambito e le modalità di esercizio del pertinente potere discrezionale conferito alle autorità pubbliche, in modo da garantire alle persone il livello minimo di tutela previsto dallo Stato di diritto in una società democratica [82]. Inoltre, la liceità richiede garanzie adeguate ad assicurare, in particolare, l'osservanza del diritto spettante ai singoli ai sensi dell'articolo 8 della Carta.

Quanto poi alla verifica della necessità e della proporzionalità, allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore nazionale e dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano il settore interessato, la natura del diritto in questione garantito dalla Carta, la natura e la gravità dell'ingerenza nonché l'obiettivo di quest'ultima [83], dovendo essere idonee a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi. Inoltre, la misura non deve superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi [84]. Secondo la costante giurisprudenza della CGUE, di cui si darà brevemente conto nel prosieguo (si veda *infra*, par. 5), le deroghe e le restrizioni alla tutela dei dati personali devono operare entro i limiti dello stretto necessario [85].

E con riferimento all'utilizzo di database di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di *intelligence*, il Parlamento europeo aveva già a suo tempo espresso «profonda preoccupazione» nella risoluzione del 6 ottobre 2021 [86].

In effetti, e in estrema sintesi, tre erano i punti che emergevano nella stessa: in primo luogo, l'invito alla Commissione ad «interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa indiscriminata nei luoghi pubblici» (punto 31); in secondo luogo il rilievo dei profili di criticità del trattamento di dati genetici e DNA (punto 29); nonché una presa di posizione netta a favore del divieto di qualsiasi sistema di *scoring* su larga scala di cittadini, sulla considerazione che «qualsiasi forma di "*citizen scoring*" normativo sul larga scala da parte delle autorità pubbliche (…) conduce alla perdita di autonomia, indebolisce il principio di non

[82] Corte EDU, n. 20071/07, 17 aprile 2012, *Piechowicz c. Polonia*.
[83] Corte Giustizia UE, C-594/12, punto 47. Cfr., per quanto riguarda l'articolo 8 della CEDU, sentenza Corte EDU, *S. e Marper c. Regno Unito* [GC], nn. 30562/04 e 30566/04, § 102, CEDU 2008-V., su cui *infra* nel testo, par. 5.
[84] CGUE, C-594/12, punto 46; sentenze *Afton Chemical*, C-343/09, EU:C:2010:419, punto 45; *Volker und Markus Schecke e Eifert*, EU:C:2010:662, punto 74; *Nelson e a.*, C-581/10 e C-629/10, EU:C:2012:657, punto 71; *Sky Österreich*, C-283/11 EU:C:2013:28, punto 50; nonché *Schaible*, C-101/12, EU:C:2013:661, punto 29.
[85] Cfr. Corte di Giustizia UE, C-594/12, punto 52; sentenza *IPI*, C-473/12, EU:C:2013:715, punto 39 e giurisprudenza ivi citata.
[86] Risoluzione del parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale il suo utilizzo da parte delle autorità di polizia giudiziaria in ambito penale (2020/2016 (INI).

discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana».

Facendo leva sul principio di finalità, il Parlamento raccomanda un controllo democratico rigoroso e una supervisione indipendente per qualunque tecnologia basata su intelligenza artificiale che venga utilizzata da parte delle autorità di contrasto e giudiziaria, in particolare se destinata alla sorveglianza e alla profilazione di massa; prende atto con grande preoccupazione del potenziale di determinate tecnologie impiegate in tali settori per la sorveglianza di massa e sottolinea altresì «l'esigenza giuridica di prevenire la sorveglianza di massa tramite le tecnologie di IA, che per definizione non corrisponde ai principi di necessità e proporzionalità, e di vietare l'uso delle applicazioni che potrebbero risultare in tale sorveglianza» [87].

Sulla base di queste premesse e preso atto dei diversi tipi di utilizzo di riconoscimento facciale a fini di sorveglianza, il Parlamento chiedeva il «divieto permanente dell'utilizzo dei sistemi di analisi o riconoscimento automatico degli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali»; nonché una moratoria sulla diffusione di sistemi di riconoscimento facciale per le attività di contrasto con funzioni di identificazione, a meno che queste non siano usate strettamente a fini di identificazione delle vittime dei reati, almeno finché le norme tecniche non si potranno considerare »pienamente conformi con i diritti fondamentali» (punti 25, 26 e 27).

Una lettura, quindi, che esprimeva già forte preoccupazione per la deriva che alcuni meccanismi, più o meno velatamente, di sorveglianza di massa, rischiano di prendere nell'odierna società informazionale e digitale.

5. La questione dei rischi correlati al trattamento di categorie particolari di dati nel circuito di dialogo tra Corte di Giustizia e Corte europea dei diritti dell'Uomo

Il tema del controllo dei dati, in special modo categorie particolari di dati, è altresì una preoccupazione da sempre ricorrente nella giurisprudenza, sia della Corte di Lussemburgo, che di Strasburgo.

Nella giurisprudenza della Corte di Strasburgo in tema [88], da leggersi secondo i criteri della *case law* inglese [89], più in generale la protezione dei dati personali riveste un ruolo quasi del tutto strumentale alla tutela

[87] Sottolineando peraltro come l'approccio adottato da alcuni paesi terzi sotto il profilo delle tecnologie di sorveglianza di massa, interferendo in modo sproporzionato con i diritti fondamentali, non possa essere seguito dall'Unione Europea. (punto7).

[88] In tema si veda BLASI, *La protezione dei dati personali nella giurisprudenza della Corte Europea dei diritti dell'uomo*, in *Riv. intern. dir. uomo*, 1992, p. 543.

[89] Cfr. ZAGREBELSKY, *La giurisprudenza casistica della Corte europea dei diritti dell'uomo. Fatto e diritto alla luce dei precedenti*, in *L'essenza della democrazia. I diritti umani e il ruolo dell'avvocatura*, a cura di G. ALPA, Roma, 2010, p. 205 ss.

del diritto al rispetto della vita privata [90], giocando un ruolo fondamentale [91] per l'esercizio del diritto stesso, atteso che, a differenza rispetto alla Carta di Nizza, non esiste nella CEDU un riferimento esplicito alla protezione dei dati personali.

Sul punto, la Corte Europea dei Diritti dell'Uomo ha in più occasioni ribadito che «un'ingerenza [nel diritto al rispetto della vita privata e familiare] può essere giustificata ai sensi dell'articolo 8, paragrafo 2 [della Convenzione europea dei diritti dell'uomo – "CEDU"], solo se essa è conforme alla legge, se persegue uno o più degli obiettivi legittimi a cui si riferisce il paragrafo 2 dell'articolo 8 e se è necessaria in una società democratica per raggiungere tali obiettivi» [92]. Tale ingerenza si verifica anche allorquando siano impiegati dispositivi video in luoghi pubblici che prevedono la registrazione delle immagini [93]. Oltre che contemplata dalla legge, ogni ingerenza da parte delle pubbliche autorità nei diritti fondamentali delle persone, tra i quali il diritto alla protezione della vita privata, deve essere, infatti, prevedibile, nel senso che la legge deve essere sufficientemente chiara nei suoi termini per dare ai singoli un'indicazione adeguata sulle circostanze e le condizioni in cui le autorità sono autorizzate a ricorrere alle misure previste dalla legge [94]. È, peraltro, irrilevante che l'ingerenza riguardi attività o condotte che si svolgono in un luogo pubblico (si ricordi, in proposito, la definizione contenuta nell'*IA Act*, su cui *supra*, par. 3). Come, infatti, anche di recente ribadito dalla Corte Europea dei Diritti dell'Uomo, «il concetto di "vita privata" è un ampio e non suscettibile di una definizione esaustiva [e] non esclude le attività che si svolgono in un contesto pubblico», atteso che «esiste […] una zona di interazione di una persona con gli altri, anche in un contesto pubblico, che può rientrare nell'ambito della "vita privata" [95].

In tema di trattamento di categorie particolari dati, riveste un rilievo significativo nella giurisprudenza della Corte EDU in materia la sentenza *Marper c. Regno* unito del 2008 ed avente ad oggetto la c.d. *privacy* genetica, nella creazione di banche dati genetiche e del DNA a fini di giustizia. La Corte, in questo caso, afferma che la conservazione delle impronte digitali e dei campioni biologici di DNA, a prescindere dall'effettivo utilizzo degli stessi da parte delle autorità, rappresenta un'ingerenza nella vita privata dei soggetti, attesa la sicura qualificazione delle impronte e dei campioni di DNA alla stregua di dati sensibili

[90] Cfr. R. MASTROIANNI (et al), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 137.
[91] Cfr. Corte EDU, sentenza 4 dicembre 2008, *S. e Marper c. Regno Unito*, ric. n. 30562/04 e 30566/04, part. par. 103, in cui «La protezione dei dati personali è di fondamentale importanza ai fini dell'esercizio individuale del diritto al rispetto della vita privata e familiare come consacrato nell'art. 8 della Convenzione». Cfr. anche, nello stesso senso, *Z. c. Finlandia.*
[92] Corte EDU, *Glukhin v. Russia, application no.* 11519/20, 4 luglio 2023, par. 75.
[93] Corte EDU, *Peck v. United Kingdom*, Application no. 44647/9, 28 gennaio 2003, punto 59; v. anche, ancorché in un contesto diverso, *Perry v. United Kingdom*, application no. 63737/00, 17 luglio 2003, punto 38.
[94] Corte EDU, *Copland v. United Kingdom, Application no.* 62617/00", 3 aprile 2007, par. 46.
[95] Corte EDU, *Glukhin v. Russia", cit., par. 64;* v. anche sentenza *Satakunnan Markkinapörssi Oy andSatamedia Oy v. Finland", application no.* 931/13, 27 giugno 2017, parr. 129-131.

nella nozione contenuta dalla Convenzione del 1981 [96]. E proprio su queste premesse la Corte poi sottolinea come la giustificazione prevista dall'art. 8 comma 2 della CEDU debba essere ancorata, per porsi in termini di necessarietà della misura per una società democratica, a regole chiare, dettagliate, oltre che a garanzie minime, che nel caso concreto il Regno Unito non assicurava affatto, dal momento che non venivano previste regole minime e neppure criteri di cancellazione o distruzione dei dati genetici. La Corte, anzi, in uno dei passaggi più interessanti della sentenza [97] che peraltro compie una ricostruzione completa del quadro di riferimento in materia di protezione dei dati personali, facendo ampio richiamo a tutta la normativa di carattere nazionale e comunitario coinvolta si dice addirittura «sorpresa» dal carattere generale e indifferenziato con cui in Inghilterra opera il meccanismo di conservazione di tali dati, laddove invece uno Stato che intendesse porsi in un'ottica pionieristica dal punto di vista dell'evoluzione tecnologica nel campo, dovrebbe prendersi anche in carico la responsabilità di compiere dei bilanciamenti [98], che nel caso concreto non sono stati compiuti affatto, con tutti i conseguenti rischi, anche in termini di stigmatizzazione sociale riconnessi al trattamento dei dati per i soggetti, tra l'altro minori all'epoca dei fatti [99].

L'ottica nella quale si pone la Corte pare la stessa anche quando si tratta di dati relativi allo stato di salute: la Corte nel tempo si è occupata in più casi, soprattutto quanto all'aspetto della divulgazione dei dati.

Nel caso *Z c. Finlandia* del 1997, la divulgazione dell'identità e dei dati attinenti alla sieropositività del soggetto da parte della Corte d'appello di Helsinki nel contesto di un processo per omicidio per contagio da HIV pendente a carico dell'*ex* marito della stessa, costituisce, nel ragionamento della Corte, una violazione dell'art. 8 CEDU, laddove tale violazione non viene riscontrata invece nel sequestro delle cartelle mediche o nell'obbligo di testimoniare imposto ai suoi sanitari nel contesto del medesimo procedimento, a fini di accertamento e perseguimento dei reati. Anche in questo caso, la Corte ribadisce

[96] Sul punto la Corte assimila tali dati alle fotografie e alla registrazione dei campioni vocali. Infatti, essa, al par. 84 della sentenza *Marper*, ritiene che l'approccio adottato relativamente alla questione delle fotografie e dei campioni vocali possa senz'altro ricevere applicazione anche alle impronte digitali e richiama sul punto il già citato caso *Friedl c. Austria* (19 maggio 1994), in cui aveva stabilito che la conservazione di fotografie scattate nel corso di una manifestazione politica non costituisse un'ingerenza nella vita privata, attribuendo un peso particolare al fatto che le fotografie non erano state inserite in alcun sistema di trattamento automatico dei dati e che le autorità non avevano adottato alcuna misura per identificare i soggetti fotografati attraverso il trattamento di detti dati. Invece nel caso *PG e JH c. Regno Unito* n. 44787 del 1998, la Corte aveva affermato che la registrazione dei dati e il carattere permanente o sistematico della registrazione sollevasse una questione relativa al rispetto della vita privata anche nel caso in cui dati fossero di dominio pubblico o disponibili in qualsiasi altra maniera; la Corte ha altresì osservato che la registrazione della voce di un individuo su un supporto fonetico permanente di fatto facilita, se combinato con altri dati personali, l'identificazione dell' individuo, concludendo pertanto che la registrazione delle voci costituisca di per sé un'ingerenza nel diritto al rispetto della vita privata.

[97] Par. 119 della sentenza.

[98] Par. 112 della sentenza.

[99] Medesimi problemi ha poi avuto modo di affrontare, in più occasioni la Corte anche con riferimento alle banche dati dei casellari giudiziari. In tema, si vedano *B.B. c. Francia*, n. 5335/06, 17 dicembre 2009 *M.M. c. Regno Unito*, n. 24029/07, 13 novembre 2012.

il ruolo fondamentale della protezione dei dati rispetto alla tutela della vita privata, già affermato nella sentenza *Marper*, in relazione al diritto alla confidenzialità con riguardo alle informazioni a carattere sanitario, istituendo anche in questa occasione un solido collegamento tra l'art. 8 della Convenzione e gli articoli della Convenzione del 1981 che «*mutatis mutandis*, perseguono i medesimi interessi di tutela» [100].

La sentenza *Marper* risulta richiamata anche dalla Corte di giustizia dell'Unione europea, nel dialogo instaurato tra le Corti nel sistema multilivello di tutela dei diritti, in particolare [101] nella famosa sentenza *Digital Rights Ireland*, su cui *infra.*

Il tema del controllo sui dati rappresenta, più in generale, un tema molto affrontato dalla giurisprudenza di Strasburgo sotto il profilo delle interferenze con il diritto al rispetto della vita privata di cui all'art. 8 CEDU. Si ripropone, quindi, quella preoccupazione che l'utilizzo di particolari categorie di dati «possono condurre ad una sorveglianza indiscriminata», nella formulazione del nuovo Regolamento in tema di intelligenza artificiale, con particolare riferimento ai sistemi di identificazione biometrica remota (su cui *supra*, par. 3).

Così, fin dalla storica sentenza *Leander c. Finlandia* del 1987, in un caso di raccolta e memorizzazione di dati in un registro segreto di polizia, in cui però ancora non si fa alcun riferimento alla protezione dei dati personali, limitandosi la Corte a vagliare se tale memorizzazione costituisca un'ingerenza giustificabile alla luce del comma 2 dell'art. 8, e concludendo per un'assenza di violazione in tal senso. A poco più di un decennio di distanza, invece, nella sentenza *Rotaru c. Romania*, la Corte in un caso analogo di memorizzazione di dati relativi alla affiliazione politica e risalenti alla gioventù del soggetto interessato, con conseguente creazione di un dossier che lo riguardava, muta orientamento, assumendo a referente esterno di valutazione inerente la protezione dati personali (come accadrà poi in altre pronunce successive) la Convenzione del Consiglio d'Europa n. 108 del 1981, sottolineando «la rispondenza di un'interpretazione estensiva della nozione di vita privata e quella elaborata dalla Convenzione del 1981, il cui scopo è garantire il rispetto della vita privata con riferimento ai trattamenti automatizzati» [102].

Proprio valorizzando tale riferimento e il suo collegamento con l'art. 8 CEDU, la Corte afferma che anche dati pubblici possono rientrare nella sfera privata del soggetto se sistematicamente acquisiti, memorizzati e utilizzati dalle pubbliche autorità, per cui è ravvisabile un'ingerenza laddove vi siano tre

[100] La Corte di Strasburgo ha altresì censurato la divulgazione, in un procedimento penale per falso, di dati raccolti in occasione della perquisizione del domicilio professionale dell'imputato, relativi alle cure psichiatriche intraprese da quest'ultimo, nella misura in cui tali informazioni non erano rilevanti per il procedimento in corso. Cfr. Corte Edu 29 giugno 2006 *Panteleyenko c. Ucraina*. In altri casi, invece la Corte ha ritenuto che il diritto alla confidenzialità dei dati fosse comprimibile al fine di salvaguardare altri interessi meritevoli di tutela secondo il par. 2 dell'art. 8 CEDU, come nel caso della comunicazione di dati relativi allo stato di salute di una paziente da una struttura sanitaria all'istituto previdenziale nazionale, giustificata dall'esigenza di tutela del benessere economico del paese (Corte EDU *MS c. Svezia* del 27 agosto 1997).

[101] Par. 47 della sentenza.

[102] Cfr. anche la sentenza della Corte EDU 16 febbraio 2000, n. 27798/95, *Amann c. Svizzera*.

condizioni, consistenti nella memorizzazione dei dati, nel loro utilizzo da parte dell'autorità, nonché nella impossibilità di confutare tali informazioni da parte dell'interessato. Tale ingerenza viene ritenuta non giustificabile dalla Corte alla luce del carattere generalizzato, indistinto e sistematico con cui le autorità trattano i dati *de quibus*, nell'assoluta assenza di criteri oggettivi di selezione e individuazione delle informazioni e dei soggetti, nonché di procedure e di meccanismi di controllo di tali operazioni, tali da implicare concretamente «il rischio di minare, persino distruggere, la democrazia per difenderla», creando di fatto un sistema di sorveglianza su base indiscriminata e generalizzata.

In tema, va registrata, peraltro, una vera e propria inversione di tendenza nell'atteggiamento della stessa corte EDU. Nel 2010, infatti, nel caso *Kennedy c. Regno Unito*, la Corte, pronunciandosi sulla compatibilità con l'art. 8 CEDU di alcuni sistemi di captazione delle informazioni su base generalizzata e sistemica implementati dal Regno Unito, aveva rigettato la questione in assenza di allegazione da parte del ricorrente di una violazione specifica, assumendo e mantenendo quella prospettiva di *individual justice* che da sempre l'aveva contraddistinta. Ma nel 2015, nel caso *Zakharov c. Russia* [103], tale interpretazione subisce una vera e propria battuta d'arresto, nella misura in cui viene riconosciuto, in accordo con le precedenti statuizioni in tema dei giudici di Lussemburgo, che la mancata allegazione di un pregiudizio o una conseguenza ricollegata al sistema di sorveglianza non costituisce un ostacolo per concludere sulla incompatibilità con l'art. 8 CEDU del sistema russo di captazione delle comunicazioni su base generalizzata e non ancorato a criteri oggettivi né a procedure di controllo specifiche.

Impostazione poi mantenuta nelle più recenti sentenze della Corte di Strasburgo in tema. Ci si riferisce qui, anzitutto, alla sentenza del 5 marzo 2020, resa nel caso *ARM / Hambardzumyan* (ric. 43478/11), nonché, più di recente, con sentenza 8 marzo 2021, nel caso *MDA/Bostan* (ric. 52507/09), in relazione ad una perquisizione condotta dalla polizia presso l'abitazione del ricorrente nell'ambito di un procedimento per contravvenzione nei confronti di una terza persona, senza mandato o permesso giudiziario, contrariamente al diritto interno.

E ancora, può farsi richiamo alla celebre sentenza del 25 maggio 2021 resa nel caso *UK./Big Brother Watch and Others* (ric. 58170/13), in tema di intercettazione di massa e ottenimento di dati sulle comunicazioni da fornitori di servizi di comunicazione nel Regno Unito prima del 2018, nonché nel caso *SWE/Centrum for Rättvisa* (ric. 35252/08), con sentenza del 25 maggio 2021, in relazione al presunto rischio che le comunicazioni della fondazione ricorrente venissero intercettate ed esaminate tramite segnali di intelligence, in quanto comunicava quotidianamente con individui, organizzazioni e società in Svezia e all'estero via e-mail, telefono e fax, spesso su questioni delicate, ha rilevato, in particolare, che il regime delle intercettazioni in blocco presentava tre carenze. In primo luogo, l'assenza di una norma chiara sulla

[103] Corte EDU, sentenza del 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 47143/06.

distruzione del materiale intercettato che non conteneva dati personali; l'assenza di un requisito nel *Signals Intelligence Act* o in altra legislazione pertinente che, quando si decide di trasmettere materiale di intelligence a partner stranieri, si tenga conto degli interessi privati delle persone; e l'assenza di un effettivo riesame *ex post*. Di conseguenza, il sistema non soddisfaceva il requisito delle tutele "*end-to-end*", oltrepassava il margine di discrezionalità lasciato allo Stato convenuto al riguardo e, nel complesso, non metteva in guardia dal rischio di arbitrarietà e abusi [104].

Il tema è stato affrontato anche dalla Corte di Giustizia, in particolare, nella prima di quel trittico di sentenze [105] in materia di *privacy* e protezione dei dati personali, assunte tra il 2014 e il 2015, che hanno contribuito all'«emersione, sempre più prepotente, (…), di un vero e proprio digital right to *privacy*» [106], poi confluito nel GDPR.

La Corte si è infatti occupata della circolazione dei dati personali nella «dimensione interna» nel noto caso *Digital Rights Ireland*, con sentenza, resa l'8 aprile 2014 [107], con riferimento al regime di conservazione dei dati previsto dalla dir. 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

Sulla base della constatazione che l'obbligo di conservazione dei dati contenuto nella disciplina è suscettibile di consentire di «trarre conclusioni molto precise riguardo la vita privata delle persone», permettendo, in ultima analisi di tracciare un quadro completo e fedele dell'identità individuale e relazionale della persona, quale essa si esplica nell'ambito della propria vita privata [108], la Corte ravvisa nel sistema approntato dalla direttiva un'ingerenza «di vasta portata e (...) e particolarmente grave» [109] nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, sottolineando come l'obbligo di conservazione dei dati costituisca di per sé un'interferenza nel diritto al rispetto della vita privata, mentre l'accesso costituisca «un'ingerenza supplementare in tale diritto fondamentale», richiamando significativamente sul punto la

[104] Cfr. Report settembre 2022, *Personal data protection, Thematic factsheet, Department for the Execution of Judgments of the European Court.*

[105] Cfr. O. POLLICINO e M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Dir. inform.*, 2015.

[106] O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Dir. inform.*, 2014, p. 7 ss.

[107] Per alcuni commenti, L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. it.*, 8-9, 2014, p. 1850 ss.; F. FABBRINI, *The European Court of justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights J.*, 28, 2015, p. 65.

[108] Analoghe considerazioni si ritrovano anche nella giurisprudenza costituzionale tedesca. Cfr. *BverfG,* 2 marzo 2010, I, Bvr 256/08, 1 BvR 263/08, 1 BvR 586/08., in cui la Corte costituzionale tedesca, nel dichiarare l'incostituzionalità della normativa tedesca di recepimento della Direttiva del 2006 per contrasto con l'art. 10.1 del *Grundgesetz,* ha considerato particolarmente grave l'ingerenza prodotta dalla sorveglianza delle comunicazioni nella vita privata degli utenti intercettate, perché le relazioni sociali di ciascuno sarebbero potute essere agevolmente ricostruite, proprio muovendo dai dati personali sul traffico telematico o telefonico.

[109] Cfr. par. 37 della sentenza.

giurisprudenza della Corte EDU sull' art. 8 CEDU [110] in tema di memorizzazione di dati a fini di creazione di dossier. E ciò indipendentemente dal carattere sensibile dell'informazione o degli eventuali inconvenienti o pregiudizi subiti dagli interessati a seguito di tale ingerenza, finendo per ingenerare nelle persone interessate «la sensazione che la loro vita privata sia oggetto di costante sorveglianza», amplificata peraltro dal fatto che tale conservazione e utilizzo ulteriore possono essere effettuati senza che l'utente ne sia neppure informato [111].

D'altra parte, le limitazioni contenute nella direttiva rispondono indubbiamente, nel ragionamento della Corte, all'obiettivo di interesse generale della lotta contro la criminalità atteso che «l'art. 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma altresì alla sicurezza».

Giungendo poi al vaglio di proporzionalità dell'ingerenza constatata, la Corte si sofferma su tre profili: la mancanza generale di limiti alla conservazione dei dati nella dir. 2006/24/CE, l'assenza di alcun criterio oggettivo che permetta di delimitare l'accesso a tali dati da parte delle autorità nazionali, nonché la durata stessa della conservazione.

Sulla base della valutazione di questi tre profili, la Corte conclude che «adottando la dir. 2006/24/CE, il legislatore dell'Unione ha ecceduto i limiti imposti dal principio di proporzionalità alla luce degli artt. 7, 8, 52 par. 1 della Carta», dal momento che la stessa da un lato non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali in questione, tali da garantire che essa sia effettivamente limitata a quanto strettamente necessario; né prevede garanzie sufficienti che consentano una protezione efficace dei dati contro i rischi di abusi, accessi ovvero utilizzi illeciti degli stessi.

Sul punto, la segnalata inversione di tendenza in tema di intercettazioni nella giurisprudenza della Corte europea dei diritti dell'uomo (v. *supra*, par. 4) appare successiva e correlata proprio alla giurisprudenza della Corte di Giustizia, segnatamente al caso *Digital Right Ireland*, ma ancor di più al successivo caso *Schrems* [112], in cui la Corte ripropone le medesime argomentazioni fornite nel primo caso nel bilanciamento tra esigenze di sicurezza e protezione dei dati personali nella dimensione esterna della loro circolazione (flusso transfrontaliero con gli USA). Proprio la sentenza *Schrems* - e la successiva *Schrems II* [113] - si iscrivono in un filone di giurisprudenza che, assieme ai crescenti interventi per la regolazione delle reti e alle operazioni di sorveglianza così condotte, rivela il collegamento con la contesa fra «due super-potenze internazionali (...) per il controllo di una risorsa essenziale quale le reti globali di telecomunicazioni». In

[110] Corte EDU, sentenze *Leander c. Svezia,* 26 marzo 1987, nonché *Rotaru c. Romania* n. 28341/1995, e *Weber e Saravia c. Germania*, n. 54934/00, richiamate al punto 35 della sentenza.

[111] Sullo sfondo di questa vicenda, e più in generale degli sforzi recente della Corte di giustizia, si colloca proprio la problematica della sorveglianza globale. Cfr. anche ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in *Riv. dir. int. priv. proc.*, 4, 2016, p. 1020 ss.

[112] Tanto da essere definita il c.d. «follow up» di *Schrems*. Cfr. O. POLLICINO- M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit., p. 101.

[113] Corte di Giustizia dell'Unione europea, 16 luglio 2020, causa C-311/18.

tale contesto, lo strumento impiegato dall'Unione Europea è stato proprio una regolazione fortemente territoriale con effetti indirettamente (ma programmaticamente) ultra-territoriali. In linea con tale impostazione, la Corte UE si erge nei casi sopracitati a strenua difesa dei diritti fondamentali per proclamare la c.d. «sovranità digitale» dell'Unione [114].

Un punto che emerge sovente, sia nella giurisprudenza EDU che UE, è quello della durata della conservazione e del fattore tempo [115], uno degli aspetti salienti che trovano maggiore sottolineatura anche nel regolamento in tema di intelligenza artificiale. Esso costituisce, infatti, un nodo problematico centrale nel bilanciamento degli interessi in gioco e che in linea di principio deve essere proporzionato alle finalità di raccolta degli stessi. Sul punto, non può non farsi un riferimento storico alla Convenzione n. 108 del 1981[116], che conteneva previsioni specifiche, in ottica di limitazione della conservazione dei dati a tutela dei diritti e delle libertà dell'interessato, volte a contenerne la durata ad un tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento, rivelando ancora una volta come il principio di conservazione dei dati personali sia sottoposto a limiti che dipendono strettamente dalle finalità per cui essi sono stati raccolti e trattati, per cui il principio di conservazione dei dati è avvinto da uno stretto nesso strutturale con la finalità del trattamento, in relazione al quale va valutato in termini di proporzionalità [(117)].

Anche sotto il profilo informativo, l'art. 13 GDPR prevede, in tema di informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, che il titolare del trattamento fornisca all'interessato specifiche informazioni relative al «periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo», esplicitamente qualificate siccome necessarie per garantire un trattamento corretto e trasparente [118].

---

[114] V. ZENO ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA E V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy Shield"*, p. 7-9. Cfr. Anche G. RESTA- F. SIMONETTI, *La c.d. sovranità digitale e il progetto Gaia-X,* in *Contr. e impr./Europa*, 3, 2022, p. 479 ss.

[115] Sul fattore tempo la Corte di Strasburgo ha adottato un orientamento maggiormente restrittivo rispetto al trattamento di dati risalenti anche nel caso *Haralambire c. Romania* del 27 ottobre 2009, in cui ha constatato il diritto dei singoli all'accesso ai dossier formati dei servizi segreti all'epoca della dominazione sovietica, al fine di contestarli e rettificarne il contenuto. Allo stesso modo Corte EDU *Turek c. Slovacchia*, 16 febbraio 2006

[116] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108, firmata a Strasburgo il 28 gennaio 1981 ed entrata in vigore il 1° ottobre 1985. Cfr., sul tema, M. FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali, in Diritto comunitario e degli scambi internazionali*, 2016, p. 12 e M. E. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e Diritto internazionale*, 2011, p. 449.

[117] Sul punto, cfr. anche Art. 29 WP, *Opinion* 1/2014 *on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 536/14/EN, WP 211, 27 febbraio 2014.

[118] Con specifico riferimento al tema delle categorie particolari di dati, può farsi qui riferimento, seppur in diverso contesto, alla disciplina contenuta nel D.P.R. 7 aprile 2016, n. 87, recante disposizioni di attuazione della l. 30 giugno 2009, n. 85, concernente l'adesione dell'Italia al Trattato di Prüm, che prevede tra l'altro l'istituzione di una banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, introducendo regole piuttosto rigide per disciplinare gli accessi alle informazioni in essi contenute e il loro successivo trattamento. In particolare, all'art. 25 è

Le considerazioni sopra riportate, corroborate dalla giurisprudenza delle due Corti, valgono anche in relazione a forme di ingerenza da parte delle pubbliche autorità che sono prospettate ai consociati come soltanto meramente propedeutiche allo sviluppo di nuove tecnologie, come, nel caso di specie, l'addestramento di algoritmi di intelligenza artificiale[119].

6. Gli orientamenti delle autorità di controllo in tema di trattamento di dati biometrici e tecnologie di riconoscimento facciale

Come lo stesso *IA Act* non manca di precisare[120], nell'applicazione dell'art. 9, par. 1 GDPR, l'uso dell'identificazione biometrica remota anche per fini diversi dalle attività di contrasto è già stato oggetto di decisioni di divieto da parte delle autorità nazionali per la protezione dei dati, facendo riferimento ad una già cospicua attività provvedimentali delle autorità di controllo sul punto.

Sul versante nazionale, l'atteggiamento del Garante per la protezione dei dati personali risulta particolarmente restrittivo nel ritenere necessaria una valutazione di insieme per evitare che «singole iniziative aventi ad oggetto il trattamento di dati particolari come quelli biometrici, sommate fra loro, definendo un nuovo modello di sorveglianza, introducano di fatto un cambiamento non reversibile nel rapporto tra individuo ed autorità».

L'attività provvedimentale dell'Autorità garante sul punto tiene conto proprio di queste premesse e considerazioni.

Già nel febbraio del 2020 l'Autorità aveva avuto modo di pronunciarsi [121] sull'utilizzo di dispositivi di video sorveglianza tramite riconoscimento biometrico in tempo reale adottati dagli enti locali, vietando, nello specifico, con parere adottato nei confronti del Comune di Como, prima amministrazione che intendeva fare ricorso a questa tipologia di sistema di IA. Secondo l'Autorità, la raccolta di dati biometrici – funzionale in particolare all'identificazione dei soggetti interessati nei soli casi nei quali emergano specifiche esigenze investigative, segnatamente ai sensi dell'art. 349 c.p.p. – può effettuarsi solo in presenza di un'idonea previsione normativa ai sensi dell'art. 7 d.lgs. n. 51/2018, che non pareva rinvenibile nel caso concreto.

Orientamento in linea con le posizioni coeve assunte delle Autorità nazionali di altri paesi, ad esempio in Spagna l'AEPD ha tratteggiato nel parere N/REF 010308/2019 i limiti dei trattamenti legati all'utilizzo di tecniche di riconoscimento facciale, atteso che «l'esistenza di un interesse pubblico non legittima alcun

espressamente previsto un periodo di conservazione del materiale biologico non superiore a trenta anni dalla data dell'ultima registrazione, prorogabile a quaranta in casi particolari.

[119] Si vedano in proposito le sopracitate "*Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*", *supra*, par. 4.

[120] Cfr. considerando 39.

[121] Garante per la protezione dei dati personali, provvedimento del 26 febbraio 2020, [doc. web n. 9309458].

tipo di trattamento dati personali, ma devono essere, prima di tutto, presidiati da una norma di legge in combinato con i principi di limitazione delle finalità e minimizzazione dei dati». In Francia, la normativa di riferimento in materia di utilizzo di dispositivi per il riconoscimento facciale è contenuta, oltre che nel GDPR, nella Legge primaria di Informatica e Libertà, che esordisce all'art. 1 con una dichiarazione di principio che ricorda la formulazione del considerando 4 del GDPR: «La tecnologia dell'informazione deve essere al servizio di ogni cittadino. […] Non deve attentare né all'identità umana, ai diritti umani, alla privacy o alle libertà individuali o pubbliche». In questo contesto, il CNIL ha dato atto in via formale con un paper [122] del 15 novembre 2019 che il riconoscimento facciale è sempre più presente nel dibattito pubblico a livello nazionale, europea e globale e solleva anzi nuove questioni relative a scelta della società, pronunciandosi in più occasioni in senso restrittivo su trattamenti di dati biometrici (nella fattispecie, riconoscimento facciale in due scuole superiori [123] e sistemi di videosorveglianza intelligente utilizzati da gestori di mezzi pubblici di linea a fini di prevenzione sanitaria nella gestione della pandemia da Sars-Cov-2 [124]). E provvedimenti non dissimili, emanati dalle rispettive Autorità garanti, sono rinvenibili anche in Olanda [125], Svezia e Danimarca [126].

Tornando, per quanto qui di interesse, all'attività provvedimentale del Garante italiano, è opportuno richiamare la posizione assunta con riferimento ad alcuni importanti casi che l'Authority ha vagliato. In primo luogo, il caso *Sari real time* [127], avente ad oggetto una tecnologia di riconoscimento facciale in grado di coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, oppure in relazione a specifiche esigenze di polizia giudiziaria, in cui il Garante, con provvedimento del 25 marzo 2021, ha reso un parere negativo, dimostrando anzi una spiccata preoccupazione in ordine all'«evoluzione della

122 CNIL, *Reconnaissance faciale pour un debat à la hauteur des enjeux*.
123 CNIL, *réunis en séance plénière* le 17 octobre 2019, provvedimento consultabile nel sito istituzionale dell'Autorità.
124 *Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports*.
125 L'Autorità garante olandese (AP) è intervenuta, ad esempio, il 29 ottobre 2019, con una nota formale (reperibile nel sito istituzionale https://autoriteitpersoonsgegevens.nl/) di fronte dell'uso indiscriminato da parte di aziende di vendita al dettaglio, sicurezza, sport e intrattenimento, trasporti dei dispositivi di riconoscimento facciale.
126 La DPA svedese ha esaminato il caso di una scuola comunale che ha condotto un progetto pilota di riconoscimento facciale per tenere traccia della frequenza scolastica degli studenti irrogando una sanzione di 200.000 SEK per la violazione le norme del GDPR, avendo la scuola ha elaborato dati biometrici sensibili illegittimamente e non essendo riuscita a eseguire un'adeguata valutazione dell'impatto, compresa la consultazione preventiva con il DPA svedese. La scuola ha basato il trattamento sul consenso, ma il DPA svedese ritiene che il consenso non fosse una base giuridica valida dato il chiaro squilibrio tra l'interessato e il responsabile del trattamento. Un altro paese scandinavo ha però valutato l'impatto del'IA in maniera diversa riguardo l'utilizzo dei dispositivi di riconoscimento facciale, dando un vero e proprio via libera all'installazione di telecamere intelligenti all'interno dello stadio di cui è proprietaria la squadra di calcio professionista di serie A del Broendby. Si tratta di un provvedimento che ha autorizzato un privato a dotarsi di un sistema di IA per finalità di interesse pubblico finalizzate ad impedire l'accesso allo stadio a una lista di tifosi che avevano ricevuto in passato un provvedimento amministrativo o giudiziale di ammonizione per fatti violenti. Il parere reso dall'Autorità Garante ha però delimitato un perimetro preciso entro cui effettuare tale trattamento, quali l'obbligo di non conservare i dati biometrici di chi accede allo stadio, obbligo di cancellazione post partita di tutti i dati residuali, obbligo di segnaletica ad hoc, conservazione dei dati temporanei in un server protetto da algoritmi crittografati, autenticazione a due fattori e divieto di accesso ai server da remoto.
127 Provvedimento del Garante n. 127 del 25 marzo 2021, [doc. web n. 9575877].

natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui».

In particolare, richiamando gli articoli 8 CEDU, nonché 7, 8 e 52 CDFUE, l'Autorità ha ritenuto allo stato non sussistente una base giuridica idonea a consentire il trattamento dei dati biometrici nel caso concreto, fondato su un algoritmo di riconoscimento facciale che consente di analizzare in tempo reale i volti dei soggetti ripresi confrontandole con una banca dati predefinita per lo specifico servizio denominata "*watch-list*" [128].

Successivamente, nel 2022, l'Autorità garante ha poi adottato un altro interessante provvedimento [129], con cui ha comminato una sanzione particolarmente elevata a *Clearview AI Inc.*, in ragione dell'assenza di una base giuridica del trattamento di immagini, avvenuto senza il consenso e il mancato riscontro alle richieste degli interessati, specificatamente sull'accesso ai dati. Alla prima richiesta di informazioni dell'Autorità la società rispondeva di non effettuare il monitoraggio degli interessati all'interno dell'Unione secondo quanto stabilito dall'art. 3, par. 2, lett. b) GDPR, in quanto lo stesso presuppone un'osservazione che sia continua e perdurante nel tempo, mentre il servizio in questione non offre la possibilità di monitorare e tracciare le persone nel tempo, ma offre esclusivamente la funzionalità di ricerca delle immagini, come un semplice motore di ricerca, offrendo un'istantanea dei risultati. Ponendosi l'attività predetta quale «mera raccolta di dati», le conclusioni che vengono tratte dalla ricerca sarebbero quindi, nell'ottica della convenuta, il risultato dell'operato delle forze dell'ordine che, grazie ai risultati forniti dal servizio, conducono ulteriori indagini investigative, condotte dagli organi inquirenti (e non dal software; quindi, non si potrebbe ritenere che si tratti di un monitoraggio attraverso mezzi automatizzati) [130].

Il Garante, con riferimento all'attività di monitoraggio, ritiene che il servizio offerto da *Clearview* non sia sovrapponibile a quello di un motore di ricerca, in quanto consistente in un'operazione di rielaborazione delle immagini per ricavarne dati biometrici al fine di effettuare la comparazione tra immagini; le informazioni relative alle immagini vengono altresì arricchite nel tempo grazie alle ulteriori immagini che vengono aggiunte, così da evidenziare altresì i cambiamenti degli individui nel corso del tempo. L'attività

[128] Cfr. anche provvedimento n. 54 del 26 febbraio 2020, reperibile sul sito istituzionale dell'autorità, [doc. web n. 9309458].

[129] Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di *Clearview AI* - 10 febbraio 2022, [doc. web n. 9751362].

[130] In riferimento alla profilazione richiama le linee guida del Gruppo di lavoro Articolo 29, Linee guida sul Processo decisionale individuale automatizzato e Profilazione ai fini del Regolamento 2016/679 (wp251rev.01), in cui vengono elencate le fasi attraverso le quali si esplica l'attività di profilazione: raccolta dei dati; analisi automatizzata per ricercare le correlazioni; applicazione delle correlazioni emerse per predire i comportamenti futuri. La Società ritiene che, anche se le prime due fasi sono presenti nell'attività svolta da *Clearview*, l'ultima non sarebbe presente, in quanto se anche fossero individuate delle caratteristiche future, sarebbe ascrivibile ad un comportamento del cliente del servizio, da qualificarsi quale titolare del trattamento.

svolta da *Clearview* consiste, quindi, nella classificazione degli individui, ma anche nell'estrazione dei dati biometrici e nell'acquisizione di informazioni ulteriori riguardanti gli interessati.

Infine, più di recente, agli inizi del 2024, il Garante ha sanzionato il Comune di Trento [131] per aver condotto due progetti di ricerca scientifica, utilizzando telecamere, microfoni e reti sociali, in violazione della normativa sulla protezione dati, stigmatizzando le massive e invasive modalità di trattamento poste in essere dall'ente, che hanno comportato significativi rischi per i diritti e le libertà degli interessati, anche di rango costituzionale, dal momento che «simili forme di sorveglianza negli spazi pubblici possono modificare il comportamento delle persone e condizionare anche l'esercizio delle libertà democratiche». In particolare, il trattamento dei dati era svolto nell'ambito *del progetto Marvel ("Multimodal Extreme Scale Data Analytics for Smart Cities Environments"*), un progetto finanziato con fondi europei, avente come obiettivo lo sviluppo di soluzioni tecnologiche volte a migliorare la sicurezza in ambito urbano, secondo il paradigma delle "città intelligenti" (*smart cities*). Esso prevedeva l'acquisizione di filmati dalle telecamere di videosorveglianza già installate nel territorio comunale per finalità di sicurezza urbana, nonché dell'audio ottenuto da microfoni appositamente collocati sulla pubblica via. I dati, che ad avviso del Comune sarebbero stati immediatamente anonimizzati dopo la raccolta, venivano analizzati per rilevare in maniera automatizzata, mediante tecniche di intelligenza artificiale, eventi di rischio per la pubblica sicurezza. *A latere*, il progetto *Protector ("PROTECTing places of wORship"*) prevedeva invece, oltre all'acquisizione dei filmati di videosorveglianza (senza segnale audio), la raccolta e l'analisi di messaggi e commenti d'odio pubblicati sui social, rilevando finanche eventuali emozioni negative ed elaborando informazioni d'interesse per le Forze dell'ordine, allo scopo di identificare rischi e minacce per la sicurezza dei luoghi di culto.

Vari i profili di censura rinvenibili nel provvedimento dell'autorità di controllo. In primo luogo, Il Comune di Trento, che non annovera la ricerca scientifica tra le proprie finalità istituzionali, non ha comprovato la sussistenza di alcun quadro giuridico idoneo a giustificare i trattamenti dei dati personali, peraltro relativi anche a categorie particolari, e la conseguente ingerenza nei diritti e nelle libertà fondamentali delle persone, atteso pure che i dati venivano condivisi anche con soggetti terzi, tra cui i partner di progetto. Inoltre, sono state ritenute insufficienti le tecniche di anonimizzazione impiegate per ridurre i possibili rischi di reidentificazione per gli interessati; oltre che ravvisate criticità sotto il profilo della trasparenza, non avendo il Comune compiutamente descritto i trattamenti nelle informative di primo e di secondo livello. Infine, l'ente non ha comprovato di aver effettuato una valutazione d'impatto *ex* art. 35 GDPR prima di iniziare il trattamento, nonostante i due progetti comportassero l'impiego di nuove tecnologie e la sorveglianza sistematica di zone accessibili al pubblico.

[131] Provvedimento del Garante 11 gennaio 2024 [doc. web n. 9977020].

In particolare, nel provvedimento il Garante, richiamando i propri precedenti sul punto [132], ha ribadito pure che anche l'acquisizione e la temporanea memorizzazione di dati personali, come l'immagine del volto ripresa da dispositivi video, ancorché per una ridotta frazione temporale, costituisce un trattamento di dati personali, che nel caso specifico, oltre ad essere privo di base giuridica, non rispondeva affatto ai necessari criteri di trasparenza richiesti (anche sotto il profilo delle informazioni di primo e secondo livello [133]) nei confronti degli interessati, captando anche il segnale audio acquisito mediante microfoni installati sulla pubblica via e dunque anche conversazioni private, il cui contenuto è assistito dalle più elevate garanzie sul piano costituzionale [134]. Le massive e invasive modalità di trattamento poste in essere hanno così comportato, secondo il Garante, significativi rischi per i diritti e le libertà degli interessati, non solo con riguardo al diritto alla protezione dei dati ma anche agli altri diritti, di rango costituzionale, connessi alla libera manifestazione del pensiero di cui agli art. 21 Cost., 9 e 10 CEDU e artt. 10 e 11 CDFUE, ma anche alla partecipazione alla vita politica e sociale *ex* artt. 2 e 3 Cost., nonché alla libertà di riunione *ex* artt. 18 Cost., 11 CEDU e 12 CDFUE) e finanche alla libertà di manifestare la propria fede religiosa (art. 19 Cost., artt. 9 CEDU e 10 CDFUE), di cui il diritto alla riservatezza, in quanto funzionale all'autodeterminazione dell'individuo, costituisce un necessario presupposto. Secondo l'Autorità di controllo «simili forme di sorveglianza negli spazi pubblici possono, infatti, modificare il comportamento

[132] Cfr. provvedimenti 13 aprile 2023, nn. 122 e 123 [doc. web nn. 9896808 e 9896412], relativi al trattamento, posto in essere da soggetti pubblici, in assenza di idonea base giuridica, di dati personali contenuti in filmati ottenuti mediante dispositivi video, nell'ambito di un progetto che prevedeva l'impiego di algoritmi di rilevamento dei volti basati su reti neurali; v. anche, in senso conforme, anche il provvedimento 21 dicembre 2017, n. 551, [doc. web n. 7496252].

[133] Nello specifico caso, infatti, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, il titolare del trattamento deve infatti fornire agli interessati anche delle «informazioni di secondo livello», che devono «contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]» ed «essere facilmente accessibili per l'interessato, ad esempio attraverso una pagina informativa completa messa a disposizione in uno snodo centrale […] o affissa in un luogo di facile accesso» Cfr. Comitato europeo per la protezione dei dati, "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", del 29 gennaio 2020, in particolare par.7. Sul punto, cfr. il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, [doc. web n. 1712680], in particolare par. 3.1, nonché la FAQ del Garante n. 4 in materia di videosorveglianza, doc. web n. 9496574; cfr., pure, i provvedimenti 20 ottobre 2022, n. 341, doc. web n. 9831369; 28 aprile 2022, n. 162, doc. web n. 9777974, 7 aprile 2022, n. 119, doc. web n. 9773950, 16 settembre 2021, n. 327, doc. web n. 9705650 e 11 marzo 2021, n. 90, [doc. web n. 9582791].
In particolare, secondo le Linee guida citate le informazioni di primo livello (cartello di avvertimento) «dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento» (punto. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato (ad esempio, trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, o periodo di conservazione). Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi) (Linee guida, cit., punto. 115). Ancora, la segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

[134] Cfr., ancora, Linee guida 3/2019, cit., in particolare punto 129, ove si afferma che «le soluzioni individuate non dovrebbero prevedere funzioni non necessarie (ad esempio, […] registrazioni audio)», nonché il successivo punto 131, ove si afferma che tra gli elementi che i titolari dovrebbero prendere in considerazione vi è «l'utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video)».

delle persone e condizionare finanche l'esercizio delle libertà democratiche, specialmente quando la sorveglianza contravviene alla ragionevole aspettativa di riservatezza degli interessati».

Medesima linea ha mantenuto il Garante nelle più recenti iniziative promosse, sempre nel 2024, nei confronti del Comune di Torino [135] e, poco prima, del Comune di Roma [136], sottolineando, in particolare, come fino a tutto il 2025 viga una moratoria sull'installazione di impianti di videosorveglianza con sistemi di riconoscimento facciale attraverso l'uso di dati biometrici, in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sicché tale trattamento è consentito solo all'autorità giudiziaria, nell'esercizio delle funzioni giurisdizionali, e alle autorità pubbliche, a fini di prevenzione e repressione dei reati, e comunque previo parere favorevole del Garante stesso. Considerazioni sovrapponibili si ritrovano anche nell'attività provvedimentale del Garante di inizio 2024 [137], in cui si richiama infatti il d.l. 10 maggio 2023, n. 51, conv. in l. 3 luglio 2023, n. 87, che con l'art. 8-*ter* ha prorogato al 31 dicembre 2025 la sospensione dell'installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale «in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati», proprio al fine di «disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea» [138].

7. Conclusioni

Nel già citato "Rapporto sulla competitività europea" del 9 settembre scorso (vedi *supra*, par. 1), si sottolinea la frammentazione normativa, specialmente nel settore digitale, ostacoli l'innovazione, citando proprio le interferenze e sovrapposizioni tra GDPR e AI Act quali esempi critici, sottolineando come esse possano porsi quale freno per l'innovazione, soprattutto per le piccole e medie imprese occorrendo

[135] Garante protezione dati personali, 19 luglio 2024.

[136] Garante protezione dati personali, 9 maggio 2024, con riferimento al progetto di videosorveglianza nelle stazioni della metropolitana, dotato di telecamere con riconoscimento facciale, «in grado di verificare azioni scomposte» all'interno dei vagoni e sulle banchine da parte di chi in passato si è reso protagonista «di atti non conformi».

[137] Garante protezione dati personali, provvedimento del 22 febbraio 2024 [doc. web n. 9995680], in cui si sottolinea, fra il resto, come vi sia trattamento di dati biometrici sia nella fase di registrazione (c.d. *enrolment*), consistente nella acquisizione delle caratteristiche biometriche dell'interessato (ad esempio, caratteristiche del volto), sia nella fase di riconoscimento biometrico, all'atto della rilevazione delle presenze. Sul punto, cfr. anche il provvedimento del Garante del 12 novembre 2014, n. 513, in www.garanteprivacy.it, doc. web n. 3556992), in particolare punti 6.1, 6.2 e 6.3 dell'allegato al citato provvedimento. Pertanto, anche in caso di estrazione del c.d. template, vi sarebbe trattamento di dati biometrici, con conseguente applicazione della specifica disciplina prevista dall'ordinamento.

[138] Cfr. *European data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, adottate il 26/7/2023, già richiamate, in particolare i punti 17, 34 e 35 sui rischi del riconoscimento facciale; nonché le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020, spec. punti 4 e 73. Infine, si veda sul punto, altresì, il provvedimento del Garante per la protezione dei dati personali del 10 febbraio 2022, n. 50, [doc. web n. 9751362], adottato sempre in materia di riconoscimento facciale.

invece «un equilibrio tra regolamentazione e innovazione, per non soffocare le PMI, cuore dell'economia europea».

Il report evidenzia infatti «come l'Unione abbia più di 100 normative specifiche nel settore digitale, e oltre 270 autorità di regolamentazione, delineando un approccio complessivo eccessivamente cautelativo, che rischia di soffocare lo sviluppo tecnologico». Sul punto, uno studio pubblicato *dall'European Parliament Research Service* (EPRS) dedicato a "*The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*" [139] ha proprio evidenziato le problematiche che sorgono dall'intersezione di queste due discipline. Vari i nodi problematici individuati, tra cui quelli relativi alla base giuridica, al principio di finalità e di trasparenza. In primo luogo, la possibilità di utilizzare la medesima base giuridica per finalità diverse ma compatibili diventa questione particolarmente complessa nel dinamico e volatile campo dell'IA, nell'ambito del quale i dati possono essere riutilizzati per finalità neppure immaginabili al momento della loro prima condivisione. Ciò si ricollega inevitabilmente alla questione della trasparenza, rispetto a un potenziale uso nell'ambito dell'addestramento di modelli di IA, ma anche in relazione, ad esempio, alle decisioni automatizzate.

Ancora, si sottolinea sotto altro profilo, la soddisfazione dei requisiti di specificità, granularità e libera manifestazione del consenso – ove necessario per il trattamento specifico – possono porre problemi di attuazione pratica nel campo dell'IA, talvolta anche al punto di inficiare l'esperienza d'uso. Per questi motivi, il rapporto dell'EPRS raccomanda alle autorità competenti, in particolare quelle preposte alla protezione dei dati, di emanare linee guida, fornire chiarimenti sull'interpretazione delle disposizioni del GDPR in relazione a tale nuovo fenomeno. Tale approccio, tuttavia, rischia di perpetuare proprio le criticità evidenziate dal Rapporto sopracitato in punto alla frammentazione giuridica, posto che lasciare l'interpretazione e l'applicazione di tale intersezione tra GDPR e AI Act alle autorità, oltre che porsi in contrasto con il principio per cui è demandato alla sola Corte di Giustizia il compito di interpretare il diritto comunitario, porta con sé il rischio che si venga a creare un quadro normativo disomogeneo e frammentario.

D'altra parte, l'attenzione tributata alla tutela dei diritti fondamentali deve rimanere massima.

Come efficacemente sottolineato [140], «il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti», utilizzando alcuni dati quale «surplus comportamentale privato», sottoposto a processi governati dall'intelligenza artificiale per essere trasformato in prodotti predittivi, destinati poi ad essere scambiati su un nuovo tipo di mercato per le previsioni comportamentali, definito quale «mercato dei comportamenti futuri».

---

[139] "*The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*", pubblicato dall' *European Parliament Research Service (EPRS)*.

[140] S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, II ed., Luiss University Press, 2023.

Una visione della protezione dei dati personali, quale «precondizione per il pieno godimento di altri diritti fondamentali» [141], nonché «espressione particolarmente forte quasi metonimica della dignità personale, meta-valore riassuntivo dell'impianto assiologico sui cui si innestano le situazioni giuridiche costituzionalmente protette» [142] impone, dunque, un approccio *data driven*, non solo in funzione del miglioramento di diagnosi e cura nel quadro dell'impiego dei dati biometrici, ma proprio come approccio di processo che restituisca centralità alla persona, la cui identità viene in gioco sotto vari profili [143], adottando una prospettiva che faccia leva sul bilanciamento [144] tra i principi che di volta in volta vengano in conflitto [145], da condursi secondo ragione [146], avendo sempre come punto di riferimento la dignità della persona [147].

Ma vi è di più. Come recentemente sottolineato [148], «non può bastare limitarsi a dire che occorre un sistema regolatorio che metta l'uomo al centro, ma bisogna invece mettere lucidamente al centro la necessità di adottare regole che rendano comprensibili i programmi usati dalla (o dalle) IA, verificabili e sindacabili i dati usati per l'addestramento di queste tecnologie», proprio in bilanciamento con la necessità di salvaguardare e rafforzare il mercato unico digitale europeo e la competizione globale.

Solo per questa via potrà realizzarsi in pieno quella tensione ideale alla diffusione di quell'intelligenza artificiale «antropocentrica e affidabile», che il nuovo Regolamento intende perseguire.

---

141 Cfr. G. ALPA, *Diritto privato europeo*, Giuffrè, Milano, 2016, p. 182; G. BUTTARELLI, *Banche dati e tutela della riservatezza,* Giuffrè, Milano, 1997.

142 N. LIPARI, *Diritto civile e ragione*, Giuffrè, Milano, 2019, p. 183 ss.

143 Sull'approccio del legislatore europeo nella regolazione dell'intelligenza artificiale, si veda G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.,* 4, 2022, 1085 ss. Per una riflessione di più ampio respiro sulle principali direttrici giuridiche del mercato digitale, cfr. G. FINOCCHIARO, L. BALESTRA e M. TIMOTEO (a cura di), *Major Legal Trends in the Digital Economy*, Il Mulino, Bologna, 2022.

144 Si vedano le sempre attuali riflessioni sulla prudenza nel bilanciamento di G. ZAGREBELSKY, *Il diritto mite*, Einaudi, Torino, 1992, 200.

145 A. MORRONE, voce *Bilanciamento (giustizia costituzionale)*, in *Enc. dir.*, Annali, Milano, 2008, vol. II, tomo II, p. 185-204.

146 Cfr. P. GIANNITI, *I diritti fondamentali nell'unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, cit., p. 223, in cui cita in proposito F. GALGANO, *Democrazia politica e legge della ragione*, in *Contr. e impr.*, 2007, p. 393 ss., nonché ID., *Globalizzazione dell'economia e universalità del diritto*, in *Pol. dir.*, 2009, p. 177 ss.

147 Cfr anche R. PARDOLESI, in nota a Trib. Milano, 28 settembre 2016, in *Foro it.*, 2016, I, 3594, che sottolinea come tale impostazione sia l'unica compatibile con il principio personalistico e con la visione della persona umana quale valore etico in sé.

148 F. PIZZETTI, *Con AI Verso la Società digitale*, in *federalismi.it*, 23, 2023.