ISSN 1826-3534

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

FOCUS LAVORO, PERSONA, TECNOLOGIA
18 OTTOBRE 2023

Poteri datoriali e dati biometrici nel contesto dell'AI Act

di Laura Tebano
Professoressa ordinaria di Diritto del lavoro
Università degli studi di Napoli "Federico II"

Poteri datoriali e dati biometrici nel contesto dell'AI Act*

di Laura Tebano
Professoressa ordinaria di Diritto del lavoro
Università degli studi di Napoli "Federico II"

Abstract [It]: Il contributo si propone di indagare le ricadute della proposta di regolamento europeo sull'intelligenza artificiale nel contesto lavorativo con riguardo ai dati biometrici. Ponendo a confronto il perimetro delle (plurali) nozioni presenti nell'AI Act e della (compatta) nozione contenuta nel GDPR si traccia un primo bilancio delle implicazioni del disomogeneo apparato di tutela che caratterizza i due blocchi normativi, fino ad auspicarne un allineamento valoriale e operativo.

Title: Employer prerogatives and biometric data in the AI Act
Abstract [En]: The essay aims to investigate the impact of the proposed European regulation on artificial intelligence in the work context concerning the use of biometric data. By comparing the boundaries of the (plural) notions present in the AIA and the (compact) notion contained in the GDPR, an initial assessment of the implications of the uneven apparatus of protection that characterises the two regulatory blocks is drawn to the point of advocating a restyling of them to align values and operations.

Parole chiave: Intelligenza artificiale; dati biometrici; dati basati sulla biometria; Regolamento UE 2016/679
Keywords: Artificial intelligence; biometric data; biometric-based data; Regulation EU 2016/679

1. La proposta di regolamento sull'intelligenza artificiale: un lungo percorso costellato di novità

La proposta di regolamento sull'intelligenza artificiale (d'ora in poi AI Act), pur non avendo ancora esaurito il suo *iter*, è giunta a una fase avanzata del processo legislativo: l'approvazione da parte del Parlamento europeo, intervenuta lo scorso 14 giugno, ha dato la stura ai cd. triloghi di negoziazione di merito fra Europarlamento, Consiglio e Commissione e si auspica che entro novembre si arrivi all'intesa finale[1]. Per comprendere la logica di fondo che ha guidato la definizione del complesso di regole

* Articolo sottoposto a referaggio. Questo lavoro è stato sviluppato dalla Prof.ssa Tebano nell'ambito del progetto PNRR MUR PE0000013-FAIR.

[1] Cfr. COM(2021) 206 final del 21 aprile 2021. Il testo adottato il 14 giugno è consultabile sul sito del Parlamento Europeo. Va poi ricordato che i triloghi sono quei negoziati informali a cui partecipano alcuni rappresentanti del Parlamento, del Consiglio e della Commissione, durante i quali tali istituzioni concordano orientamenti politici e bozze di emendamento rispetto alle proposte legislative avanzate dalla Commissione. L'esito di tali negoziati viene poi sottoposto alla votazione del Consiglio e del Parlamento. Sul tema in generale G. RUGGE, *Il ruolo dei triloghi nel processo legislativo dell'UE*, in *Il Diritto dell'Unione europea*, 2015, p. 809 ss.; V. SALMASO, *I triloghi nel processo decisionale europeo*, in *Forum di Quaderni costituzionali – Rassegna*, 20 dicembre 2016, p. 1 ss. Sul superamento dell'informalità e l'affermazione dell'idea

armonizzate sull'intelligenza artificiale occorre rammentare che la proposta mira a realizzare uno degli obiettivi indicati nel Libro bianco sull'AI pubblicato dalla Commissione il 19 febbraio 2020, cioè affrontare il problema dei rischi associati a determinati utilizzi di tale tecnologia[2]. Per un verso, infatti, il Libro bianco definiva le opzioni strategiche funzionali al conseguimento degli obiettivi di promozione e di affidabilità dell'utilizzo dell'AI, per altro verso paventava il rischio di un ricorso abusivo all'AI da parte dei datori di lavoro che – in violazione delle regole europee in materia di tutela dei dati personali o di altre previsioni – avrebbero potuto utilizzare tali moderni sistemi per monitorare i comportamenti dei dipendenti[3].

Rispetto all'originaria versione del 21 aprile 2021[4], la proposta ha subìto nel tempo numerosi ritocchi: i testi di compromesso che si sono susseguiti, pur senza intaccare l'impianto di fondo e l'approccio basato sul rischio, hanno significativamente alterato le sembianze dell'AI Act. Senza ripercorrere nel dettaglio le singole modifiche, sembra sufficiente in questa sede soffermarsi brevemente su alcuni aspetti che (direttamente o indirettamente) assumono rilevanza rispetto al tema che si intende sondare. Innanzitutto pare opportuno rimarcare un'importante rettifica relativa alle basi giuridiche della proposta: come da più parti sottolineato l'AI Act risultava inizialmente sbilanciato sul versante mercantilistico in quanto il suo pilastro centrale era rappresentato dall'art. 114 TFUE[5]. Il che spiegava (e in qualche misura giustificava) l'assenza di profili di natura sociale trattandosi di una proposta diretta a migliorare il funzionamento del mercato interno e a garantire la libera circolazione (transfrontaliera) di beni e servizi basati sull'AI. In posizione defilata si collocava l'art. 16 TFUE, richiamato a fondamento delle (sole) regole specifiche sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, in particolare con riguardo alle restrizioni sull'utilizzo di sistemi di AI per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico[6].

---

che le riunioni in forma di trilogo siano parte integrante dell'*iter* di formazione degli atti legislativi, F. BATTAGLIA, *La trasparenza del procedimento legislativo europeo all'esame del giudice dell'Unione nel caso De Capitani*, in *Federalismi*, n. 15, 2018. All'incontro del 18 luglio dovrebbe seguirne uno il 26 settembre e un ultimo il 26 ottobre.

[2]Lo stesso Libro bianco (COM (2020) 65 final) rappresenta l'ultima tappa di un percorso che viene da lontano: dalla strategia per il mercato unico digitale del 2015 (cfr. COM(2015) 192) e COM (2017) 228final) e più direttamente dalla strategia europea per l'AI presentata nell'aprile 2018 (COM (2018) 237final).

[3]Proprio sul fronte della garanzia dei diritti fondamentali, la Commissione ventila l'insufficienza dell'attuale armamentario giuridico e la conseguente necessità di un adattamento del quadro normativo europeo. Sul punto L. TEBANO, *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale scientifica, Napoli, 2020, p. 222 ss.

[4]Cfr. COM (2021) 206 final.

[5] L. TEBANO, *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *Ianus*, 2021, n. 24, p. 45 ss.

[6] È appena il caso di ricordare che l'art. 16 TFUE riconosce il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano; conferisce al Parlamento europeo e al Consiglio il compito di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione; e affida il controllo del rispetto di tali norme alle autorità indipendenti.

Ben diversa l'impostazione adottata nel testo recentemente approvato dal Parlamento europeo, ove si registra un più equilibrato bilanciamento delle basi giuridiche: l'ossatura del regolamento appare cioè rappresentata tanto dall'art. 114 TFUE quanto dall'art. 16 TFUE, entrambi indispensabili per la stabilità dell'edificio. Come dire che proprio muovendo dalla consapevolezza che l'intelligenza artificiale spesso si basa sul trattamento di grandi volumi di dati e che molti sistemi e applicazioni di AI si fondano sul trattamento di dati personali, si è ritenuto opportuno poggiare sul pilastro dell'articolo 114 TFUE la trave dell'articolo 16 TFUE che sancisce il diritto alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e prevede l'adozione di regole sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali[7].

Inoltre, nel testo approvato dal Parlamento europeo si ravvisa una modifica nella classificazione dei sistemi di AI che attiene sia al metodo sia ai contenuti. Con riguardo al primo profilo, non pare trascurabile il passaggio da una classificazione rigida di tipo *top-down* a una flessibile in quanto soggetta a riesame permanente mediante una valutazione periodica[8] e fondata non già su una previsione astratta, bensì sulla portata dell'impatto negativo che il sistema di AI determina sui diritti fondamentali protetti dalla Carta dell'Ue[9]. Dal punto di vista contenutistico, basti qui ricordare che nella versione iniziale dell'AI Act figuravano classificati "ad alto rischio" (tra gli altri) i sistemi destinati a essere utilizzati con riguardo all'occupazione, alla gestione dei lavoratori e all'accesso al lavoro autonomo e i (soli) sistemi di identificazione biometrica remota delle persone fisiche[10]. Diversamente nell'Allegato III oggi si ritrovano sistemi di AI dai confini decisamente più ampi: sono infatti classificati "ad alto rischio" anche (alcuni) sistemi biometrici e basati su elementi biometrici che, come si chiarirà in seguito, ricomprendono una serie di situazioni in precedenza etichettate come a basso rischio.

Una vera e propria svolta attiene alla dimensione collettiva. Se è vero infatti che nella versione del 2021 le parti sociali non vantavano alcun diritto di informazione, né venivano coinvolte nella regolamentazione dei sistemi di AI utilizzati nel contesto lavorativo[11], è altrettanto vero che nel testo approvato dal

[7] Considerando 2*bis*.
[8] Considerando 27.
[9] Considerando 28*bis*; 32.
[10] E precisamente sia l'identificazione biometrica remota "in tempo reale" (cioè ai sensi dell'art. 3 .37 quel sistema in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi. Sono incluse non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione della normativa) sia "a posteriori" (vale a dire un sistema diverso da un sistema di identificazione biometrica remota "in tempo reale").
[11] Salvo naturalmente che si trattasse di piattaforme di lavoro digitale, nel qual caso il loro ruolo veniva "recuperato" nella misura in cui si ricadeva nell'ambito di applicazione della proposta di direttiva sul lavoro tramite piattaforme digitali. Sul punto, L. TEBANO, *La digitalizzazione del lavoro …*, *cit.*, p. 47 s.; P. TULLINI, *La nuova proposta europea sull'intelligenza artificiale e le relazioni di lavoro*, in *Trabajo, Persona, Derecho, Mercado*, 2022, p. 107. Nello stesso senso, E. KLENGEL – J. WENCKEBACH, *Artificial intelligence, work, power imbalance and democracy - why codetermination is essential*, in *Italian Labour Law E-Journal*, 2022, pp. 157-171.

Parlamento europeo gli obblighi incombenti sugli operatori dei sistemi di AI ad alto rischio vengono amplificati e comprendono pure quello di consultazione dei rappresentanti dei lavoratori, che deve precedere l'immissione in servizio o l'utilizzo di un sistema di AI ad alto rischio sul luogo di lavoro[12]. Si tratta di una novità importante sia perché finora, come anticipato, nell'AI Act la dimensione collettiva era sostanzialmente rimasta nell'ombra, sia perché nella nuova previsione la consultazione risulta funzionale alla ricerca di un accordo in conformità alla direttiva 2002/14/CE (che viene esplicitamente richiamata)[13]. Certo resta da indagare come "calare" la consultazione diretta all'accordo di cui alla direttiva 2002/14 all'interno della complessa (e articolata) cornice regolativa dell'AI Act. Per un verso, infatti, potrebbe ritenersi richiamato l'accordo sulle modalità di informazione dei lavoratori (ai sensi dell'art. 5 della citata direttiva) che valga a dettagliare il contenuto dell'art. 29, co. 5*bis* dell'AI Act (ossia l'informazione ai "dipendenti interessati che saranno soggetti al sistema")[14]. Per altro verso non può escludersi che la consultazione sfoci in un accordo ex art. 4, par. 4, lett. e), direttiva 2002/14 che, come noto, ha per oggetto le "decisioni che dipendono dal potere di direzione del datore di lavoro". D'altronde nell'AI Act la consultazione interviene "prima di mettere in servizio o utilizzare un sistema di AI ad alto rischio sul luogo di lavoro", sicché le decisioni alle quali si fa riferimento non riguardano necessariamente il ricorso a sistemi di AI, ma piuttosto, in sintonia con l'ambito materiale in cui la consultazione assume rilevanza[15], le modalità di utilizzo di tali sistemi e il loro impatto sull'organizzazione del lavoro e i contratti di lavoro. Da questo punto di vista, il testo emendato va salutato con favore perché pare accogliere l'auspicio di tarare i diritti di informazione e consultazione sulla rivoluzione tecnologica in atto, consentendo alle parti collettive di giocare "d'anticipo" rispetto alle scelte aziendali[16].

Infine almeno un cenno meritano i (timidi) passi in avanti relativi ai profili etici dell'AI che traspaiono da alcune (mere) affermazioni di principio quali la promozione di un approccio coerente e antropocentrico a un'AI etica e affidabile, un esplicito richiamo alla Carta dei diritti fondamentali dell'Unione europea e ai valori su cui si fonda l'Unione (nonché al diritto internazionale in materia di diritti umani) e, soprattutto, l'opportunità di prevedere misure per garantire lo sviluppo e l'utilizzo di un'AI eticamente integrata[17]. Invero tali novità non sembrano spingersi oltre i buoni propositi, non paiono cioè imprimere una nitida direzione di marcia nel senso auspicato dalla dottrina di identificare nella filosofia e nell'etica gli strumenti per realizzare il "*design* concettuale" funzionale a una *governance* delle tecnologie e alla costruzione di una

[12] Cfr. art. 29.
[13] Sulla direttiva 2002/14, v. L. ZOPPOLI, *Lavoro, impresa e Unione europea*, Franco Angeli, 2006.
[14] In tal senso M. DELFINO, *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *questa Rivista*, in questo numero.
[15] L. ZOPPOLI, *cit.*, p. 95
[16] In questi termini T. TREU, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, *Federalismi,* n. 9, 2022, p. 206.
[17] Cfr. considerando 4 *bis* e 9 *bis*, nonché art. 4 *bis*.

nozione di AI per il bene sociale (*AI4SG*)[18]. Né sembrano risolvere i dilemmi di natura etica gli emendamenti aventi a oggetto l'autonoma considerazione dei dati basati sulla biometria che concorre al superamento, anche sul piano strettamente normativo, della tradizionale (e ormai anacronistica) distinzione tra identificazione e identità[19].

Muovendo dalla cornice regolativa appena delineata e ancora in costruzione, il presente contributo si propone di indagare le ricadute della proposta di regolamento europeo sull'intelligenza artificiale nel contesto lavorativo con riguardo a quella specifica tipologia di dati personali rappresentata dai dati biometrici. A tal fine si procederà a un raffronto tra il perimetro delle (plurali) nozioni presenti nell'AI Act e la (compatta) nozione contenuta nel GDPR e si traccerà un primo bilancio delle implicazioni del disomogeneo apparato di tutela che caratterizza i due blocchi normativi e che induce ad auspicarne un *restyling* funzionale a un allineamento valoriale e operativo.

2. I dati biometrici nel quadro normativo europeo: l'approccio nel GDPR

I dati personali rappresentano il crocevia di un complesso scacchiere regolativo di rango europeo che si caratterizza per una marcata vocazione trasversale: prima il regolamento n. 679/2016 (d'ora in poi GDPR) e poi l'AI Act non sono stati concepiti per erigere un baluardo a difesa dei diritti dei lavoratori, ma sicuramente le nozioni adottate e le misure approntate sono foriere di ricadute sul piano giuslavoristico[20].

Focalizzando l'attenzione sul GDPR, si palesa utile rilevare che la stessa filosofia di fondo del regolamento europeo si invera nella responsabilizzazione di un generico titolare del trattamento (non necessariamente corrispondente a un datore di lavoro) e si traduce in ogni caso nell'obbligo di valutare il rischio di lesione dei diritti fondamentali della persona e di predisporre le misure idonee a prevenire o a mitigare tale rischio[21]. Il principio di *accountability* rappresenta, in altre parole, la chiave di volta del

[18] L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, 2022, p. 300. Per l'A. le caratteristiche eticamente rilevanti dell'AI4SG sono ravvisabili nella: falsificabilità e implementazione incrementale; garanzie contro la manipolazione dei predittori; intervento contestualizzato in ragione del destinatario; spiegazione contestualizzata in ragione del destinatario e finalità trasparenti; tutela della *privacy* e consenso dell'interessato; equità concreta; e semantizzazione adatta all'umano.

[19] E. C. RAFFIOTTA, M. BARONI, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioDiritto*, n. 1, 2022, p. 8.

[20] Questa scelta a monte si riverbera a livello nazionale: ben prima dell'adozione del GDPR (che, come noto, ha abrogato la Direttiva 95/46/Ce) con riguardo al codice in materia di protezione dei dati personali (d. lgs. 196/03) si è rilevata la mancanza nell'ordinamento italiano di una completa normativa settoriale per il trattamento dei dati personali nel rapporto di lavoro, v. A. BELLAVISTA, *La tutela dei dati personali nel rapporto di lavoro*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Giuffrè, 2004, p. 398; ID., *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in LDE, n. 1, 2023 p. 3.

[21] Cfr. A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci, 2018, p. 75 s.; EAD., *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi*, in A. BELLAVISTA, R. SANTUCCI, *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli, 2022, p. 131.

regolamento europeo nella misura in cui impone al titolare del trattamento di essere in grado di dimostrare che sono state adottate tutte le misure tecniche e organizzative idonee a garantire la conformità del trattamento ai principi di liceità, trasparenza e correttezza e ciò a prescindere dalla eventualità che i dati personali siano riferibili ai protagonisti di un rapporto di lavoro[22].

In prospettiva analoga muove la distinzione, interna al più ampio contenitore dei dati personali, tra dati comuni e dati particolari (o sensibili secondo l'etichetta coniata dal legislatore italiano). Questi ultimi ricomprendono una vasta gamma di informazioni che spaziano da quelle idonee a rivelare "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale" ai dati genetici, a quelli biometrici, ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il trattamento di tali dati risulta circondato da una visibile diffidenza che traspare dal divieto di raccogliere, comunicare e utilizzare gli stessi, allo scopo di "mettere al riparo" da penetranti ingerenze le informazioni che attengono alla sfera più intima dell'individuo in sé, lavoratore o cittadino che sia. Al contempo va sottolineato che tale divieto arretra in presenza di una serie di eccezioni tra cui - meritano qui di essere ricordate - il *consenso esplicito* dell'interessato per specifiche finalità o la *necessità del trattamento* dei dati biometrici per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui il trattamento "sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri" e al cospetto di "garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato"[23].

Esclusa l'inderogabilità del divieto, va segnalato che la delimitazione dell'ambito applicativo dello speciale regime viene perseguito mediante un'accorta perimetrazione delle diverse nozioni di dati particolari. In particolare il GDPR definisce biometrici quei "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". Decisivo, quindi, nell'impostazione del regolamento europeo è che tali dati personali siano ottenuti tramite un trattamento tecnico specifico e che consentano l'identificazione univoca o l'autenticazione di una persona fisica[24].

[22] L'unica previsione dedicata al trattamento dei dati personali nel contesto lavorativo è l'art. 88 che riconosce alla legislazione degli Stati membri e ai contratti collettivi la facoltà di introdurre "norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro". Nel senso che l'autonomia nazionale e collettiva deve limitarsi a interventi di dettaglio, senza alterare il principio di liceità del trattamento e la *ratio* del bilanciamento tra libertà di circolazione e diritto alla *privacy*, cfr. A. SARTORI, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Giappichelli, 2020, p. 46 s.

[23] Cfr. art. 9.2 lett. a) e b).

[24] Ai sensi del considerando 51 *Il trattamento di fotografie non costituisce sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando vengono trattate attraverso un dispositivo tecnico*

Basti pensare all'impronta digitale, alla scansione della retina, al riconoscimento facciale, che rappresentano poderosi e affidabili metodi per la verifica dell'identità di qualsivoglia utente di uno strumento o di un servizio[25].

In un'ottica più spiccatamente lavoristica, tale stringente costruzione si riflette sulla latitudine del dialogo che, all'indomani della riforma del 2015, connota *per tabulas* la relazione tra disciplina generale del trattamento dei dati personali e regole speciali di diritto del lavoro. Come dire che se in linea di principio il GDPR impatta sull'esercizio del potere datoriale - nel senso che impone l'adempimento di obblighi informativi, l'operatività del menzionato principio di responsabilizzazione e l'applicazione dei principi del trattamento - con specifico riguardo ai dati biometrici l'integrazione tra regole generali e norme lavoristiche speciali presuppone la natura particolare del dato su cui incide il potere. Soltanto il superamento della barriera di tipo definitorio consente cioè di affrontare la problematica relativa al ricorso ai dati biometrici del lavoratore e di verificare se al datore di lavoro sia precluso, nell'esercizio del proprio potere di controllo (*rectius* di controllo direttivo) captare tali dati particolari o se, piuttosto, occorra realizzare un bilanciamento fra interessi contrapposti[26]. Né pare trascurabile che la menzionata barriera risulta palesemente condizionata da un testo legislativo (quello in tema di *privacy*) figlio di un tempo in cui le potenzialità tecnologiche consentivano di decifrare soltanto alcuni tipi di dati connessi alla biometria e di conferire certezze esclusivamente sul piano dell'identificazione delle parti coinvolte, tagliando fuori tutta una serie di operazioni funzionali a risultati diversi dal riconoscimento e nondimeno assai rilevanti nella relazione lavorativa (si pensi all'attività di controllo direttivo finalizzata alla valutazione del dipendente).

3. Le (plurali) nozioni nell'AI Act

Decisamente più articolato il panorama regolativo presente nell'AI Act ove, nella versione iniziale, alla definizione di dato biometrico sovrapponibile a quella contenuta nel GDPR[27] si affiancava uno sventagliamento tipologico di sistemi di AI basati sull'utilizzo di dati biometrici, di modo che la loro

specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Diversamente sono tutelati come dati personali comuni.

[25] È appena il caso di ricordare che non sempre i dati del volto di una persona acquisiti mediante una foto sono dati biometrici in quanto la foto di per sé è neutra. Così è stato escluso che fossero dati biometrici i dati del volto dei partecipanti a un corso di formazione (in diretta streaming) acquisiti mediante foto scattate tramite la webcam del pc (ma in cui la verifica dell'identità dei partecipanti al corso non è automatizzata tramite l'ausilio di appositi strumenti *software* o *hardware*). Si veda la decisione del Garante Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming - 26 luglio 2017 [6826368].

Diverso il caso del riconoscimento facciale in cui il trattamento automatizzato riguarda immagini digitali che contengono il volto di un individuo allo scopo di identificarlo o verificarne l'identità o categorizzarlo. Cfr. la definizione di riconoscimento facciale elaborata dal Gruppo Art. 29 nella Opinion 02/2012 del 22 marzo 2022.

[26] Cfr. A. INGRAO, *Il controllo a distanza*, cit., p. 91 s.

[27] Cfr. art. 3 par. 33 e considerando 7.

configurazione come tipologia di sistemi di AI implicava il ricorso a tale specifica categoria di dati. Basti pensare alle prime definizioni contenute nella proposta di regolamento: il sistema di riconoscimento delle emozioni veniva fotografato come sistema di AI finalizzato all'identificazione o alla deduzione di emozioni o intenzioni di persone fisiche *sulla base* dei dati biometrici; il sistema di categorizzazione biometrica risultava connotato dall'*utilizzo di dati biometrici* di persone fisiche al fine di assegnarle a categorie specifiche, con un riferimento esplicito a fattori che concorrono a tale inserimento quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, l'origine etnica o l'orientamento sessuale o politico; o ancora il sistema di identificazione biometrica remota (cioè un sistema di AI finalizzato all'identificazione a distanza di persone fisiche mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, e senza che l'operatore del sistema di AI sappia in anticipo se la persona sarà presente e può essere identificata) che risulta a sua volta articolato in sistema di identificazione biometrica remota "in tempo reale" (in cui il rilevamento dei dati, il confronto e l'identificazione avvengono senza ritardi significativi) e sistema di identificazione biometrica remota "a posteriori" (ricavabile per differenza).

Tratto comune di tali sistemi di AI è proprio l'accorta definizione del loro presupposto: in tanto si configura un sistema (ad esempio) di riconoscimento delle emozioni, in quanto si utilizza un dato biometrico nell'accezione di cui al GDPR.[28]. Soluzione, questa, che al di là di ulteriori valutazioni, induce a qualificare questa tipologia di sistemi come derivati, nel senso che gli stessi sottendono la sussistenza della monolitica nozione di dato biometrico contenuta nel GDPR. Come dire che un sistema di riconoscimento delle emozioni è qualificabile come tale nella misura in cui risulta finalizzato all'identificazione o alla deduzione di emozioni o intenzioni di persone fisiche che vengono ricavate non già genericamente da elementi biometrici, bensì esattamente da dati biometrici.

Per cogliere le implicazioni di un simile assetto occorre muovere dal rilievo che le tecnologie di seconda generazione non utilizzano soltanto i tradizionali dati biometrici che consentono l'identificazione univoca di una persona (es. l'impronta digitale), ma ricorrono anche a dati che non sono biometrici in senso stretto perché non univoci (es. frequenza del polso, temperatura corporea, espressioni facciali non univoche come un'alzata di sopracciglio). Si tratta cioè di dati basati sulla biometria che possono consentire (o meno), o confermare (o meno) l'identificazione univoca. A titolo esemplificativo: un sistema di AI che utilizza la retina per l'accesso ai locali aziendali è un sistema alimentato da dati biometrici, un sistema di AI che usa segnali vocali non univoci come l'intonazione o il tremolio della voce per misurare la *performance* del lavoratore è un sistema alimentato da dati che non sono biometrici dal punto di vista tecnico-giuridico, nel senso che non rientrano nel perimetro della nozione sposata dal GDPR (e neppure

[28] Cfr. art. 3 parr. 34, 35, 36, 37 e 38.

nel campo di applicazione dell'AI Act, quantomeno nella versione iniziale che appunto si limitava a richiamare la nozione del GDPR).

Ora, come anticipato, l'assetto appena descritto è in corso di evoluzione e alcune novità significative si registrano tanto sul piano definitorio quanto - come accennato e come si illustrerà (v. *infra* § 4) - sulla classificazione in ragione del rischio dei sistemi di AI che utilizzano dati (anche non biometrici in senso stretto).

Tra le innovazioni foriere di ricadute interpretative sul piano del rapporto di lavoro va innanzitutto censita l'autonoma considerazione dei dati anche non biometrici in senso stretto (come quelli vocali evocati poc'anzi: tremolio, intonazione, accento, volume) che possono consentire (o meno) o confermare (o meno) l'identificazione univoca di una persona fisica, e che, secondo uno studio del 2021 commissionato dal Parlamento europeo, richiedono una regolamentazione particolarmente rigorosa in quanto si tratta di dati che una persona non può modificare facilmente[29]. Di qui l'inserimento, nell'ultima versione della proposta di regolamento, di una nuova categoria di dati basati sulla biometria che si affiancano a quelli biometrici di cui al GDPR (pure richiamati) e che sono caratterizzati dal fatto che lo specifico trattamento tecnico (da cui il dato viene ricavato) ha per oggetto segnali fisici, fisiologici o comportamentali di una persona fisica, che assumono rilevanza a prescindere dall'attitudine identificativa (univoca) di una persona fisica. Questa gamma di dati, secondo la nuova impostazione dell'AI Act, al pari di quelli biometrici possono alimentare i sistemi di AI di riconoscimento delle emozioni e di categorizzazione biometrica. Nel testo europeo si profila cioè all'orizzonte una equiordinazione dei dati biometrici e dei dati basati sulla biometria ai fini della configurazione dei sistemi di riconoscimento delle emozioni e di categorizzazione biometrica.

Di conseguenza non sembra azzardato ritenere che tale assetto apra nuovi scenari interpretativi con riguardo a tecniche di misurazione delle emozioni e degli stati d'animo dei lavoratori da parte del datore di lavoro nell'esercizio dei propri poteri[30]. Per definire i contorni di tali scenari occorre innanzitutto chiarire che di regola i soggetti presenti nel contesto lavorativo sono già noti e censiti, il che se da un lato comporta un affievolimento della valenza identificativa dei dati personali, dall'altro non esclude che i dati non univoci dei dipendenti siano suscettibili di alimentare sistemi di AI atti a misurare - per esempio - la *performance* lavorativa (si pensi per es. a un sistema di AI che utilizza la pressione sui tasti del pc per valutare il grado di concentrazione del lavoratore). Inoltre va considerato che proprio la natura non univoca di tali informazioni ne determina la fuoriuscita dall'orbita dei dati biometrici ai sensi del GDPR, con la conseguenza che in tali casi il datore dovrà attenersi "soltanto" alla disciplina prescritta per i comuni dati

[29] Cfr. *Study Biometric Recognition and Behavioural Detection – August* 2021, p. 68.

[30] Sul controllo dello stato mentale, delle emozioni e del livello di stress dei lavoratori mediante l'AI, v. L. GAMET, *Le travailleur et (les deux visages de) l'algorithme*, in *Droit Social*, 2022, n. 10, p. 779.

personali, disciplina che, come noto, trova il suo perno nel consenso del lavoratore[31]. *Last but not least* all'indomani del varo definitivo dell'AI Act all'apparato di tutela in materia di *privacy* si andrà ad affiancare un pacchetto di garanzie idonee (in qualche misura) a integrare quelle connesse all'ormai anacronistica impostazione del GDPR che - sul piano pratico e a dispetto dell'asse valoriale di riferimento (v. *infra* § 5)- consente lo slittamento nell'area dei dati comuni di dati che (non meno di quelli biometrici) attengono alla sfera più intima e incontrollabile della persona. In altre parole, in prospettiva la tutela dei lavoratori al cospetto di poteri datoriali esercitati per il tramite di sistemi di AI trova un primo baluardo nel tradizionale dialogo tra disciplina lavoristica e normativa generale sulla protezione dei dati, e un ulteriore argine nelle cautele previste per l'immissione sul mercato e per l'utilizzo da parte del *deployer* di sistemi che ricorrono a dati basati sulla biometria, e in particolare sistemi di riconoscimento delle emozioni e di categorizzazione biometrica.

4. *Segue.* La (nuova) classificazione dei sistemi di AI e le (insidie) delle difformi scelte regolative per i luoghi aperti al pubblico

Come anticipato la versione dell'AI Act approvata a giugno dal Parlamento europeo lascia inalterata la distinzione dei sistemi di AI in base al livello di rischio (inaccettabile, alto, basso o minimo) e, per converso, interviene sui relativi meccanismi di classificazione e sulla definizione dell'area dei sistemi ad alto rischio. Procedendo con ordine nella versione iniziale della proposta di regolamento si registrava una disomogenea classificazione dei "sistemi derivati" (cioè *basati* su dati biometrici) e, per contro, un'omogenea e compatta classificazione dei sistemi di AI destinati a essere utilizzati con riguardo all'occupazione e alla gestione dei lavoratori. Vale a dire che mentre nella versione dell'aprile 2021 i sistemi di AI destinati a essere utilizzati con riguardo all'occupazione e alla gestione dei lavoratori venivano classificati sempre "ad alto rischio", la tassonomia dei "sistemi derivati" figurava plurale e la relativa classificazione diversa secondo che si trattasse di sistemi di identificazione biometrica remota (anch'essi espressamente qualificati ad alto rischio[32]) oppure di sistemi di categorizzazione biometrica e di sistemi di riconoscimento delle emozioni (qualificati "a basso rischio"[33]).

Tale assetto alimentava alcuni equivoci interpretativi in ordine al carattere assorbente (o meno) della connotazione "ad alto rischio" dei sistemi di AI nell'accesso all'occupazione e nella gestione dei lavoratori

[31] Il trattamento dei dati personali ai fini del riconoscimento emotivo o della categorizzazione biometrica sarà soggetto solo all'articolo 6 del GDPR, compreso il semplice consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), e altri motivi legali disponibili per i dati personali in generale.

[32] Allegato III, testo aprile 2021.

[33] E assoggettati a un diverso regime con riguardo agli obblighi di trasparenza (ai sensi del considerando 70 - considerando 70 ove si sottolinea l'opportunità che le persone fisiche, quando sono esposte a un sistema di riconoscimento delle emozioni o a un sistema di categorizzazione biometrica ricevano una notifica - e dell'art. 52, testo aprile 2021).

quando entravano in gioco i dati biometrici del personale. Nell'originario approccio cioè residuavano spazi ermeneutici per dubitare dell'effetto dissolvenza della varietà tassonomica (e regolativa) allorché il sistema di AI basato su dati biometrici veniva utilizzato in ambito lavorativo (si pensi al ricorso alle caratteristiche biometriche o ai comportamenti individuali dei lavoratori ai fini dell'assegnazione dei compiti). Al di là di un generico (e non esplicitato) principio di prevalenza delle tutele più intense su quelle meno intense, infatti, nell'iniziale impostazione mancavano indizi decisivi per situazioni che si profilavano miste, e cioè di coesistenza di sistemi il cui rischio si presentava eterogeneo sul piano teorico. E anche le regole sulla sorveglianza umana - dirette a garantire che l'operatore-datore di lavoro non compia azioni o adotti decisioni sulla sola base dell'identificazione risultante dal sistema - non dissipavano tutte le perplessità nella misura in cui si riferivano a sistemi aprioristicamente inclusi nell'area dell'alto rischio, senza fornire indicazioni operative con riguardo a situazioni miste[34].

Ben più lineare l'ultimo testo dell'AI Act, che non solo supera il rigido approccio *top-down* per i sistemi ad alto rischio di cui all'Allegato III (introducendo - come anticipato - un controllo sul rischio che il sistema comporta, tra gli altri, sui diritti fondamentali), ma soprattutto inserisce tra i sistemi ad alto rischio di cui all'Allegato III alcune ipotesi di utilizzazione critica di sistemi biometrici e basati sulla biometria (compresi i sistemi di riconoscimento delle emozioni), che oggi presentano lo stesso inquadramento dei sistemi di AI in materia di occupazione, gestione dei lavoratori e accesso al lavoro autonomo[35]. Certo, si tratta di una classificazione relativa in quanto circoscritta ai casi critici e temporanea in quanto soggetta a revisione periodica (almeno annuale[36]), e nondimeno atta a dissipare eventuali dubbi circa l'operatività delle tutele più intense in una serie di situazioni miste[37].

Non altrettanto incisive in termini di novità le modifiche definitorie dei sistemi di identificazione biometrica. Come rilevato (v. § 3), nell'originaria versione della proposta di regolamento la delimitazione dei sistemi di identificazione biometrica remota risultava imperniata sul "confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento" e sul fatto "che l'operatore del sistema di intelligenza artificiale *non* sappia in anticipo se la persona sarà presente e potrà essere identificata" (mio il corsivo)[38]. Il che implicava una riduzione dell'ambito di riferimento delle previsioni

[34] Cfr. art. 14, testo aprile 2021. Sulla nozione di operatore (*deployer*) v. considerando 59, testo aprile 2021.
[35] Considerando 33*bis* e 36 del testo approvato il 14 giugno 2023 e Allegato III (come risultante dal coordinamento del testo del 9 maggio 2023 e del 14 giugno 2023). Peraltro va segnalato che nell'ambito ei sistemi di AI ad alto rischio, per la valutazione di conformità di alcuni sistemi (cioè quelli destinati a essere utilizzati per dedurre caratteristiche personali di persone fisiche sulla base di dati biometrici o basati su elementi biometrici, inclusi i sistemi di riconoscimento delle emozioni) si ritiene opportuno prevede il coinvolgimento di un organismo notificato, terzo e rispetto al fornitore (cfr. considerando 64 del testo approvato il 14 giugno 2023).
[36] Considerando 85 *bis*, testo approvato il 14 giugno 2023.
[37] Cfr. considerando 70 ove si sottolinea l'opportunità che le persone fisiche, quando sono esposte a un sistema di riconoscimento delle emozioni o a un sistema di categorizzazione biometrica ricevano una notifica.
[38] Art. 3.36, testo aprile 2021.

alle sole tecniche di identificazione connotate (innanzitutto) dalla mancata conoscenza, da parte dell'operatore del sistema di AI, della presenza della persona da identificare. Come dire che, nella sistematica dell'AI Act, si sottraevano al perimetro dei sistemi di identificazione biometrica remota tutte le ipotesi in cui l'operatore era già consapevole che il soggetto da identificare si sarebbe trovato in quel luogo. Possono addursi come esempi significativi di tali situazioni il ricorso a sistemi di AI all'interno dei locali aziendali: l'identità dei dipendenti, infatti, risulta nota e sussiste un'elevata probabilità che gli stessi vengano identificati dal sistema.

Tale impostazione figura in larga parte ripresa nella versione di giugno 2023, ove per un verso viene riproposta la definizione di sistema di identificazione biometrica remota agganciata al profilo conoscitivo dell'operatore circa la presenza del soggetto da identificare, per altro verso viene introdotta l'autonoma considerazione della verifica biometrica intesa come "verifica automatizzata di persone fisiche mediante il confronto dei dati biometrici di una persona fisica con i dati biometrici forniti in precedenza (verifica uno a uno, compresa l'autenticazione)"[39]. Soluzione, questa, che di certo valorizza il profilo della collaborazione del soggetto nella misura in cui inserisce nel perimetro definitorio di tali sistemi di AI la pregressa indicazione spontanea dei dati biometrici; ma al contempo circoscrive la rilevanza della partecipazione (*id est* collaborazione) alla verifica "uno a uno", continuando per contro a negarne l'incidenza nell'operazione di corrispondenza "uno a molti" ove assumeva (e assume) valore decisivo la consapevolezza della presenza della persona fisica in capo all'operatore del sistema di AI. Di qui il paradosso che, a parità di collaborazione, la delimitazione dell'area dei processi di corrispondenza ("uno a uno" oppure "uno a molti") risulta assai difforme (per esempio la partecipazione del soggetto mediante il posizionamento del pollice sullo scanner delle impronte digitali all'ingresso di un ufficio assume rilievo decisivo nella verifica biometrica, e non già nell'identificazione biometrica remota). La difformità di approccio tra i due tipi di sistemi appena evocati traspare pure da una diversa classificazione degli stessi: quelli di identificazione biometrica remota sono considerati ad alto rischio, mentre quelli destinati a essere utilizzati per la verifica biometrica (che include l'autenticazione) non sono inclusi in tale raggruppamento in quanto si ritiene che gli stessi non presentino un rischio significativo di pregiudizio per la salute, la sicurezza e i diritti fondamentali in quanto volti esclusivamente a confermare che una determinata persona fisica è la persona che dice di essere e convalidarne l'identità al solo scopo di accedere a un servizio, a un dispositivo o a locali[40].

Parallelamente una spiccata dissonanza si registra tra i sistemi di identificazione biometrica remota che, come si è accennato, si distinguono secondo che il rilevamento dei dati biometrici, il confronto e

[39] Art. 3.33 *quater*, testo approvato il 14 giugno 2023. Sulla differenza tra i perimetri dei sistemi v. anche considerando 8.
[40] Considerando 33 *bis*, testo 14 giugno 2023.

l'identificazione avvengano istantaneamente (o quasi e comunque senza ritardi significativi, cd. in tempo reale) o con un ritardo significativo (cd. a posteriori)[41]. A parità di perimetro definitorio, infatti, le scelte regolative interne si presentano decisamente divergenti: soltanto per i sistemi di identificazione biometrica remota "in tempo reale" viene introdotta una disciplina ad hoc, a sua volta articolata in base al luogo in cui il sistema viene utilizzato. Così nell'ultima versione della proposta di regolamento si vieta l'uso dei sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico, mentre analogo disfavore non si registra nelle ipotesi in cui il medesimo sistema di AI venga utilizzato in luoghi privati[42]. Per ritagliare l'area del divieto non basta, tuttavia, controllare il dato formale: esclusa la rilevanza della proprietà (pubblica o privata), il *discrimen* risulta ancorato al profilo dell'accessibilità del luogo in questione da parte di terzi. In quest'ottica la proposta di regolamento enumera, a titolo esemplificativo, come luoghi di natura privata (rispetto ai quali il divieto non opera) non solo le abitazioni, ma anche gli uffici, i magazzini e le fabbriche, che non sono di norma accessibili a terzi[43].

Ora, tale impostazione appare degna di nota perché alla (apprezzabile) riduzione degli spazi di manovra all'esercizio della sorveglianza nei luoghi fisici accessibili al pubblico, fa da contraltare una modulazione dell'incombenza normativa di incerta applicazione. Una volta agganciato lo specchio operativo dell'interdizione al dato dell'accessibilità da parte di terzi, il testo del regolamento indica una serie di spazi formalmente etichettati come pubblici (strade, come pure scuole, università, banche etc.) o privati (uffici, fabbriche etc.), ma potenzialmente, gli uni come gli altri, a connotazione mista. Come dire che nella banca come nella fabbrica si registra una (pressoché inevitabile) coesistenza di soggetti che con quel luogo hanno un mero "contatto" e di soggetti che si trovano in quello spazio in virtù di un contratto. Ora, è vero che nell'AI Act si rinviene (per i luoghi privati) una salvezza per l'accesso da parte di soggetti autorizzati o invitati e (in generale) si rimanda a un controllo di accessibilità caso per caso; è altrettanto vero, tuttavia, che, una volta captati, i dati biometrici dei soggetti che (a qualsivoglia titolo) si muovono in quello spazio possono essere confrontati (a fini identificativi) dal sistema di AI con i dati contenuti in un database di riferimento[44]. Insomma, per essere più chiari, le ultime novità dell'AI Act, pur apprezzabili in linea di principio, rischiano di sbiadire (ulteriormente) i confini del legittimo ricorso a sistemi di AI funzionali all'identificazione biometrica remota "in tempo reale" e di contribuire alla sovrapposizione (e confusione)

[41] Cfr. considerando 8, testo 14 giugno 2023.

[42] Art. 5.1., lett. d) che nel testo del 14 giugno non contempla la salvezza (e quindi il venir meno del divieto) per il perseguimento di obiettivi legati a fatti di rilevanza penale. E v. anche le altre modifiche relative all'art. 5 e il considerando 18.

[43] Considerando 9, art. 3.39, testo 14 giugno 2023.

[44] Se l'identificazione è in tempo reale tutta da valutare appare la nuova previsione (art. 5.1, lett. d*ter*, testo 14 giugno 2023) che vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di AI 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.

di dati biometrici del "mero" cittadino, del dipendente, del lavoratore parasubordinato o autonomo che insistono sul medesimo spazio fisico.

5. Alcune considerazioni conclusive sulla protezione dei lavoratori implicati nei sistemi di AI: difformità dei perimetri e duplicazione delle *Authorities*

Per concludere qualche considerazione sulle implicazioni del nuovo approccio definitorio e della nuova classificazione dei sistemi di intelligenza artificiale. Come anticipato, l'AI Act si pone come tassello aggiuntivo nel panorama regolativo europeo, destinato a convivere con il preesistente diritto dell'Unione e in particolare (per quanto qui interessa) con il GDPR. Tanto sul piano delle affermazioni di principio, quanto sul versante operativo, l'approccio è dichiaratamente di non belligeranza: per un verso infatti si richiamano le condizioni di applicazione e il rispetto dei requisiti fissati nel GDPR in una logica complessiva di integrazione delle regole[45], per altro verso si prevede un completamento in concreto dei due blocchi normativi nella misura in cui (per esempio) la valutazione d'impatto sui diritti fondamentali per i sistemi di AI ad alto rischio (a certe condizioni) viene condotta dall'operatore insieme alla valutazione d'impatto sulla protezione dei dati[46].

Nella stessa direzione si colloca la norma relativa al diritto alla spiegazione dei singoli processi decisionali che riconosce in capo alle "persone interessate soggette a una decisione presa dall'operatore sulla base dell'*output* di un sistema di AI ad alto rischio che produca effetti giuridici o che incida in modo analogo e significativo sulle persone stesse in un modo che esse ritengono abbia un impatto negativo sulla salute, la sicurezza, i diritti fondamentali, il benessere socioeconomico o qualsiasi altro dei loro diritti derivanti dagli obblighi stabiliti" nella proposta di regolamento, il diritto di chiedere all'operatore spiegazioni chiare e significative (ai sensi dell'art. 13.1) sul ruolo del sistema di AI nella procedura decisionale, sui principali parametri della decisione presa e sui relativi dati di *input*[47]. Una previsione, questa, emblematica delle potenzialità lesive dei moderni sistemi di AI e diretta a rafforzare l'apparato di tutela della persona approntato dal GDPR, le cui norme sono espressamente richiamate e fatte salve proprio in un'ottica di cumulo dei due meccanismi protettivi[48].

Parallelamente, nell'AI Act si ritrovano, qui e lì, sparpagliate in articoli diversi e lontani tra loro, previsioni relative a un'informativa cui è tenuto l'operatore che utilizza un sistema di AI ad alto rischio allorquando

[45] Basti pensare alla relazione che introduce la versione iniziale della proposta di regolamento, ma v. anche ad esempio considerando 2*ter*, 24, 33*bis*, 44, art. 2.5 *bis*, testo 14 giugno 2023.
[46] Cfr. art. 29 *bis*, testo 14 giugno 2023.
[47] Cfr. art. 68 *quater*, testo 14 giugno 2023 che al par. 2 esclude dal campo di applicazione della previsione i casi di uso di sistemi di AI per i quali il diritto dell'Unione o nazionale preveda eccezioni o limitazioni all'obbligo di cui al paragrafo 1 nella misura in cui tali eccezioni o limitazioni rispettino l'essenza dei diritti e delle libertà fondamentali e siano una misura necessaria e proporzionata in una società democratica.
[48] Cfr. art. 68 *quater*, par. 3, testo 14 giugno 2023.

tale sistema lo assiste in un processo decisionale o nell'assunzione di decisioni che riguardano persone fisiche e che ha come destinatarie proprio le persone interessate[49]. Al di là del (pure) rilevante rapporto di funzionalità di tale informativa rispetto al diritto a una spiegazione, ciò che preme sottolineare in questa sede è l'ampiezza del raggio di azione di quest'obbligo. Nella misura in cui la versione dell'AI Act approvata a giugno dal Parlamento europeo contempla tra i sistemi ad alto rischio anche alcuni casi di usi critici di sistemi biometrici e basati sulla biometria (compresi i sistemi di riconoscimento delle emozioni), tale obbligo di informativa finisce con l'offrire una tutela il cui spettro non collima con quello approntato dal GDPR perché copre sia l'area relativa al trattamento previsto per i comuni dati personali, sia quella riservata ai dati sensibili. Senonché, le tutele parallele risultano apprezzabili (e in linea con le declaratorie di principio dell'AI Act) solo quando i dati utilizzati rientrano in nozioni connotate da un perimetro definitorio comune ai due blocchi normativi; quando viceversa i dati che alimentano i sistemi di AI sono riconducibili a nozioni che sottendono un asse valoriale di riferimento non armonico, emerge con tutta evidenza l'opportunità di un intervento correttivo funzionale a un allineamento teorico e operativo. Semplificando al massimo, un conto è l'obbligo di informativa e il diritto alla spiegazione quando sono in gioco dati personali comuni, un conto è l'applicazione di tali meccanismi protettivi della persona quando risultano implicati dati sensibili, un altro ancora è l'operatività delle previsioni dell'AI Act al cospetto di dati che, stando all'impianto del GDPR, fuoriescono dall'area dei dati sensibili e slittano nell'area dei comuni dati personali (verosimilmente) per un difetto di taratura dello strumento regolativo rispetto alle potenzialità delle moderne tecnologie.

Il già auspicato intervento sulla consonanza (prima di tutto) assiologica tra l'AI Act e il GDPR avrebbe anche il vantaggio di semplificare il lavoro delle autorità nazionali di controllo chiamate a governare l'intelligenza artificiale. Già nella versione iniziale della proposta di regolamento, l'attuazione e il rispetto della nuova normativa risulta affidata ad autorità di controllo designate dagli Stati membri e affiancate da un comitato europeo per l'intelligenza artificiale (oggi ufficio dell'Unione europea[50]). Ora, è vero che tra i compiti dell'organismo europeo figurano (in generale) quelli di sostegno attivo delle autorità nazionali e (in particolare) di consultazione e di coordinamento, tra cui l'emanazione di pareri, raccomandazioni, consulenze o orientamenti su questioni relative all'attuazione del regolamento sull'AI; è altrettanto vero tuttavia che l'individuazione dell'autorità nazionale viene rimessa agli Stati membri e già si registrano determinazioni di Paesi che hanno optato per la creazione dell'ennesima e autonoma *Authority*[51]. Il che apre ulteriori spazi di sovrapposizione di competenze tra più autorità amministrative indipendenti, tutte

[49] Cfr. Considerando 84*ter*, art. 29.6*bis* e anche art. 13.2, testo 14 giugno 2023.
[50] Considerando 76, 49, 32 *bis*, testo 14 giugno 2023.
[51] Cfr. E. C. RAFFIOTTA, *Quale autorità governerà l'intelligenza artificiale*, in *Il Sole 24Ore*, 27 marzo 2023 che fa riferimento a quanto accaduto in Spagna.

potenzialmente legittimate a esaminare una stessa condotta con le lenti della disciplina settoriale[52]. Proprio in quanto i dati possono rappresentare un terreno di intersezione di più normative, la molteplicità di organismi preposti e la divergente ispirazione valoriale dei testi di riferimento possono rappresentare una miscela esplosiva tanto sotto il profilo dell'instabilità (teorica) del campo di gioco, quanto nell'ottica dello strabismo delle valutazioni concrete. Per evitare incertezze applicative e disinnescare il rischio di sconfinamenti e/o di esiti contraddittori, insomma, sembra opportuno promuovere un migliore coordinamento dell'apparato di regole che concorrono a formare l'AI Act e il GDPR.

[52] Emblematica al riguardo la cd. plurioffensività dei comportamenti lesivi del diritto antitrust, su cui M. MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018, p. 109 ss.; A. SOLA, *Ambiti di interesse per la regolazione delle economie dei dati nel rapporto tra diritto e tecnologia*, in *questa Rivista*, n. 10, 2023. Si pensi da ultimo alla questione pregiudiziale proposta dinnanzi alla Corte di Giustizia da un tribunale tedesco in relazione alla competenza dell'autorità nazionale garante della concorrenza a esaminare una violazione del divieto di abuso di posizione dominante utilizzando come indice della violazione del diritto *antitrust* la difformità della condotta dell'impresa rispetto alle norme a tutela dei dati personali (sentenza, 4 luglio 2023, causa C-252/21).