One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*

Marco Orofino**

Sommario: 1. Introduzione. – 2. L'intervento dell'Unione europea nella disciplina della circolazione dei dati attraverso la direttiva 95/46/CE – 3. La regolamentazione europea del riuso delle informazioni del settore pubblico: la circolazione dei dati al servizio dell'*open government*. – 4. La disciplina della circolazione dei dati personali nel GDPR: un ponte tra il passato e il futuro. – 5. La *Data Strategy* della Commissione europea e il cambio di paradigma: la circolazione dei dati per garantire i diritti dei cittadini nella società digitale. – 6. L'impatto della *Data Strategy* sulla normativa del cd. decennio digitale. – 6.1. Il *Data Governance Act*. – 6.2. Il Regolamento sullo spazio europeo dei dati sanitari. – 7. Osservazioni conclusive.

1. Introduzione

L'approccio *One Digital Health* (ODH) rappresenta una visione innovativa e integrata della salute che combina tecnologie digitali, medicina, scienze ambientali e sanità pubblica, con l'obiettivo di migliorare la salute umana, animale e ambientale in un contesto globale. Si tratta di un concetto che si basa su due pilastri fondamentali: *One Health*, che sottolinea l'interconnessione tra salute umana, animale e ambientale, e *Digital Health*, che sfrutta la potenza delle tecnologie digitali per affrontare le sfide sanitarie del nostro tempo.

---

* Lo scritto costituisce la rielaborazione dell'intervento tenuto dall'Autore al XXII Convegno nazionale di Diritto sanitario "Corti supreme e One Health. Vent'anni di giurisprudenza" (Alessandria, 21-22 ottobre 2024), organizzato nell'ambito del PRIN "Il diritto costituzionale della salute e dell'organizzazione sanitaria dopo l'emergenza della pandemia" (p.i. prof. Renato Balduzzi).

** Professore ordinario di Diritto costituzionale e pubblico presso il Dipartimento di Studi Internazionali, Giuridici e Storico-Politici dell'Università degli Studi di Milano.

ISSN 2611-8882

Per ciò che attiene all'approccio *One Health*, esso è al tempo stesso antico, poiché la medicina è per definizione crocevia di saperi[1], e attualissimo, perché le recenti emergenze sanitarie sono tutte epidemie di zoonosi favorite dai cambiamenti climatici[2]. L'approccio *One Health* è ormai riconosciuto come necessario a livello internazionale – dalla FAO, dall'Organizzazione Mondiale per la Salute - OMS, dal Programma per l'Ambiente - UNEP, e dall'Organizzazione Mondiale per la Salute Animale-WOAH – e a livello nazionale dagli Istituti nazionali specializzati[3]. La letteratura giuridica ha iniziato a studiare come questo approccio influenzi l'organizzazione della sanità, mettendo in relazione diritti fondamentali, come il diritto alla salute, con interessi costituzionali come la tutela dell'ambiente e degli animali. Si sottolinea anche l'importanza di integrare pienamente la prevenzione, intesa in senso ampio, nel diritto alla salute sancito dalle Costituzioni[4].

Più nuovo è il concetto di *Digital Health*. Esso ha, negli ultimi anni, guadagnato terreno rispetto al termine più datato di "e-Health", segnando un'evoluzione significativa nel modo in cui pensiamo al rapporto tra tecnologia e salute.

Con "e-Health", il focus era principalmente sull'uso delle tecnologie dell'informazione e della comunicazione (ICT) per migliorare l'efficienza dei sistemi sanitari. L'attenzione era rivolta alla digitalizzazione dei processi, come la gestione elettronica dei dati sanitari, la creazione di reti tra operatori e strutture e primi esperimenti di telemedicina. In quel

[1] Ippocrate di Kos nel suo *Trattato sulle arie, sulle acque e sui luoghi* già postulava una stretta connessione tra la salute umana e la salubrità dell'ambiente circostante. Cfr. R.M. Atlas, *One Health: Its origins and future* in *Curr. Top. Microbiol. Immunol.,* 2013, 365, pp. 1–13.

[2] Il caso del Covid 19 è certamente il più noto ed il più discusso, ma vi sono state e vi sono molte altre epidemie (nuove e già note) come l'aviaria, la SARS, la Chikungunya, il virus del Nilo occidentale, lo Zika, la tripanosomiasi, l'echinococcosi e la malaria che sono zoonosi innescate da movimenti della fauna selvatica, dipendenti, a loro volta, dai cambiamenti climatici nonché da una mitezza delle temperature che consente un'innaturale sopravvivenza alle larve di zanzara.

[3] Le origini moderne di *One Health* risalgono al 2004, quando il concetto fu introdotto nei 12 Principi di Manhattan, che proponevano un approccio internazionale e interdisciplinare per prevenire le malattie, in particolare quelle trasmissibili tra animali e umani. Questo approccio integra prospettive sistemiche sulle scienze della vita e sull'ambiente per progettare programmi e politiche mirati a migliorare la salute pubblica. Cfr. S. Pitto, *Cambiamento climatico e sicurezza alimentare: dall'approccio One Health ai modelli olistici del Global South*, in *BioLaw Journal*, 2023, 2, pp. 315 ss. La FAO ha collegato *One Health* agli obiettivi di sviluppo sostenibile, sottolineando l'importanza di monitorare l'impatto dei rischi ambientali su sistemi sanitari, biodiversità e sicurezza alimentare. V. *Sustainable development goals. Food and Agricultural Organization of the United Nations*. URL: *http://www.fao.org/sustainable-development-goals/goals/goal-3/en/*. A dicembre 2023, il "quadripartito" delle organizzazioni delle Nazioni Unite che coordinano la governance globale di *One Health* (FAO, UNEP, OMS e WOAH) ha pubblicato il documento *A Guide to Implementing the One Health Joint Plan of Action at National Level*. Questa guida fornisce indicazioni per l'implementazione del *Piano d'Azione Congiunto One Health* (OH JPA) 2022-2026, sviluppato nell'ottobre 2022, con l'obiettivo di gestire in modo integrato le minacce alla salute globale e prevenire future pandemie. Cfr. A. Latino, *Il paradigma One Health nell'ordinamento internazionale: un'analisi critica di origini, protagonisti, strumenti normativi* in *Corti Supreme e Salute,* 3, 2022, pp. 779 ss.

[4] Sul punto v. anche gli altri interventi alla XXII edizione del Convegno nazionale di Diritto sanitario pubblicati in questa *Rivista*. In materia v. anche G. Ragone, *One Health e Costituzione italiana, tra spinte eco-centriche e nuove prospettive di tutela della salute umana, ambientale e animale* in *Corti Supreme e Salute*, 3, 2022, pp. 809 ss.

contesto, il paziente era visto soprattutto come un destinatario dei servizi sanitari, mentre l'obiettivo principale era ottimizzare i flussi informativi e ridurre i costi operativi[5].
Oggi, tuttavia, viviamo in nuovo contesto in cui il digitale permea ogni aspetto della società, e con esso è cambiata anche la prospettiva sulla salute. "Digital Health" non è soltanto un aggiornamento linguistico, ma un vero e proprio cambiamento di paradigma. Questo termine abbraccia, infatti, una visione più ampia e complessa, che non si limita al settore delle comunicazioni elettroniche, ossia alla dimensione puramente infrastrutturale di *e-Health* per concentrarsi sull'uso strategico di strumenti come l'intelligenza artificiale, i big data, l'*Internet of Things* (IoT)[6]. Queste tecnologie non sono semplicemente supporti per ottimizzare i processi sanitari, ma diventano protagoniste di una trasformazione culturale. Pensiamo, ad esempio, ai dispositivi indossabili che monitorano in tempo reale i parametri vitali, o ai sistemi basati sull'intelligenza artificiale capaci di analizzare milioni di dati per aiutare la prevenzione, fornire diagnosi più accurate e personalizzare le cure.
Questo determina un mutamente legato al ruolo del paziente. Se con *e-Health* il paziente era spesso un soggetto passivo, con *Digital Health* il paziente diventa un attore attivo e consapevole. Grazie ad app mobili, piattaforme digitali e dispositivi connessi, le persone oggi hanno la possibilità di accedere alle informazioni sulla propria salute, monitorarla autonomamente e persino partecipare alla definizione di strategie personalizzate di prevenzione e cura. Questo passaggio riflette un cambiamento più ampio nella cultura della salute, in cui il benessere non è più solo una questione di trattamento medico, ma un percorso condiviso tra paziente, tecnologia e professionisti sanitari.
C'è poi un altro aspetto distintivo che merita attenzione: la portata globale di *Digital Health*. Mentre *e-Health* era spesso concepita all'interno di un contesto locale o nazionale, *Digital Health* non si limita a migliorare i sistemi sanitari esistenti, ma si propone di rispondere a questioni che richiedono una collaborazione globale. Pensiamo, ad esempio, all'impatto delle tecnologie digitali sulla prevenzione delle pandemie o sul monitoraggio dei cambiamenti climatici.
In sintesi, se e-*Health* rappresentava un primo passo verso la digitalizzazione della sanità, *Digital Health* si configura come un cambio di prospettiva radicale, che considera la tecnologia non solo come uno strumento, ma come un fattore di trasformazione per affrontare le sfide globali.
L'approccio *One Digital Health*, partendo dai due paradigmi che lo ispirano, si propone quindi alcuni obiettivi ambiziosi, ma molto concreti. Da un lato, punta a sfruttare tecnologie come l'intelligenza artificiale, l'*Internet of Things* (IoT), i *big data* e la telemedicina per rac-

[5] Sulla difficoltà di tale prima transizione, v. le osservazioni puntuali di E. Catelani, *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in *Corti Supreme e Salute*, 2, 2023.

[6] Cfr. in materia C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni, in Diritto pubblico comparato ed europeo*, n. spec., 2019, pp. 101 ss.; E.A. Ferioli, *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, in *BioLaw Journal*, 1, 2019, pp. 163 ss.

cogliere, analizzare e condividere dati sanitari, dati climatici e dati relativi alla salute animale in tempo reale o quasi reale. Dall'altro, punta a trattare questi dati congiuntamente offrendo una prospettiva olistica che mette in relazione la salute umana, animale e ambientale e supera le tradizionali barriere tra le discipline. Un aspetto centrale di questo approccio è l'*empowerment* delle persone, che attraverso dispositivi indossabili, applicazioni mobili e piattaforme digitali, possono diventare protagonisti attivi nella gestione della propria salute. Il presupposto di questo approccio è la disponibilità e la circolazione dei dati sulla scala più ampia possibile.

La tesi che si intende sviluppare e che la disponibilità e la circolazione dei dati stiano fuoriuscendo da un contesto solo economico per divenire centrali nella garanzia dei diritti fondamentali e degli interessi costituzionalmente protetti come il diritto alla salute, la tutela dell'ambiente, dell'ecosistema e degli animali. Basti pensare al fatto che le nuove tecnologie in associazione con l'IA, consentono già oggi, e sempre di più lo faranno in futuro, previsioni accurate delle emergenze epidemiche, climatiche nonché, in campo sanitario, misure di prevenzione più efficaci, diagnosi più rapide e trattamenti di cura personalizzati. Questo processo, tuttavia, non è esente da rischi vecchi e nuovi.

Ai tradizionali rischi legati alla privacy delle persone si aggiungono quelli legati alla mancata diffusione di dati e tecnologie. Se i dati non circolano in maniera uniforme, se le tecnologie che li utilizzano non si diffondono in modo omogeneo si rischia, infatti, sia di amplificare le disuguaglianze esistenti sia di crearne di nuove determinando una frattura tra chi può beneficiare delle tecnologie avanzate e chi ne resta escluso. In tal senso, occorre tener presente che la disponibilità di un'infrastruttura adeguata, resiliente ed interoperabile non è solo una questione tecnica, ma un passo fondamentale per rispettare il principio di uguaglianza.

Nei paragrafi che seguono si darà conto dello stato dell'arte, delle più recenti innovazioni legislative adottate a livello europeo e delle criticità che occorre superare per realizzare quell'effettiva condivisione e circolazione dei dati che l'approccio *One Digital Health* richiede.

2. L'intervento dell'Unione europea nella disciplina della circolazione dei dati attraverso la direttiva 95/46/CE

La circolazione delle informazioni è stata, per lungo tempo, disciplinata e gestita a livello dei singoli Stati. Ogni Paese ha adottato norme per disciplinare la gestione, l'accesso e la protezione delle informazioni e dei documenti in possesso delle pubbliche amministrazioni e dei privati.

La diversità negli approcci nazionali rifletteva le priorità, la cultura e il contesto politico di ogni Stato. Con l'aumento delle relazioni economiche transnazionali, prima, e con la digitalizzazione e la globalizzazione, poi, si è fatta strada una crescente esigenza di armonizzazione legislativa, sia a livello sovranazionale regionale sia a livello internazionale.

L'intervento dell'Unione europea in materia muove proprio da questi presupposti come si può comprendere già dall'intestazione della storica Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, *nonché alla libera circolazione di tali dati*.

Il quadro giuridico delineato perseguiva due obiettivi, che erano esplicitati nei due paragrafi di cui si componeva l'art. 1. Essi erano "la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali" e la libera circolazione dei dati tra gli Stati membri[7].

L'intervento dell'allora Comunità europea si fondava sull'art. 100A del Trattato CE e, quindi, su un riavvicinamento legislativo ai fini dell'instaurazione e del funzionamento del mercato interno europeo che esigeva, fin da allora, oltre alla libera circolazione delle merci, delle persone, dei servizi e dei capitali, anche quella dei dati personali da uno Stato membro all'altro. La libera circolazione dei dati era però ammissibile solo se contestualmente poteva dirsi garantito un livello di tutela dei diritti fondamentali e delle libertà delle persone relativamente al trattamento di tali dati equivalente in tutti gli Stati membri.

Questo apriva la strada ad una regolamentazione armonizzata piuttosto dettagliata – certamente per la fonte direttiva – che si fondava su una logica difensiva di cui erano espressione, in quel contesto normativo, la centralità del consenso, una disciplina stringente del trattamento dei dati sensibili, nonché i diritti dell'interessato costruiti su una logica di tipo proprietario.

Se dal dato positivo, si passa a considerare l'interpretazione di quel quadro giuridico appare in modo ancor più evidente la valorizzazione del fine di protezione della persona rispetto al fine di favorire la circolazione dei dati. Il che era anche ragionevole in quel contesto tecnologico e politico in cui era più facile scorgere i rischi che la circolazione del dato comportava piuttosto che i suoi vantaggi, limitati al buon funzionamento dei mercati e, in particolare, del mercato unico europeo.

Una conferma di questa impostazione la ritroviamo anche nel fatto che le autorità di controllo previste dalla direttiva 95/46/CE sono state *ab origine* qualificate come autorità di protezione e chiamate a sorvegliare l'applicazione delle disposizioni di attuazione della direttiva in funzione della tutela del diritto fondamentale alla protezione dei dati personali. Questo ha avuto un peso, e lo ha forse ancora oggi in un diverso quadro regolatorio, nell'approccio difensivo che le autorità nazionali di protezione dati hanno avuto nello svolgimento dei loro compiti.

[7] La norma impediva agli Sati membri di introdurre divieti o restrizioni ulteriori rispetto a quelle previste dalla direttiva per motivi connessi alla protezione dei dati personali.

3. La regolamentazione europea del riuso delle informazioni del settore pubblico: la circolazione dei dati al servizio dell'*open government*

Una nuova stagione della regolamentazione europea della circolazione dei dati si apre con l'approvazione della direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.

L'Unione europea interviene, per la prima volta, fuori dal perimetro dei dati personali, al fine di riavvicinare le normative degli Stati membri riguardanti il riuso dei documenti in possesso degli enti pubblici degli Stati membri. Il presupposto esplicitato nel considerando 4 è che «il settore pubblico raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni in molti settori di attività, ad esempio informazioni di tipo sociale, economico, geografico, climatico, turistico, informazioni in materia di affari, di brevetti e di istruzione» e che tali informazioni potrebbero essere sfruttate dalle imprese europee contribuendo così alla crescita economica e alla creazione di posti di lavoro.

Il titolo di competenza utilizzato per giustificare l'intervento normativo è nuovamente l'instaurazione del mercato interno (in questo momento artt. 14 e 95 del TCE).

Da un punto di vista sostanziale, a fronte del principio generale, di cui all'art. 3, che esprime un *favor* per il riuso a fini commerciali o non commerciali, la normativa europea del 2003 definisce estese aree di esclusione nonché ampi margini discrezionali a favore degli Stati membri nella determinazione di quali documenti e di quali amministrazioni debbano consentire il riuso. Solo laddove effettivamente l'apertura e la circolazione delle informazioni sia permessa, la direttiva provvede a definire un quadro minimo di norme e principi che disciplinano le modalità e gli strumenti del riutilizzo dei documenti detenuti da enti pubblici degli Stati membri. I principi, gli istituti e le procedure sono tutti orientati ad evitare il formarsi di ostacoli che pregiudichino la concorrenza.

Il legame tra circolazione dei dati e mercato rimane quindi predominante.

Ciò nondimeno, in alcuni considerando della direttiva del 2003, è già possibile riscontrare un'attenzione verso una circolazione delle informazioni e, quindi, dei dati, funzionale a consentire al cittadino «nuove vie di accesso alle conoscenze e di acquisizione delle stesse» (considerando 2), nonché l'affermazione del principio per cui «rendere pubblici tutti i documenti generalmente disponibili in possesso del settore pubblico – concernenti non solo il processo politico ma anche quello giudiziario e amministrativo – rappresenta uno strumento fondamentale per ampliare il diritto alla conoscenza, che è principio basilare della democrazia» (considerando 14).

Il germe della *disclosure* che emerge dai citati considerando attecchisce quando, alla fine del primo decennio del nuovo secolo, nel dibattito politico emerge con forza il tema degli *open data* e quello correlato *dell'open Government*[8].
Di questa tendenza troviamo conferma nella direttiva 2013/37/UE *che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico*. Essa specifica, infatti, fin dal considerando 3 che le politiche relative all'apertura dei dati che incoraggiano un'ampia disponibilità e il riutilizzo delle informazioni del settore pubblico sia a fini privati che commerciali possono al tempo stesso contribuire alla crescita economica e favorire l'impegno sociale[9].
Da un punto di vista normativo, la principale innovazione introdotta è l'obbligo per gli Stati membri di rendere riutilizzabili tutti i documenti a meno che l'accesso sia limitato o escluso ai sensi delle disposizioni nazionali sull'accesso ai documenti e fatte salve le altre eccezioni stabilite nella presente direttiva.
Questa previsione, agganciando il riutilizzo all'accesso, limita significativamente la discrezionalità degli Stati membri. La direttiva non interviene sui regimi di accesso che permangono di competenza degli Stati, ma prevede che se accessibili i documenti siano anche riutilizzabili.
In modo più preciso rispetto al passato, la direttiva 2013/37/UE specifica inoltre a quali settori le regole armonizzate debbano applicarsi e quali settori siano invece esclusi. Questo comporta evidentemente una limitazione della discrezionalità degli Stati nell'individuazione dei dati e delle amministrazioni interessate dalle esclusioni.

4. La disciplina della circolazione dei dati personali nel GDPR: un ponte tra il passato e il futuro

Il quadro brevemente descritto cambia, in modo significativo, con l'approvazione nel giro di un quadriennio, del Regolamento UE 2016/679 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (cd. GDPR)*, del Regolamento UE 2018/1807 *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea* e della Direttiva UE 2019/1024 *relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione) cd. Direttiva* Open Data.
Innanzitutto il GDPR. Nell'ambito di questo lavoro sono tre le innovazioni che occorre innanzitutto considerare perché sono la spia evidente di un cambio di paradigma.

[8] Il tema degli *Open Data* e, conseguentemente, dell'*Open Governement* come si ricorderà, emerse con forza nel 2009 a seguito della pubblicazione da parte del Presidente Obama, nel giorno del suo insediamento, di un *Memorandum sulla trasparenza e l'Open Government*, indirizzato ai dirigenti della sua amministrazione. Il medesimo anno l'UE, con la *Dichiarazione di Malmoe sulle politiche di e-governement* proponeva un nuovo percorso di apertura dei dati delle amministrazioni pubbliche.

[9] In quest'ottica si comprende anche il fatto la direttiva del 2013 intervenga ad ampliare l'ambito di applicazione della direttiva del 2003, includendo ora specificamente le biblioteche, comprese le biblioteche universitarie, i musei e gli archivi.

In primo luogo, la base normativa. Non sono l'art. 114 TFUE sull'instaurazione del mercato interno bensì anche l'art. 16 TFUE che autorizza il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, a stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale (…), e le norme relative alla libera circolazione di tali dati.
In secondo luogo, gli obiettivi. Il GDPR pone sullo stesso piano, nel suo articolo 1, la protezione delle libertà e dei diritti ed in particolare del diritto alla protezione dei dati personali e la necessità di favorire la libera circolazione dei dati[10].
I due obiettivi erano già, come detto, esplicitati nella direttiva del 1995. In questo caso, però, il par. 1 dell'art. 1 *parla* di libera circolazione dei dati *in generale* senza cioè specificazione dell'ambito europeo che, invece appare nel par. 3 del medesimo articolo, ma come divieto a discipline nazionali che impediscano o limitino la libera circolazione dei dati personali tra gli Stati membri dell'UE per motivi attinenti alla protezione delle persone fisiche con riferimento al trattamento dei dati personali[11].
Se questa distinzione terminologica può apparire un indizio di un nuovo equilibrio tra protezione e circolazione, la conferma arriva dai considerando 5, 6 e 7 del GDPR che specificano come la nuova disciplina sia necessaria per offrire «un quadro più solido e coerente in materia di protezione dati dell'Unione, affiancato ad efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno». La circolazione dei dati appare quindi inevitabile, le norme di protezione sono lo strumento per minimizzare i rischi.
In terzo luogo, il contenuto del GDPR.
Come è stato correttamente affermato, il GDPR si trova a cavallo di quelle che, tenuto conto dell'incessante innovazione tecnologica, possono essere definite due epoche[12].
Il GDPR cerca quindi di aggiornare la normativa precedente per renderla adatta a una realtà ormai dominata dalla digitalizzazione dei dati. Per far questo rinnova l'armamentario della protezione dei dati personali riequilibrando il rapporto tra le condizioni di legittimità, aumentando la possibilità di deroga al divieto di trattamento dei dati sensibili (ora dati particolari), valorizzando la figura del titolare attraverso il concetto di accountability, orientando il trattamento in modo compatibile rispetto ai diritti fondamentali degli individui attraverso i concetti di "*privacy by design*" e "*privacy by default*", prevedendo condizioni nuove per il trasferimento dei dati personali all'esterno dell'UE in assenza di una decisione di adeguatezza. Il tutto nell'ottica di favorire la circolazione dei dati personali salvaguardando però i diritti e le libertà fondamentali delle persone.

[10] V. sulla portata di tale distinzione ed innovazione rispetto alla precedente direttiva, F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 12-14.

[11] *Ibidem*, 12.

[12] *Ibidem*.

Nel momento in cui il GDPR diviene pienamente applicabile si trova a dover fare i conti con una nuova profonda trasformazione tecnologica – l'irrompere dell'Intelligenza Artificiale – che richiede subito una re-interpretazione delle sue norme[13].
Sulla scia del GDPR, l'Unione europea ha provveduto anche all'adozione del Regolamento UE 2018/1807 *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*. Come specificato nel considerando 10, tale Regolamento è strettamente connesso con il GDPR con il quale condivide il medesimo principio di libera circolazione all'interno dell'Unione per i dati non personali, tranne nei casi in cui una limitazione o un divieto sono giustificati per motivi di sicurezza pubblica.
Da questo punto di vista i due atti regolamentari, congiuntamente considerati, forniscono un primo insieme coerente di norme che disciplinano la libera circolazione, in ambito europeo, di diversi tipi di dati. Il che è fondamentale per tutte quelle operazioni di trattamento dei dati che utilizzano sia dati personali che dati non personali.
Gli strumenti con cui il Regolamento UE 2018/1807 persegue la libera circolazione sono: la rimozione degli obblighi di localizzazione dei dati esistenti – ossia di qualsiasi misura legale o amministrativa che dichiari che il trattamento dei dati deve svolgersi in uno specifico territorio dell'UE – consentendo, di conseguenza, il trattamento di dati in più località distribuite nel territorio dell'Unione; la portabilità dei dati da parte dell'utente professionale vale a dire qualsiasi «persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione»; la messa disposizione dei dati alle autorità competenti che ne facciano richiesta. Gli unici limiti che possono essere mantenuti sono quelli legati alla sicurezza nazionale che a norma dell'articolo 4 del Trattato sul Funzionamento Unione europea (TFUE), resta di esclusiva competenza di ciascuno Stato membro.
Il quadro complessivo di questa normazione divenuta "di transizione" è completato dalla Direttiva UE 2019/1024, cd. Direttiva *Open Data*. Con essa si è proceduto alla rifusione con rilevanti innovazioni dei precedenti atti normativi in materia, ossia della direttiva 2003/98/CE e della direttiva 2013/37/UE, definendo così un quadro unitario per il riutilizzo delle informazioni del settore pubblico. La direttiva europea sul riutilizzo dei dati pubblici si fonda su alcuni principi chiave che mirano a promuovere l'accesso e l'uso dei dati per generare benefici economici e sociali. In primo luogo, c'è un forte impegno verso l'accessibilità, con l'obiettivo di rendere i dati pubblici facilmente disponibili per cittadini e imprese. Questo significa eliminare barriere tecniche, legali ed economiche che possano ostacolare l'accesso, garantendo così maggiore trasparenza e partecipazione.
Un altro punto fondamentale riguarda il riutilizzo gratuito o a basso costo. La direttiva incoraggia politiche che favoriscano l'uso dei dati senza oneri economici, o almeno a costi

[13] Così F. Pizzetti, *Intelligenza artificiale, protezione dei dati e personali e regolazione*, Torino, 2018.

molto contenuti. Questo approccio punta a incentivare la diffusione dei dati, rendendoli accessibili a un pubblico più ampio e stimolando così l'innovazione.
Un aspetto centrale è poi rappresentato dagli standard e dall'interoperabilità. I dati devono essere forniti in formati aperti e leggibili dalle macchine, così da facilitarne non solo l'accesso, ma anche il riutilizzo e l'integrazione in sistemi o applicazioni. In questo modo, si promuove un uso più efficiente dei dati e la loro valorizzazione all'interno dell'ecosistema digitale.
Infine, la direttiva dà particolare rilievo ai *dataset* ad alto valore, ossia ad insiemi di dati che hanno un grande potenziale economico e sociale. Si tratta, ad esempio, di dati relativi alla sanità, ai trasporti, all'ambiente o all'energia. Questi dataset vengono identificati come prioritari per l'apertura, poiché il loro utilizzo può generare un impatto positivo significativo, sia per l'innovazione che per il benessere collettivo. In sintesi, questa direttiva rappresenta un passo importante verso una società più aperta e digitale, dove i dati pubblici diventano una risorsa chiave per promuovere sviluppo, efficienza e innovazione[14].

5. La *Data Strategy* della Commissione europea e il cambio di paradigma: la circolazione dei dati per garantire i diritti dei cittadini nella società digitale

L'ultima tappa, ancora in corso, del percorso qui ricostruito si apre il 19 febbraio 2020 con la pubblicazione da parte della Commissione europea della Comunicazione recante *Una strategia europea per i dati*[15].
Essa mostra, fin dalle sue premesse, una forte accelerazione – legata all'avvento della società digitale – del cambio di paradigma riguardante la circolazione dei dati che è qui in discussione.
Dato atto che le tecnologie digitali hanno trasformato l'economia e la società, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei, la Comunicazione prevede che l'utilizzo dei dati genererà benefici enormi per i cittadini, ad esempio tramite il miglioramento della medicina personalizzata, le nuove soluzioni di mobilità e il suo contributo al *Green Deal* europeo. La disponibilità di dati ed informazione inoltre consentirà alle persone e alle Istituzioni di assumere decisioni migliori. Infine, l'utilizzo dei dati garantirà una maggiore produttività e mercati competitivi.

[14] V. in proposito il Regolamento di esecuzione (UE) 2023/138 che stabilisce un elenco di specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo

[15] Il 19 febbraio 2020 la Commissione europea ha presentato un pacchetto di proposte per la transizione digitale dell'UE. Di questo pacchetto fanno parte oltre alla *Strategia europea per i dati* anche la Comunicazione *Plasmare il futuro digitale dell'Europa* e il *Libro bianco sull'Intelligenza Artificiale*. La lettura dei tre atti è molto importante per collocare correttamente le successive iniziate normative della Commissione Von der Leyen nell'ambito del cd. decennio digitale.

La circolazione dei dati (che è il presupposto logico del loro utilizzo) è quindi riconosciuta dalla Commissione necessaria, prima ancora che per il mercato, proprio per garantire i diritti dei cittadini nella società digitale.
Per sostenere questa visione, la strategia prevede sia innovazioni normative sia importanti investimenti in infrastrutture avanzate, come un *cloud* europeo di nuova generazione, e nello sviluppo di tecnologie innovative, tra cui l'intelligenza artificiale e la *blockchain*. Questi strumenti permetteranno, secondo gli intendimenti della Commissione, di migliorare l'elaborazione e l'analisi dei dati, rendendo l'UE più competitiva in un panorama globale sempre più digitalizzato.
Un aspetto distintivo della Strategia dei dati è la creazione di spazi comuni europei di dati in settori che la Commissione definisce come strategici. Tra di essi vi sono specificamente la sanità, l'ambiente e il clima, settori fondamentali per l'approccio *One Digital Health*[16]. Questi spazi sono quadri interoperabili specifici, settoriali o intersettoriali di norme e prassi comuni pensati per condividere o trattare congiuntamente i dati, con lo scopo di valorizzarli sia economicamente che a beneficio della società.

6. L'impatto della *Data Strategy* sulla normativa del cd. decennio digitale

La *Data Strategy* elaborata dalla Commissione europea ha influenzato tutti gli atti che l'Unione ha elaborato ed adottato, nell'ultimo quinquennio, nell'ambito del cd. decennio digitale[17]. Non solo. Essa ha influito, e continua a farlo, anche sull'interpretazione di norme preesistenti e sulle misure di attuazione o di legislazione secondaria ivi previste[18].

[16] Gli altri settori individuati sono quelli dell'energia, della mobilità, dell'industria manifatturiera, dei servizi finanziari, dell'agricoltura. La Strategia apre anche ad una combinazione di settori citando esplicitamente clima ed energia e ad ambiti strategici quali il *Green Deal* e la Pubblica Amministrazione

[17] Altri Regolamenti riconducibili al medesimo disegno volto ad implementare la circolazione dei dati sono innanzitutto il *Data Act* e l'*AI Act*. Il *Data Act* mira a rafforzare l'economia dei dati nell'UE e a promuovere un mercato competitivo, rendendo i dati (soprattutto industriali) più accessibili e utilizzabili. Pur avendo tale atto un approccio più propriamente privatistico ai dati, di cui sono espressione le regole per la condivisione obbligatoria dei dati tra imprese e le misure per aumentare la concorrenza nei servizi cloud, l'interoperabilità dei data set, e per proteggere da termini contrattuali iniqui gli utenti dei prodotti connessi, esso contiene anche disposizione molto interessanti nell'ottica dell'*empowerment* dei cittadini in riferimento ai dati da loro generati. Sugli aspetti pubblicistici del *Data Act*, v. A. Iannuzzi, *I regolamenti intersettoriali per l'istituzione dei data spaces: Data Governance e Data Act*, in F. Pizzetti, A. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Torino, 2024, 123. Per ciò che attiene all'AI Act, la circolazione dei dati è il presupposto essenziale dell'intera regolamentazione. Sia consentito rinviare a F. Pizzetti, A. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea dell'Intelligenza Artificiale nella società digitale*, Torino, 2025.

[18] Il riferimento è innanzitutto al GDPR e al progressivo ampliamento delle basi legali che legittimano il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. In particolare, v. l'ampliamento del legittimo interesse del titolare che il BEREC (*Body of European Regulators for Electronic Communications*) sembra ammettere come base legale per

6.1. Il *Data Governance Act*

Nonostante la *Data Strategy* sia all'origine di un'ampia attività normativa, il suo perno è, senza dubbio, il Regolamento UE 2022/868 *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724*, meglio noto come *Data Governance Act* (DGA)[19].

Esso mira a contribuire al rafforzamento del mercato interno dell'Unione Europea, riducendo al minimo le distorsioni della concorrenza e garantendo il rispetto dei diritti fondamentali dei cittadini (Considerando 1). L'obiettivo è creare una società e un mercato interno dei dati antropocentrici, affidabili e sicuri (Considerando 3). Un altro pilastro fondamentale è il rafforzamento dell'autonomia strategica aperta dell'Unione Europea. Questo significa promuovere la libera circolazione dei dati a livello internazionale, garantendo al contempo la capacità dell'Unione di esercitare il controllo strategico sui dati, cruciale per sostenere la competitività e l'innovazione dell'Europa in uno scenario globale sempre più digitalizzato (Considerando 1).

Il DGA si propone, inoltre, di ridurre il divario digitale. Parallelamente, si punta a sviluppare competenze europee all'avanguardia nel settore tecnologico, rafforzando così le capacità dell'Unione di guidare la trasformazione digitale in modo inclusivo ed equo (Considerando 2). Un altro elemento chiave del DGA è il suo ruolo prodromico nella creazione di spazi europei comuni di dati. (Considerando 2)[20].

L'ambito di intervento del Reg. UE 2022/868 comprende quattro punti principali.

In primo luogo, il DGA definisce le condizioni per il riutilizzo, all'interno dell'Unione, di quelle categorie di dati detenuti da enti pubblici che erano esclusi dal perimetro di applicazione della Direttiva *Open data*. Si tratta di dati protetti per motivi di: a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; b) riservatezza statistica; c) protezione dei di-ritti di proprietà intellettuale di terzi; d) protezione dei dati personali. Questo consente di valorizzare al massimo il patrimonio informativo pubblico, garantendo che anche i dati precedentemente esclusi dal riuso, perché non accessibili, possano essere utilizzati (anonimizzati quando necessario) in modo efficace e conforme agli standard di trasparenza e sicurezza[21].

---

l'ottimizzazione dei servizi digitali e lo sviluppo di nuove tecnologie e tra queste dell'intelligenza artificiale. Cfr. *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*.

[19] In dottrina su tale Regolamento v. A. Iannuzzi, *I regolamenti intersettoriali per l'istituzione dei data spaces: Data Governance e Data Act*, in *La regolazione europea della società digitale*, cit., pp. 107 ss.

[20] *Ibidem*, 128.

[21] Ai sensi dell'art. 3, par. 2, del DGA, restano quindi esclusi dal suo ambito di applicazione e, di conseguenza, dagli obblighi europei di riuso: a) i dati detenuti da imprese pubbliche; b) i dati detenuti dalle emittenti di servizio pubblico e dalle società da esse controllate e da altri organismi o relative società controllate per l'adempimento di un compito di radiodiffusione di servizio pubblico; c) i dati detenuti da enti culturali e di istruzione; d) i dati detenuti da enti pubblici e protetti per motivi di pubblica sicurezza, difesa o sicurezza nazionale; e) i dati la cui fornitura è un'attività che esula dall'ambito dei compiti di servizio pubblico degli enti pubblici

Per far questo, il *Digital Governance Act* (DGA), ricalca la strada già percorsa dall'UE con la direttiva *Open Access* e quindi detta le regole per garantire un accesso equo e trasparente ai dati detenuti da enti pubblici e per promuovere un ecosistema digitale equo, inclusivo e orientato al beneficio collettivo, vietando la stipula di accordi o l'adozione di pratiche che prevedano diritti esclusivi sul riutilizzo di tali dati oppure la limitazione di un successivo riutilizzo, orientando al costo le tariffe applicabili etc.[22].

In secondo luogo, il Reg. UE 2022/868 detta una prima disciplina dei servizi di intermediazione dei dati. Il DGA interviene quindi su quello che è oggi ancora una nicchia di mercato introducendo un quadro di notifica e controllo per i fornitori di servizi di intermediazione dei dati ossia di quei soggetti che si assumeranno il compito di fornire i set di dati necessari, ad esempio per l'addestramento dei sistemi o dei modelli di intelligenza artificiale. Questo intervento mira a garantire che tali servizi siano affidabili, rispettino norme rigorose, contribuiscano a creare un ecosistema digitale basato sulla fiducia e non assumano posizioni di dominanza tali da ostacolare la condivisione dei dati

In terzo luogo, il DGA disciplina l'altruismo dei dati. Per altruismo dei dati si intende la condivisione volontaria dei propri dati personali. Tale condivisione è legata a scopi altruistici come ad esempio far progredire la ricerca. Come appare evidente, essa può avere un impatto significativo in campo sanitario. Al fine di assecondare la volontà di condivisione, il DGA prevede un sistema di regole che disciplinano la registrazione volontaria delle entità che raccolgono e trattano dati messi a disposizione per fini altruistici nonché la necessaria separazione degli scopi altruistici da quelli commerciali. L'obbiettivo è promuovere la condivisione responsabile e solidale dei dati, incentivando progetti che generano benefici sociali e collettivi[23].

Infine, il DGA istituisce il Comitato europeo per l'innovazione in materia di dati. Questo organismo ha il compito di promuovere (più che di proteggere) lo sviluppo di politiche innovative, favorendo la cooperazione tra Stati membri e garantendo una *governance* efficace del mercato dei dati.

6.2. Il Regolamento sullo spazio europeo dei dati sanitari

Il Regolamento UE 2025/327 sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 20242847 (*European Health Data Space* - EHDS) è stato adottato l'11 febbraio 2025, dopo un *iter* piuttosto lungo e accidentato[24]. Pubblicato il

[22] L'unica eccezione, comunque da intendersi come temporanea, al divieto di esclusive è, ai sensi dell'art. 4, par. 2, del DGA, legata alla fornitura di un servizio o di un prodotto di interesse generale che non sarebbe altrimenti possibile.

[23] V. in proposito A. Iannuzzi, *I regolamenti intersettoriali per l'istituzione dei data spaces: Data Governance e Data Act*, cit., p. 116.

[24] L'iter di approvazione si è infatti interrotto con il termine della Legislatura europea. Tuttavia, l'art. 240, par. 2, del Regolamento del Parlamento europeo prevede che la Conferenza dei Presidenti possa decidere di quali progetti continuare a riprendere l'esame in deroga alla regola generale della loro decadenza al termine della legislatura. Questo è accaduto nel caso di specie evitando di vanificare un percorso che era ormai giunto alle fasi finali.

5 marzo 2025 è entrato in vigore il 25 marzo 2025. Come molti Regolamenti adottati dall'UE per disciplinare la società digitale prevede un'applicazione differita e scaglionata delle sue norme che parte il 26 marzo 2027 per giungere addirittura fino al 26 marzo 2035.[25]
Passando all'esame del suo contenuto, per quanto qui di interesse, occorre innanzitutto dire che si tratta del primo spazio europeo comune di dati istituito ai sensi della *Strategia digitale* e del *Data Governance Act*.
L'obiettivo specifico di questo Spazio europeo comune di dati sanitari è quello di definire un quadro normativo armonizzato per facilitare l'accesso delle persone fisiche ai loro dati sanitari elettronici e il riutilizzo dei dati sanitari in formato elettronico su due livelli principali: l'uso primario e l'uso secondario.
L'uso primario concerne, *ex* art. 2, par. 2, lett. d), del Regolamento, il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso. L'uso secondario, invece, concerne *ex* art. 2, par. 2, lett. e) di trattare i dati sanitari elettronici per finalità diverse rispetto a quelle iniziali per le quali i dati sono stati raccolti o prodotti.
Il primo livello di riutilizzo dei dati primari è destinato ad avere un impatto diretto sulla prevenzione, sulla diagnosi e sulla cura dei pazienti. Questa stretta correlazione tra uso primario e le attività sanitarie mette in evidenza l'impatto che l'accesso e la circolazione dei dati sanitari elettronici può avere sul diritto fondamentale alla salute.
Il secondo livello di riutilizzo, quello secondario, è quello più propriamente necessario per il successo di un approccio ODH perché consente il riutilizzo, a norma dell'art. 53, dei dati sanitari elettronici per finalità di pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro; per la definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, per attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; statistica; per la ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica, ivi inclusa l'attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; per il miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria[26].

[25] Occorre dire come un termine decennale di differimento appare, in una società a cambiamento velocissimo, come quella attuale una scelta quanto meno discutibile.

[26] Il successivo art. 54 del Reg. UE 2025/327 individua anche esplicitamente gli usi secondari vietati con una tecnica che ricalca quella sperimentata nell'AI Act. In proposito si v. il saggio di E. Longo, *Le pratiche di IA vietate e i sistemi di IA ad alto rischio: metodi e strumenti per la società del "rischio digitale"*, in *La regolazione europea dell'intelligenza artificiale nella società digitale*, cit., pp. 63 ss.

Si tratta a tutta evidenza di finalità che ben si inquadrano in un approccio olistico come quello dell'*One Digital Health*.

Per rendere possibile la condivisione primaria e secondaria dei dati, in un quadro di opportune garanzie, il Regolamento UE 2025/327 interviene in numerosi ambiti. In particolare:

a) specifica e integra i diritti di cui al Regolamento (UE) 2016/679 delle persone fisiche in relazione all'uso primario e all'uso secondario dei loro dati sanitari elettronici personali;
b) stabilisce norme comuni per i sistemi di cartelle cliniche elettroniche e per le applicazioni per il benessere che si dichiarano interoperabili con i sistemi di cartelle cliniche elettroniche[27];
c) stabilisce norme e meccanismi comuni per l'uso primario dei dati sanitari elettronici e l'uso secondario dei dati sanitari elettronici;
d) istituisce un'infrastruttura transfrontaliera che rende possibile l'uso primario e secondario dei dati sanitari elettronici personali in tutta l'Unione;
e) istituisce meccanismi di *governance* e di coordinamento a livello di Unione e nazionale sia per l'uso sia primario dei dati sanitari elettronici che per l'uso secondario dei dati sanitari elettronici.

Ciascun ambito di intervento è strumentale alla circolazione dei dati sanitari elettronici in ambito europeo, pur in un quadro di necessaria attenzione ai rischi che il trattamento di tali dati (personali e non) può comportare sia per gli individui e sia la società nel suo complesso[28].

Per quanto riguarda la circolazione dei dati primari, la normativa si apre con il rafforzamento dei diritti delle persone fisiche in relazione ai propri dati sanitari elettronici: questo avviene sia attraverso la previsione di un diritto di accesso, gratuito e in un formato leggibile, a tali dati elettronici immediatamente dopo la loro registrazione in un sistema di cartelle cliniche elettroniche, sia attraverso il riconoscimento di un diritto di scaricare gratuitamente una copia elettronica di tali dati[29]. Ulteriori diritti che, in parte mutuati dal GDPR, sono qui declinati con riferimento ai dati sanitari elettronici nel tentativo di bilan-

[27] Per sistemi si intende qualsiasi software o combinazione di hardware e software, destinati dal fabbricante a essere utilizzati da una persona fisica, per il trattamento dei dati sanitari elettronici, specificamente per fornire informazioni sulla salute di una persona fisica o per fornire cure assistenziali per scopi diversi dalla prestazione di assistenza sanitaria.

[28] Molto importanti sono, in questo senso, i continui rinvii alle norme europee in materia di cybersecurity. Sulla rilevanza delle cibersicurezza nella società digitale v. E. Longo, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in *La regolazione europea della società digitale*, cit., pp. 203 ss.

[29] L'accesso e il diritto di copia devono riguardare, almeno, le cd. categorie prioritarie dei dati sanitari elettronici personali ossia, ai sensi dell'art. 14 del Regolamento: a) profili sanitari sintetici dei pazienti; b) prescrizioni elettroniche; c) dispensazioni elettroniche; d) esami diagnostici per immagini e relativi referti di immagini; e) risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti; f) lettere di dimissione. L'indicazione più dettagliata è rimessa a un Allegato al Regolamento stesso che la Commissione può aggiornare, come ormai comune a tutti gli atti della cd. società digitale.

ciare l'obiettivo della massima condivisione con quello di garantire sempre e comunque il controllo sui dati sono il diritto di rettifica, il diritto di inserire informazioni nella propria cartella clinica elettronica, alla portabilità, il diritto di limitare l'accesso e il diritto di ottenere informazioni sull'accesso ai dati.

Per l'implementazione di tali diritti e del sistema nel suo complesso gli Stati membri devono prevedere obbligatoriamente che i prestatori di assistenza sanitaria registrino, in formato elettronico all'interno di un sistema di cartelle cliniche elettroniche, i dati sanitari; l'implementazione di servizi di accesso ai dati sanitari elettronici per le persone fisiche che garantiscano l'esercizio di tali diritti[30]; la predisposizione di servizi d'accesso dedicati agli operatori sanitari.

Se il principio della condivisione dei dati elettronici sanitari appare, nell'EHDS la regola, ciò nondimeno il Regolamento consente agli Stati membri di prevedere eccezioni nelle loro legislazioni. Un punto delicato è quello del cd. *opting out* ossia la possibilità che i cittadini impediscano l'accesso dei professionisti sanitari a tutti o parte dei loro dati sanitari. Il Regolamento, ex art. 10, nel rimettere agli Stati il compito di legiferare in merito specifica, però, la necessità di garantire la reversibilità del diritto e consiglia (Considerando 17) di mettere mano al regime di responsabilità dei medici nonché di informare i cittadini sui gravi possibili effetti della loro scelta[31].

Per quanto attiene all'uso secondario dei dati sanitari elettronici, il Regolamento EHDS prevede, innanzitutto, che i titolari dei dati sanitari mettano a disposizione, a norma dell'art. 51, per il riuso secondario i: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute; c) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all'assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l'assistenza sanitaria e sul suo finanziamento; d) dati sugli agenti patogeni che incidono sulla salute umana; dati amministrativi relativi all'assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi; f) dati genetici, epigenomici e genomici umani; g) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; h) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; i) dati provenienti dalle applicazioni per il benessere; j) dati relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; k) dati provenienti da registri dei dati

[30] Molto interessante è la previsione – *ex* art. 6 del Regolamento – che le richieste di rettifica riguardanti i dati nelle cartelle sanitarie elettroniche debbano essere verificate dal Titolare insieme a un professionista sanitario competente.

[31] Il Regolamento, nel riconoscere tale possibilità, aggiunge anche sulla base del par. 2 dell'art. 10, che gli Stati membri possono individuare, anche se il paziente ha esercitato il diritto di esclusione, il prestatore di assistenza sanitaria o il professionista sanitario che possa accedere ai dati sanitari elettronici personali nei casi in cui il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica. Così anche rispettando il GDPR che, *ex* art. 9, par. 2, lett. c), individua proprio nell'interesse vitale un'eccezione al divieto di trattamento dei dati sensibili.

sanitari basati sulla popolazione, come i registri di sanità pubblica; l) dati provenienti da registri medici e da registri della mortalità; m) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni; n) altri dati sanitari provenienti da dispositivi medici; o) dati provenienti da registri di medicinali e dispositivi medici; p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; q) dati sanitari provenienti da biobanche e banche dati associate.

Per ovviare agli evidenti rischi connessi con una tale mole di dati resi disponibili, il Regolamento EHDS disciplina le modalità d'accesso ad essi in modo assai stringente.

In primo luogo, il Regolamento subordina l'accesso dell'utente dei dati – vale a dire la persona fisica o giuridica (incluse le istituzioni, gli organi o gli organismi) che fa la richiesta – al rilascio di un'autorizzazione amministrativa. L'art. 55 del Regolamento prevede che gli Stati membri provvedano alla designazione di uno o più organismi responsabili dell'accesso ai dati e che tali organismi decidano in merito al rilascio di dette autorizzazioni.

In secondo luogo, il Regolamento definisce gli obblighi per l'utente dei dati personali. In proposito, occorre segnalare l'obbligo di trattare i dati per l'uso secondario previsto dall'autorizzazione, di effettuare i trattamenti all'interno di ambienti di trattamento sicuro, di non re-identificare o cercare di re-identificare le persone a cui i dati si riferiscono, di rendere pubblici (in forma anonima) i risultati e gli esiti dell'uso secondario.

In terzo luogo, il Regolamento prevede che l'accesso debba avvenire rispettando il principio di minimizzazione. Questo significa che l'accesso ai dati debba essere concesso in via ordinaria previa anonimizzazione dei dati personali. Quest'obbligo può, però, essere superato se l'utente dei dati dimostra che la finalità del trattamento che egli persegue non può essere conseguita con dati anonimizzati. In questi casi, il Regolamento prevede allora che si ricorra alla pseudonomizzazione – che, come noto, è una misura di sicurezza e non di anonimizzazione – e che le chiavi per la re-identificazione siano soltanto nella disponibilità dell'organismo responsabile dell'accesso ai dati sanitari.

7. Osservazioni conclusive

L'analisi svolta, approfondendo l'importanza e le implicazioni della circolazione dei dati per l'affermazione dell'approccio *One Digital Health*, evidenzia come la circolazione dei dati sia ormai un mezzo essenziale per promuovere e tutelare sia i diritti fondamentali, quali il diritto alla salute, sia interessi costituzionalmente tutelati, come ad esempio la salute stessa, la tutela dell'ambiente, dell'ecosistema e degli animali.

La chiave di volta di questa trasformazione risiede nell'adozione di tecnologie avanzate come l'intelligenza artificiale, i big data, l'Internet of Things (IoT), che permettono di raccogliere, analizzare e condividere grandi volumi di dati in tempo reale. Queste tecnologie che offrono strumenti concreti per affrontare sfide globali, come le pandemie, i cambiamenti climatici e le emergenze sanitarie, proponendo soluzioni innovative e personalizzate hanno tutte bisogno di grandi quantità di dati di buona qualità.

In questo scenario, l'Unione Europea si è posta come protagonista in particolar modo attraverso l'adozione del *Data Governance Act* (DGA) e del Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS). Questi strumenti regolamentari, tra loro coordinati, mirano infatti a creare un ecosistema digitale sicuro, interoperabile e trasparente, dove la condivisione dei dati possa avvenire come regola generale ancorché nel pieno rispetto della privacy e dei diritti individuali. Il *Data Governance Act*, in particolare, pone le basi per ridurre il divario digitale, promuovendo un accesso equo ai dati e riducendo il rischio che le innovazioni tecnologiche amplifichino le disuguaglianze esistenti. Parallelamente, l'EHDS si concentra sulla gestione dei dati sanitari, distinguendo tra l'uso primario, volto a migliorare direttamente l'assistenza sanitaria, e l'uso secondario, che supporta la ricerca scientifica e lo sviluppo di politiche sanitarie basate sull'evidenza.

Nonostante l'innegabile sforzo compiuto a livello di UE, che tra l'altro fà da contraltare all'inerzia degli Stati membri, il successo dell'azione è tutt'altro che scontato, vuoi per il difficile contesto internazionale in cui la transizione si colloca, vuoi per le innegabilità criticità che l'attuazione di questo imponente *corpus* normativo è destinato ad incontrare. Infatti, sia l'attuazione dei Regolamenti DGA e EHDS sia la realizzazione completa dell'approccio EHDS richiedono importanti azioni sia a livello europeo sia a livello degli Stati membri.

Da un lato, l'UE è chiamata a dar seguito all'impegno di provvedere a disciplinare gli altri Spazi comuni europei di dati previsti nella Strategia e, per quanto qui di interesse, quello sui dati ambientali e/o climatici. La Commissione ha, inoltre, il compito di adottare tutti gli atti di normazione secondaria previsti nei Regolamenti DGA e EHDS.

Da un altro lato, gli Stati membri hanno un compito ancora più arduo.

Essi devono, infatti, provvedere ad adattare i loro sistemi sanitari – in punto di organizzazione, di sicurezza, di responsabilità dei medici e delle strutture nonché di formazione – per renderli idonei a garantire l'attuazione degli obiettivi di accesso ai dati sanitari elettronici e di riuso primario e secondario.

Nel fare questo, essi devono impegnarsi per contrastare il rischio che le nuove infrastrutture e tecnologie si diffondano a macchia di leopardo in maniera tale da rendere disomogeneo l'accesso dei pazienti. Infatti, è assolutamente da evitare che la transizione digitale, anziché aiutare a combattere le diseguaglianze esistenti ne crei di nuove, potenzialmente anche più pericolose per la tenuta del principio di eguaglianza su cui si basa la nostra società. Il rischio, d'altra parte, è stato avvertito anche da taluni Governi nazionali che in sede di definitiva approvazione nell'ambito del Consiglio, hanno verbalizzato il loro timore circa un percorso di attuazione e di ammodernamento che potrebbe comportare grandi difficoltà di ordine economico e sociale.

È del tutto evidente, quindi, che una transizione di questo tipo non possa avvenire con risorse ordinarie. È importante quindi fin d'ora prevedere, a livello europeo e nazionale, un programma adeguato di investimenti.

Detto, in altri termini, l'approccio *One Digital Health* – di cui la circolazione dei dati è elemento essenziale – è un progetto ambizioso che per realizzarsi pienamente ha bisogno di un impegno condiviso da parte di legislatori, pubbliche amministrazioni, operatori sa-

nitari, aziende tecnologiche e cittadini. Solo attraverso una collaborazione inclusiva sarà, infatti, possibile costruire un ecosistema digitale che non solo favorisca l'innovazione e lo sviluppo economico, ma che sia anche equo, sostenibile e capace di rispondere alle sfide della società digitale, tutelando in particolare i diritti fondamentali di tutti.
In conclusione, le sfide che si presentano dinnanzi per l'utilizzo di tali tecnologie e per l'effettiva circolazione dei dati sono molteplici e tutte straordinariamente sfidanti. Ciascuna di esse meriterebbe specifiche osservazioni che dovranno certamente essere oggetto di molte future riflessioni individuali e collettive.