L'USO DELLE "TECNOLOGIE MOBILI" APPLICATE ALLA SALUTE: RIFLESSIONI AL CONFINE TRA LA FORZA DEL PROGRESSO E LA VULNERABILITÀ DEL SOGGETTO ANZIANO*

Di Claudia Irti

ABSTRACT. Il contributo indaga il regime giuridico applicabile alla massa di dati relativi alla salute dei cittadini reperibili grazie al sempre più diffuso utilizzo di servizi e applicazioni digitali mobili di uso quotidiano rivolte al "mondo della salute". La questione assume particolare rilievo quando il trattamento di questi dati riguarda la fascia di popolazione più avanzata di età, stante la quasi totale assenza di considerazione nelle tematiche connesse alla circolazione dei dati personali della condizione di individuo vulnerabile in ragione dell'avanzare dell'età.

The contribution investigates the legal regime applicable to the massive amount of data related to citizens' health that can be retrieved thanks to the increasingly widespread use of everyday digital mobile services and applications aimed at the "world of health". The issue becomes particularly relevant when the data processing concerns the most advanced age group of the population, given the almost total absence of consideration in the issues related to the circulation of personal data regarding the condition of vulnerable individuals due to advancing age.

1. Politiche europee sulla salute e nuove tecnologie: dallo e-*Health Action Plan* allo *European Health Data Space*.

Il progressivo e inarrestabile invecchiamento della popolazione mondiale[1] rappresenta uno dei cambiamenti demografici più significativi della storia recente, fattore che sta incidendo – e di più lo farà nei prossimi decenni – su molti equilibri sociali ed economici. La situazione emergenziale dovuta ai recenti eventi pandemici ha ben messo in luce come il settore sanitario-assistenziale è tra quelli che più risente di tale cambiamento, ponendo all'attenzione dell'Unione Europea e dei singoli Stati membri il problema immediato di sostenere ed efficientare un sistema che nel corso degli anni è stato gravemente 'depotenziato' (per le note esigenze di sostenibilità del quadro macroeconomico), finendo così con il riportare la sanità, dopo molte decadi, al centro dell'agenda politica.

Non sorprende, dunque, come una delle missioni del Piano Nazionale di Ripresa e Resilienza (la sesta) sia interamente dedicata alla "Salute", con uno stanziamento di 18,5 miliardi per finanziamenti destinati in larga parte a modernizzare e digitalizzare il sistema sanitario[2]. Molti dei problemi presenti e futuri di questo complesso settore si ritiene, infatti, possano e debbano essere risolti attraverso l'implementazione dell'uso delle nuove tecnologie e, più in particolare, dell'intelligenza artificiale a servizio della salute, accelerando quel processo già in atto da alcune decadi che va sotto il nome di *e-Health*[3].

Con il termine *e-Health* si è soliti far riferimento a quell'ambito sanitario che emerge nell'intersezione tra informatica medica, sanità pubblica e attività economica, ricomprendente tutti quei servizi e quelle informazioni sanitarie forniti o condivisi attraverso l'uso di tecnologie informatiche e di telecomunicazione[4], anche se, in senso ampio, lo stesso esprime piuttosto un modo di pensare, un'attitudine e un impegno per migliorare l'assistenza sanitaria utilizzando le tecnologie dell'informazione e della comunicazione.

È un ambito in costante crescita nei Paesi europei ed è stato oggetto di attenzione da parte della Commissione europea fin dal 2004, quando fu pubblicato il primo piano d'azione per implementare la cosiddetta 'sanità digitale': l'*e-Health Action Plan*[5].

Più di recente - con la Comunicazione *A European Health Data Space: harnessing the power of health data for people, patients and innovation*[6], che accompagna la Proposta di Regolamento sullo spazio europeo dei dati sanitari[7] per la costituzione di uno *European Health Data Space* - la Commissione è tornata a ribadire come la digitalizzazione

---

* Il presente contributo è destinato agli Studi in onore di Rosalba Alessi.

[1] "La rivoluzione silenziosa" fu la suggestiva definizione utilizzata Kofi Annan, Premio Nobel per la Pace e già Segretario Generale delle Nazioni Unite (ONU) nel 2002.

[2] Tra gli obiettivi del PNRR si segnala quello di "potenziare e innovare la struttura tecnologica e digitale del servizio sanitario nazionale a livello centrale e regionale al fine di garantire un'evoluzione significativa delle modalità di assistenza sanitaria, migliorando la qualità e la tempestività delle cure; valorizzando il ruolo del paziente come parte attiva del processo clinico assistenziale; e garantendo una maggiore capacità di governance e programmazione sanitaria guidata dalla analisi dei dati, nel pieno rispetto della sicurezza e della tutela dei dati e delle informazioni".

[3] Secondo lo studio *Artificial Intelligence and life in 2030 – One Hundred Year Study on Artificial Intelligence,* pubblicato dall'Università di Stanford nel 2016, il settore sanitario è uno degli otto settori in cui l'impatto dell'intelligenza artificiale sarà maggiormente rilevante. Il mercato dell'intelligenza artificiale è inoltre uno dei più fiorenti; secondo un report della *Coherent Market Insights* il mercato dell'AI, dal valore attuale di 3285 milioni di dollari, crescerà di oltre ventidue volte nei prossimi sei anni, arrivando al valore complessivo di 74650 milioni di dollari nel 2027 (https://www.coherentmarketinsights.com/market-insight/artificial-intelligence-in-healthcare-market-436)

[4] G. EYSENBACH, *"What is e-health?"*, in *Journal of Medical Internet Research*, III, 2, 20, 2001 (traduzione della scrivente).

[5] Adottato nel 2004 attraverso la Comunicazione 2004/356 e poi rinnovato per mezzo della Comunicazione 2012/736. Successivamente con la Comunicazione 2018/233, «relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana», la Commissione è tornata ad enfatizzare i benefici ottenibili grazie alla digitalizzazione dei sistemi sanitari, fra cui la possibilità di «accrescere il benessere di milioni di cittadini e cambiare radicalmente il modo in cui i servizi sanitari e assistenziali vengono forniti ai pazienti», sottolineando come lo sviluppo dei servizi sanitari digitali consentirebbe di «sostenere la riforma dei sistemi sanitari e la loro transizione verso nuovi modelli di assistenza, basati sui bisogni delle persone, e (di) consentire un passaggio da sistemi incentrati sugli ospedali a strutture assistenziali integrate e maggiormente basate sulle comunità». La Commissione europea ha altresì chiarito come il raggiungimento di tali obiettivi sia stato sinora frenato dall'assenza di un'effettiva interoperabilità dei dati sanitari e dalla frammentazione del mercato, fattori che «rappresentano un ostacolo ad un approccio integrato alla prevenzione delle malattie e ad una cura e assistenza meglio adattate alle esigenze dei cittadini». Nel contesto attuale, infatti, le attività di condivisione e scambio dei dati sanitari a livello europeo sono limitate alla cooperazione volontaria fra paesi membri, i quali si avvalgono a tal fine di una *eHealth Digital Service Infrastructure:* la cooperazione è tuttavia rimasta circoscritta allo scambio dei fascicoli sanitari dei pazienti e delle prescrizioni in formato telematico. È per questo motivo che la Commissione europea ha assunto un impegno concreto volto all'adozione di standard europei per la qualità, affidabilità e sicurezza dei dati sanitari e per l'adozione di un formato europeo che renda possibile la standardizzazione delle cartelle cliniche elettroniche e quindi lo scambio (Raccomandazione (UE) 2019/243 della Commissione, del 6.2.2019, relativa a un formato europeo di scambio delle cartelle cliniche elettroniche).

[6] COM(2022) 196 del 3.5.2022.

[7] COM(2022) 197 del 3.5.2022.

sia assolutamente essenziale per il futuro dell'assistenza sanitaria e la trasformazione digitale sia fondamentale per fornire un'assistenza sanitaria migliore ai cittadini, per costruire sistemi sanitari economicamente e qualitativamente stabili e affidabili, per sostenere la competitività e l'innovazione a lungo termine nel settore medico dell'UE. In tale documento la Commissione ha altresì riaffermato come i dati siano una risorsa indispensabile che, se utilizzata in modo responsabile e nel pieno rispetto dei diritti fondamentali, possa apportare immensi benefici a ogni aspetto della nostra vita quotidiana, compresa la salute. Sebbene ogni secondo venga generata un'enorme quantità di dati sulla salute, che fornisce ai servizi sanitari e ai ricercatori potenziali informazioni preziose[8], la complessità e la divergenza di norme, strutture e processi all'interno e tra gli Stati membri rende difficile accedere e condividere facilmente i dati sanitari; ciò crea ostacoli all'erogazione dell'assistenza sanitaria e all'innovazione, impedendo ai pazienti di beneficiare dei conseguenti vantaggi. Per permettere all'UE di sfruttare appieno il potenziale offerto da uno scambio, un uso e un riutilizzo sicuri e protetti dei dati sanitari, la Commissione ha dunque presentato una proposta legislativa volta a creare uno spazio europeo dei dati sanitari, per consentire alle persone di assumere il controllo dei propri dati e di utilizzarli per una migliore erogazione dell'assistenza sanitaria, ampliando anche in questo settore la Strategia europea dei dati[9] il cui obiettivo finale è quello di «incrementare l'utilizzo e la domanda di dati e di prodotti e servizi basati sui dati in tutto il mercato unico».

2. La *Mobile-health.*

Indubbiamente il funzionamento e l'efficientamento delle strutture tecnologiche impiegate in ambito sanitario dipendono e dipenderanno sempre più dal costante monitoraggio dei dati sanitari e comportamentali in grado di rivelare lo stile di vita dei singoli individui, oggi potenzialmente possibile in via capillare grazie all'utilizzo di sistemi di intelligenza artificiale che permettono l'immagazzinamento e la stratificazione di un enorme quantità di dati di singoli e di gruppi di individui.

In forma più tradizionale il monitoraggio dei parametri vitali e sanitari dei pazienti - attività necessaria per la diagnosi e il controllo di molte patologie - è perlopiù stato attuato mediante l'utilizzo di dispositivi medici portatili sotto la direzione e il controllo di un'istituzione sanitaria (si pensi ai dispositivi di monitoraggio cardiaco come l'holter).

Oggi, tuttavia, si assiste all'ampia diffusione di applicazioni *software* destinate al controllo e raccolta di dati sanitari, parametri vitali e dati comportamentali degli individui, progettate per funzionare su dispositivi portatili di uso comune come *tablet*, *smartphone* e *smartwatch*, capaci di monitorare attraverso biosensori e analizzare attraverso l'intelligenza artificiale la condizione fisica dell'utente: i valori biologici degli utilizzatori vengono monitorati costantemente e in tempo reale, raccolti, analizzati e restituiti attraverso statistiche mediante l'uso di apposite app - le c.d. *Health app* - in grado di fornire *output* relativi al miglioramento del proprio stile di vita e stato di salute, anche senza che un tale processo sia assoggettato ad uno specifico controllo medico[10].

L'assenza di controllo da parte di un sanitario, esercitato anche solo a distanza, esclude che l'attività di monitoraggio possa essere fatta rientrare nel più definito ambito della c.d. telemedicina[11] - intendendosi con tale espressione fare riferimento a quella modalità di erogazione di assistenza sanitaria effettuata "tramite il ricorso a tecnologie innovative, in particolare alla *Information and Communication Technologies* (ICT), in situazioni in cui il professionista della salute e il paziente non si trovano nella stessa località"- ma non esclude che la stessa possa essere assoggettata a quella apposita normativa comunitaria[12] diretta a regolamentare l'utilizzo dei

[8] Si stima che il riutilizzo dei dati sanitari abbia un valore di circa 25-30 miliardi di euro all'anno. Si prevede che questa cifra raggiunga circa 50 miliardi di euro entro 10 anni.

[9] *A European data strategy,* 2020.

[10] Un fenomeno, quest'ultimo, che viene nomenclativamente ricondotto nella c.d. "*mobile-health*" (*mHealth*), espressione con la quale si fa riferimento all'insieme di "tecnologie mobili" a comunicazione *wireless* applicate in ambito medico sanitario o in ambiti correlati alla salute, definizione contenuta al punto 1 del documento *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, approvato dal Comitato Nazionale per la Bioetica il 28.5.2015.

[11] La cui definizione è fornita dal documento di *soft law* "Telemedicina – Linee di indirizzo nazionale" approvato d'intesa tra Governo, Regioni e Province autonome di Trento e Bolzano nel 2014. In proposito si vedano i rilievi di C. BOTRUGNO, *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Pol. dir*., 4, 2014, 639 ss., che rileva come "Rispetto alla più ampia sfera dell'*e-health*, (…) il tratto distintivo della telemedicina risiede nel presupporre comunque una forma di interazione, in tempo reale o differito, tra il paziente e il professionista sanitario. Conformemente all'orientamento adottato in sede comunitaria, infatti, la telemedicina presuppone l'erogazione di una prestazione medica, ovvero di una *performance* di natura intellettuale, resa da un professionista abilitato all'esercizio della professione".

[12] Il Reg. (UE) 2017/745 e il Reg. (UE) 2017/746 (succeduti alle Direttive Comunitarie 93/42/CEE sui dispositivi medici, 98/79/CE sui dispositivi medici diagnostici in vitro e 90/385/CEE sui dispositivi medici impiantabili attivi) che regolamentano in modo uniforme in tutti i Paesi della Unione Euro-

"dispositivi medici". In base alla definizione fornita dal Reg. (UE) 2017/745, infatti, anche il *software* progettato per funzionare su apparecchiature portatili di uso comune può essere considerato "dispositivo medico"[13], purché sia esplicitamente destinato dal fabbricante a essere impiegato per una o più destinazioni d'uso medico (quali ad esempio diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie) [14].

La distinzione tra *Medical MobileApp* - qualificate quali dispositivi medici[15] e sottoposte a specifiche forme di validazione scientifica, autorizzazione e controllo da parte di appositi organismi – e generiche *Health MobileApp* - di libera commercializzazione - risiede dunque in una espressa destinazione d'uso del fabbricante.

Una distinzione che, evidentemente, non può non suscitare alcune perplessità.

Ai produttori di software "per la salute" che intendono sfuggire alla regolamentazione destinata ai soli dispositivi medici è infatti sufficiente presentare i loro servizi digitali come semplici strumenti di controllo del benessere e dello stile di vita, per rimanere "vicini" al mercato della salute, tenendosi a debita distanza da quel complesso di regole e controlli cui sono assoggettati i soli software qualificati quali dispositivi medici. Una scelta economicamente premiante se solo si considera – come opportunamente evidenziato dal Comitato di Bioetica nel documento *"Mobile-health" e applicazioni per la salute: aspetti bioetici"* – che "*ciò che tende a prevalere nel mercato delle* app *sulla salute è, in luogo della valutazione di esperti, il parere delle persone che lo hanno scaricato e provato. È questo il criterio di valutazione in questo campo, in cui tutto cambia molto velocemente: ciò che ha un impatto reale è ciò che gli utenti giudicano come affidabile, ricavabile dal numero dei download e dalle valutazioni espresse in rete. In questo senso ciò che guida gli utenti ad installare una app non è tanto la validazione scientifica quanto piuttosto il tasso di gradimento in rete espresso dai consumatori*" [16].

Tenuto conto che le informazioni generali riferite alla salute e al benessere devono essere comunque accurate e affidabili, perché su di esse si basano scelte e decisioni che possono incidere negativamente sulla salute degli individui, resta aperto il problema di come sopperire alla mancanza e carenza di un'adeguata validazione scientifica delle citate applicazioni rispetto a parametri di sicurezza e di efficacia, potendosi al momento - in assenza di previsioni normative che subordinino la commercializ-

pea il settore dei dispositivi medici, demandano all'Autorità Competente di ciascun Stato membro la designazione degli Organismi Notificati, che valutano, controllano e verificano i dispositivi medici. Per maggiori approfondimenti sulla disciplina si veda G. CAPILLI, *Diritto Privato sanitario*, Pisa, 2022, 54 ss.

[13] A norma dell'art. 2 Reg. (UE) 2017/745 è considerato dispositivo medico "qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: - diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, - diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, - studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, - fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere qua giovata da tali mezzi".

[14] "È necessario precisare che il software specificamente destinato dal fabbricante a essere impiegato per una o più delle destinazioni d'uso mediche indicate nella definizione di dispositivo medico si considera un dispositivo medico, mentre il software destinato a finalità generali, anche se utilizzato in un contesto sanitario, o il software per fini associati allo stile di vita e al benessere non è un dispositivo medico. La qualifica di software, sia come dispositivo sia come accessorio, è indipendente dall'ubicazione del software o dal tipo di interconnessione tra il software e un dispositivo" (considerando 19 Reg. (UE) 2017/745). Rilievo essenziale viene attribuito alla *destinazione d'uso* impressa dal fabbricante, e ciò a prescindere dal contesto nel quale l'applicazione è utilizzata e dalle modalità di utilizzo. In tal senso si era già espressa la Corte di Giustizia dell'Unione Europea nella sentenza relativa alla Causa C-329/16, *Snitem e Philips France*, la quale - nel vigore della dir. 93/42/CEE – aveva affermato che per ricadere nell'ambito di applicazione della direttiva, non è sufficiente che un software sia utilizzato in un contesto medico, ma occorre anche che la sua finalità, definita dal fabbricante, debba essere specificamente medica. Contestualmente ha ritenuto irrilevante, ai fini della qualificazione come dispositivo medico, il fatto che il software agisca o non agisca direttamente sul corpo umano, rinvenendo quale unica condizione fondamentale quella legata alla sua finalità: pertanto un software che tra le sue funzionalità, consenta l'utilizzo dei dati personali di un paziente, allo scopo di rilevare le controindicazioni, le interazioni tra medicinali e le posologie eccessive, costituisce, quanto a tale funzionalità, un dispositivo medico, indipendentemente dal suo agire o meno direttamente nel o sul corpo umano.

[15] La *Food and Drug Administration* (FDA) statunitense ha pubblicato nel settembre del 2019 una proposta (*Proposed regulatory framework for modifications to artificial intelligence/machine learning-based software as a medical device*) su come intende applicare la sua regolamentazione al *software* destinato alle piattaforme mobili, utilizzate in ambito medico, le Applicazioni Mobili Mediche (*Mobile Medical App*). Anche per la FDA la destinazione d'uso di una Applicazione Mobile determina se il relativo *software* soddisfa la definizione di "dispositivo medico" e, come indicato nel 21 CFR 801.4, la destinazione d'uso può essere dichiarata attraverso l'etichettatura, materiale pubblicitario, o attraverso dichiarazioni orali o scritte da parte dei fabbricanti o dei loro rappresentanti. L'Applicazione Mobile è un dispositivo medico quando la sua destinazione d'uso è rivolta alla: diagnosi, cura, attenuazione, trattamento o prevenzione di una malattia, oppure incide sulla struttura o su una funzione del corpo dell'uomo.

[16] In *"Mobile-health" e applicazioni per la salute: aspetti bioetici",* documento risalente al maggio del 2015, 8-9, *cit.*; per riferimenti bibliografici si veda la nota 5.

zazione di *app* non classificabili come dispositivi medici ad apposita sperimentazione[17] - fare appello al solo senso di auto-responsabilità dei produttori.

Sebbene sia opinione comune che i numerosi software legati al mondo della salute rappresentino un utile strumento di controllo e promozione per una vita più attiva e più sana, l'ampia diffusione degli stessi comporta un concreto rischio che gli utenti inizino a confidare eccessivamente nell'auto-monitoraggio e nelle diagnosi "fai da te" indotte dalle elaborazioni di algoritmi non validati da specialisti del settore medico.

La questione è degna di particolare attenzione soprattutto allorquando vengano presi in considerazione utilizzatori più vulnerabili quali gli anziani, presumibilmente meno capaci di valutare il grado di funzionalità e affidabilità del singolo servizio. Ne discendono in ambito giuridico riflessioni che spaziano dal versante etico-programmatico – destinate a sollevare dubbi circa l'opportunità di implementare l'uso della tecnologia nell'ambito della salute, se non supportata da adeguati programmi di accrescimento delle abilità e competenze digitali degli utenti meno avvezzi all'uso di tali strumenti e da una rete di relazioni umane che comunque assicuri loro il necessario supporto[18] – a quello della responsabilità[19] – ove si discute di chi e a che titolo debba rispondere dei possibili pregiudizi dannosi che l'utente possa subire a causa di indicazioni e "suggerimenti" impartiti dall'intelligenza artificiale[20].

Questo complesso scenario pone, tuttavia, un'altra questione di rilievo che si intende affrontare: quella relativa al regime giuridico applicabile alla enorme massa di dati relativi alla salute dei cittadini reperibili proprio grazie al diffuso utilizzo di servizi e applicazioni digitali mobili di uso quotidiano rivolte al "mondo della salute", e agli strumenti e alle modalità con le quali accrescere la consapevolezza degli utenti, specie se anziani, come partecipanti sia attivi che passivi di questo "fiorente mercato".

2.1. La base giuridica per il lecito trattamento dei dati relativi alla salute nelle *Medical MobileApp.*

Nell'indagare dal punto di visuale prescelto quale sia il regime giuridico di trattamento applicabile all'uso massivo dei dati nella *mobile health* è opportuno partire da due ordini di considerazioni: l'assenza all'interno del Reg. (UE) 2016/679 di uno statuto giuridico specifico per i dati sanitari (nel senso che si verrà a precisare); l'assenza di attenzione nelle tematiche connesse alla circolazione dei dati personali della condizione di individuo anziano e/o vulnerabile.

La prima considerazione muove dal fatto che nonostante il Regolamento fornisca una definizione di «dati relativi alla salute» come quei dati di una persona fisica in grado di rilevare «informazioni relative al suo stato di salute» (all'art. 4, § 1, n.15), specificandone ulteriormente il contenuto al considerando 35[21], gli stessi vengono fatti rientrare nella

[17] La *Food and Drug Administration* (FDA) ha dichiarato che intende comunque monitorare le prestazioni di quelle Applicazioni Mobili che non sembrano rientrare nella definizione di dispostivi medici secondo le indicazioni date, per determinare se dovessero essere necessarie azioni diverse o aggiuntive al fine di proteggere la salute pubblica, ricordando ai produttori Applicazioni Mobili di essere comunque messi nella condizione di scegliere se avviare spontaneamente il processo di autorizzazione seguendo il *Quality System Regulation* (che comprende le buone pratiche di fabbricazione) nella progettazione e nello sviluppo delle loro applicazioni mobili .

[18] "Un (..) problema etico, con particolare riferimento agli anziani, riguarda il divario digitale o alla disuguaglianza di accesso alle nuove tecnologie dell'informazione e della comunicazione; bisognerebbe infatti fornire strumenti di accesso alle nuove tecnologie e implementare capacità e motivazione all'uso delle nuove tecnologie informatiche, affinché tutti possano partecipare pienamente alla società e non essere emarginati dalla rete. Al tempo stesso va garantito un accesso alternativo ai servizi, specie quelli sanitari, per chi preferisce non entrare nella sfera digitale, senza per questo dover subire discriminazioni. La promozione dell'accesso per tutti deve essere accompagnata da un'adeguata educazione alle abilità digitali e alle competenze digitali, anche con una motivazione per chi non vuole le nuove tecnologie informatiche", L. Palanzani, *Etica nella gestione dei dati digitali e persone anziane*, in *Ipotesi per il futuro degli anziani*, a cura di C. Sangalli e M. Trabucchi, Bologna, 2021, 67 ss., 74. Per altre riflessioni di natura etico-giuridica G. Di Rosa, *I robot medici*, in *Mercato e persona*, 1, 2022, 12 ss.

[19] C. Perlingieri, *Responsabilità civile e robotica medica*, in *Tecnologia e dir.*, 2020, 173 ss.

[20] In argomento G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ.*, 2021, 823 ss.; A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo,* in *Nuova giur. civ. comm.,* 2020, 1344 ss.; G. Comandè, *Multilayered (Accountable) Liability for Artificial Intelligence*, in *Liability for Artificial Intelligence and the Internet of Things,* a cura di S. Lohsse, R. Schulze, D. Staudenmayer, Baden-Baden, 2019, 168 ss.

[21] Considerando 35 Reg. (UE) 2016/679 «Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla dir. 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio

macro categoria dei dati "particolari" (insieme a ogni altra informazione da cui sia possibile evincere l'orientamento sessuale, l'origine razziale o etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'appartenenza sindacale degli individui) la cui disciplina è dettata dall'art. 9 dello stesso Regolamento[22].

In quanto genericamente rientrante nella categoria dei dati personali, il trattamento dei dati sanitari è dunque da considerarsi vietato, salvo non si ricada in una delle deroghe appositamente previste dalla citata norma, che ruotano attorno ai due poli (a) della autorizzazione per casi eccezionali e (b) del consenso dell'avente diritto.

Il primo ordine di eccezioni comprende una serie di ipotesi in cui entrano in gioco interessi superindividuali (quali ricerca scientifica, salute collettiva etc.) o una finalità di ordine terapeutico[23], previsione quest'ultima che rende superfluo l'espresso consenso alla raccolta e gestione dei dati personali ai fini di diagnosi e cura ogni qual volta il "paziente" abbia deciso di assoggettarsi alle terapie[24], esprimendo il consenso informato alla luce della l. 22.12.2017, n. 219[25], dal momento che i dati vengono trattati sotto la responsabilità del medico, dei suoi ausiliari o comunque di altri soggetti investiti del rapporto di cura in essere, nel rispetto di specifici obblighi di riservatezza.

Una base di trattamento che può considerarsi operante, in linea di massima, anche in quelle ipotesi in cui l'attività terapeutica avvenga utilizzando servizi di telemedicina[26], in quanto trattasi comunque di prestazioni sanitarie fruibili a distanza sotto la direzione e il controllo di un'istituzione medica per le quali è richiesto all'utente/paziente il rilascio di uno specifico consenso informato al trattamento di cura, perlopiù in forma digitalizzata[27].

La questione assume, tuttavia, un più elevato grado di complessità allorquando si prendano in considerazione applicazioni con funzioni di intelligenza artificiale e apprendimento automatico in grado di indicare al paziente una terapia o un protocollo *in sostituzione del medico* o *in sua assenza*, ipotesi nelle quali i dati dei pazienti/utenti sono evidentemente trattati per fornire decisioni automatizzate destinate ad impattare in maniera diretta sulla loro stessa salute e sul loro benessere[28]. Ai sensi del § 4 dell'art. 22 del Regolamento, infatti, le decisioni automatizzate che si servano di «dati particolari» sono vietate «a meno che non sia d'applicazione l'art. 9, § 2, lettera *a* o *g* e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato». Ne consegue che l'utilizzo automatizzato di questi dati risulta lecito solo nel caso in cui vi sia il consenso dell'interessato (art. 9, § 2, lett. a, o quando rilevino motivi d'interesse pubblico (art. 9, § 2, lett. g).

di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro».

[22] Il quadro normativo delineato dal Reg. (UE) 269/2016 non muterebbe con l'approvazione della Proposta di Regolamento sullo spazio europeo dei dati sanitari (*cit.*), la quale persegue l'obiettivo primario di migliorare l'accesso e lo scambio in ambito europeo di diversi tipi di dati sanitari elettronici (quali cartelle cliniche elettroniche, dati genomici, registri di pazienti ecc.) nel pieno rispetto di quanto stabilito dal Regolamento rispetto ai dati sanitari personali e alle garanzie supplementari per il loro trattamento da quest'ultimo sancite (art. 1, § 4).

[23] Cfr. M. CIANCIMINO, *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, Napoli, 2020, 36 ss.

[24] Il d. lgs. 10.8.18, n.101 ha adeguato il nostro ordinamento al Reg. (UE) 269/2016, facendo venire meno l'obbligo di consenso quando i dati sono tratti per finalità di diagnosi e cura (art. 2-septies, Codice Privacy). Fornendo chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – Provvedimento 7.3.2019, n. 5 - il Garante della privacy ha però precisato che le finalità di cura devono essere solo quelle essenziali, mentre quelle non strettamente necessarie richiedono il consenso espresso.

[25] Dal che si suggerisce oggi di distinguere tra consenso informato e consenso informatico posto che dal punto di vista puramente semantico la differenza tra consenso informato e consenso al trattamento dei dati personali è fuorviante. Ed essendo i due termini molto simili si ha il rischio di trarre in inganno i pazienti sebbene i due consensi coprano ambiti molto differenti

[26] Anche in tali ipotesi è tuttavia necessario il consenso espresso del paziente quando ai dati dell'interessato possono aver accesso soggetti diversi dai professionisti sanitari o da altri soggetti tenuti al segreto professionale.

[27] Moduli firmati per via telematica, scambi di messaggi, registrazioni video, etc., forme che raccolgono (o dovrebbero raccogliere) l'espressione della volontà del paziente quale frutto, tuttavia, di un processo informativo e anamnestico basato sull'interazione personale di tipo relazionale: l'art. 1, 4° co., l. 22.12.17, n. 219 prevede che «il consenso informato, acquisito nei modi e con gli strumenti più consoni alle condizioni del paziente, è documentato in forma scritta o attraverso videoregistrazioni o, per la persona con disabilità, attraverso dispositivi che le consentano di comunicare». Un livello di digitalizzazione della sanità, quello da ultimo descritto, che comunque già solleva molti quesiti circa le possibili ricadute su persone fragili e vulnerabili "quali l'accessibilità delle tecnologie (la loro disponibilità e comprensibilità), l'usabilità e l'accettabilità familiare e sociale delle tecnologie, la definizione e sperimentazione di modelli decisionali non consueti che fanno riferimento a pratiche di decisione condivisa del paziente con la famiglia – si pensi alla situazione di anziani che non possono essere definiti incapaci ma le cui capacità cognitive si sono indebolite e devono essere supportati all'interno del contesto familiare e sociale in modo tale che siano aiutati a affrontare tutte le fasi della cura digitale, fra cui il consenso informato non fornito *de visu*", così C. DI COSTANZO, *Consenso informato e impiego delle tecnologie. Implicazioni per il diritto pubblico e (auspicabile) ibridazione delle pratiche di cura*, in *Media Laws*, 2, 2022, 180 ss., spec. 192.

[28] C. BOTRUGNO, *Tecnologie dell'informazione e della comunicazione e tutela della salute le sfide aperte tra protezione, circolazione e riutilizzo dei dati*, in *Diritto e questioni pubbliche*, 2020, 137 ss., 150; M. CIANCIMINO, *op. cit.*, 95.

La base giuridica per il trattamento dei dati di pazienti da parte di sistemi di intelligenza artificiale integrati in *Medical mobile-app* è dunque, nella maggior parte dei casi[29], il consenso esplicito; un consenso che, a ben guardare, diventa veicolo per una elaborazione degli stessi funzionale all'*output* decisionale, una "prescrizione di cura" - una terapia o un protocollo, ad esempio - ma anche una diagnosi predittiva originata dall'applicazione, peraltro non necessariamente prevedibile o controllabile *ex ante*, sulla base dei rischi connessi alle peculiarità del singolo sistema[30]. Esprimendo il consenso richiesto dall'articolo 22, § 4 del Regolamento l'interessato/utente/paziente è così chiamato a manifestare la sua (forse consapevole) approvazione sia al trattamento automatizzato dei dati sanitari che alla connessa decisione terapeutica automatizzata, di modo che il consenso del paziente rilasciato quale manifestazione della sua autodeterminazione informativa finisce per intersecarsi - se non addirittura sovrapporsi - con quello rilasciato quale espressione della sua autodeterminazione terapeutica[31].

L'applicazione della normativa posta a tutela dei dati personali dell'interessato si traduce per i titolari di trattamento/produttori dei *software* applicati in ambito medico nell'obbligo di tutelare il paziente che acconsente a che i suoi dati siano assoggettati ad un processo automatizzato, garantendo chiarezza di informazioni circa la logica algoritmica applicata al trattamento (art. 5, § 1, lett. a, Reg. (UE) 269/2016) e assicurando un intervento umano di sorveglianza, controllo e verifica del sistema. Tali previsioni si scontrano tuttavia con l'effettiva possibilità che i sistemi di intelligenza artificiale applicati siano sufficientemente "trasparenti" all'esterno - in modo da consentire agli utenti di interpretare correttamente il processo decisionale che conduce al risultato rivolto al medico e/o al paziente - così come internamente - tanto da rendere evidenti eventuali anomalie e distorsioni applicative all'occhio umano (per quanto esperto) preposto al controllo.

Rispetto all'uso di queste tecnologie in ambito medico si pone, altresì, in modo pregnante la difficile questione di che valore attribuite e come regolare forme di espressione del consenso racchiuse in "strutture digitali" quali "gesti telematici procedimentalizzati" (tasti virtuali, spunta di caselle, etc. [32]), dal momento che questi gesti sono preposti ad esprimere un consenso di natura incontestabilmente ibrida, a cavallo tra consenso informativo e consenso terapeutico.

Nel parere "*Mobile-health" e applicazioni per la salute: aspetti bioetici*, il Comitato italiano di bioetica ha espresso consapevolezza circa le difficoltà di "realizzare un consenso informato e di tutelare la privacy degli utenti in questo nuovo campo applicativo" dal momento che "ottenere un consenso informato nel campo medico presuppone una comuni-

[29] Base giuridica per la liceità del trattamento di dati relativi alla salute nei sistemi di intelligenza artificiale può essere altresì identificata in quella indicata all'art. 9, §, lett. j del Regolamento che richiama l'art. 89, § 1 dello stesso Regolamento, ove si fa espresso riferimento alla necessità di predisporre garanzie adeguate per i diritti e le libertà dell'interessato, ossia l'anonimizzazione, quale tecnica di protezione dei dati generalmente utilizzata per evitare di dover richiedere il consenso del paziente. La questione è molto delicata soprattutto nel campo della biomedicina: in molti ambiti di questa branca della medicina/ricerca è stato dimostrato che l'anonimizzazione non è mai definitiva, nel senso che è spesso possibile la reidentificazione, e dunque l'unico strumento che garantisce il più alto standard di legittimità al trattamento è proprio il consenso; tuttavia le modalità di richiesta del consenso devono evolvere verso una forma di "consenso dinamico" e partecipativo, ove l'interessato sia messo in grado di prendere coscienza della importanza delle partecipazione alla ricerca e anche della restituzione dei dati interpretati e gli sia comunque garantita la possibilità di mutare opinione (il diritto di revoca). In argomento, sui vari aspetti, A. SPINA, *La medicina degli algoritmi*, in *Intelligenza artificiale, protezione dei dati personali e regolazione,* a cura di F. PIZZETTI, Torino, 2018, 319 ss.; F.K. DANKAR, M. GERGELY, S.K. DANKAR, *Informed Consent in Biomedical Research*, in *Comput Struct Biotechnol J.*, 2019, 463 ss.; C. IRTI, *Personal data, non-personal data, anonymised data, pseudonymised data, de-identified data, a cura di R. SENIGAGLIA, C. IRTI, A. BERNES, Privacy end Data Protection in Software Service, Singapore, Springer, 2021, 49 ss.; A.* BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica, in Nuov. Giur. Civ. Comm, 2020, 175 ss.*

[30] L'uso della intelligenza artificiale per monitorare lo stato di salute di un paziente potrebbe rilasciare come output una diagnosi predittiva su rischio di malattie non richiesta e/o non voluta dal paziente al momento del rilascio del consenso, violando il suo diritto a non essere informato circa le reali condizioni del suo stato di salute.

[31] M. CIANCIMINO, *op. cit.*, 98. Sia consentito rinviare anche a C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, 2021, *passim*, dove ci siamo occupati della parallela problematica della interazione tra autodeterminazione informativa e autodeterminazione economica nelle *non monetary transaction*.

[32] Si segnala in proposito il provvedimento 7.7.2022, n. 242 con il quale il Garante della Privacy ha sanzionato la Società *Senseonics Inc.,* produttrice di un sistema di monitoraggio continuo del glucosio per persone affette da diabete che si avvale di una applicazione mobile (app medica), in quanto «in occasione del *download* della applicazione con un unico "clic" sul tasto "accetto" gli utenti erano chiamati ad accettare sia "i termini del contratto di licenza con l'utente finale" che "l'informativa privacy e le condizioni di utilizzo di *Senseonics*, autorizzando contestualmente la conservazione, la trasmissione e l'uso dei dati, comprese, senza limitazioni la conservazione nel Regno Unito, la trasmissione negli USA per finalità limitate (ad esempio ingegneristiche e di assistenza clienti) secondo i termini dell'EULA e dell'informativa privacy". Pertanto, la circostanza che sia stato richiesto un unico atto dispositivo da parte dell'interessato determina il mancato rispetto del requisito della specificità del consenso per le diverse finalità perseguite dal titolare del trattamento, ciò a maggior ragione in relazione al trattamento dei dati sulla salute, rispetto ai quali, il consenso deve altresì essere esplicito (art. 9, § 2, lett. a, Regolamento)».

cazione simmetrica e reciproca" - intendendo come simmetrica una comunicazione in cui i due interlocutori sono parimenti forti nell'interazione e reciproca quando le posizioni fra chi dà l'informazione e chi la riceve si realizzi nel riconoscimento delle rispettive autonomie -, una condizione che appare poco realizzabile da assicurare nell'utilizzo di app mediche, dove manca il contesto relazionale.

Essenziale è e resta la fase propedeutica al rilascio del medesimo, la fase "comunicativa"[33] – non meramente informativa – funzionalizzata a una fase curativa (almeno in parte[34]) delegata all'intelligenza artificiale: "È … un obbligo etico e giuridico che coloro che si sottopongono a trattamenti sanitari innovativi, attraverso l'IA, siano informati nelle modalità più consone e comprensibili al paziente di ciò che sta accadendo, di essere (se è il caso) oggetto di sperimentazione e validazione; di essere a conoscenza che ciò che è loro applicato (sul piano diagnostico e terapeutico) implica dei vantaggi, ma anche dei rischi. Va specificato in modo esplicito nel consenso informato se i trattamenti applicati (diagnostici o terapeutici) provengano solo da una macchina (IA, robot) o se e quali sono gli ambiti e i limiti del controllo umano o supervisione sulla macchina".

Stante la ontologica opacità degli algoritmi[35] - opacità sugli elementi essenziali e sul processo con cui un sistema di IA arrivi ad una conclusione decisionale - resta la difficoltà di comprendere come il medico possa fornire una comprensibile ed esauriente informativa nel momento in cui ci si avvale di trattamenti che ne fanno uso[36]: "questo solleva un problema per il medico nel confronto con la macchina (decidere se affidarsi o meno agli algoritmi) e nei confronti del paziente, al quale non può fornire una spiegazione e una informazione trasparente"[37].

2.2. … e nelle *Health MobileApp.*

Il consenso espresso rappresenta la base giuridica per il trattamento dei dati dell'utente (relativi allo stato di salute e allo stile di vita degli utenti, eventualmente anche dati sanitari[38]) in tutte le ulteriori ipotesi di utilizzo di *Health app* che li raccolgono e trattano per fornire indicazioni relative alle condizioni di salute dell'utilizzatore prive di dichiarate finalità terapeutiche (monitoraggio dell'attività sportiva e di fitness, dieta e nutrizione, coaching per la perdita di peso, ciclo del sonno, monitoraggio del ciclo mestruale etc.)

Si tratta nella maggior parte dei casi di app scaricabili "gratuitamente", ove tuttavia, se il consenso al trattamento dei dati inseriti dall'utilizzatore e/o da questo appresi durante l'impiego del *device* non è rilasciato al solo fine dell'espletamento del servizio richiesto ma per finalità proprie del fornitore, il "ritorno economico" risiede proprio nell'autorizzazione ricevuta a profilare l'utente, potenziale fruitore di un settore di mercato - quello legato al mondo della salute - ove il confine tra ricerca scientifica e ricerca per finalità commerciali diviene sfumato ed indistinguibile, a discapito di un utente digitale spesso inconsapevole.

La gratuità del servizio è, evidentemente, solo apparente, con il che diventa essenziale, ai fini della corretta autodeterminazione informativa dell'utente, specie se anziano, imporre ai fornitori delle app il rispetto della normativa privacy mediante la predisposizione di una interfaccia che garantisca trasparenza e intellegibilità - una protezione *by default* e *by design* che realizzi l'effettività delle regole giuridiche pensate per una legittima circolazione dei dati degli utenti[39] - ma anche il rispetto dei limiti "etici",

---

[33] Si sofferma sulla importanza della comunicazione e sulla "impossibilità di limitare la comunicazione a mera informazione", G. Di Rosa, *I robot medici, cit*., 18.

[34] "L'IA va considerata esclusivamente come un aiuto nelle decisioni del medico, che rimangono controllate e supervisionate dall'uomo. Resta compito del medico, in ogni caso prendere la decisione finale, in quanto la macchina fornisce solo ed esclusivamente un supporto di raccolta e analisi dei dati, di natura consultiva. Un sistema di "assistenza cognitiva automatizzata" nella attività diagnostica e terapeutica non è un "sistema decisionale autonomo". Esso effettua la raccolta di dati clinici e documentali, li confronta con statistiche relative a pazienti simili, accelerando il processo di analisi del medico", così il Comitato di bioetica nel Parere *Intelligenza artificiale e medicina: aspetti etici*, 29.5.2020, 10.

[35] Sulla estrinseca così come intrinseca opacità dell'algoritmo F. Pasquale, *The Black Box Society, The secret Algorithms that Control Money and Information,* Londra, Harvard Univ Pr., 2015, *passim*; J. Burrell, *How the machine 'think': Understanding opacity in machine algorithms*, in *Big data & Society*, 2016, *passim*.

[36] In argomento C. De Menech, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in *Rivista di Biodiritto*, 2022, 181 ss., spec. 184 ss., che sottolinea, peraltro, come "la scelta di includere dettagli tecnici nell'oggetto dell'informazione diagnostico-terapeutica dovrebbe essere lasciata alla discrezionalità del medico; discrezionalità da esercitarsi secondo ragionevolezza", ossia – (…) – nella prospettiva di un adeguamento del contenuto informativo alla condizione morale e alle capacità intellettive del singolo paziente, sì da evitare che un'eccessiva forzatura di queste ultime pregiudichi, in uno, salute e autodeterminazione" (193) .

[37] Comitato di bioetica nel Parere *Intelligenza artificiale e medicina: aspetti etici*, *cit.*, 11.

[38] Si tenga conto che la Proposta di regolamento sullo spazio europeo dei dati sanitari (*cit.*) prevede che le applicazioni per il benessere possano essere in futuro collegate ai sistemi di cartelle cliniche elettroniche (considerando 35) stabilendo per esser alcuni requisiti di etichettatura volontaria circa l'interoperatività dei sistemi (artt. 31 e 32).

[39] In altro studio (*Consenso negoziato e circolazione dei dati personali*, *cit.*, 135 ss.) abbiamo avuto modo di sostenere come il servizio o prodotto digitale offerto attraverso un'applicazione

oltre che giuridici, nell'uso di applicazioni di intelligenza artificiale[40] che si dimostrano essere in grado, grazie al sistema di profilatura mediante l'utilizzo di *cookies* e altri strumenti, sia di determinare fenomeni di emarginazione e discriminazione[41], che di generare e trasmettere impulsi subliminali destinati ad indirizzare le scelte degli utenti rispetto alle decisioni che li riguardano (il c.d. "*nudging*"[42]), fenomeno particolarmente grave allorquando il condizionamento finisce per avere ricadute sulle salute[43] (si veda dopo paragrafo 4). Un importante passo avanti nella tutela degli utilizzatori di queste app è oggi, tuttavia, rappresentata dal *Digital Services Act* (DSA), che vieta ai fornitori di piattaforme online di presentare pubblicità ai destinatari dei servizi basate sulla profilazione utilizzando le categorie speciali di dati particolari di cui all'art. 9, § 1, Reg. (UE) 2016/679.

3. Il lecito trattamento dei dati relativi alla salute del soggetto interessato anziano-vulnerabile.

Tali ultime riflessioni ci riportano alla seconda delle due considerazioni dalle quali siamo partiti nell'analizzare il regime giuridico di trattamento applicabile all'uso massivo dei dati nella *mobile health* dal nostro punto di visuale: la quasi totale assenza di considerazione nelle tematiche connesse alla circolazione dei dati personali della condizione di individuo anziano, vulnerabile.

A dire il vero, fatta eccezione per l'attenzione rivolta ai soggetti minori di età[44], è il tema della vulnerabilità[45] in quanto tale che non sembra aver ricevuto grande attenzione dal legislatore che si è occupato a livello europeo di privacy, pur trattandosi di una nozione che può giocare un ruolo fondamentale nell'inquadrare la posizione dell'individuo rispetto al trattamento dei suoi dati. Quello assunto dalla legislazione europea sulla privacy è stato infatti definito un "approccio universalistico"[46], nel senso che le regole sulla protezione dei dati personali sono dirette a tutelare tutti gli individui in egual misura perché nell'ecosistema digitale siamo tutti ugualmente esposti a potenziali violazioni. La nozione di "soggetto interessato" è, di conseguenza, unica e diversamente dal versante consumeristico, ove si è concettualizzata la nozione di "consumatore medio", non è dato comprendere se il legislatore intenda far riferimento in tale ambito ad un "soggetto interessato medio" (un individuo normalmente infor-

mobile possa considerarsi non conforme ai sensi della dir. (UE) 2019/770, relativa alla fornitura di contenuti digitali e di servizi digitali, allorquando non sia garantita da chi ha predisposto l'interfaccia di accesso al servizio una protezione dei dati personali dell'utente *by the default* o *by design* ai sensi dell'art. 3, § 8, della direttiva stessa. A ben vedere, in base a quanto affermato dal considerando 29 della citata direttiva, la stessa non dovrebbe applicarsi all'assistenza sanitaria né ai contenuti digitali o servizi digitali che costituiscono un dispositivo medico; tuttavia lo stesso considerando prevede una eccezione per i contenuti digitali o servizi digitali di un dispositivo medico - come le applicazioni sanitarie - che possa essere ottenuto dal consumatore senza che lo stesso sia prescritto o fornito da un professionista sanitario. La dir. (UE) 2019/770 è pertanto destinata a trovare applicazione per le app mediche che possano essere ottenute dal consumatore senza prescrizione medica e per tutte le app relative al benessere ed al lifestyle. In argomento G. CAPILLI, *op. cit*., 63-64.

[40] Si segnalano in proposito le *Linee guida in materia di intelligenza artificiale e protezione dei dati* redatte dal Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108/1981), approvate a Strasburgo nel 2019 ove all'art. 1 si riafferma come la tutela della dignità umana e delle libertà fondamentali, in particolare il diritto alla protezione dei dati personali, assumono un ruolo imprescindibile nello sviluppo e nell'adozione di applicazioni IA, e si sollecita un dialogo diretto sia con i legislatori e i diversi decisori politici, sia con gli sviluppatori, i produttori e i fornitori di servizi, al fine di favorire «un approccio volto a tutelare i diritti umani fin dalla progettazione di tali servizi ("*human rights by design*") ed evitare qualsiasi potenziale pregiudizio (bias), anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati»

[41] Non è escluso, ad esempio, che basti frequentare siti o acquistare applicazioni relative a problemi cardiaci per essere classificati come soggetti cardiopatici. I dati così ottenuti possono poi essere venduti a terzi per ricerche ulteriori non previste al momento della raccolta o per ricerche non correlate alle ricerche originarie: venduti, ad esempio, a compagnie assicurative che poi li utilizzano per valutare il rischio o addirittura per automatizzare la fornitura di assicurazioni.

[42] R.H. THALER, C. R. SUSTEIN, *Nudge: Improving Decisions About Health, Wealth and Happiness*, New Haven, Penguin Books, 2008; C.R. SUSTEIN, *Human Agency and Behavioral Economics. Nudging Fast and Slow*, Londra, Palgrave Macmillan, 2017.

[43] C. DE MENECH, *op. cit*., 201.

[44] Tra i primi contributi F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Diritto dell'informazione e dell'informatica*, 2018, 27 ss.; per un ampio approfondimento R. SENIGAGLIA, *Minore di età e contratto*, Torino, 2020, spec. p. 75 ss.

[45] Vulnerabilità è in realtà un termine che può assumere diversi significati, è una condizione universale degli esseri umani, ma è anche vero che tale condizione di debolezza può variare da un individuo all'altro, può avere diversi gradi di gravità e dipendere da molti fattori diversi. Da alcuni anni gli studiosi della materia tendono a proporre un approccio "stratificato" della vulnerabilità, che ne individua diversi livelli, ai quali i singoli individui o gruppi di individui non afferiscono in ragione di una "etichetta" che li contraddistingue, ma di condizioni determinate da plurimi fattori spaziali, temporali, sociali, economici etc.; così F. LUNA, "*Elucidating the Concept of Vulnerability: Layers Not Labels*" in *International Journal of Feminist Approaches to Bioethics*, 1, 2009, 121 ss.

[46] R. CALO, *Privacy, Vulnerability and affordance*, in *DePaul L. Rew*, 66, 2017, 592 ss.

mato e ragionevolmente attento ed avveduto, tenuto conto di fattori sociali, culturali e linguistici)[47].

Nella realtà dei fatti, tuttavia, i soggetti interessati possono presentare caratteristiche molto diverse: essi hanno diverse capacità di comprensione, diversi livelli di consapevolezza e capacità decisionale, presentano diverse gradazioni e tipologie di debolezza. L'affermare che tutti i soggetti interessati cui si riferiscono i dati personali oggetto di trattamento sono universalmente vulnerabili, può portare ad ignorare differenze significative tra di essi, negando protezione proprio a coloro che ne avrebbero più bisogno[48].

L'aggettivo *vulnerabile* è utilizzato in tutto il Reg. (UE) 2016/679 un'unica volta, al considerando 75, lì dove trattando dei rischi rilevanti da considerare quando si esegue una valutazione d'impatto sulla protezione dei dati, si suggerisce di porre particolare attenzione quando sono trattati «dati personali di persone fisiche *vulnerabili*, in particolare i minori». Scorrendo il resto del testo si può osservare come, in effetti, la situazione dei minori di età sia l'unica affrontata in modo specifico, con un atteggiamento che, a prima lettura, può apparire ambivalente: se da un lato, infatti, viene fissato un limite di età minimo per l'autonomo rilascio del consenso al trattamento dei dati per i servizi della società dell'informazione al di sotto della soglia della maggiore età (16 anni, che gli Stati membri possono ridurre fino a 13) (articolo 8) [49] – così presumendo l'acquisizione della necessaria consapevolezza propedeutica all'atto da parte di soggetti non ancora maggiorenni – dall'altro si impongono obblighi di trasparenza particolari da rispettare nei confronti dei soggetti minorenni (articolo 12, § 1)[50], motivando tale scelta proprio sulla base del fatto che questi ultimi «meritano una protezione specifica per quanto riguarda i loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle tutele previste e dei loro diritti in relazione al trattamento dei dati personali» (considerando 38, ma si vedano anche i considerando 58, 65 e 71). A tal proposito è, però, opportuno ricordare come l'atto mediante il quale il soggetto autorizza il trattamento dei propri dati personali – il consenso informato – è la manifestazione di un diritto fondamentale della persona – il "diritto all'autodeterminazione informativa" – che, come tale, dovrebbe essere esercitato direttamente dalla persona interessata, anche se minore di età; la delega al rappresentante, specie in questo ambito, svolge una funzione di protezione del soggetto minore, destinata ad operare fin tanto che lo stesso non abbia assunto una sufficiente capacità di intendere e di volere (che il legislatore presume essere acquisita in questo ambito ben prima del compimento del diciottesimo anno di età) trasformandosi, altrimenti, in una inopportuna e lesiva limitazione del diritto del minore ad accedere ed utilizzare liberamente i servizi della società dell'informazione[51].

Anche il parere *Mobile-health" e applicazioni per la salute: aspetti bioetici* si sofferma in via prevalente sulle problematiche inerenti all'uso di que-

[47] Il tema della vulnerabilità non è in verità estraneo al panorama normativo consumeristico, ove le istituzioni europee hanno da tempo riconosciuto anche la figura del *consumatore vulnerabile,* con il che quella di "consumatore" (medio) ha cessato di essere considerata una categoria omogenea (già di per sé beneficiaria di protezione) per palesarsi quale gruppo eterogeneo di soggetti all'interno del quale taluni necessitano di maggior tutela rispetto ad altri. Della condizione di vulnerabilità dell'individuo/consumatore si occupano oggi diverse disposizioni del Codice del consumo (il consumatore vulnerabile, non a ragione di fattori esterni o economici, bensì personali, era già presente nel considerando 34 della dir. 2011/83/UE sui diritti dei consumatori nell'ambito delle informazioni precontrattuali): in particolare, l'art. 20, co. 3, cod. cons. in tema di pratiche commerciali sleali che prende in considerazione la figura dei consumatori particolarmente vulnerabili «alla pratica o al prodotto cui essa si riferisce a motivo della loro infermità mentale o fisica, della loro età o ingenuità», individuando dunque quali specifiche cause di vulnerabilità solo quelle che fanno riferimento a caratteristiche personali quali l'infermità mentale o fisica, l'età o l'ingenuità, Una figura di consumatore vulnerabile da più parti criticata in quanto troppo concentrata sulla vulnerabilità personale e non aperta a prendere in considerazione altri fattori che possono contribuire a rendere gli individui vulnerabili, in particolare quelli di natura socio-economica. Per un approfondimento sul tema cfr. A. SACCOMANI, *Le nozioni di consumatore e di consumatore medio nella direttiva 2005/29/CE*, in *Le pratiche commerciali sleali, Direttiva comunitaria e ordinamento italiano,* a cura di A. MINERVINI, L. ROSSI CARLEO, Milano, 2007, 141 ss.; N. ZORZI GALGANO, *Il consumatore medio ed il consumatore vulnerabile nel diritto comunitario*, in *Contratto e impresa/Europa*, 2010, 2, 549 ss.; C. RIEFA, S. SAINTIER (a cura di), *Vulnerable consumers and the law*, Londra-New York, Routledge, 2021, *passim*.; si veda anche S. PAGLIANTINI, in *Il consumatore frastagliato*, Pisa, 2021, spec. p. 87.

[48] G. MALGIERI, J.NIKLAS, *Vulnerable data subject*, in *Computer Law & security Review*, 37, 2020, 1 ss.

[49] Ove il minore abbia un'età inferiore, il trattamento dei dati è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

[50] I documenti di trasparenza e qualsiasi comunicazione nell'ambito dell'esercizio dei diritti di protezione dei dati devono essere "in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice, in particolare per le informazioni rivolte specificamente a un minore".

[51] Sul tema specifico ci sia permesso rinviare a C. IRTI, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ*., 3, 2019, 617 ss., e alla bibliografa ivi citata. L'interesse degli utilizzatori del web (anche minori di età) alla condivisione dei propri dati (compreso il c.d. *tying*) è stato recentemente definito come "un interesse alla *comunicazione personalizzata* e ai *contenuti digitali*, ossia (…) un interesse a trovare, a rimanere dentro, o a non essere esclusi da, *il proprio posto nell'ecosistema digitale*" così S. ORLANDO, *Per un sindacato di liceità del consenso*, in *Pers. Merc*., 2, 2022, 527 ss.

ste app da parte di soggetti minori di età, rispetto ai quali - si sottolinea - possono risultare carenti elementi di competenza necessari a comprendere le decisioni da assumersi, rendendosi palese l'esigenza di offrire loro "informazioni semplici, concise, che includono anche riferimenti educativi che sollecitino la presa di coscienza dei problemi, con un linguaggio adatto". Per il Comitato di Bioetica appare, comunque, giuridicamente discutibile che il consenso al trattamento dei dati richiesto per l'utilizzo di queste app possa essere dato soltanto dal minore, trattandosi di vicende che, riguardando la sua salute, debbono necessariamente ricadere nell'ambito della responsabilità dei genitori o del rappresentante legale: "se i rischi connessi a questi dispositivi medici sono consapevolmente assunti da un adulto, non altrettanto può essere nei confronti di un minore, dove il suo miglior interesse nell'ambito della cura è ancora quello di un utilizzo tradizionale del rapporto paziente-medico. Tanto più che le app più scaricate dagli utenti, come già detto, chiedono l'accesso a una gran quantità di dati, senza ancora spiegare adeguatamente per quali scopi queste informazioni sarebbero usate e sugli eventuali dati personali che verranno raccolti e sul loro uso"[52].

Occupandoci qui di soggetti anziani ci si può in primo luogo chiedere se le garanzie poste a tutela dei minori possano essere applicate per analogia anche a costoro, la cui vulnerabilità può emergere, così come per i soggetti minori, quale espressione di una limitata capacità di fornire un consenso libero per la raccolta di dati personali, di comprendere le informazioni sul trattamento dei dati e sui rischi connessi al trattamento, di esercitare adeguatamente i diritti di protezione che gli sono attribuiti dalla legge. Con particolare riguardo alla possibilità che il rilascio del consenso di un anziano vulnerabile sia normativamente delegato ad un soggetto terzo – sulla falsariga di quanto previsto per i minori di 16/13 anni – l'unica possibile similitudine è quella che riguarda le persone legalmente incapaci, rispetto alle quali si può sostenere che il consenso o l'autorizzazione al consenso debba essere rilasciata da parte dei loro rappresentanti legali, sulla scorta di quanto espressamente previsto dalla l. 2.12.2017, n. 219 in materia di consenso informato in ambito sanitario ove all'art. 3 è prevista la delega al rappresentante legale per il rilascio del consenso al trattamento sanitario non solo dei soggetti minori di età ma anche dei soggetti interdetti e sottoposti ad amministrazione di sostegno (nel caso in cui la nomina dell'amministratore preveda l'assistenza necessaria o la rappresentanza esclusiva in ambito sanitario), sebbene sia precisato come l'incapace debba essere coinvolto il più possibile nella decisione che si va ad assumere. Al di là di questi casi limite, in tutte le ipotesi di utilizzo di *medical app* resta essenziale l'interazione con chi svolge attività di accudimento e sostegno del soggetto anziano vulnerabile (familiari, *care giver* etc.) per agevolare quel necessario processo di acquisizione e comprensione delle informazioni propedeutico al rilascio del medesimo.

In termini più generali si deve ritenere che la condizione di vulnerabilità del soggetto adulto interessato implichi che i responsabili del trattamento debbano adottare garanzie speciali quando raccolgono i di loro dati: ai sensi dell'art. 24 del Regolamento, il titolare del trattamento deve analizzare il livello di rischio (per i diritti e le libertà fondamentali degli interessati) e quindi il livello di vulnerabilità dell'interessato prima di procedere al trattamento dei dati. Di conseguenza, quando si sceglie la base giuridica per il trattamento (consenso, interesse legittimo, etc.), è necessario effettuare una valutazione dei possibili livelli di vulnerabilità degli interessati per predisporre le più opportune garanzie, anche in ragione delle finalità di utilizzo dei dati.

Se la base giuridica del trattamento è il consenso i rischi maggiori riguardano – come evidenziato –la "vulnerabilità decisionale" del soggetto interessato anziano, in ragione di una sua presumibile ridotta capacità di comprensione; di conseguenza particolare attenzione dovrà essere posta dal titolare del trattamento alle politiche informative e di comunicazione, al fine di rispettare gli obblighi di trasparenza (art. 12 del Regolamento). In base a quanto definito dalle Linee guida sulla trasparenza elaborate dal Gruppo art. 29, "se un titolare del trattamento è consapevole che i suoi beni o servizi sono utilizzati da (o destinati a) (…) membri vulnerabili della società, tra cui persone con disabilità o persone che possono avere difficoltà a comprendere le informa-

[52] «Tuttavia, è difficile sapere se l'utilizzo dell'app medica è svolto da un adulto o da un minore. È questo un problema che, anche nell'ambito delle ICT, va evidenziato: bisogna pensare a specifiche garanzie aggiuntive per i minori, identificando, ad esempio, requisiti e meccanismi informatici per verificare online l'età dell'acquirente di una applicazione per la salute. Ne consegue anche l'esigenza di offrire, proprio nei confronti dei minori, informazioni semplici, concise, che includono anche riferimenti educativi che sollecitino la presa di coscienza dei problemi, con un linguaggio adatto. L'educazione dei minori, utenti attivi di tali nuove tecnologie, risulta particolarmente urgente e rilevante sul piano bioetico: una educazione che rafforzi strumenti di autodifesa dei giovani nell'ambito dell'uso delle tecnologie. Dovrebbe anche essere compito dei genitori, acquirenti per i propri figli delle tecnologie mobili, far uso di sistemi di controllo (parental control) per l'accesso che il produttore dell'app dovrebbe prevedere nel sistema. Si potrebbe inoltre auspicare che l'app medica, che contiene dati e cure finalizzate per i minori, sia progettata, supportata e avallata da società scientifiche o istituzioni sanitarie specializzate nelle diagnosi e cure pediatriche. La stessa proposta sul mercato dovrebbe essere distinta rispetto ai destinatari (adulti o minori)», p. 13 del documento del 28.5.2015.

zioni, le vulnerabilità di tali soggetti dovrebbero essere prese in considerazione dal titolare del trattamento nella valutazione sul come garantire il rispetto dei suoi obblighi di trasparenza in relazione a tali soggetti".

La base giuridica che legittima il trattamento potrebbe, però, non essere il consenso dell'interessato. L'insieme dei dati raccolti dagli utenti di applicazioni destinate all'ambito sanitario può essere, infatti, adoperato con finalità pubblicistiche, per la determinazione - grazie all'utilizzo combinato di sistemi di intelligenza artificiale - delle politiche sanitarie per la salute pubblica, specie di tipo preventivo. Le informazioni così raccolte possono essere altresì preziose per la ricerca scientifica e lo sviluppo di diverse branche della medicina, come quella di precisione o personalizzata che le utilizza per proporre strategie di intervento *uti singoli*, in base alle caratteristiche specifiche dell'individuo, con riferimento alla sua biografia e al suo stile di vita[53].

Anche quando operata per finalità di pubblico interesse la raccolta di questi dati comporta, tuttavia, l'assunzione di una pluralità di rischi quali, in primo luogo, quelli connessi al reperimento dei cosiddetti "*big bad data*", dovuto ad errori commessi nei processi di trasmissione delle informazioni raccolte, magari proprio a causa della attività compiuta dall'utente nell'uso delle applicazioni, che potrebbe ingannare o frettolosamente e distrattamente fornire dati non congruenti. Un fenomeno, quello appena descritto, che può falsare la conoscenza scientifica, con pericolose conseguenze per la salute individuale e collettiva.

Strettamente connesso a questo problema è, poi, quello delle possibili discriminazioni algoritmiche, legate per lo più al processo di profilazione degli individui: il comportamento standard sulla base del quale vengono assunte decisioni algoritmiche è generalmente identificato come quello statisticamente più frequente; restano di conseguenza esclusi dalla stessa profilazione tutti coloro che, ad esempio, per ragioni di età o di emarginazione sociale-digitale, non sono generatori di dati. "Ciò può dare luogo a forme di discriminazione algoritmica, con un impatto sull'uguaglianza e l'inclusione. Se un algoritmo sanitario, ad esempio, apprende da un database informazioni in cui alcuni gruppi di pazienti sono sottorappresentati o esclusi, può portare questi gruppi a correre un rischio maggiore di diagnosi errata o prognosi errata. Rispetto a tali situazioni si è parlato anche di "*ageism*", ossia discriminazioni in base all'età nelle piattaforme digitali che introducono forme di emarginazione dei gruppi vulnerabili, quali quelli della popolazione anziana"[54].

3.1. L'altra faccia della vulnerabilità: i rischi connessi all'uso dell'intelligenza artificiale e del *machine learning* nell'ambito sanitario.

Le problematiche da ultimo evidenziate rappresentano l'"altra faccia" della vulnerabilità, quella legata ai possibili, spesso imprevedibili, risultati dell'uso della intelligenza artificiale e del *machine learning* basato sui dati, tecnologie che hanno il potenziale di trasformare (anche) l'assistenza sanitaria ricavando nuove e importanti conoscenze dalla grande quantità di dati sanitari generati ogni giorno, ma l'utilizzo delle quali non è esente da un certo rischio di discriminazione nei confronti di determinati gruppi di persone (bias), dovuto alla qualità e quantità dei campioni di dati valutati (soprattutto ove appartenenti a gruppi sottorappresentati in ragione di età, sesso, razza etc.)[55] o all'uso di sistemi di IA progettati, ad esempio, per efficientare le risorse, che potrebbero tuttavia compromettere la dignità umana e l'accesso equo alle cure[56].

Negli Stati Uniti la *Food and Drug Administration* – dopo aver approvato l'uso di 39 algoritmi basati sull'IA (soprattutto in ambiti radiologici, cardiologici ed endocrinologici) e nel 2018 la prima diagnosi totalmente basata su IA - ha pubblicato nel 2019 (in collaborazione con l'agenzia regolatoria canadese,la *Health Canada*, e la *Medicines and Healthcare Products Regulatory Agency* del Regno Unito) un documento contenente dieci principi guida per lo sviluppo di una *Good Machine Learning Practice*[57], destinato agli sviluppatori di software con funzioni di intelligenza artificiale e apprendimento automatico qualificabili come dispostivi me-

[53] M. Ciancimino, *op. cit*., 69 ss.; L. Palanzani, *op.* cit., 67 ss.

[54] L. Palanzani, *op. ult. cit.,* 73.

[55] Si sofferma con attenzione sui rischi per i diritti e le libertà delle persone connessi all'uso della intelligenza artificiale il *Parere congiunto 5/2021* rilasciato dal *Comitato europeo per la protezione dei dati* e il *Garante europeo della protezione dei dati* (EDPB- GEDP) sulla *Proposta di Regolamento europeo in materia di Intelligenza artificiale del 18 giugno 2021.*

[56] Sistemi che potrebbero far sì che le decisioni sull'opportunità di fornire determinate terapie o operazioni costose si basino sulla previsione della durata della vita e sulle stime delle aspettative di vita, basati sull'uso di dati magari errati o parziali. Anche quando l'IA non viene utilizzata, i pazienti vengono già suddivisi in gruppi per ottimizzare il flusso di pazienti e tali decisioni spesso riguardano coloro che sono più vulnerabili quali anziani, persone di colore e quelle con difetti genetici o disabilità. Tutti aspetti rilevati nel documento dell'Oms, *Ethics and governance of artificial intelligence for health*, 28.6.2021.

[57] *https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles*

dici. Tra i principi ivi elencati, proprio al fine di limitare rischi di *bias* e discriminazioni, si segnala quello secondo il quale i set di dati utilizzati per il processo di *machine learning* debbano essere i più rappresentativi possibili della popolazione di pazienti interessata. I protocolli di raccolta dei dati devono garantire che le caratteristiche rilevanti della popolazione di pazienti prevista (ad esempio, in termini di età, sesso, razza ed etnia), l'uso e gli input di misurazione siano sufficientemente rappresentati in un campione di dimensioni adeguate nello studio clinico e negli insiemi di dati di addestramento e di prova, in modo che i risultati possano essere ragionevolmente generalizzati alla popolazione di interesse prevista. Viene inoltre sancito il principio *Human in the loop* che colloca la conoscenza e l'esperienza delle persone al centro dei processi di apprendimento automatico: gli esseri umani devono partecipare all'impostazione dei sistemi, alla messa a punto e alla verifica del modello in modo da migliorare il processo decisionale e la conseguente attuazione delle decisioni suggerite[58]. Da ultimo si sottolinea l'importanza di fornire agli utenti informazioni chiare e pertinenti, tra cui informazioni complete sulla destinazione d'uso del prodotto e le indicazioni per il suo utilizzo, le caratteristiche dei dati utilizzati per addestrare e testare il modello, oltre che eventuali modifiche e aggiornamenti dei dispositivi.

Per quanto concerne il versante europeo[59], in attesa di conoscere se e come evolverà la *Proposta di Regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale* (IA) presentata dalla Commissione nell'aprile del 2021 (di seguito Proposta di regolamento IA)[60], l'unica normativa di riferimento al momento vigente – oltre a quella contenuta nei regolamenti (UE) 2017/745 e (UE) 2017/746 relativi ai dispositivi medici – è proprio la disciplina dettata in materia di protezione dei dati personali[61] che, tuttavia, a detta di molti[62], non si dimostra adeguata per regolare le applicazioni delle tecnologie di IA e *machine learning,* soprattutto in un'ottica di tutela *result-oriented*, che prenda atto della necessità di allargare – più che restringere[63] – la quantità e varietà di dati utilizzati per addestrare e convalidare i software al fine di garantire la creazione di algoritmi il più possibili precisi e *fair*[64].

Le "discriminazioni algoritmiche" e l'utilizzo di tecniche di *nudging*, evidentemente più che verosimili anche in ambito medico[65], devono essere con-

[58] L'intervento umano nel loop può individuare i problemi della tecnologia prima che vengano implementati su vasta scala, come nel caso di bias: un esempio si è presentato nel 2019 quando l'azienda Apple è stata tacciata di sessismo dopo che i modelli di apprendimento automatico della sua carta di credito avevano deciso di assegnare alle donne limiti di credito molto più bassi rispetto agli uomini, anche quando le donne guadagnavano di più.

[59] Per un'ampia panoramica C. Camardi (a cura di) *La via europea per l'intelligenza artificiale*, Cedam, 2021, *passim*.

[60] Per una prima attenta disamina della Proposta di regolamento IA, G. Contissa, F. Galli, F. Godano, G. Sartor, *Il regolamento europeo sull'intelligenza artificiale (analisi informatico-giuridica)*, in www.i-lex.it, 2021; S. Orlando, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di* Artifcial Intelligence Act, in *Persona e Mercato*, 2022, 346 ss.; Id., in *La via europea per l'intelligenza artificiale, cit.*, 267 ss. Si segnala che nel mese di novembre 2022 il Consiglio europeo ha adottato una posizione comune (*General approach*) che apporta alcune modifiche al testo proposto dalla Commissione (il documento è consultabile al seguente link https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/).

[61] Come sottolineato dal Garante per la protezione dei dati personali nella *Memoria sulla Proposta di regolamento (UE) sull'intelligenza artificiale* presentata alla Camera dei deputati il 9.3.2022, esiste in verità una stretta relazione fra le due "materie", posto che ad alimentare i sistemi di IA in vista del loro apprendimento sono, per lo più, i dati personali che a tali fini possono essere assoggettati a trattamento. Analoghe riflessioni sono state svolte dal Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati (EDPB-GEDP) sulla Proposta di Regolamento europeo in materia di Intelligenza artificiale, 18.6.2021.

[62] Secondo molti autori la disciplina di protezione dei dati personali contenuta nel Regolamento non si dimostra adeguata, in quanto non è stata pensata, per regolare le applicazioni delle tecnologie di IA e *machine learning*; così G. Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1657 ss.; G. Olivi, *Big data, metadati e intelligenza artificiale*, in *Dir. ind.*, 2020, 181 ss.; A. Cinque, *Privacy, Big-Data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute*, in *Nuova giur. civ. comm.*, 2021, 957 ss. Del resto, come correttamente rilevato (A. La Spina, *Complessità e identità personale*, Napoli, 2022, 458), obiettivo primario della proposta di Regolamento IA è proprio quello di superare i limiti che il sistema introdotto dal Regolamento Privacy ha già manifestato, ovvero di «affrontare l'opacità, la complessità, la faziosità, un certo grado di imprevedibilità e un comportamento parzialmente autonomo di taluni sistemi di intelligenza artificiale, onde garantirne la compatibilità con i diritti fondamentali» (relazione di accompagnamento alla proposta).

[63] In virtù di una protezione rafforzata come quella garantita nel combinato disposto degli artt. 9 e 22 del Regolamento ai dati particolari, categoria comprensiva dei dati sanitari.

[64] G. Resta, *Cosa c'è di europeo nella proposta di regolamento Ue sull'intelligenza artificiale*, in Camardi (a cura di), *op. cit.*, 53 ss., spec. 69.

[65] «Non si deve dimenticare che l'assistenza medica comporta anche grandi interessi economici, pertanto l'IA può essere orientata, attraverso la costruzione degli algoritmi, ad influenzare in vari modi le decisioni del medico, ad esempio, facilitando le prescrizioni attraverso un aumento o una diminuzione dei valori di normalità per una serie di parametri funzionali o biochimici. Pertanto, l'IA può indurre a privilegiare una classe di farmaci rispetto ad una altra classe che abbia le stesse indicazioni per un determinato sintomo o patologia. Può privilegiare un percorso diagnostico che favorisca l'utilizzo di determinati reattivi piuttosto di altri. Può suggerire l'impiego di determinate apparecchiature e tecnologie più costose in alternativa ad altre più economiche. Può influenzare il medico a prescrivere tratta-

trastate, da un lato con una corretta gestione dei dati, garantendo per lo sviluppo dei software medicali un apporto significativo e largamente rappresentativo di dati, qualitativamente controllati e costantemente aggiornati; dall'altro perseguendo obiettivi di eticità delle funzionalità dei software applicati nell'ambito della salute[66], ovvero facendo in modo che le finalità di trattamento ingegnerizzate in detti software mirino a realizzare solo scopi legittimi[67].

Entrambi gli obiettivi sembrano essere perseguiti dalla già citata proposta di Regolamento IA che, nell'ottica di salvaguardare i valori e i diritti fondamentali dell'Unione europea e la sicurezza degli utenti, pone al centro della sua valutazione i rischi connessi all'uso dell'intelligenza artificiale e del *machine learning* e introduce misure volte a contenerli. Il Regolamento è costruito in modo da definire varie classi di rischio per i sistemi basati sull'utilizzo dell'intelligenza artificiale, distinguendo applicazioni proibite, perché causa di rischi inaccettabili per i diritti e le libertà fondamentali, applicazioni ad alto rischio - non proibite ma sottoposte a specifiche condizioni per gestire i rischi (art. da 9 a 13) – e applicazioni a rischio medio o basso, comunque governabile.

Con riferimento ai sistemi ad alto rischio che prevedono l'uso di dati per l'addestramento di modelli – categoria nella quale possono certamente essere fatti rientrare i software medicali – l'art. 10 in particolare, rubricato *Dati e governance dei dati*, si preoccupa di delineare requisiti atti ad assicurare la completezza del dataset di addestramento dei software[68], unitamente ad altre caratteristiche di conformazione[69]; il rispetto di tali requisiti sarà verificato nell'ambito delle procedure di valutazione della conformità ai sensi della normativa di settore, che per i dispositivi medici prevede il vaglio di organismi notificati prima dell'immissione in commercio dei prodotti; se, dunque, la proposta entrerà in vigore i meccanismi di valutazione dovranno garantire la conformità dei software medicali non solo a quanto stabilito dalla normativa sui dispositivi medici, ma anche a quanto previsto nel Regolamento sull'IA[70].

Per quanto concerne un eventuale vaglio di "eticità" in termini funzionali[71] delle applicazioni software utilizzate in ambito medico, o comunque destinate ad avere ampie ricadute sulla salute degli utenti, potrebbero risultare invece utili le previsioni

menti piuttosto che a stimolare il paziente a migliorare buoni stili di vita. Queste fra le altre ragioni di rischio spingono il Comitato a ritenere che debbono essere fatti controlli accurati, anche attraverso la validazione degli algoritmi, in modo da ottenere la più probabile certezza che l'introduzione delle varie forme di IA siano vantaggiose per migliorare la qualità delle prestazioni del Servizio Sanitario Nazionale» Comitato di bioetica, Parere *Intelligenza artificiale e medicina: aspetti etici*, *cit.* p.12.

[66] Si segnalano in proposito gli *Orientamenti etici per un'intelligenza artificiale affidabile* del 2019 redatti dall'High-*Level Expert Group on AI* costituito dalla Commissione Europea del 2018 e il documento dell'Oms, *Ethics and governance of artificial intelligence for health*, 28.6.2021. Si vedano anche le indicazioni rinvenibili nel Parere *Intelligenza artificiale e medicina: aspetti etici* (*cit.*), ove il Comitato raccomanda «di predisporre *ex ante* accurati controlli per l''addestramento' delle macchine sulla base di dati di qualità, aggiornati e interoperabili e di condurre sperimentazioni adeguate nell'ambito della IA per garantire sicurezza ed efficacia nell'uso di queste nuove tecnologie e sollecitare la ricerca di strumenti di validazione e certificazione delle tecnologie e di sorveglianza e monitoraggio, come elementi indispensabili per creare un "patto sociale di fiducia e affidabilità" delle tecnologie in ambito medico; sarebbe auspicabile integrare nell'ambito dei comitato etici per la sperimentazione la figura di un *computer scientist* o un esperto di IA, e aggiornare anche la normativa sulla sperimentazione con riferimento a software in ambito medico» e «di introdurre la rilevanza dei principi etici di autonomia, responsabilità, trasparenza, giustizia nei codici di condotta e nei corsi di formazione degli ingegneri, informatici, sviluppatori, con particolare riferimento all'etica nel disegno delle tecnologie (*ethics by design/in design/for designers*), assicurando una tecnologia che sia orientata ad incorporare i valori e assicurare la centralità del paziente».

[67] Interessanti, in proposito, le riflessioni di S. Orlando, *Per un sindacato di liceità del consenso*, cit., spec. p. 536 ss.

[68] Commi da 1 a 4 dell'art. 10 intitolato "*Dati e governance dei dati*"; al comma 5 si stabilisce peraltro che «[n]ella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali […], fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita»,

[69] Si precisa come "Le soluzioni tecniche precise atte a conseguire la conformità a tali requisiti possono essere previste mediante norme o altre specifiche tecniche o altrimenti essere sviluppate in conformità alle conoscenze ingegneristiche o scientifiche generali, a discrezione del fornitore del sistema di IA. Tale flessibilità è particolarmente importante in quanto consente ai fornitori di sistemi di IA di scegliere il modo in cui soddisfare i requisiti che li riguardano, tenendo conto dello stato dell'arte e del progresso tecnologico e scientifico nel settore".

[70] Quella proposta dal regolamento IA è infatti una disciplina definita "orizzontale", destinata a combinarsi con le diverse normative di settore che già regolano i prodotti che possono incorporare o essere costituiti da sistemi di IA.

[71] Un approccio alternativo è quello proposto dal c.d. "*Design for values*", una proposta di metodo per basare la progettazione dei software sui valori della dignità umana, della libertà, dell'uguaglianza e della solidarietà e per interpretarli come requisiti non funzionali, in merito J. Van den Hoven , P.E. Vermaas , I. Van de Poel, (a cura di) *Handbook of ethics, values, and technological design*: *Sources, theories, values, and application domains*, Dordrecht, Springer, 2015, *passim*., una evoluzione delle c.d. *Privacy Enhancing Technologies* sulle quali si rinvia a A. Bernes, *Privacy Enhancing Technologies, trasparenza e tutela della persona nell'ambiente digitale*, in *Annuario OGID, 2022, Yearbook JODI 2022*, a cura di S. Orlando e G. Capaldo, Roma, 2022, 23 ss.

contenute alle lettere *a* e *b* del comma 1 dell'art. 5 della Proposta IA, ove si dispone il divieto di immissione sul mercato, la messa in servizio e l'uso di prodotti software (a) che utilizzano "tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico" o (b) che sfruttano "le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico"[72]; divieti che operano a prescindere dalla base giuridica che giustifica il trattamento dei dati funzionale all'operatività del software, quindi a prescindere dal fatto che gli utenti abbiano rilasciato il consenso al trattamento dei loro dati o che lo stesso trattamento sia giustificato da ragioni di interesse pubblico.

Rispetto alla prima previsione – quella sub a) – è stato rilevato come, sebbene appaia manifesto che si tratti di una disposizione diretta a vietare che le persone possano essere "manipolate"[73] grazie all'uso di sistemi di intelligenza artificiale, non risulta ben chiaro cosa si intenda per "tecniche subliminali"[74] e in cosa debba o possa consistere la consapevolezza rispetto a queste pratiche che si vorrebbero vietate[75]: l'assenza di indicazioni specifiche fa temere, difatti, che un tale divieto "rimanga una dichiarazione di intenti senza alcuna applicazione concreta"[76]. A nostro modo di vedere, tuttavia, ove questa previsione dovesse essere sfruttata per sottoporre le funzionalità dei software ad una vaglio di "eticità"[77], l'attenzione dovrebbe essere spostata dalla 'pratica' utilizzata al 'risultato' perseguito, di modo che ogni qual volta sia possibile dare la prova[78] che il comportamento di una persona risulti "materialmente distorto"[79] in ragione dell'utilizzo di un software tanto da poter provocare un danno fisico o psicologico[80], l'immissione sul mercato, la messa in servizio e l'uso di tale software debbano considerarsi vietate. Semmai, come pure è stato sottolineato[81], quel che lascia perplessi è il fatto che restino esclusi

[72] In ragione delle modifiche apportate al testo della proposta dal documento del Consiglio europeo del novembre 2022 (General approach) la disposizione che vieta l'uso di sistemi di IA che sfruttano le vulnerabilità di un gruppo specifico di persone dovrebbe coprire anche le persone vulnerabili a causa della loro situazione sociale o economica: « (b) t*he placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm*».

[73] P. Hacker, *Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection and Privacy Law*, in *European Law Journal*, September 2021, 1 ss.

[74] A titolo esemplificativo si possono segnalare architetture software contenenti i cd. *dark pattern* o uso di tecniche adattive e personalizzate di analisi di dati che generano nell'individuo comportamenti irrazionali ed impulsivi, cd. *hyper-nudging*. Per una analisi approfondita delle possibili tipologie di interazioni di natura "persuasiva" fra un software di IA e l'utente umano si veda C. Burr, N. Cristianini, J. Ladyman, *An Analysis of the Interaction Between Intelligent Software Agents and Human Users*, in *Minds and Machines*, 2018, 28, 735 ss.

[75] G. Contissa, F. Galli, F. Godano, G. Sartor, *op. cit.*, 11 ss.; in termini analoghi S. Orlando, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di* Artifcial Intelligence Act, cit., 356.

[76] G. Contissa, F. Galli, F. Godano, G. Sartor, *op. ult. cit.*, 13.

[77] Alcuni autori sostengono da tempo che gli "agenti artificiali" (software di IA) sono moralmente responsabili delle loro azioni, il che significa che possono essere sottoposti a varie forme di censura (ad esempio, 'manutenzione', rimozione, ecc.), ma non presentano le caratteristiche rilevanti che ci permetterebbero di etichettarli come moralmente responsabili (ad esempio, meritevoli di ricompensa o punizione), così L. Floridi, J. W. Sanders, *On the morality of artificial agents,* in *Minds and Machines,* 14, 3, 2004, 349 ss.

[78] L'applicazione del principio di precauzione dovrebbe, peraltro, far propendere per una prova di natura presuntiva. Sul ragionamento presuntivo da ultimo si veda S. Patti, R. Poli (a cura di), *Il ragionamento presuntivo*, Torino, 2022, *passim*.

[79] "L'espressione che nella versione in lingua inglese dell'AIA è resa con le parole "*to materially distort*" – presente in entrambe le previsioni di cui alle lettere a e b) dell'art. 5, § 1, AIA - è stata resa nel testo italiano con le parole "distorcere materialmente". Reputiamo che si tratti di una traduzione errata. Innanzitutto, l'avverbio così reso in lingua italiana è, in questo contesto, privo di senso. In secondo luogo, è pertinente osservare che la stessa espressione ("*to materially distort*") la troviamo nell'art. 5, dir. 2005/29/CE delle pratiche commerciali scorrette, che, nella versione italiana della medesima direttiva, è tradotta con "falsare in misura rilevante", così S. Orlando, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di* Artifcial Intelligence Act, *cit.*, 357.

[80] Sarebbe poi da comprendere se nella definizione di "danno psicologico" si possano far rientrare tutte quelle forme di ingerenza indesiderata nella propria sfera decisionale che le attività di *nudging* sono destinate ad esercitare sfruttando i bias cognitivi "automatici", così operando al di sotto della consapevolezza, in quanto mirano a bypassare i processi deliberativi attraverso i quali un individuo può riflettere se il suo comportamento sia effettivamente coerente con i suoi desideri di ordine superiore. Sul funzionamento dei nudges C. Burr, N. Cristianini, J. Ladyman, *op. cit.*, 762 ss.

[81] Nel Parere congiunto del 18.6.2021 rilasciato da EDPB-GEPD, *cit.*, al Punto 28 si legge infatti "[…] L'articolo 5 della proposta rischia di sostenere solo a parole i «valori» e il divieto di sistemi di IA che siano in conflitto con tali valori. Infatti, i criteri citati all'articolo 5 per classificare i sistemi di IA come vietati limitano l'ambito di applicazione del divieto in misura tale che il divieto stesso rischia di diventare irrilevante nella pratica [ad esempio: «in un modo che provochi o possa provocare [...] un danno fisico o psicologico» nell'articolo 5, paragrafo 1, lettere a) e b) …".

dalla previsione di divieto (almeno nella versione attuale della Proposta) tutte quelle applicazioni software atte a manipolare gli utenti, ma che siano in grado di determinare 'solo' pregiudizi di carattere economico o sociale, e dunque sia ammesso l'utilizzo di sistemi di IA volti a condizionare non solo scelte economiche[82], ma anche scelte che possono avere un significativo impatto sociale (come ad esempio le preferenze politiche[83]). Una esclusione che, peraltro, riguarda anche la previsione sub b), ove il rinforzo di tutela contro possibili attività di manipolazione del comportamento che sfruttino la condizione di particolare vulnerabilità di uno specifico gruppo di persone dovute all'età o alla disabilità fisica o mentale (bambini, anziani, etc.), vede perdere gran parte della sua rilevanza.

Almeno per quanto riguarda il settore di nostro interesse un importante innalzamento nel livello di tutela degli utenti di servizi digitali destinati all'ambito della salute (come peraltro già rilevato) è stato comunque introdotto del *Digital Service Act*[84] che vieta di utilizzare la profilazione ottenuta grazie al trattamento di dati personali di cui all'articolo 9, § 1, del Reg. (UE) 2016/679 (categoria comprensiva dei dati relativi alla salute) per fornire pubblicità targhettizzata sulle piattaforme[85], all'uso della quale vengono riconnessi capacità manipolative con effetti negativi gravi, in alcuni casi con impatti su interi gruppi e significative ricadute sociali.

3.1.1. Dalla vulnerabilità strutturale alla vulnerabilità complessa. L'anziano come soggetto vulnerabile.

L'interazione tra uomo e sistemi di intelligenza artificiale rivela quella che può essere definita una "vulnerabilità strutturale" degli individui[86], che non ha origine nelle caratteristiche personali o circostanziali che possono interessare il singolo, ma si radica nel carattere intrinsecamente asimmetrico della relazione soggetto umano - agente artificiale. La dimensione congenita della vulnerabilità umana nel mondo digitale è alla base del c.d. "approccio universalistico" adottato dal regolamento europeo sulla protezione dei dati personali che considera tutti gli individui ugualmente esposti a potenziali violazioni della propria sfera personale digitale (si veda sopra paragrafo 3) e così facendo, nell'ignorare la stessa parola vulnerabilità (abbiamo visto come l'aggettivo vulnerabile è utilizzato una sola volta, in un considerando del pur lungo testo normativo), finisce per non rilevare l'esigenza di specifiche tutele[87].

L'idea che rispetto all'intelligenza artificiale sussista una condizione di vulnerabilità comune a tutti gli individui, intesa perlopiù come dipendenza[88] e fiducia[89], non può offuscare il fatto – del qua-

[82] Rispetto alle quali trova comunque applicazione la dir. 2005/29/CE sulle pratiche commerciali scorrette; cos P. HACKER, *op. cit.*, *passim.*

[83] Si pensi all'uso di *deepfake* che riprendono immagini o video di personaggi pubblici, politici, completamente fasulli al fine di condizionare le nostre valutazioni. Il problema è più compiutamente affrontato dalla proposta di regolamento sulla trasparenza e *targeting* della pubblicità politica del 25.11.2021, che prevede espressamente il divieto di tecniche di targeting o amplificazione in ambito di pubblicità politica che comportano il trattamento dei dati personali di cui all'art. 9, § 1 del Regolamento.

[84] Approvato dal Parlamento Europeo il 5.7.2022 unitamente al *Digital Markets Act*. I due provvedimenti compongono il *Digital Services Package*, che diventerà esecutivo dal 2023.

[85] Correttamente si rileva come, in termini di coordinamento con la disciplina contenuta nel *Digital Serivce Act*, l'art.5 della proposta di Regolamento IA dovrebbe includere tra i sistemi di IA assoggettati ai divieti di cui al medesimo articolo i sistemi di IA di profilazione a fini di marketing che trattano dati personali sensibili ai sensi dell'art. 9, § 1, Reg. (UE) 269/2016, S. ORLANDO, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di* Artifcial Intelligence Act, *cit.*, 365.

[86] Nel nostro dire da tenersi distinta dalla vulnerabilità ontologica dell'individuo come tratto distintivo della sua "finitezza umana". Per una attenta ricostruzione della "epistemologia" della vulnerabilità S. ZULLO, *Lo spazio sociale della vulnerabilità tra pretese di giustizia e pretese di diritto. Alcune considerazioni critiche*, in *Politica del diritto*, 2016, 475 ss.

[87] "La parola «vulnerabilità» tende ad assumere, nell'odierno dibattito etico e giuridico, un significato valutativo. Tendenzialmente, l'affermazione che un certo individuo è «vulnerabile» non informa cioè del semplice fatto che egli si trova in una certa situazione (da chiarire, data la genericità di «vulnerabile»), ma suggerisce anche che sarebbe bene porre rimedio a questa situazione, garantendo a quell'individuo una particolare protezione, o eliminando una discriminazione cui è soggetto, o riducendo uno svantaggio di cui soffre, ecc. Sotto questo aspetto, la parola «vulnerabile» è simile alla parola «discriminazione» (che peraltro indica una particolare specie di vulnerabilità), poiché una discriminazione non è una mera diseguaglianza di trattamento, ma è una diseguaglianza irragionevole o ingiusta. Pertanto, non riconoscere una vulnerabilità non significa solo non rendersi conto del fatto che si è verificata o si sta verificando una certa situazione, ma significa anche non rilevare, forse colpevolmente, che in quella situazione vi è qualcosa di (almeno *prima facie*) ingiusto", così E. DICIOTTI, *La percezione e i problemi della vulnerabilità*, in *Etica & Politica*, XXII, 2020, 1, 239 ss., 245.

[88] A. CARNEVALE, *Tecno-vulnerabili. Per un'etica della sostenibilità tecnologica*, Napoli-Salerno 2017, 35-39. In termini più generali A. MACINTYRE, *Animali razionali dipendenti*, 2001, Milano, passim.

[89] Parla per la prima volta della fiducia come una condizione di "vulnerabilità accettata" (l'accettazione della impossibilità di

le si reclama una presa di coscienza, soprattutto a livello politico istituzionale – che ulteriori condizioni di vulnerabilità, dipendenti da caratteristiche proprie dei singoli, come età e disabilità, ma anche da fattori esterni mutevoli ed eventualmente transitori, possano sovrapporsi alla prima, anche in forma plurima, determinando l'insorgere in capo al singolo individuo o a gruppi di individui di una situazione che potremmo definire di "vulnerabilità complessa".

La proposta di regolamento sulla IA prende atto di tale complessità soffermando la sua attenzione sulla vulnerabilità di alcune categorie (gruppi) di individui in relazione all'età o alla disabilità fisica o mentale - nella versione varata dalla Commissione - nonché in relazione alla situazione sociale o economica - in quella emendata dal Consiglio - con un passaggio che testimonia un atteggiamento di progressiva attenzione al tema della vulnerabilità e alle sue molteplici implicazioni[90], ma allo stesso tempo rischia, nel far riferimento a criteri potenzialmente più flessibili per individuare classi di individui vulnerabili, di rendere molto discrezionale l'ambito di applicazione del divieto[91]. Il fatto è che discettando di vulnerabilità, quando si passa dal piano filosofico-concettuale al piano giuridico-fattuale, la questione di quali criteri utilizzare per selezionare coloro ai quali garantire una protezione particolare diventa centrale.

Nella dicotomia tra fattori interni, intesi quali caratteristiche intrinseche al soggetto cui si intende riconoscere una condizione di vulnerabilità rilevante per il diritto (età, incapacità, stato di salute), e fattori esterni, quali elementi contestuali ed eventualmente transitori che possono rilevare allo stesso fine (fattori sociali ed economici), i primi sembrano garantire un più elevato grado di certezza nel processo di selezione.

Sennonché proprio con riferimento all'oggetto della nostra indagine - gli individui anziani - a fronte di una opinione comune che non esita a qualificarli come "soggetti vulnerabili" (e i recenti eventi pandemici hanno certamente contribuito a rafforzare una tale idea), si palesa in ambito giuridico un fronte molto meno unitario[92], per la difficoltà di individuare caratteristiche comuni e costanti dipendenti dall'età (avanzata) che possano qualificarli tali[93] e, come tali, vulnerabili e bisognosi di tutela. Nella visione di molti il considerare gli anziani come soggetti vulnerabili solo in ragione dell'avanzare del tempo, senza peraltro che sia davvero possibile individuare una soglia di età al di sopra della quale un soggetto possa essere definito come tale[94], potrebbe infatti palesarsi quale una forma di "discriminazione soggettiva" basata su di un ragionamento di natura presuntiva[95].

Al fine di evitare derive paternalistiche[96], con probabili ricadute in termini di emarginazione[97],

esercitare una forma di controllo) A. BAIER, *Trust and Anti-Trust*, «Ethics», 96, 1986, 231 ss.

[90] C. MACKENZIE, W. ROGERS, S. DODDS (a cura di), *Vulnerability. New Essays in Ethics and Feminist Philosophy,* Oxford,Oxford University Press, 2014, passim.

[91] Sul tema le puntuali osservazioni di E. DICIOTTI, *op. cit.*, 243 ss.

[92] In ambito consumeristico è possibile rilevare come la maggior parte delle norme contenute nel codice del consumo che si occupano di tutelare i consumatori vulnerabili individuano come tali i minori e gli incapaci (art. 4 cod. cons. dedicato all'educazione del consumatore; art. 31 cod. cons. in materia di televendita; art. 67 *quater* cod. cons., in materia di informazione nei contratti di commercializzazione a distanza di servizi finanziari ai consumatori) ma in alcune disposizioni si fa espressa menzione anche degli anziani (il riferimento è alla disciplina generale sulla sicurezza dei prodotti, ove la nozione di «prodotto sicuro» impone di tenere in considerazione le «categorie di consumatori che si trovano in condizione di rischio nell'utilizzazione del prodotto, in particolare dei minori e degli anziani» (art. 103, co. 1, lett. a, n. 4, cod. cons.) e all'art. 11, d. lgs. 8.11.2021, n. 210, attuativo della dir. (UE) 2019/944 relativa a norme comuni per il mercato interno dell'energia elettrica, che nella definizione di cliente vulnerabile annovera, tra gli altri, alla lettera f quelli «di età superiore ai 75 anni».

[93] Anche "il dibattito relativo al riconoscimento della soggettività delle persone anziane appare maggiormente "polarizzato", tanto che anche il confronto relativo all'opportunità che le Nazioni Unite adottino una specifica convenzione a tutela dei loro diritti sembra essersi arenato, principalmente a causa della difficoltà di individuare i "confini" del gruppo in questione e di ravvisare al suo interno una qualche omogeneità", così M.G. BERNARDINI, *(In)visibili? La vulnerabilità alla violenza di chi non ha l'età*, in *GenIUS,* 2, 2020, 1 ss., 10.
A livello di Carta costituzionale l'età viene più volte in rilievo con riferimento alle persone minori, ma non a quelle anziane; nella Carta dei diritti fondamentali dell'Unione europea sussiste uno specifico divieto di discriminazione in ragione dell'età (art. 21), e sono prese in considerazione sia la soggettività delle persone minori (art. 24), sia quella delle persone anziane (art. 25).

[94] Dal punto di vista degli studi antropologici la soglia di ingresso nella c.d. terza età tende progressivamente a spostarsi verso avanti. In occasione del 63° Congresso Nazionale della Società Italiana di Gerontologia e Geriatria (SIGG) del novembre 2018, è stata data una nuova definizione dinamica di anzianità (soglia da 65 a 75 anni), più confacente alle attuali *performance* fisiche e mentali, alla situazione demografica della popolazione italiana e, in generale, alle condizioni psicofisiche dei soggetti appartenenti a Paesi ad alto reddito. Per l'allungamento medio della speranza di vita alla nascita (in Italia 85 anni per le donne e 82 per gli uomini) è stata creata una nuova categoria di anzianità, dividendo le persone con più di 65 anni tra chi appartiene alla terza età (condizionata da buone condizioni di salute, inserimento sociale e disponibilità di risorse) e alla quarta età (caratterizzata da dipendenza da altri e decadimento fisico).

[95] N. ZORZI GALGANO, *op. cit.*, 587 ss. In termini più generali DOGLIOTTI, *I diritti degli anziani*, in *Riv. trim. dir. e proc. civ.*, 1987, 714 ss.

[96] B. CARDELLA TEDESCHI, *Diritto degli anziani/diritto per gli anziani*, in *Anziani, diritti, bisogni, prospettive*, a cura di V. CAPPELLATO, B. GARDELLA TEDESCHI, E. MERCURI, Torino, 2021, 191 ss.

l'idea suggerita dai più è che la condizione di vulnerabilità del soggetto anziano debba essere valutata di volta in volta, in ragione delle reali condizioni psico-fisiche della persona[98], che tuttavia risultano concretamente rilevabili solo in ragione di un'indagine *ad hoc*, perlopiù effettuata *ex post*.

Il tipo di protezione che qui si intende garantire è tuttavia di ordine preventivo: si vogliono vietate quelle pratiche di intelligenza artificiale che sfruttano le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di influenzare il loro comportamento fino al punto di provocare o poter provocare loro un danno fisico o psicologico. In relazione a tale tipo di politiche di protezione l'individuare un limite di età superato il quale si possa ritenere che il progressivo decadimento delle forze fisiche e mentali che accompagna l'invecchiamento determini in via generalizzata una condizione di maggiore vulnerabilità dell'individuo[99], potrebbe invero apparire opportuno, anche e soprattutto in termini di effettività della previsione normativa[100]. Si tratta di elaborare una "nozione sociale di anziano", che possa giovarsi di criteri di identificazione della categoria ricavabili dalle scienze sociali e mediche, soggetti come tali a possibili mutamenti nel tempo, ma pur sempre necessari per non cadere vittime di un relativismo foriero di costante indeterminatezza.

[97] DOGLIOTTI, *I diritti degli anziani*, in *Riv. trim. dir. e proc. civ.*, 1987, 714. In tal senso si vedano anche le riflessioni di P. PERLINGIERI, *Diritti della persona anziana, diritto civile e stato sociale*, in *Anziani e tutele giuridiche*, a cura di P. STANZIONE, Napoli, 1991, 96.
[98] C.M. BIANCA, *Senectus ipsa morbus?*, in Aa.Vv., *Studi in onore di Pietro Rescigno*, II, Milano, 1998, 98.
[99] S. PATTI, *Senilità e autonomia negoziale della persona*, in *Fam. pers. succ.*, 2009, 259 ss.
[100] G. VETTORI, *Effettività fra legge e diritto*, Milano, 2020, *passim*.