RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0262 • articolo sottoposto a peer review • pubblicato in anteprima il 22 gen. 2026

Federica Scialoia

L'utilizzo di dati sanitari, *real-world data* e dati sintetici nello sviluppo di tecnologie sanitarie innovative nell'Unione europea

Il presente lavoro esplora le potenzialità dei dati sanitari nello sviluppo di tecnologie innovative, analizzando le possibili strategie per agevolare l'utilizzo di tali dati senza compromettere il diritto alla privacy dell'interessato. In particolare, l'indagine si soffermerà sull'importanza del trattamento di dati provenienti dal mondo reale per lo sviluppo di tecnologie sanitarie, in quanto più precisi e affidabili e dunque in grado di contribuire al miglioramento della salute dei pazienti. Tuttavia, trattandosi di dati sensibili ai sensi del GDPR è necessario il consenso dell'interessato al loro trattamento. Infine, vengono esaminate le possibili soluzioni per "anonimizzare" i dati sanitari, riflettendo sulla possibilità di introdurre una disciplina europea sui dati sintetici.

GDPR – Dati sanitari – Dati provenienti dal mondo reale – Tecnologie sanitarie – Dati sintetici

The use of health data, real-world data and synthetic data in the development of innovative health technologies in the European Union

This paper explores the potential of health data in the development of innovative technologies, analysing possible strategies to facilitate the use of such data without compromising the right to privacy of the data subject. In particular, the investigation will focus on the importance of real-world data processing for the development of healthcare technologies as more accurate and reliable and thus contributing to improved patient health. However, since it is sensitive data pursuant the GDPR, the consent of the data subject is required for their processing. Finally, are examined possible solutions for "anonymizing" health data, reflecting on the possibility of introducing a European discipline on synthetic data.

GDPR – Health data – Real-world data – Health technology – Synthetic data

L'Autrice è dottoressa di ricerca in diritto dell'Unione europea presso l'Università di Napoli "Parthenope"

Sommario: 1. Cenni introduttivi. – 2. Il trattamento dei dati sanitari alla luce del GDPR e le interazioni con il Regolamento sull'intelligenza artificiale. – 3. L'attuale quadro normativo in materia di "Real World Data". – 4. La nuova frontiera dei "dati sintetici". – 5. Possibili risvolti evolutivi di una disciplina europea in materia di dati sintetici.

1. Cenni introduttivi

Proteggere la salute e i diritti dei pazienti significa non soltanto garantire la sicurezza dei medicinali, dei dispositivi medici e in generale delle applicazioni tecnologiche impiegate nel settore sanitario, come previsto dall'art. 168, par. 4 TFUE[1], ma anche tutelare i dati sanitari dei pazienti trattati per lo sviluppo di tecnologie innovative. La maggior parte delle applicazioni tecnologiche come le terapie digitali[2] richiedono per il loro sviluppo il

1. Cfr. Oddenino 2010, p. 131 ss.; Fares–Campagna 2011, p. 325 ss.; Bestagno 2017-a, p. 119 ss.; Di Federico 2017, p. 664 ss.; Pesce 2021, p. 469 ss.; Bestagno 2017-b, p. 317 ss. In particolare, i "problemi comuni di sicurezza in materia di sanità pubblica, per quanto riguarda gli aspetti definiti nel presente trattato" rientrano nelle competenze concorrenti, come espressamente previsto dalla lett. k) del par. 2 dell'art. 4 TFUE. Nondimeno, siffatta competenza, attribuita nell'ambito esclusivo di intervento del par. 4 dell'art. 168 TFUE, si differenzia nettamente da quella che spetta all'Unione negli altri paragrafi del richiamato articolo, trattandosi, ai sensi dell'art. 2, par. 5, TFUE, di azioni intese a sostenere, coordinare o completare l'azione degli Stati membri, senza tuttavia potersi sostituire alla loro competenza, oppure come stabilito ai sensi del successivo art. 6, lett. a), TFUE, di azioni intese a sostenere, coordinare o completare l'azione degli Stati membri in settori quali la "tutela e il miglioramento della salute umana". È evidente, dunque, che tali ultimi articoli sono derogati dal citato par. 4 dell'art. 168 TFUE che, come noto, nelle altre ipotesi indicate, relega alla dimensione sovranazionale un ruolo di sostegno, coordinamento e completamento rispetto all'azione dei Paesi membri, rimanendo la "sanità", di cui al Titolo XIV del TFUE, declinata nell'art. 168, esclusa dall'elenco di cui all'art. 3 TFUE che stabilisce le competenze attribuite in modo esclusivo all'Ue. Tuttavia, si deroga a tale principio, solo per le misure ricomprese nell'alveo del par. 4 dell'art. 168 TFUE, attribuendo in tale settore all'Unione una competenza concorrente con quella degli Stati membri. Per esemplificare, nell'ambito delle misure circa organi e sostanze di origine umana, medicinali e dispositivi di impiego medico, nonché misure nei settori veterinario e fitosanitario, l'Unione si vede assegnate ben più significative, sebbene non esclusive, competenze, mentre nel quadro complessivo e generale dell'art. 168 TFUE essa può intervenire con azioni di mero completamento delle politiche interne degli Stati. Ciononostante autorevoli esponenti della dottrina hanno già avuto modo di precisare come sia necessario ridefinire i criteri di riparto delle competenze tra Stati membri e Unione in tale delicato settore, in tal senso vedi Rossi 2013, p. 749 ss.; Hodson–Maher 2018. Mentre per un commento della recente risoluzione del Parlamento europeo del 22 novembre 2023 sui progetti del Parlamento europeo intesi a modificare i trattati (2022/2051(INL)) vedi in particolare Adinolfi 2024, p. 8 ss.; Lazzerini 2023; Duff 2023, p. 9 ss.; Di Federico 2021-a, p. 71 ss.; Di Federico 2021-b, p. 8 ss.; Rinoldi 2022, p. 280.
2. Trattasi di applicazioni tecnologiche conosciute anche con l'acronimo *Dtx*, che deriva dal termine "*Digital Therapeutics*", utilizzato per indicare un settore specifico della sanità digitale quello relativo alle terapie digitali. In tale settore vengono ricomprese tutte quelle terapie effettuate tramite l'utilizzo di programmi software di alta qualità, supportati da evidenze scientifiche e cliniche. La possibilità di accedere ad una terapia digitale, tuttavia,

trattamento di dati personali con la conseguenza che il legislatore europeo dovrà fornire una duplice tutela: nei confronti dei destinatari di dette tecnologie e nei confronti dei fornitori di tali dati specie quando il trattamento venga effettuato da aziende private. In verità, già la comunicazione della Commissione europea del dicembre 2018[3] chiariva come lo sviluppo di sistemi di intelligenza artificiale non potesse trascendere dal quadro giuridico preesistente, in particolare, da quello posto a protezione dei dati personali[4]. Gli orientamenti del gruppo di esperti incaricati di elaborare i principi etici da rispettare per lo sviluppo dei sistemi di intelligenza artificiale mostravano un'attenzione specifica per la tutela dei dati personali precisando l'importanza di garantire la riservatezza e la protezione dei dati durante l'intero ciclo di vita del sistema[5], essendo a tal fine fondamentale l'intervento di un supervisore umano[6]. Questi ultimi aspetti ben evidenziati dal gruppo di esperti risultano peraltro presenti nella versione definitiva del testo del regolamento. Più concretamente, gli sviluppatori dovranno vagliare accuratamente la qualità, la natura, l'origine e la quantità di dati personali utilizzati, riducendo i dati inutili, ridondanti o marginali durante lo sviluppo e le fasi di addestramento e poi monitorare l'accuratezza del modello man mano che viene alimentato con nuovi dati[7]. Emerge pertanto una chiara intenzione delle istituzioni europee di regolare l'intelligenza artificiale senza pregiudicare i diritti fondamentali e, per quanto ci riguarda ai fini del prosieguo di questo scritto, della disciplina sulla protezione dei dati personali[8]. Senza soffermarsi in questa sede sulla struttura del regolamento sull'intelligenza artificiale che è stata ampiamente approfondita da molti esponenti

deve essere comunque valutata da un medico caso per caso e ciò avuto riguardo ad un'attenta disamina delle esigenze del paziente, prestando particolare attenzione sul livello di autonomia e di motivazione dello stesso. Non meno trascurabile pare la valutazione delle capacità tecnologiche di quest'ultimo per l'utilizzo dello strumento digitale in questione. Nondimeno, l'utilizzo delle *Dtx*, qualora ne sussistano i presupposti, potrebbe consentire l'identificazione precoce di eventuali ricadute di disturbi o malattie mediante il monitoraggio regolare dei sintomi e la valutazione dei progressi terapeutici, costituendo un valido strumento nelle mani tanto del medico quanto del paziente. Per un approfondimento esaustivo del tema in esame si rimanda a Scialoia 2024, p. 767 ss.; Salvatore 2023-b, p. 29 ss.

3. Comunicazione della Commissione *Piano coordinato sull'Intelligenza Artificiale*, 7 dicembre 2018, COM (2018) 795, preceduta, come noto, dalla Comunicazione della Commissione L'intelligenza artificiale per l'Europa, 25 aprile 2018, COM (2018) 237.
4. La Comunicazione della Commissione, *Piano coordinato sull'Intelligenza Artificiale* stabiliva che l'apertura ai flussi di dati internazionali dovrà continuare ad essere garantita nel pieno rispetto delle norme dell'Ue per la protezione dei dati personali e in conformità agli strumenti giuridici applicabili.
5. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per un'IA affidabile*, punto 72.
6. Il punto 65 degli *Orientamenti etici per un'IA affidabile* stabiliva che "la sorveglianza umana aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi. La sorveglianza può avvenire mediante meccanismi di governance che consentano un approccio con intervento umano (*human-in-the-loop* - HITL), con supervisione umana (*human-on-the-loop* - HOTL) o con controllo umano (*human-in-command* - HIC). L'approccio HITL prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile né auspicabile. L'approccio HOTL prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema".
7. *Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), approvato dal Consiglio d'Europa in occasione della riunione del 17 e 18 maggio 2018, ad Elsinore, in Danimarca. La Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108) è stata aperta alla firma a Strasburgo il 29 gennaio 1981.
8. Sul punto vedi Pollicino–De Gregorio 2021, p. 205 ss.; González de la Garza 2008, p. 62 ss.

della dottrina[9], basti qui ricordare che per il funzionamento di tali sistemi è necessario l'utilizzo di una grande mole di dati. Le modalità di raccolta e trattamento degli stessi, tuttavia, risultano assoggettate alla disciplina prevista dal regolamento 2016/679[10] il cui obiettivo è quello di bilanciare i vantaggi della sanità digitale rispetto ai rischi derivanti dalla divulgazione delle informazioni che discendono dal trattamento di dati sensibili. Il presente lavoro non ha l'obiettivo di ricostruire in maniera sistematica tutti gli aspetti relativi alla sanità digitalizzata, piuttosto, partendo dall'analisi dei dati sanitari come strumento utilizzabile per lo sviluppo di tecnologie altamente sofisticate in grado di contribuire al miglioramento della salute umana in conformità a quanto previsto dall'art. 35 della Carta dei diritti fondamentali dell'Unione europea[11], si propone di valutare l'apporto in tale settore dei meccanismi di "anonimizzazione", per sfuggire agli obblighi imposti dal GDPR senza pregiudicare il diritto alla protezione dei dati sanitari dei pazienti. Un'attenzione particolare sarà pertanto dedicata ai *real-world data* (di seguito nell'acronimo RWD) per tale intendendosi non una mera formula descrittiva bensì una categoria specifica di dati, corrispondente ai "dati provenienti dal mondo reale", al fine di renderli facilmente accessibili incrementando la loro disponibilità per finalità legate alla ricerca scientifica tramutandoli in "dati sintetici" e dunque anonimi.

2. Il trattamento dei dati sanitari alla luce del GDPR e le interazioni con il Regolamento sull'intelligenza artificiale

Occorre innanzitutto ricordare che la protezione dei dati personali è un diritto fondamentale che, ai sensi degli artt. 16 TFUE[12], 8 CDFUE[13], nonché dell'art. 8 CEDU[14], non ammette limitazioni a meno che non siano presenti scopi legittimi di natura medica e sanitaria, purché previsti dalla legge e solo nel caso in cui rispettino il contenuto essenziale di tale diritto e qualora siano proporzionati e necessari e dunque rispondenti a finalità di interesse generale riconosciute dall'Unione[15].

9. Vedi in particolare Carta 2024, p. 188 ss.; Inglese 2024; Rugani 2024; Zaccaroni 2024; Volpato 2024; Lattanzi 2024.
10. Per un commento vedi Fumagalli 2016, p. 1 ss.; Bassini 2016, p. 587 ss.; Mariottini 2016, p. 905 ss.; Ricci 2017; Cuffaro–D'Orazio–Ricciuto 2019.
11. In tal senso vedi Salvatore 2023-a, p. 3 ss.
12. "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea."
13. Vedi in particolare González Fuster 2014, p. 198 ss. Pollicino–Bassini 2017, p. 134 ss.; Calzolaio 2017, p. 594 ss.
14. Sul punto si rimanda alla Corte EDU, sentenza 25 febbraio 1997, *Z. c. Finlandia*, ricorso n. 22009/93, punto 95, in cui si afferma che le legislazioni nazionali devono garantire la riservatezza dei dati sanitari ai sensi dell'art. 8 CEDU.
15. L'art. 52 CDFUE stabilisce che "1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. 2. I diritti riconosciuti dalla presente Carta per i quali i trattati prevedono disposizioni si esercitano alle condizioni e nei limiti dagli stessi definiti. 3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa. 4. Laddove

Coerentemente alle richiamate norme di diritto primario, la disciplina prevista nell'ambito della direttiva 95/46/CE[16] viene modificata e sostituita dal più recente Regolamento Ue 679/2016, favorendo un innalzamento dello standard di protezione a livello nazionale essendo la normativa in esso contenuta direttamente applicabile. A ben vedere, il regolamento offre una nozione molto ampia di dati sanitari definiti come "dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute"[17]. Più specificamente, questi ultimi "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 direttiva 2011/24/UE del Parlamento europeo e del Consiglio[18]; 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 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"[19]. Probabilmente l'intenzione del legislatore europeo nell'individuazione della nozione di "dati relativi alla salute" è quella di apprestare una tutela maggiore ai singoli, tuttavia, l'efficacia concreta della normativa in questione dipende dal contributo fornito da nuove figure professionali introdotte dal regolamento quali il titolare del trattamento e il responsabile del trattamento e dal rispetto dei principi che regolano la legislazione europea in materia di dati sanitari. Tra questi si annovera la "finalità" del trattamento, in quanto i dati personali e ancor più quelli sulla salute possono essere trattati solo nell'ambito delle finalità che si intendono perseguire[20] informando, in ogni caso, adeguatamente gli interessati[21]. In conformità al principio di "minimizzazione", inoltre, i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"[22]. Ad esempio, la documentazione in possesso di strutture pubbliche a scopi puramente amministrativi non dovrebbe contenere i parametri vitali del paziente in quanto tali aspetti appaiono superflui rispetto al profilo meramente gestionale[23]. Il trattamento dei dati sanitari inoltre è lecito soltanto nell'ipotesi in cui ricorrano le condizioni stabilite dal Regolamento. Invero, l'art. 6, par. 1 richiede il consenso dell'interessato, la necessità di proteggere i suoi interessi

la presente Carta riconosca i diritti fondamentali quali risultano dalle tradizioni costituzionali comuni agli Stati membri, tali diritti sono interpretati in armonia con dette tradizioni. 5. Le disposizioni della presente Carta che contengono dei principi possono essere attuate da atti legislativi e esecutivi adottati da istituzioni, organi e organismi dell'Unione e da atti di Stati membri allorché essi danno attuazione al diritto dell'Unione, nell'esercizio delle loro rispettive competenze. Esse possono essere invocate dinanzi a un giudice solo ai fini dell'interpretazione e del controllo di legalità di detti atti. 6. Si tiene pienamente conto delle legislazioni e prassi nazionali, come specificato nella presente Carta. 7. I giudici dell'Unione e degli Stati membri tengono nel debito conto le spiegazioni elaborate al fine di fornire orientamenti per l'interpretazione della presente Carta".

16. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
17. Vedi art. 4, n. 14 del GDPR.
18. Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.
19. Vedi considerando n. 35 del GDPR.
20. Nell'ambito sanitario le finalità possono essere principalmente di tre tipologie: di cura, di ricerca o amministrativo/contabili.
21. Strettamente collegati a detto principio sono i principi di proporzionalità, necessità, pertinenza e non eccedenza.
22. Vedi art. 5, par. 1, lettera c del GDPR.
23. Califano 2018, p. 20.

vitali o ancora l'esistenza di un interesse pubblico derivante dal trattamento. Prima di svolgere qualunque considerazione specificamente attinente al tema oggetto di indagine, è opportuno interrogarsi sulla figura del titolare del trattamento in quanto su quest'ultimo graverà, coerentemente con il principio di *accountability*, l'individuazione della base giuridica più idonea. Sappiamo infatti che quest'ultimo deve redigere un registro relativo alle attività di trattamento svolte sotto la propria responsabilità dovendo altresì adottare le misure tecniche e organizzative che risultino adeguate a garantire un livello di sicurezza adatto al rischio[24]. Detto obbligo è però esteso anche al responsabile del trattamento vale a dire "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali[25] per conto del titolare del trattamento"[26]. Nondimeno i maggiori problemi si riscontrano con riguardo all'esatta individuazione di quest'ultima figura, specie quando lo sviluppo delle tecnologie sanitarie richieda l'applicazione cumulativa del regolamento sull'intelligenza artificiale e del regolamento sulla protezione dei dati personali[27]. Invero, mentre quest'ultimo pone gli obblighi specifici suesposti in capo al titolare del trattamento, l'altra fonte derivata si sofferma invece esclusivamente sui "fornitori", con la conseguenza che nell'ambito dei sistemi di IA nel settore sanitario, non è facile comprendere chi debba rivestire la qualifica del "titolare del trattamento". Alcuni esponenti della dottrina hanno sostenuto che quest'ultimo debba coincidere con lo stesso sistema di intelligenza artificiale[28], detta impostazione appare tuttavia fuorviante in quanto finisce per dotare i sistemi di intelligenza artificiale di un'autonomia decisionale che

24. Art. 30 del GDPR.

25. Sulla definizione di dati personali si veda López Pina 2022, p. 51 ss.

26. Art. 4, par. 1, n. 8 del GDPR.

27. Vedi in particolare Contaldi 2021, p. 1203. Sebbene con riguardo specifico alla proposta di regolamento sull'intelligenza artificiale l'autore militi a favore della tesi che predilige l'approccio cumulativo di entrambe le fonti di diritto derivato. Invero dal momento che il regolamento sulla protezione dei dati mira a tutelare un diritto fondamentale previsto dalla normativa europea, i conflitti tra le due fonti normative non possono essere risolti in base al principio di specialità dovendo entrambe le fonti derivate applicarsi in maniera cumulativa. L'autore rileva inoltre che molte disposizioni, già presenti nella proposta di regolamento sull'intelligenza artificiale sembrerebbero deporre per la suddetta tesi. In particolare il considerando 24 il quale stabilisce che "qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica… dovrebbe *continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679*". Oltre al considerando 72 che prevede che la creazione di spazi nei quali si procede a sviluppare ed istruire i sistemi di intelligenza artificiale debba avvenire tenendo conto delle prescrizioni dell'art. 6, paragrafo 4, del regolamento 2016/679 che stabilisce che "laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione". Per una puntuale disamina delle implicazioni derivanti dal trattamento dai dati personali rispetto alla proposta di regolamento sull'intelligenza artificiale vedi Resta 2022, p. 323 ss; Rossi Dal Pozzo 2020, p. 13 ss.

28. Simone 2020, p. 275 ss., p. 283.

prescinde da qualsiasi controllo umano[29]. Peraltro, dal dato testuale è possibile immediatamente escludere tale equiparazione non solo per il fatto che il regolamento sull'intelligenza artificiale non consente l'operatività di detti sistemi in maniera autonoma prevedendo sempre la necessità di un controllo umano, ma anche poiché lo stesso regolamento sulla protezione dei dati personali nell'individuare all'art. 4, par. 1 n. 7 i soggetti che potrebbero rivestire la qualifica di "titolare del trattamento" precisa che quest'ultimi possono coincidere con qualunque "persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento". Sebbene il contenuto della disposizione appaia abbastanza ampio è comunque inequivocabile l'intenzione del legislatore di richiedere un minimo di personificazione per l'assunzione di tale veste. In tale prospettiva, lo stesso art. 22 del GDPR nello stabilire che "l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona" sembrerebbe orientarsi per il riconoscimento di tale diritto al soggetto passivo che deve necessariamente coincidere con un individuo o un ente che abbia piena capacità giuridica, dotato dunque del potere di assumere decisioni in vece del sistema di IA[30]. Nell'attuale panorama regolatorio, deve pertanto negarsi la possibilità di concepire sistemi di IA totalmente automatizzati. Tale conclusione appare tanto più logica se si riflette sui profili di responsabilità derivanti dall'utilizzo di tecnologie particolarmente innovative nel settore sanitario. Così, soprattutto quando queste ultime siano fondate sull'utilizzo di sistemi di intelligenza artificiale sorge spontaneo chiedersi su chi debbano gravare gli obblighi discendenti dal GDPR nello sviluppo di tali tecnologie[31]. Verosimilmente la soluzione più appropriata sarebbe quella di rimettere in capo al fornitore il compito di rispettare le norme sulla protezione dei dati personali, dovendo nello sviluppo di dette applicazioni, attenersi anche agli obblighi imposti dal regolamento sull'intelligenza artificiale a seconda del "rischio" rispetto ai diritti fondamentali[32]. Più segnatamente, in conformità alle disposizioni del GDPR, quest'ultimo dovrà valutare attentamente i costi, la natura, l'oggetto, il contesto e la finalità del trattamento, avuto riguardo ai rischi potenziali per i diritti e le libertà dei singoli. L'onere probatorio relativo alla sicurezza del sistema incombe invece sulla stessa struttura, mentre sul titolare del trattamento grava la valutazione d'impatto sulla protezione dei dati sanitari[33],

29. Pizzetti 2018.

30. In tal senso Adinolfi 2020, p. 13 ss.

31. La letteratura riguardante il trattamento dei dati personali nello sviluppo di sistemi di intelligenza artificiale risulta molto ampia vedi in particolare Adinolfi–Simoncini 2022; Caggiano–Contaldi–Manzini 2024; Pajno–Donati–Perrucci 2022; Grieco 2023; Carta 2024, p. 188 ss.

32. L'Unione europea ha adottato una disciplina che non si basa sulle caratteristiche tecniche nell'utilizzo dell'intelligenza artificiale e dei suoi effetti ma sul sistema dei rischi collegati all'utilizzo di tali tecnologie. In quest'ottica, l'individuazione delle norme applicabili si fonda sulla ripartizione dei sistemi in quattro distinte categorie calibrate in base ai diversi fattori di "rischio". Nella prima categoria rientrano le applicazioni di IA i cui rischi risultano "inaccettabili". Tra queste, si annovera l'identificazione biometrica in tempo reale e gli algoritmi per il *social scoring*. Nella prospettiva dell'applicazione di tali sistemi al campo medico è interessante notare come tra le pratiche vietate siano incluse "l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta 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" vedi art. 5 lett. b. Tale previsione normativa tende a tutelare i pazienti che in contesti sanitari si trovino molto spesso in condizioni di vulnerabilità, potendo il loro comportamento essere distorto o influenzato.

33. Valutazione d'impatto sulla protezione dei dati (nell'acronimo DPIA, "*Data Protection Impact Assessment*"). Per una puntuale disamina del relativo meccanismo si rimanda a Hervey–Lavy 2020, p. 384. La procedura in questione è obbligatoria quando il trattamento possa "*presentare un rischio elevato per i diritti e le libertà delle*

potendo quest'ultima ai sensi dell'art. 35 del GDPR contenere l'esame di più trattamenti simili che presentino rischi analoghi. Per tutte le applicazioni tecnologiche che comportino un rischio particolarmente elevato l'art. 36 del GDPR prevede una preventiva consultazione con le organizzazioni dei pazienti e, se possibile, con i rispettivi garanti della protezione dei dati personali degli Stati membri[34].

3. L'attuale quadro normativo in materia di "real-world data"

Analizzate le linee essenziali della normativa relativa allo sviluppo di tecnologie innovative nel settore sanitario è possibile ora passare in rassegna la tipologia di dati sanitari che dovrebbero essere trattati per lo sviluppo di dette tecnologie. Non essendo qui dato analizzare tutte le tipologie di dati utilizzabili, si focalizzerà l'attenzione esclusivamente sui "real-world data" ciò in virtù del loro valore particolarmente significativo in termini di sicurezza ed efficacia del dispositivo. Occorre subito chiarire che trattandosi di dati generati da pazienti durante il loro percorso di cura e dunque direttamente desumibili dalla pratica clinica sono particolarmente precisi e accurati[35]. La loro eterogeneità consente infatti di ottenere informazioni aggiornate con riguardo al reperimento di evidenze scientifiche che andranno poi impiegate in procedimenti di HTA a livello di Unione[36] per lo sviluppo di nuove tecnologie. Saranno tuttavia utilizzati ai fini delle valutazioni cliniche congiunte esclusivamente i dati relativi al rischio/beneficio dei dispositivi escludendo qualsiasi valutazione di tipo economico/organizzativo e in relazione all'allocazione delle risorse. Ciononostante, nelle fasi di sviluppo dei farmaci e dei dispositivi medici la *real-world evidence* (RWE)[37] potrà fornire diverse e ulteriori informazioni in grado di migliorare le conoscenze in termini di efficacia, sicurezza e *compliance*. Con specifico riguardo allo sviluppo di medicinali è infatti evidente la crescente rilevanza di detti dati in quanto come precisato dall'EMA la maggior parte delle autorizzazioni di immissione in commercio rilasciate dagli enti regolatori conseguono alla valutazione dell'esistenza di prove di efficacia derivanti dal mondo reale[38]. L'uso della RWE per supportare il processo decisionale normativo non è però una novità. Sebbene tali dati siano stati utilizzati per decenni nella fase post-autorizzazione per valutare la sicurezza del medicinale, diversi studi ne apprezzano la rilevanza anche con riguardo al procedimento di valutazione[39]. Sul punto è bene precisare come il nuovo regolamento sullo spazio europeo dei dati sanitari[40], in linea con gli obiettivi tracciati dalla strategia europea in materia di dati[41], sembri orientarsi verso il riconoscimento del valore dell'uso di prove derivanti dal mondo reale per i processi decisionali correlati allo

persone fisiche". Va da sé, dunque, che la DPIA si differenzi dalla valutazione d'impatto prevista dal regolamento europeo sull'intelligenza artificiale *Fundamental Rights Impact Assessment*, di seguito "FRIA" per la maggiore specificità, non essendo rivolta alla totalità dei diritti fondamentali ma solo alla protezione dei dati personali.

34. Van Veen 2018, p. 70 ss.
35. Si tratta di dati provenienti da diverse fonti, tra cui database clinici, database amministrativi, registri di popolazione e di malattia, registri farmaceutici, cartelle cliniche elettroniche, *population health surveys* e dati di mobile *devices*, *wearable* e *apps*.
36. Regolamento (UE) 2021/2282 del Parlamento europeo e del Consiglio del 15 dicembre 2021 relativo alla valutazione delle tecnologie sanitarie e che modifica la direttiva 2011/24/UE. Per un approfondimento vedi Danieli 2023, p. 111 ss.
37. Con l'espressione *Real World Evidence* (RWE) deve intendersi l'analisi strutturata e organizzata di dati provenienti dalla reale pratica clinica (RWD), che consente di generare informazioni a integrazione delle evidenze prodotte dagli studi clinici sperimentali.
38. Flynn–Pluschke–Quinten et al. 2021, p. 90 ss.
39. Arlett–Kjær–Broich–Cooke 2022, p. 21 ss.
40. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847; per un commento della proposta di regolamento si veda Scialoia 2023.
41. Comunicazione della Commissione europea, *Una strategia europea per i dati*, COM (2020) 66.

sviluppo, all'autorizzazione e al monitoraggio non solo dei farmaci ma anche dei dispositivi medici e delle tecnologie digitali nel settore sanitario. Nello specifico, nell'individuare le categorie di dati sanitari elettronici che possono essere trattati per l'uso secondario, il regolamento include dati pertinenti provenienti dal sistema sanitario (cartelle cliniche elettroniche, dati relativi alle domande di rimborso, registri di malattia, dati genomici ecc.), dati che hanno un impatto sulla salute (ad esempio, consumo di varie sostanze, posizione socioeconomica, comportamento), inclusi i fattori ambientali (ad esempio, inquinamento, radiazioni, uso di determinate sostanze chimiche) e infine dati generati automaticamente provenienti da dispositivi medici o generati direttamente dalla persona attraverso applicazioni per il benessere[42]. Orbene, anche se nel regolamento non si rinvenga un espresso riferimento normativo ai dati provenienti dal mondo reale non introducendosi alcuna definizione in merito, dall'elenco di cui all'art. 33 è facile comprendere come esso si fondi esclusivamente sul riutilizzo di tale tipologia di dati[43]. Va da sé dunque ritenere che il dato proveniente dal mondo reale non sia limitato alla mera valutazione *ex post* del dispositivo in termini di sicurezza ed efficacia ma ben si estenda al procedimento normativo nel suo complesso. Pertanto, non è da trascurare il contributo che esso potrà avere in tutte le fasi del ciclo di vita della tecnologia e dunque anche nel supporto dell'iter valutativo dei farmaci. Le informazioni raccolte potrebbero infatti essere utilizzate dagli enti regolatori per monitorare costantemente il medicinale e valutare l'appropriatezza dell'intervento terapeutico nella pratica clinica. In conclusione può ritenersi che, pur creando le condizioni per il riutilizzo dei dati sanitari per finalità di ricerca attraverso una data governance condivisa, in vista dello sviluppo di trattamenti innovativi, le potenzialità dello spazio europeo dei dati sanitari, potrebbero essere migliorate, ad esempio, regolando e rendendo disponibili i RWD per disporre di informazioni integrative necessarie a rendere le prestazioni sanitarie più personalizzate. A tal fine, sarebbe auspicabile l'individuazione di definizioni chiare e condivise sulle varie tipologie di dati, essendo tuttora assente una nozione giuridicamente rilevante di *real-world data*. Oltre tutto non sembra trascurabile neppure l'obiettivo di armonizzare i criteri di accesso e gli standard di interoperabilità tra piattaforme individuando un meccanismo di partecipazione a livello di Unione in base al quale l'interessato presti il consenso all'uso secondario dei dati in un'ottica di GDPR *by design*, per evitare di dover richiedere il consenso ai singoli pazienti in un momento successivo alla progettazione del prodotto.

4. La nuova frontiera dei "dati sintetici"

L'analisi sin qui condotta lascia trasparire ancora talune ombre che devono dipanarsi. Benché sia soluzione condivisibile ritenere che spetti all'Unione europea intervenire sui richiamati profili per creare un connubio perfetto tra il modello europeo di protezione dei dati sanitari e la promozione del mercato digitale europeo, restano da chiarire le modalità operative per il raggiungimento di tale atteso risultato. Come anticipato, il regolamento sullo spazio europeo (EHDS) mira a facilitare l'accesso e la condivisione dei dati sanitari, promuovendo l'utilizzo di dati provenienti dal mondo reale. Fermo restando che il trattamento di tali dati è fondamentale per lo sviluppo di tecnologie sanitarie, occorrerebbe individuare la metodologia da

42. Vedi in particolare il considerando n. 39 del Regolamento sullo spazio europeo dei dati sanitari.

43. Vedi art. 33 del Regolamento sullo spazio europeo dei dati sanitari che elenca le categorie di dati sanitari elettronici per l'uso secondario inglobando: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti comportamentali, socioeconomici e ambientali della salute; c) dati sugli agenti patogeni pertinenti che incidono sulla salute umana; d) dati amministrativi relativi all'assistenza sanitaria, compresi i dati relativi alle domande di rimborso e ai rimborsi; e) estratti dei dati genetici, genomici e proteomici umani, quali i marcatori genetici; f) dati sanitari elettronici generati automaticamente mediante dispositivi medici; f bis) dati delle applicazioni per il benessere; g) dati identificativi relativi ai prestatori di assistenza sanitaria e alle categorie di professionisti sanitari coinvolti nella cura di una persona fisica o nella ricerca; j) dati sanitari elettronici provenienti da sperimentazioni cliniche soggetti alle disposizioni in materia di trasparenza a norma del diritto dell'Unione; l) dati derivanti da coorti di ricerca, questionari e indagini in materia di salute.

adottare per anonimizzarli conformemente ai requisiti normativi in materia di protezione dei dati personali. In particolare, ai sensi del considerando n. 26 del GDPR[44] se il dato è reso "anonimo" al punto tale da impedire o da non consentire più l'identificazione dell'interessato non si applicheranno le norme ivi contenute, con la conseguenza che l'adeguata anonimizzazione dei dati sanitari del paziente "a valle" consentirà di sfuggire agli adempimenti in materia di protezione dei dati personali, evitando *in toto* l'applicazione del GDPR[45]. La conseguenza più immediata di detto meccanismo è l'irrilevanza dell'art. 33 del regolamento sullo spazio europeo dei dati sanitari essendo superfluo il rifiuto dell'interessato, risultando pienamente garantita la sua riservatezza e il rispetto del principio di minimizzazione. L'analisi dei dati provenienti dal mondo reale come già precisato richiede necessariamente il consenso dell'interessato per il trattamento, trattandosi di dati sensibili, a meno che non si decida di tramutarli in "dati sintetici". Questi ultimi "sono dati artificiali generati da dati originali" attraverso "un modello che viene addestrato a riprodurre le caratteristiche e la struttura dei dati originali". Cosicché, i dati sintetici e i dati originali, se sottoposti alla medesima analisi statistica dovrebbero fornire, almeno in linea di massima, risultati molto simili. L'utilizzo di algoritmi di intelligenza artificiale per sintetizzare dati reali consentirà di creare nuovi dati che imiteranno quest'ultimi senza tuttavia contenere alcun elemento identificativo del paziente. Se adeguatamente generati non solo detti dati rifletteranno le caratteristiche di quelli reali ma renderanno impossibile ricondurre le relative informazioni a singoli pazienti. Per comprendere appieno il funzionamento dell'algoritmo che è alla base di detto meccanismo è opportuno riportare un esempio. Immaginiamo di avere a disposizione numerose informazioni riguardanti lo stato di salute dei pazienti di una clinica ospedaliera da cui si desumono i trattamenti che questi ultimi hanno ricevuto, i progressi compiuti, le eventuali patologie e i vari referti. Queste informazioni sono fondamentali per lo sviluppo di nuove tecnologie sanitarie in quanto indicano, qualora analizzate su larga scala, le patologie più comuni, l'età dei pazienti e tutta una serie di informazioni significative a fini statistici potendo orientare la ricerca scientifica e tecnologica nel settore sanitario. Senonché, trattandosi di dati sensibili richiederebbero ai sensi del GDPR il consenso degli interessati. Ma, se ipotizziamo di alimentare l'algoritmo di sintetizzazione con i suddetti dati, il risultato che otterremo riguarderà informazioni provenienti da una clinica ospedaliera di fatto inesistente con pazienti non riconducibili a quelli effettivi. Cionondimeno, le risposte derivanti dal database artificiale saranno statisticamente le medesime di quello reale, conducendo il procedimento di sintetizzazione alla creazione di nuovi dati, statisticamente equivalenti a quelli originali, ma differenti da quest'ultimi per l'anonimato degli interessati. Pertanto, nel settore sanitario i "dati sintetici" consentirebbero la condivisione di informazioni per finalità legate alla ricerca di nuove soluzioni diagnostiche e terapeutiche senza tuttavia esporre i pazienti a rischi di divulgazione dei propri dati sensibili e senza necessità di ottenere il preventivo consenso da parte di quest'ultimi per il trattamento degli stessi. Non a caso i dati sintetici si definiscono come dati "anonimizzati" e non "pseudonimizzati"[46]. Quest'ultima procedura infatti, sebbene dovrebbe essere utilizzata dai titolari del trattamento conformemente agli obblighi di cui all'art. 32 del GDPR[47], non esclude la "natura sensibile" dei dati trattati potendo attribuire

44. Per anonimizzazione si intende il processo volto a rendere anonimi i dati personali; i dati anonimi sono pertanto "le informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

45. In tal senso vedi Bolognini–Zipponi 2024.

46. Per un approfondimento delle differenze relative all'anonimizzazione e alla pseudonimizzazione vedi Agencia Española Protecciòn Datos e European Data Protection Supervisor, *10 Misunderstandings Related to Anonymisation,* 2021.

47. In base a tale norma il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la

all'individuo i dati cui si riferiscono attraverso l'utilizzo di informazioni aggiuntive[48], dovendo, pertanto, comunque applicarsi la normativa in materia di protezione dei dati personali. In conclusione, risulta di fondamentale importanza in un'ottica di classificazione del procedimento di sintetizzazione come tecnica di anonimizzazione differenziare quest'ultima rispetto alla pseudonimizzazione. Difatti, i dati sintetici appartengono alla prima categoria, e, qualora siano effettivamente anonimi ossia le relative informazioni non siano più riferibili al paziente, consentono di superare i limiti imposti dal GDPR offrendo nuove opportunità di utilizzo dei dati in sicurezza[49]. Del resto lo stesso regolamento (UE) 2024/1689 all'art. 59 prevede che quando i sistemi di IA siano impiegati per garantire la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari i dati personali raccolti possono essere utilizzati per altre finalità[50]. Nel caso di sistemi ad alto rischio è preferibile tuttavia procedere al trattamento di dati anonimizzati, sintetici o di altri dati non personali. A ben vedere, la maggior parte dei sistemi impiegati nel settore sanitario rientrano in tale categoria e ciò non soltanto per la particolare destinazione d'uso dello strumento medicale per fini prevalentemente diagnostici e terapeutici[51], ma soprattutto per la sua qualificazione in termini di dispositivo medico. In base alla disciplina di cui al Regolamento MDR[52], devono ritenersi ad alto rischio tutti i dispositivi

capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

48. L'art. 4, par. 5, del GDPR definisce la pseudonimizzazione come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".
49. In tal senso vedi Wiewiórowski 2021.
50. Vedi in particolare art. 59 lett. a).
51. L'Allegato III al punto 1, considera ad alto rischio "a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi; d) i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza". Occorre a tal proposito segnalare che mentre la citata letta a) menziona espressamente "autorità pubbliche" e "autorità private che operano per conto di autorità pubbliche", la lett. d) invece si limita a menzionare la tipologia del servizio indipendentemente dalla natura pubblica o privata del soggetto che lo eroga. In tal senso vedi Puigpelat 2023, p. 238 ss.
52. Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.

medici e i dispositivi medico-diagnostici che sono sottoposti ad un controllo da parte di un organismo terzo. Di talché, non tutti i dispositivi medici rientrano nella categoria dei sistemi ad alto rischio ma solo quelli che richiedono una specifica valutazione di conformità. Per quelli che invece rientrano ai sensi del Regolamento (UE) 2017/745 nella classe I è sufficiente una mera autocertificazione[53], con la conseguenza che configurandosi quali applicazioni a basso rischio sono sottoposti a meri obblighi di auto-condotta. In base a tale logica i dispositivi indossabili come *smartwatch* – al di là della loro natura giuridica – non essendo sottoposti a specifici controlli da parte di organismi a ciò preposti non sono assoggettati alle regole previste per le applicazioni ad "alto rischio". Al contrario strumenti in grado di misurare i livelli di serotonina nel sangue dovrebbero qualificarsi a tutti gli effetti come dispositivi medici richiedendo, tra l'altro, l'intervento di un organismo di valutazione della conformità prima dell'immissione in commercio applicandosi tutti gli obblighi previsti dal regolamento sull'intelligenza artificiale per i sistemi ad alto rischio[54]. Dall'analisi delle norme del Regolamento sull'intelligenza artificiale emerge come la maggior parte dei sistemi di IA impiegati nel settore sanitario siano riconducibili a tale ultima categoria (alto rischio) con la conseguenza che, da un'interpretazione estensiva di tale disposizione si potrebbe concludere nel senso di ritenere che il legislatore europeo incentivi l'utilizzo nel settore sanitario di dati sintetici. D'altra parte occorre osservare che la lett. b) dell'art. 59[55], nel richiamare quest'ultima tipologia di dati equiparandoli a quelli anonimi e non personali, sembra confermare la natura giuridica "anonimizzata" di tali dati. Sta di fatto che i tentativi di regolazione tanto dei dati provenienti dal mondo reale quanto di quelli sintetici appaiono ancora troppo timidi. L'Unione europea dovrebbe sfruttare a pieno il potenziale della sintetizzazione dei dati, dacché quest'ultima se realizzata con adeguate metodologie, tutte ancora da definire, potrà garantire un giusto compromesso tra tutela e condivisione dei dati sanitari, mitigando i rischi di identificazione del paziente e supportando l'innovazione tecnologica nel settore sanitario, rappresentando pertanto un'idonea base per la futura costruzione del mercato unico della sanità digitale.

5. Possibili risvolti evolutivi di una disciplina europea in materia di dati sintetici

Sin dalle battute iniziali di questo breve scritto abbiamo avuto modo di precisare come l'utilizzo di dati sia fondamentale per lo sviluppo di tecnologie sanitarie. Benché le modalità di accesso e trattamento siano state già disciplinate dal legislatore europeo attraverso il GDPR appare altrettanto importante regolare in maniera dettagliata la tipologia di dati da trattare per lo sviluppo di tecnologie sanitarie innovative, essendo la salute un diritto fondamentale dell'Unione. Invero, l'art. 35 della Carta dei diritti fondamentali dell'Unione europea stabilisce che "ogni persona ha il diritto di accedere alla prevenzione sanitaria e di ottenere cure mediche alle condizioni stabilite dalle legislazioni e prassi nazionali", aggiungendo che nella definizione e nell'attuazione di tutte le politiche e le attività dell'Unione debba essere garantito "un livello elevato di protezione della salute umana". È dunque importante notare come il diritto alla salute venga inteso in un'accezione estensiva, dovendo essere tutelato non solo nei confronti dei cittadini europei ma di qualsiasi persona[56]. Nondimeno, è altrettanto fondamentale evidenziare come il diritto alla protezione dei dati personali sia ugualmente tutelato a livello di Unione, assurgendo a diritto fondamentale alla stregua di quello alla salute. Pertanto, essendo entrambi i diritti consacrati nella Carta dei diritti fondamentali dell'Unione europea occorrerebbe effettuare un bilanciamento tra gli stessi non potendo l'uno prevalere sull'altro. In attuazione del diritto alla salute sarebbe auspicabile

53. Kiseleva 2021. Gli obblighi sono disciplinati dal Capo II del regolamento, che fa espresso riferimento a doveri specifici di trasparenza e alla tutela dei diritti fondamentali.

54. Van Oirschot–Ooms, 2022, p. 10.

55. L'art. 59 lett. b) del regolamento sull'intelligenza artificiale stabilisce infatti che i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al capo III, sezione 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali.

56. Salvatore 2021, p. 12.

incentivare l'utilizzo di dati provenienti dal mondo reale in quanto più affidabili e accurati e benché questi ultimi risultino oggetto di massima tutela da parte del GDPR per la loro natura "sensibile", ben potrebbero essere "anonimizzati" utilizzando nuove tecniche di intelligenza artificiale, tutelando parimenti il diritto alla protezione dei dati personali di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Peraltro, nonostante l'analisi condotta si sia soffermata esclusivamente sugli aspetti positivi dell'utilizzo dei dati sintetici nell'ambito sanitario non possono di certo negarsi gli innumerevoli vantaggi del loro utilizzo anche in altri settori. Infatti sono ben noti i benefici dell'utilizzo di detti dati nel marketing e le relative ricadute rispetto alla disciplina consumeristica sia in termini di maggior efficienza del servizio erogato al consumatore che per il miglioramento delle strategie di marketing aziendale riducendo così i rischi di accesso a dati sensibili[57]. Come per il regolamento sull'intelligenza artificiale si potrebbe dunque riflettere sull'introduzione di una disciplina generale da applicare concretamente ai distinti settori materiali, incentivando l'utilizzo di meccanismi di "anonimizzazione" o di "pseudonimizzazione" a seconda del rischio rispetto alla protezione dei dati personali dell'interessato. Poiché la legislazione europea è per molti aspetti ancora *in itinere*, sarebbe auspicabile la modifica delle numerose proposte di atti normativi al fine di introdurre da un lato idonee procedure di valutazione e controllo delle tecnologie sanitarie per assicurare elevati standard di qualità e sicurezza e dall'altro meccanismi di trattamento dei dati sanitari volti a mitigare i rischi rispetto alla tutela della riservatezza dei pazienti. In definitiva, non può che rilevarsi come un intervento tempestivo del legislatore europeo in tale settore appaia non solo auspicabile ma ormai improcrastinabile.

Riferimenti bibliografici

A. Adinolfi (2024), *Le ragioni di una (incerta) riforma dei trattati dell'Unione*, in "Osservatorio sulle fonti", 2024

A. Adinolfi (2020), *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), "Il ragionamento giuridico nell'era della intelligenza artificiale", Pacini Editore, 2020

A. Adinolfi, A. Simoncini (a cura di) (2022), *Protezione dei dati personali, e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Edizioni Scientifiche Italiane, 2022

P. Arlett, J. Kjær, K. Broich, E. Cooke (2022), *Real-World Evidence in EU Medicines Regulation: Enabling Use and Establishing Value*, in "Clinical Pharmacology & Therapeutics", 2022

M. Bassini (2016), *La svolta della "privacy" europea: il nuovo pacchetto sulla tutela dei dati personali*, in "Quaderni costituzionali", 2016

F. Bestagno (2017-a), *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in L. Pineschi (a cura di), "La tutela della salute nel diritto internazionale ed europeo tra interessi globali e interessi particolari", Editoriale Scientifica, 2017

F. Bestagno (2017-b), *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in "Studi sull'integrazione europea", 2017

L. Bolognini, S. Zipponi (2024), *Prospettive future in sanità spazio europeo dei dati sanitari e regolazione dei dati sintetici*, in L. Bolognini, S. Zipponi (a cura di), "Privacy e diritto dei dati sanitari", Giuffrè, 2024

G. Caggiano, G. Contaldi, P. Manzini (a cura di) (2021), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci Editore, 2021

57. Grisafi 2024, p. 155 ss.

L. Califano (2018), *Fascicolo sanitario elettronico (FSE) e dossier sanitario: il contributo del garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in G. De Vergottini, C. Bottari (a cura di), "La Sanità elettronica", Bologna University Press, 2018

S. Calzolaio (2017), *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Aggiornamento, Utet Giuridica, 2017

M. Carta (2024), *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in "Eurojus", 2024

G. Contaldi (2021), *Intelligenza artificiale e dati personali*, in "Ordine internazionale e diritti umani", 2021

V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) (2019), *I dati personali nel diritto europeo*, Giappichelli, 2019

D. Danieli (2023), *Il nuovo Regolamento UE sulla valutazione delle tecnologie sanitarie: dal rafforzamento della cooperazione tra Stati membri al possibile impatto sul riparto delle competenze*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

G. Di Federico (2017), *Protezione della salute*, in S. Allegrezza, R. Mastroianni, F. Pappalardo et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea", Giuffré, 2017

G. Di Federico (2021-a), *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. Di Federico (a cura di), "Alla (ri)scoperta del Parlamento europeo. 1979-2019", Giappichelli, 2021

G. Di Federico (2021-b), *La strategia dell'Unione europea per i vaccini tra principio di attribuzione e leale collaborazione*, in "Eurojus", 2021

A. Duff (2023), *Five Surgical Strikes on the Treaties of the European Union*, in "European Papers", 2023, n. 1

G. Fares, M. Campagna (2011), *La tutela della salute nell'ordinamento comunitario*, in P. Gargiulo (a cura di), "Politica e diritti sociali nell'Unione europea. Quale modello sociale europeo?", Editoriale Scientifica, 2011

R. Flynn, K. Pluschke, C. Quinten et al. (2021), *Marketing Authorization Applications Made to the European Medicines Agency in 2018–2019: What was the Contribution of Real-World Evidence?*, in "Clinical Pharmacology & Therapeutics", 2021

M. Fumagalli (2016), *Le nuove normative europee sulla protezione dei dati personali*, in "Il Diritto comunitario e degli scambi internazionali", 2016

L.M. González de la Garza (2008), *Sociedad de la información en Europa*, Reus, 2008

G. González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014

C. Grieco (2023), *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Editoriale Scientifica, 2023

R. Grisafi (2024), *Il dato sintetico nell'approccio ermeneutico funzionale del diritto dei consumatori*, in S. Aracu, C. Rossi Chauvenet, L. Cristofaro (a cura di), "Paradisi artificiali. La nuova frontiera dei dati sintetici tra diritto e tecnologia", Aracne, 2024

M. Hervey, M. Lavy (2020), *The Law of Artificial Intelligence*, Sweet & Maxwell, 2020

D. Hodson, I. Maher (2018), *Eight Ideas for Reforming EU Treaty Making from Part III - The Practice of EU Treaty Making*, Cambridge University Press, 2018

M. Inglese (2024), *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in "Quaderni AISDUE", 2024

A. Kiseleva (2021), *AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation, Time to Reshape the Digital Society. 40th Anniversary of the CRIDS*, in "SSRN", 2021

S. Lattanzi (2024), *Prime riflessioni sull'applicazione del nuovo regolamento sull'intelligenza artificiale al settore sanitario*, in "Quaderni AISDUE", 2024

N. Lazzerini (2023), *La risoluzione del 22 novembre 2023 del Parlamento europeo sui progetti di modifica dei Trattati nel contesto delle prospettive di riforma dell'Unione (3/2023)*, in "Osservatorio sulle fonti", 2023, n. 3

A. López Pina (2022), *El Derecho ante el reto de la transformación digital*, Editorial Aranzadi, 2022

C.M. Mariottini (2016), *Il pacchetto di riforma della Commissione europea in materia di protezione dei dati personali*, in "Rivista di diritto internazionale privato e processuale", 2016

A. Oddenino (2010), *Profili internazionali ed europei del diritto alla salute*, in R. Ferrara (a cura di), Salute e sanità, in "Trattato di biodiritto", diretto da S. Rodotà e P. Zatti, Giuffrè, 2010

A. Pajno, F. Donati, A. Perrucci (a cura di) (2022), *Intelligenza artificiale e diritto: una rivoluzione?* Vol. I, *Diritti fondamentali, dati personali e regolazione*, il Mulino, 2022

C. Pesce (2021), *Sanità*, in P. De Pasquale, F. Ferraro (a cura di), "Manuale di diritto dell'Unione europea di Giuseppe Tesauro", II, Editoriale Scientifica, 2021

F. Pizzetti (2018), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), "Intelligenza artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018

O. Pollicino, G. De Gregorio (2021), *The principle of the rule of law in the regulation of AI*, Wolters Kluwer, 2021

O. Pollicino, M. Bassini (2017), *Art. 8. Protezione dei dati personali*, in S. Allegrezza, R. Mastroianni, F. Pappalardo et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea" Giuffrè, 2017

O.M. Puigpelat (2023), *The impact of the AI Act on public authorities and on administrative procedures*, in "Rivista interdisciplinare sul diritto delle amministrazioni pubbliche", vol. 4, 2023

G. Resta (2022), *Cosa c'è di "europeo" nella proposta di regolamento UE sull'Intelligenza Artificiale?*, in "Diritto dell'informazione e dell'informatica", 2022

A. Ricci (2017), *I diritti dell'interessato*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

D. Rinoldi (2022), *«In deroga… e in conformità»: prospettive dell'Unione europea della salute muovendo dall'art. 168 TFUE per andar ben oltre (verso un comparto sanitario federale continentale?)*, in "Corti Supreme e Salute", 2022

L.S. Rossi (2013), *L'Unione Europea e il paradosso di Zenone. Riflessioni sulla necessità di una revisione del Trattato di Lisbona*, in "Il Diritto dell'Unione Europea", 2013

F. Rossi Dal Pozzo (a cura di) (2020), *Mercato unico digitale, dati personali e diritti fondamentali*, in "Eurojus", 2020

G. Rugani (2024), *La promozione di strumenti di coregolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle* regulatory sandboxes, in "Quaderni AISDUE", 2024

V. Salvatore (2023-a), *L'Unione europea disciplina l'impiego dell'intelligenza artificiale e dei processi di digitalizzazione anche al fine di promuovere la tutela della salute*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

V. Salvatore (2023-b), *The regulatory challenges of digital therapeutics*, in "European Health & Pharmaceutical Law Review", 2023

V. Salvatore (2021), *Il diritto alla salute, una prospettiva di diritto comparato*, in "EPRS | Servizio Ricerca del Parlamento europeo", 2021

F. Scialoia (2024), *Verso la costruzione di un quadro regolatorio europeo sulle terapie digitali: sfide e opportunità*, in "Corti Supreme e Salute", 2024

F. Scialoia (2023), *L'Unione europea apre la strada alla creazione dello spazio europeo dei dati sanitari*, in V. Salvatore (a cura di), "Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea", Giappichelli, 2023

G. Simone (2020), *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. Alpa (a cura di), "Diritto e intelligenza artificiale", Pacini Editore, 2020

J. Van Oirschot, G. Ooms (2022), *Interpreting the EU Artificial Intelligence Act for the Health Sector*, in "Health Action International", 2022

E.-B. Van Veen (2018), *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, in "European Journal of Cancer", 2018

A. Volpato (2024), *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in "Quaderni AISDUE", 2024

W. Wiewiórowski (2021), *Synthetic data: what use cases as a privacy enhancing technology?*, in "European Data Protection Supervisor", 2021

G. Zaccaroni (2024), *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in "Quaderni AISDUE", 2024