Consiglio Nazionale delle Ricerche

ITALIAN PAPERS ON FEDERALISM

Rivista giuridica on-line – ISSiRFA – CNR

MARCO OROFINO*

Digital Health e diritto alla salute: l'impatto del Regolamento EHDS sui sistemi sanitari nazionali**

ABSTRACT (EN): The essay analyzes the impact of the EU EHDS Regulation on the digital transformation of healthcare systems, focusing on balancing the right to health, data protection, and technological innovation. It examines the primary and secondary use of health data, highlighting both the opportunities and risks of data circulation. The author underscores the institutional, technological, and cultural challenges that Member States, particularly Italy, will face.

ABSTRACT (IT): Il saggio analizza l'impatto del Regolamento europeo EHDS sulla trasformazione digitale dei sistemi sanitari, ponendo particolare attenzione all'equilibrio tra diritto alla salute, protezione dei dati e innovazione tecnologica. Esamina l'uso primario e secondario dei dati sanitari, sottolineando le opportunità e i rischi connessi alla loro circolazione. L'autore evidenzia le sfide istituzionali, tecnologiche e culturali che i Paesi membri, e in particolare l'Italia, dovranno affrontare.

1. Introduzione

Negli ultimi anni, l'espressione *Digital Health* ha acquistato una centralità sempre maggiore nel dibattito giuridico rispetto al più datato termine di *e-Health*. Se agli inizi del nuovo millennio il concetto di *e-Health* rappresentava un'innovazione incentrata sull'uso delle tecnologie dell'informazione e della comunicazione (ICT) per migliorare l'efficienza dei sistemi sanitari, oggi appare limitato nel descrivere la complessità dell'ecosistema digitale della salute.

Con *e-Health*, infatti, l'attenzione era principalmente rivolta alla digitalizzazione dei processi sanitari, come la gestione elettronica dei dati clinici, la creazione di reti tra operatori all'interno delle strutture sanitarie ed una iniziale forma di telemedicina[1]. In questo modello, il paziente era spesso un soggetto passivo, destinatario di servizi sanitari digitalizzati con l'obiettivo principale di ottimizzare i flussi informativi al fine di semplificare la trasmissione di dati all'interno delle strutture sanitarie e, di conseguenza, ridurre i costi operativi.

* Professore ordinario di Diritto costituzionale e pubblico – Università degli Studi di Milano.

** Articolo sottoposto a referaggio (Relazione al Convegno *Transizione digitale e divari territoriali: la sfida del PNRR*, tenutosi a Foggia il 24-25 ottobre 2024). Lo scritto è a beneficio del progetto Net4Future del programma RESTART.

[1] L'Organizzazione Mondiale della Sanità definisce l'*e-health* come "the use of information and communication technology (ICT) for health" (World Health Organization, 2015).

Digital Health, invece, segna un vero e proprio cambio di paradigma, estendendo il concetto oltre la semplice digitalizzazione per abbracciare un approccio più ampio e strategico. Non c'è dubbio in proposito che una spinta verso una nuova e diversa digitalizzazione della sanità sia dovuto anche allo stress test rappresentato dalla crisi pandemica[2].

Nel nuovo contesto, le tecnologie digitali non sono solo strumenti di supporto per il settore sanitario, ma diventano protagoniste di una trasformazione culturale e organizzativa. L'integrazione di intelligenza artificiale (IA), big data, Internet of Things (IoT), dispositivi sanitari e applicazioni del benessere sta ridefinendo il modo in cui concepiamo la salute, intesa come prevenzione e cura, rendendo il paziente un attore attivo nella sua gestione.

Un ruolo fondamentale in questa trasformazione è svolto dai sistemi di intelligenza artificiale, che stanno rivoluzionando numerosi ambiti della sanità. Sistemi di diagnostica avanzata, basati su *machine learning*, sono in grado di acquisire immagini ed informazioni in modo sempre più rapido e preciso nonché di analizzare immagini mediche con un'accuratezza comparabile a quella umana, accelerando il rilevamento precoce di malattie come tumori e patologie cardiovascolari. Algoritmi predittivi possono analizzare dati clinici per identificare *pattern* nascosti e anticipare possibili complicanze. *Chatbot* medici e assistenti virtuali sono in grado di supportare efficacemente i pazienti nella gestione delle terapie fornendo consigli basati sui sintomi riportati, mentre *software* di IA applicati alla farmacologia stanno velocizzando lo sviluppo di nuovi farmaci e trattamenti personalizzati che modificano i dosaggi in tempo reale.

Inoltre, la *Digital Health* non riguarda solo il miglioramento dei sistemi sanitari esistenti, ma affronta anche sfide su scala globale, dalla prevenzione delle pandemie al monitoraggio dei cambiamenti climatici, fino alla promozione di un accesso più equo alle cure a livello internazionale[3].

Pertanto, se l'*e-Health* rappresentava il primo passo verso la digitalizzazione della sanità, *Digital Health* segna quindi una trasformazione digitale più profonda, in cui la tecnologia non è solo un mezzo, ma un fattore chiave per ridefinire il concetto stesso di salute nel mondo contemporaneo.

Alla luce di quanto finora detto, il modello *Digital Health* solleva, evidentemente, numerose questioni circa l'estensione del diritto fondamentale alla salute e circa la riorganizzazione dei sistemi sanitari. Non è solo una questione di una specifica innovazione tecnologica che entra a far parte del contenuto essenziale del diritto alla salute o, se si preferisce, del livello essenziale al di sotto del quale la stessa prestazione sanitaria perderebbe la propria ragione d'essere come è comunemente accaduto in passato. Si pensi ad esempio, alla rivoluzione prodotta dalla diffusione della risonanza magnetica nella radiodiagnostica oppure delle tecniche artroscopiche nella chirurgia. In questo caso siamo davanti ad un cambio di paradigma e di modello destinato

[2] Cfr. in proposito R. BALDUZZI, *Diritto alla salute e sistemi sanitari alla prova della pandemia. Le "lezioni" di alcuni Piani nazionali di ripresa e resilienza*, in *DPCE Online*, n. 1, 2023, 399 ss.; D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *Federalismi.it*, 28 dicembre 2022.

[3] La nozione di *Digital Health* incrocia, per la sua dimensione sovranazionale, l'approccio *One Health*. Sia consentito rinviare in proposito a M. OROFINO, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in corso di pubblicazione su *Corti Supreme e Salute*, n. 2, 2025. 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*, n. 3, 2022, p. 809 e ss.

a cambiare l'erogazione di tutte le prestazioni sanitarie e divenire, in tempi rapidi, presupposto per garantire un livello adeguato (alle aspettative) di assistenza sanitaria[4].

2. La circolazione dei dati come presupposto della *Digital Health*

L'affermarsi della *Digital Health* ha un presupposto ineliminabile: la disponibilità e la circolazione dei dati sanitari sulla scala più ampia possibile.

Questa constatazione ha una conseguenza dirompente.

Essa segna il passaggio da un'epoca in cui il dato sanitario non deve essere condiviso – se si tratta di dati sanitari personali il trattamento è vietato salvo che esso non si fondi sulle deroghe espressamente previste nelle norme in materia di protezione dei dati – ad uno scenario opposto in cui la condivisione dei dati sanitari elettronici, siano essi personali o meno, deve essere favorita proprio al fine di garantire cure sempre più appropriate. In altri termini, il dato sanitario cessa di essere una risorsa riservata per divenire una risorsa da valorizzare per garantire un'assistenza sanitaria più efficiente, personalizzata e predittiva.

Il fatto che la condivisione dei dati sanitari elettronici sia necessaria per realizzare la *Digital Health* non elimina evidentemente i rischi legati alla diffusione di dati sanitari ed in particolare di dati personali relativi alla salute; anzi proprio perché il modello Digital Health richiede una circolazione massiva, rende i rischi ancora più evidenti.

Questo cambio di prospettiva ha evidenti implicazioni di natura costituzionale che ineriscono al necessario bilanciamento di diversi diritti e interessi costituzionalmente protetti quali evidentemente il principio di eguaglianza nell'accesso alle tecnologie digitali e sanitarie, il diritto alla salute (nella sua duplice accezione di diritto individuale e di interesse collettivo), il diritto alla riservatezza e alla protezione dei dati personali nonché interessi di rango costituzionale quali l'ordine pubblico e la sicurezza nazionale.

Di qui la necessità di un equilibrio nuovo tra protezione dei diritti e innovazione digitale: da un lato, una regolamentazione troppo rigida potrebbe frenare lo sviluppo della *Digital Health*, limitando i benefici derivanti dalla condivisione dei dati e dunque un "sottoutilizzo" delle tecnologie disponibili a garanzia dei diritti fondamentali[5]; dall'altro, un'eccessiva

[4] Cfr. C. BOTRUGNO, *Transizione digitale e diritto alla salute: sfide attuali e future*, in *Diritto e salute. Rivista di sanità e responsabilità medica*, 1, 2022; U. PAGALLO, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Mimesis, Milano, 2022. V. sul punto anche E. GIUSTI, *Intelligenza artificiale e sistema sanitario*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, Pisa, 2018, p. 309 e ss.; E. CATELANI, *Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain*, in *Federalismi*, n. 4, 2022; M. FARINA, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?* in *Federalismi.it*, n. 21, 2020, p. 170 e ss. Sul tema si veda, inoltre, D. MORANA, *Diritto alla salute, ricerca tecnico-scientifica e innovazioni tecnologiche*, in G. FERRI (a cura di), *Diritto costituzionale e nuove tecnologie*, E.S.I., Napoli, 2022, p. 321 e ss.

[5] V. sulla questione U. PAGALLO, *Il dovere alla salute … cit*. Cfr. anche M. OROFINO, *La questione del sottoutilizzo dell'intelligenza artificiale in campo sanitario: spunti di rilievo costituzionale*, in *Queste Istituzioni*, n. 4, 2022, p. 157 e ss. Sulla rilevanza costituzionale dell'IA, A. SIMONCINI, *La dimensione costituzionale dell'intelligenza artificiale*, in G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022; G. DE MINICO, *Fundamental Rights, European Digital Regulation and Algorithmic Challenge*, in *Medialaws*, n. 1, 2021, p. 9 e ss. V. recentemente F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, O. POLLICINO (a cura di), *La disciplina dell'Intelligenza Artificiale*, Milano, 2025, e ivi, in particolare, i saggi

liberalizzazione esporrebbe i cittadini a rischi inaccettabili di profilazione indebita, discriminazione algoritmica o accessi non autorizzati ai loro dati sanitari. Un esempio concreto riguarda l'utilizzo dei dati sanitari da parte delle compagnie assicurative: se non adeguatamente regolamentato, potrebbe tradursi in pratiche discriminatorie, con il rischio che le persone con determinate condizioni di salute siano penalizzate nell'accesso ai servizi assicurativi.

Un ulteriore aspetto costituzionale fondamentale riguarda il principio di uguaglianza, sancito dall'articolo 3 della Costituzione italiana. La digitalizzazione dei dati sanitari non è uniforme sul territorio nazionale: esistono disuguaglianze strutturali che impediscono già oggi, ad una parte della popolazione, di beneficiare delle innovazioni digitali. Questa situazione è inevitabilmente destinata ad aggravarsi alla luce dell'esigenza di dotarsi degli strumenti necessari a incorporare sistemi di intelligenza artificiale, a dialogare in forma digitale ed automatica con i *devices* medici, a personalizzare le cure sulla base di cartelle cliniche elettroniche alimentate da tutti i dati sanitari, socio-economici e comportamentali delle persone. La disparità nell'accesso a infrastrutture digitali adeguate, nelle competenze tecnologiche dei cittadini o nella disponibilità di dispositivi connessi rischia di creare nuove forme di esclusione sanitaria proprio a detrimento del principio di eguaglianza sostanziale.

Una massiva condivisione dei dati incrocia poi il tema della sicurezza. L'infrastruttura destinata a supportare l'acquisizione e la condivisione dei dati sanitari in forma elettronica deve essere adeguata, resiliente ed interoperabile. La sua sicurezza è una componente essenziale della *Digital Health* e presenta rilevanti implicazioni di ordine pubblico e sicurezza nazionale. La digitalizzazione della sanità, infatti, implica la raccolta, la gestione e la trasmissione di una quantità enorme di dati sensibili, il che rende le infrastrutture e i molteplici *devices* connessi un obiettivo particolarmente appetibile per attacchi informatici.

Gli attacchi *ransomware* agli ospedali, ad esempio, sono già una realtà: gruppi di hacker prendono in ostaggio interi sistemi informatici, bloccando l'accesso ai dati sanitari e mettendo a rischio la continuità delle cure[6]. In scenari ancora più critici, attacchi su larga scala potrebbero compromettere intere reti sanitarie, paralizzando il sistema di emergenza di un Paese o compromettendo dati essenziali per la gestione di pandemie e crisi sanitarie.

Dal punto di vista della sicurezza nazionale, la protezione delle reti sanitarie è strategica tanto quanto la difesa delle infrastrutture critiche come le reti energetiche e di telecomunicazione. Se un attacco informatico riuscisse a compromettere il sistema sanitario digitale di un Paese, potrebbe generare conseguenze catastrofiche, come la diffusione di dati sanitari riservati di

di O. POLLICINO, *Regolare l'intelligenza artificiale: la lunga via dei diritti fondamentali*, p. 3 e ss.; F. DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'Intelligenza Artificiale*, p. 41 e ss.; E. LONGO, F. PAOLUCCI *The article 50 of the AI Act and the transparency obligations: the model and its limitations*, p. 275 e ss.

[6] Un esempio significativo di attacco informatico in ambito sanitario è stato quello subito dal Servizio Sanitario Nazionale del Regno Unito (NHS) nel 2017 con il ransomware WannaCry, che ha compromesso migliaia di dispositivi ospedalieri, causando ritardi nei trattamenti e mettendo a rischio la vita dei pazienti. Anche in Italia si sono verificati episodi simili: nel 2021, la Regione Lazio è stata colpita da un grave attacco *ransomware* che ha bloccato i sistemi informatici, rendendo inaccessibili i portali per la prenotazione dei vaccini anti-Covid. A Torino, nel 2022, un attacco hacker ha preso di mira l'azienda sanitaria locale (ASL Città di Torino), causando disagi nella gestione delle cartelle cliniche e dei servizi sanitari essenziali.

milioni di cittadini o la manipolazione di informazioni cliniche con potenziali ripercussioni dirette sulla salute pubblica.

Per questi motivi, i governi devono sia adottare strategie di cybersicurezza avanzate, investendo in infrastrutture sicure, implementando protocolli di crittografia robusti sia preparare piani di emergenza nel caso di attacchi. Da questo punto di vista il Regolamento europeo sulla cybersicurezza e la Direttiva NIS 2 definiscono standard più elevati per la protezione delle infrastrutture critiche, comprese quelle sanitarie, ma resta fondamentale l'adozione di misure proattive per prevenire minacce emergenti, come gli attacchi basati sull'intelligenza artificiale[7].

In definitiva, la sicurezza delle reti sanitarie non è solo un tema di protezione dei dati personali, ma un vero e proprio tema di ordine pubblico e sicurezza nazionale. Garantire la resilienza del sistema digitale sanitario significa proteggere non solo i diritti fondamentali dei cittadini, ma anche la stabilità del Paese di fronte a minacce sempre più sofisticate[8].

3. La nuova regolamentazione orizzontale europea per la circolazione dei dati: il *Data Governance Act* e il *Data Act*

Il complesso mutamento di paradigma in cui la circolazione dei dati cessa di essere solo un'opportunità economica da bilanciare con i rischi legati alla riservatezza delle persone e alla protezione dei loro dati per divenire necessaria all'inveramento della *Digital Health* è già presente *in nuce* nella Comunicazione della Commissione europea recante *Una strategia europea per i dati* del 9 febbraio 2020[9].

Essa fin dalle sue premesse evidenzia, infatti, che le tecnologie digitali hanno trasformato non solo l'economia, ma la società nel suo complesso, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei. Come esempio di questa trasformazione, la Commissione porta proprio l'utilizzo dei dati sanitari che è destinato a generare benefici enormi per i cittadini, ad esempio tramite il miglioramento della medicina personalizzata[10].

La visione espressa dalla Commissione nella sua *Data Strategy* è alla base di molti interventi normativi successivamente adottati dall'Unione europea nell'ambito del decennio digitale

[7] Cfr. E. LONGO, *La disciplina del "rischio digitale"* in F. PIZZETTI, A. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 53 e ss.; M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista italiana di informatica e diritto*, n. 2, 2024, p. 13 e ss.

[8] V. in argomento E. LONGO, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, n. 66, 2024, p. 313 e ss.

[9] La *Strategia per i dati* è presentata dalla Commissione europea contemporaneamente alla Comunicazione *Plasmare il futuro digitale dell'Europa* e al *Libro bianco sull'Intelligenza Artificiale*. I tre documenti sono importanti per collocare le proposte normative del cd. decennio digitale che la Commissione Von der Leyen ha successivamente presentato. Per un'analisi di tali Regolamenti sia consentito rinviare ai due volumi di F. PIZZETTI, A. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea della società digitale*, op.cit. e *La regolazione europea dell'Intelligenza Artificiale nella società digitale*, Giappichelli, Torino, 2025.

[10] L'idea di creare spazi europei comuni di dati è centrale nella Strategia dei dati della Commissione europea. Essa infatti mira a mediare tra un modello di regolazione orizzontale, che è tratto storico e distintivo della disciplina europea in materia di dati personali, e l'emergente necessità di norme *sector based*.

2030. In particolare tre Regolamenti sono centrali per questo lavoro: il Reg. UE 2022/868, meglio noto come *Data Governance Act*, o DGA; il Reg. UE 2023/2854, meglio conosciuto come *Data Act*, e il Reg. UE 2025/327 sullo spazio europeo dei dati sanitari (*European Health Data Space* - EHDS).

L'intervento europeo è sempre fondato sugli artt. 16 e 114 del TFUE e dunque sulla competenza dell'UE per la protezione e la circolazione dei dati di carattere personale e per il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno. Non c'è dubbio però che l'impianto normativo intervenga nel bilanciamento tra i diritti fondamentali e gli interessi di rango costituzionale[11].

Vi è un rapporto molto stretto tra i tre Regolamenti[12].

Secondo uno schema ben preciso, il *DGA* e il *Data Act* dettano norme orizzontali per incentivare la condivisione dei dati. Il primo mira a disciplinare una *governance* dei dati, intesa come il complesso di regole e mezzi che "disciplinano l'uso dei dati mediante procedimenti di condivisione, accordi e standard tecnici"[13]. Il fuoco dell'intervento regolatorio è la condivisione dei dati detenuti da soggetti pubblici in ragione dei loro compiti istituzionali. Il secondo Regolamento riguarda, invece, la condivisione dei dati detenuti da soggetti privati. Il punto centrale è disciplinare chi ha diritto ad utilizzare i dati di un prodotto o di un servizio, a quali condizioni e su quale base[14]. Insieme sono prodromici rispetto alla creazione di spazi comuni europei dei dati elettronici: in questo senso il Reg. EHDS, incentrato sui dati sanitari elettronici, è il primo spazio comune europeo.

Passando all'esame delle norme orizzontali del DGA occorre *innanzitutto* osservare che esso ha un ambito materiale articolato.

Il DGA definisce, *in primo luogo*, le regole per il riutilizzo di quei dati detenuti da soggetti pubblici che, fino a quel momento, erano esclusi dal perimetro delle norme europee sul riuso delle informazioni pubbliche e, in particolare, dall'ambito della Direttiva (UE) 2019/1024 *relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*, cd. Direttiva *Open Data*.

Il DGA estende e rafforza il principio di apertura dei dati perché apre al "riuso" dei dati protetti per motivi di riservatezza commerciale, compresi i segreti commerciali, dei professionali o d'impresa; dei dati statistici riservati; dei dati su cui insistono diritti di proprietà intellettuale di terzi; dei dati personali. Dall'esperienza normativa precedente, il DGA mutua, precisandoli, alcuni istituti. Si pensi ad esempio ai principi dell'accesso equo, ai divieti di esclusiva o di accordi che limitino il riutilizzo dei dati oppure alla definizione di un sistema tariffario orientato al costo. Tutto ciò, da un lato, consente di valorizzare al massimo il patrimonio informativo

[11] L'intervento dell'UE ex artt. 114, par. 2, del TFUE in materia di sanità, sicurezza, protezione dell'ambiente e protezione dei consumatori, si basa su un livello di protezione elevato, tenuto conto, in particolare, degli eventuali nuovi sviluppi fondati su riscontri scientifici.

[12] 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*, *op. cit.*, p. 107 e ss. e spec. p. 109.

[13] A. IANNUZZI, *I regolamenti intersettoriali … cit.*, 112.

[14] In particolare, il *Data Act* disciplina l'accesso equo ai dati e il loro utilizzo nel settore dei dispositivi intelligenti.

pubblico, evitando la formazione di posizioni di dominanza e valorizzando l'interesse pubblico; da un altro lato, pone le basi del cambio di paradigma in favore della circolazione garantendo che anche i dati precedentemente esclusi dal riuso possano, a determinate condizioni, quali ad esempio la loro anonimizzazione o pseudonomizzazione, divenire fruibili.

In secondo luogo, il DGA provvede ad una prima armonizzazione della disciplina inerente i servizi di intermediazione dei dati. In questo senso il Regolamento interviene a disciplinare quella che è oggi la nicchia di mercato dei *data intermediaries*[15]: la scelta di intervenire precocemente su tali soggetti si spiega sia con l'importanza che il *data sharing* sta assumendo sia con il ruolo che gli intermediari avranno sempre più nella fornitura - garantendo qualità e rappresentatività - di set di dati per l'addestramento e l'aggiornamento di modelli e sistemi di IA proprio nel settore sanitario.

Al fine di evitare che i *data intermediaries,* divenuti strategici, possano operare vanificando l'obiettivo di consentire il massimo riuso dei dati, il DGA introduce a loro carico obblighi di notifica e li sottopone al controllo delle autorità di settore.

In terzo luogo, il DGA disciplina il cd. altruismo dei dati. Per altruismo dei dati si intende la condivisione volontaria dei propri dati personali (spesso sanitari, ma anche di altro tipo) per fare progredire la ricerca, sviluppare prodotti e servizi nuovi e, financo, per contribuire all'addestramento dei sistemi di IA. La normativa mira in questo senso ad assecondare una volontà di condivisione garantendo sicurezza ai cittadini e, soprattutto, che il loro altruismo non sia oggetto di indebito sfruttamento commerciale. Per questa ragione introduce obblighi di separazione e di indipendenza tra i soggetti che operano per l'altruismo dei dati e i soggetti che operano a scopo di lucro. In proposito, il DGA prevede un sistema per la registrazione volontaria delle entità che raccolgono e trattano dati messi a disposizione per fini altruistici. Questa misura promuove la condivisione responsabile e solidale dei dati, incentivando progetti che generano benefici sociali e collettivi[16]. Nel contesto della *Digital Health*, l'altruismo dei dati può aiutare a sviluppare nuove cure, migliorare i sistemi sanitari e rendere più efficaci le politiche di salute pubblica.

Infine, il Regolamento DGA istituisce il Comitato europeo per l'innovazione in materia di dati. Questo nuovo organismo ha il compito di promuovere la circolazione dei dati attraverso lo sviluppo di politiche innovative nonché favorire la cooperazione tra Stati membri e garantire una *governance* efficace del mercato dei dati[17].

A differenza di altri organismi e autorità (quali ad esempio le Autorità di protezione dei dati) che storicamente nascono per garantire la protezione dei dati personali piuttosto che per favorirne la circolazione, il Comitato istituito dal DGA nasce con lo scopo di promuovere e incentivare la condivisione nonché l'utilizzo dei dati in modo efficace e strategico[18].

---

[15] Cfr. A. IANNUZZI, *I regolamenti intersettoriali … cit.*, p. 116. V. anche F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, n. 1, 2021, p. 199 e ss.

[16] A. IANNUZZI, *op. cit.*, p. 119. Cfr. anche M. AMENDOLA, *Il principio solidaristico e il data governance act*, in *Iura & Legal Systems*, n. 2, 2024.

[17] A. IANNUZZI, *op. cit.*, p. 122

[18] In realtà tra i compiti istituzionali delle Autorità di protezione dei dati vi è anche quello di favorire la circolazione dei dati. Una certa subalternità di tale obiettivo rispetto a quello di protezione è certamente legata all'origine storica della normativa europea. Il GDPR però mirava a un riequilibrio dei due obiettivi proprio per l'approssimarsi del

Per quanto riguarda il *Data Act*, esso ha, come è stato correttamente osservato, uno spiccato carattere privatistico, nel senso che molte delle disposizioni in esso contenute intervengono nei rapporti contrattuali che si instaurano tra i diversi soggetti dell'ecosistema digitale. Tra di essi il *Data Act* considera evidentemente anche i consumatori[19]. C'è però un punto importante di questa regolamentazione che è centrale perché ha un forte connotato pubblicistico e perché è centrale per il tema oggetto di indagine.

Si tratta dei diritti che il *Data Act* riconosce agli utenti dei dispositivi intelligenti di accedere ai dati da loro generati e di condividerli con terzi di loro scelta. Tali diritti – che certamente sono anche diritti contrattuali – rafforzano il diritto al controllo dei propri dati che è contenuto essenziale del diritto alla protezione dei dati personali e ridondano in obblighi specifici di natura pubblicistica *by design* a carico di fabbricanti e fornitori di tali dispositivi.

Inoltre i diritti di accesso e di condivisione dei dati generati – anche da dispositivi non strettamente medici come ad esempio quelli delle cd. applicazioni del benessere – sono fondamentali in campo sanitario perché consentono il loro riuso a scopo diagnostico e terapeutico.

4. Il Regolamento sullo spazio europeo dei dati sanitari elettronici

Dentro questo quadro generale, si colloca il Regolamento UE 2025/327, cd. EHDS, che è entrato in vigore il 26 marzo 2025, dopo un *iter* piuttosto lungo e accidentato che si è sviluppato a cavallo di due "legislature europee"[20]. Come detto, il Regolamento EHDS è il primo spazio europeo dei dati ad essere disciplinato tra quelli previsti dalla *Strategia europea per i dati* della Commissione europea.

L'obiettivo dichiarato dell'EHDS è disciplinare, nell'ambito del quadro generale normativo appena richiamato, la condivisione (l'accesso e il riuso) dei dati sanitari elettronici. Una condivisione che si articola su due livelli: l'uso primario e l'uso secondario.

---

nuovo modello sociale digitale. Il mutamento di approccio è certamente complesso per le Autorità di protezione dati, ma al tempo stesso inevitabile, pena il rischio di una loro marginalizzazione nella costruzione della società digitale. V. sul punto già prima della piena esplosione della società digitale, F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 53.

[19] Questo secondo A. IANNUZZI produce una certa difficoltà perché pone il medesimo in rotta di collisione sia con altri atti europei sia con il diritto contrattuale nazionale (ID, *I regolamenti intersettoriali … cit.*, p. 123). V. sul punto con diversità di accenti V. RICCIUTO, *Economia e mercato dei dati. Note a margine del c.d. Data Act* in *Accademia*, 2024, p. 477 e ss.

[20] L'adozione definitiva del Regolamento da parte del Consiglio è avvenuta il 21 gennaio 2025. Il Consiglio si è espresso, in quella data, sul testo risultante dall'accordo raggiunto in sede di trilogo nell'ambito della Legislatura precedente, Questo è stato possibile perché, diversamente da quanto accade nel procedimento legislativo italiano, a livello europeo la fine della legislatura non implica che tutte le questioni pendenti decadano. L'art. 240 del regolamento del Parlamento europeo, infatti, dopo aver previsto, al primo comma, la regola generale della decadenza "nell'ultima seduta che precede le nuove elezioni", nel secondo comma, consente, all'inizio di ogni legislatura, alla Conferenza dei presidenti di decidere in merito alle richieste motivate pervenute dalle commissioni parlamentari e delle altre istituzioni ed intese a ricominciare o proseguire l'esame di tali questioni pendenti.

4.1. L'uso primario dei dati sanitari elettronici e il suo impatto sulle attività sanitarie fondamentali

L'uso primario dei dati sanitari elettronici concerne, ex art. 2, par. 2, lett. d), EHDS, il loro trattamento 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. Tale utilizzo è considerato primario perché, garantendo una conoscenza accurata della storia clinica del paziente, contribuisce direttamente alla prevenzione, alla diagnosi e alla cura[21]. La stretta correlazione tra l'uso primario dei dati e le attività sanitarie fondamentali evidenzia il legame con il diritto alla salute, tutelato a livello costituzionale.

In questa prospettiva vanno interpretate le disposizioni dell'EDHS, le quali impongono l'assunzione dei dati sanitari direttamente in formato elettronico, la loro standardizzazione non solo in termini di formato, ma soprattutto in termini di contenuto, la definizione delle categorie primarie di dati sanitari elettronici, l'interoperabilità delle cartelle cliniche elettroniche, la fornitura di servizi di accesso per i professionisti sanitari, l'integrazione tra dati sanitari elettronici e dati generati dalle cd. applicazioni del benessere.

Le disposizioni in questione servono anche a garantire, la possibilità di ricevere cure transfrontaliere adeguate e, di conseguenza, rafforzare la libera circolazione delle persone[22]. Nell'ottica della libera circolazione transfrontaliera devono essere collocate specificamente le disposizioni del Regolamento che prevedono l'adozione di un formato europeo di scambio delle cartelle cliniche, una gestione comune dell'identificazione, standard di qualità e l'integrità dei dati condivisi tra i vari sistemi sanitari europei; un'infrastruttura transfrontaliera che renda possibile l'uso primario dei dati sanitari elettronici personali in tutta l'Unione, l'individuazione di un'Autorità responsabile per la gestione e il controllo dell'uso primario dei dati sanitari.

L'intervento normativo sulla circolazione dei dati primari mira anche a definire un equilibrio tra i diversi diritti costituzionali coinvolti. In primo luogo tra l'interesse alla circolazione dei dati (in quanto presupposto delle attività sanitarie) e la protezione dei dati personali. Tra le principali disposizioni ascrivibili a tale complesso bilanciamento, vi sono i nuovi diritti che il Regolamento riconosce all'interessato nell'ambito dei trattamenti che coinvolgono dati personali quali ad esempio il diritto ai servizi di accesso, il diritto ad inserire informazioni nella propria cartella clinica e il diritto di ottenere informazioni sull'accesso ai dati; integrazioni ai diritti definiti dal GDPR come nel caso del diritto alla portabilità, del diritto di rettifica, nonché divieti d'uso per finalità discriminatorie.

[21] È molto importante che tale attività non venga intesa come sostitutiva dell'anamnesi (che riguarda anche i membri della famiglia) e del contatto tra il medico e il paziente che è parte insostituibile della pratica medica.

[22] Cfr. ampiamente sulla questione e sui riflessi istituzionali, D. MORANA, *Diritto alle cure e mobilità sanitaria nell'Unione europea: un banco di prova per l'Europa sociale. Note introduttive*, in D. MORANA (a cura di), *L'assistenza sanitaria transfrontaliera. Verso un welfare state europeo?*, E.S.I., Napoli, 2018, p. 3 e ss.

Assai significativo è inoltre il diritto di cd. *opting out* rispetto all'accesso dei professionisti sanitari alla totalità o a parte dei propri dati sanitari[23]. La norma muove dal riconoscimento, anche in questo ambito, della libertà di cura, ossia della libertà costituzionalmente garantita alle persone di curarsi scegliendo anche il modo in cui curarsi[24]. In questo caso, però, tale libertà impatta – occultando alcuni dati sanitari – molto significativamente sulla libertà di terapia del medico e sulla conseguente responsabilità professionale. Non è un caso che il Regolamento, da un lato, preveda che i pazienti siano informati delle conseguenze derivanti dalla loro scelta sulla qualità delle prestazioni sanitarie e, da un altro lato, rinvii agli Stati per disciplinare eventuali eccezioni laddove il trattamento dei dati sanitari elettronici sia necessario per tutelare gli interessi vitali dell'interessato o di altra persona fisica, anche se il paziente ha esercitato il diritto di esclusione. Nel fare questo il Regolamento avverte che gli Stati dovranno necessariamente intervenire, operando le necessarie integrazioni, sulle norme nazionali sulla responsabilità medica[25].

4.2. L'uso secondario dei dati sanitari elettronici come interesse della collettività

L'uso secondario dei dati sanitari elettronici consiste, a norma dell'art. 2, par. 2, lett. e), EHDS, nel trattamento dei dati sanitari elettronici per finalità diverse rispetto alle finalità primarie per le quali tali dati sono stati inizialmente raccolti o prodotti.

Le finalità diverse che legittimano il riuso secondario sono elencate all'art. 53 del Regolamento. Esse sono: a) il pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro; b) la definizione delle politiche e attività regolamentari; c) finalità statistiche; d) attività d'istruzione o d'insegnamento; e) finalità di ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica; f) miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria[26].

Di particolare interesse nell'ambito della finalità di ricerca è la specificazione testuale che essa include l'attività di sviluppo e innovazione per prodotti o servizi e, soprattutto, 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. Ciò mira a tutta evidenza a rendere disponibili set di dati sanitari elettronici di alta qualità per l'addestramento dei modelli di IA e dei sistemi destinati ad essere utilizzati in campo medico.

In modo speculare alle finalità legittime, il Regolamento EHDS definisce anche i divieti al riuso secondario nel successivo art. 54. Essi impediscono l'uso dei dati sanitari elettronici per adottare decisioni pregiudizievoli per una persona fisica o per un gruppo di persone fisiche, per quanto riguarda offerte di lavoro, per la conclusione di un contratto assicurativo, per la modifica dei premi, per svolgere attività di marketing o pubblicitarie; per sviluppare prodotti o

[23] Il Considerando 17 del Regolamento immagina che l'*opting out* sia legato a questioni di salute particolarmente delicate quali quelle legate alla salute mentale o sessuale, a procedure sensibili quali l'aborto, ma in realtà nell'articolato non c'è alcuna limitazione materiale né alcun obbligo di motivazione.

[24] Cfr. A. SANTOSUOSSO, *La libertà di cura*, in *Ann Ist. Super. Sanità*, n. 4, 1999, p. 547 e ss.

[25] Come specificato nel Considerando 17 del Regolamento.

[26] Le prime tre finalità legittimano solo l'accesso e il riuso da parte degli enti pubblici, a norma del par. 2 dell'art 53.

servizi in grado di danneggiare la salute delle persone (bevande alcoliche, tabacchi, armi o prodotti o servizi concepiti in modo da creare dipendenza), violare l'ordine pubblico o la moralità; svolgere attività in contrasto con le disposizioni etiche[27].

Come emerge dalla lettura delle finalità e dei divieti, l'uso secondario dei dati sanitari elettronici pur non precludendo un uso privato è, prevalentemente, finalizzato al benessere collettivo e specificamente parafrasando la Costituzione italiana all'interesse collettivo alla salute. Questo impiego consente infatti di migliorare le politiche sanitarie, sviluppare nuove terapie e innovazioni tecnologiche, prevenire epidemie e ottimizzare anche da un punto di vista normativo l'efficienza dei sistemi sanitari.

L'uso secondario dei dati sanitari elettronici si colloca nell'ambito dei principi costituzionali di tutela della salute e giustizia sociale sanciti non solo dalla Costituzione italiana (artt. 3 e 32), ma pure dalle costituzioni di molti Paesi membri dell'Unione Europea e dalla Carta dei diritti fondamentali dell'UE[28].

A livello europeo, l'art. 35 della Carta riconosce il diritto di ogni individuo di accedere alla prevenzione sanitaria e di ottenere cure mediche alle condizioni stabilite dalle legislazioni e prassi nazionali e impone alle istituzioni pubbliche di garantire un livello elevato di protezione della salute umana. In questo contesto, la raccolta e l'analisi dei dati sanitari elettronici non solo contribuiscono a migliorare le politiche sanitarie, ma rafforzano il principio di solidarietà sociale (art. 3 TUE) e promuovono un modello di giustizia sociale che riduce le disuguaglianze e garantisce un'assistenza sanitaria più equa ed efficiente per tutti i cittadini europei.

Se è vero, dunque, che l'uso secondario dei dati sanitari si collega a principi e diritti costituzionali come il diritto alla salute, nella sua duplice accezione individuale e collettiva, e il principio di solidarietà, nondimeno esso solleva rischi per altri diritti e interessi fondamentali, tra cui il diritto alla riservatezza e alla protezione dei dati (artt. 7 e 8 della Carta UE, art. 8 CEDU), il principio di autodeterminazione informativa; il diritto alla non discriminazione (art. 21 della Carta UE), la sicurezza dei dati, poiché il rischio che tali informazioni cadano nelle mani sbagliate, ad esempio attraverso attacchi informatici, può avere conseguenze rilevanti per gli individui e per il sistema sanitario stesso.

Questi rischi impongono un bilanciamento attento e proporzionato.

Da un lato, per sostenere il riuso secondario, il Regolamento EHDS prevede, ex art. 51, che siano resi disponibili i dati sanitari elettronici: a) provenienti da cartelle cliniche elettroniche; b) relativi a fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute; c) 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) relativi agli agenti patogeni che

[27] Il tono paternalistico di taluni divieti è un tratto distintivo della regolamentazione europea contemporanea nel settore digitale. Per un inquadramento teorico della questione cfr. V. MURA, *Paternalismo e democrazia liberale: un equivoco da chiarire*, in *Meridiana: rivista di storia e di scienze sociali*, n. 1, 2014, p. 47 e ss.

[28] In alcuni casi, le Costituzioni sanciscono esplicitamente il diritto alla salute come un interesse collettivo da tutelare mediante politiche pubbliche efficaci (v. ad esempio art. 43 Costituzione spagnola); in altri casi il riconoscimento è avvenuto grazie alla giurisprudenza costituzionale. Tale interpretazione, in ogni caso, è così diffusa da potersi parlare di una tradizione costituzionale comune agli Stati membri dell'UE.

incidono sulla salute umana; e) amministrativi relativi all'assistenza sanitaria; f) genetici, epigenomici e genomici umani; g) molecolari umani; h) generati automaticamente mediante dispositivi medici; i) provenienti dalle applicazioni per il benessere; j) relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; k) provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica; l) provenienti da registri medici e da registri della mortalità; m) provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni; n) provenienti da registri di medicinali; p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; q) provenienti da biobanche e banche dati associate.

Questo vasto patrimonio informativo può essere ulteriormente ampliato dalle disposizioni nazionali, che possono prevedere l'integrazione di altri dati sanitari.

D'altro lato, il Regolamento EHDS disciplina in modo assai stringente l'accesso a tali dati.

In primo luogo, il Regolamento lo subordina al rilascio di un'autorizzazione amministrativa. L'art. 57 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 alle domande di accesso ai dati[29].

In secondo luogo, il Regolamento definisce gli obblighi per l'"utente dei dati personali", vale a dire la persona fisica o giuridica (incluse le istituzioni, gli organi o gli organismi) che fa richiesta di accesso. In proposito, occorre segnalare l'obbligo di trattarli 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 di rendere i dati anonimi può, però, essere superato se l'utente dei dati dimostra che la finalità per cui l'accesso è richiesto non può essere conseguita con dati anonimizzati. In questi casi, il Regolamento prevede che si ricorra alla pseudonomizzazione e che le chiavi per la re-identificazione siano nella disponibilità dell'organismo responsabile dell'accesso ai dati sanitari.

Tale previsione, a una prima lettura, sembra generare confusione tra i concetti di anonimizzazione e pseudonomizzazione, che fino ad ora erano stati distinti nel quadro normativo europeo della protezione dei dati personali.

In particolare, l'anonimizzazione implica una trasformazione irreversibile dei dati, che ne rende impossibile l'associazione a un individuo specifico. Proprio per questo, i dati completamente anonimizzati escono dal campo di applicazione della normativa sulla protezione dei dati personali. La pseudonomizzazione, invece, consiste in una misura di sicurezza che separa i dati identificativi dal resto delle informazioni, sostituendoli con codici o altri elementi, ma senza eliminare del tutto la possibilità di re-identificazione, che rimane possibile tramite

[29] Art. 57, par. 1 del Reg. UE 2025/327.

informazioni aggiuntive conservate separatamente. Di conseguenza, i dati pseudonimizzati restano soggetti alla disciplina sulla protezione dei dati personali.

L'apparente sovrapposizione tra questi due concetti nel Regolamento EHDS potrebbe creare ambiguità applicative, incidendo sulla corretta interpretazione delle tutele da garantire nell'uso secondario dei dati sanitari elettronici.

Infine, il Regolamento prevede che il riuso secondario sia soggetto a una stretta vigilanza. In particolare è richiesto agli Stati membri di definire le sanzioni a carico degli utenti dei dati personali che non rispettino gli obblighi regolamentari. Il sistema di *governance* è di tipo misto nel senso che intervengono, come ormai consuetudine nella società digitale, autorità nazionali, organismi europei e la stessa Commissione europea[30].

5. Osservazioni conclusive sull'impatto della regolamentazione europea sui sistemi sanitari nazionali

L'impatto della normativa europea – e, in particolare del Regolamento EHDS – sui sistemi sanitari nazionali è destinato ad essere particolarmente significativo. Questo emerge con chiarezza, oltre che dalla lettura dell'articolato normativo e dei considerando, anche dall'esame degli atti preparatori e dei pareri formulati nell'ambito del procedimento decisionale. Anche i termini di applicazione particolarmente dilatati e scaglionati, che decorrono dal 27 marzo 2027 fino ad arrivare per talune disposizioni addirittura al 26 marzo 2035, confermano questa impressione. Un periodo transitorio così ampio come quello previsto dal Regolamento EHDS riflette la complessità dell'adeguamento richiesto ai sistemi sanitari nazionali, sia in termini di infrastrutture tecnologiche che di armonizzazione normativa.

L'impatto atteso può essere utilmente considerato sia in termini di opportunità che di rischi.

In termini di opportunità, l'attuazione del disegno regolamentare può, in primo luogo, portare ad una *migliore continuità assistenziale* sia nel senso che la digitalizzazione dei dati sanitari e la loro disponibilità elettronica possono facilitare il coordinamento tra medici, ospedali e farmacie sia nel senso che l'accesso transfrontaliero ai dati sanitari elettronici, consentendo la disponibilità della storia clinica, può permettere ai pazienti di ricevere cure appropriate in qualsiasi Stato membro dell'Unione europea.

In secondo luogo, l'attuazione delle norme europee che rafforzano il diritto dei cittadini (pazienti o interessati) a mantenere il controllo sui propri dati sanitari, incluso il diritto di aggiungere dati sanitari e dati del benessere a quelli destinati a figurare obbligatoriamente nel repository personale può determinare un effettivo *empowerment del cittadino-paziente*. Il che rappresenta un importante obiettivo nell'attuazione del principio costituzionale della libertà di scelta in materia di cura sorretto però da un'assunzione di responsabilità per le scelte compiute da parte del paziente.

In terzo luogo, è auspicabile che una volta a regime, una piena condivisione dei dati possa condurre anche ad una *maggiore efficienza dei sistemi sanitari* nazionali attraverso un uso più

[30] Cfr. su questa evoluzione F. PIZZETTI, *Il Regolamento europeo sulla IA come parte integrante della normativa UE per il decennio digitale* 2030 in *La regolazione europea dell'Intelligenza Artificiale nella società digitale*, *op. cit.*, p. 5.

efficiente delle risorse disponibili. In questo senso, la disponibilità in forma elettronica dei dati sanitari può ridurre in modo anche sensibile alcuni sprechi. Si pensi alla possibilità di evitare la ripetizione di esami diagnostici non necessari, di indagini già svolte in passato nonché di percorsi di cura già rivelatisi non efficaci per lo specifico paziente. Anche il monitoraggio basato sui *big data* associato ad una precisa profilazione dei singoli pazienti, grazie alla piena conoscenza dei dati sanitari e di quelli comportamentali ricavati dalle cd. applicazioni del benessere potrebbe migliorare la prevenzione e ridurre, di conseguenza l'insorgenza di patologie e il ricorso a costose (sia in termini economici che di sistema) cure d'emergenza.

Infine, l'attuazione piena del Regolamento potrebbe condurre a benefici anche significativi in termini di *innovazione e ricerca avanzata*. Questo passa in particolare attraverso la piena disponibilità per l'uso secondario dei dati sanitari e richiede un'implementazione rapida e coerente sia a livello istituzionale sia delle procedure e degli istituti previsti dalle nuove norme. Il percorso è indubbiamente lungo ma le potenzialità sono molto significative sia per la ricerca di base e applicata sia per i decisori politici e gli amministratori dei sistemi sanitari che potrebbero basare le proprie scelte allocative su evidenze concrete, migliorando la pianificazione sanitaria e l'efficacia delle cure.

A fronte di queste opportunità, l'attuazione del Regolamento EHDS pone sfide significative.

La prima, e più rilevante, riguarda *l'attuazione normativa* e *l'adeguamento tecnologico*. Le due sfide non possono che andare di pari passo.

Per quanto riguarda l'attuazione normativa in senso stretto, il percorso – comune a tutti i Regolamenti adottati nell'ultimo quinquennio – richiede un importante ruolo della Commissione europea nell'adozione degli atti secondari richiesti (in questo caso il Considerando 105 ne individua ben 32!) nonché nell'espletamento delle attività di coordinamento che le norme richiedono e un intervento degli Stati membri soprattutto nell'individuazione (e/o nell'istituzione) delle autorità e degli enti chiamati a garantire la governance del settore. Già questa scelta, rimessa ai singoli Stati, assume un valore strategico fondamentale, poiché può influenzare in modo determinante il delicato equilibrio tra circolazione e protezione dei dati.

Per quanto riguarda l'adeguamento tecnologico, i sistemi sanitari nazionali – e per quanto riguarda il nostro Paese i sistemi sanitari regionali – dovranno, infatti, conformarsi agli standard di accessibilità e interoperabilità definiti dall'EHDS sia per ciò che attiene all'acquisizione (e all'eventuale modifica) dei dati sanitari in formato elettronico sia per quanto riguarda le cartelle cliniche elettroniche all'interno delle quali i dati dovranno essere organizzati e manutenuti sia per i portali di accesso alle cartelle cliniche e sia, infine, per il collegamento infrastrutturale necessario per connettere i sistemi nazionali e regionali con il portale europeo e-Health per la circolazione transfrontaliera.

Ciò richiederà investimenti ingenti in infrastrutture, software e *devices* digitali talmente significativi che alcuni Stati proprio nell'ambito del Consiglio UE che ha dato il via libera definitivo al Regolamento hanno avanzato preoccupazioni circa la sostenibilità economica della transizione richiesta nei termini preventivati, paventando il rischio di un'attuazione a macchio di leopardo all'interno dell'UE e dei singoli Stati membri.

Il tema è evidentemente cruciale per il sistema sanitario italiano che, come noto, da un lato si trova in carenza di risorse per gestire l'ordinaria attività e, da un altro lato, già sconta differenze regionali e, talvolta, anche a livello di ASL infraregionali, molto significative. Immaginare, quindi, che questa transizione possa essere gestita con i soli fondi ordinari è una pura illusione che, se perseguita, non potrà che rendere la situazione ancor più complessa e meno rispettosa degli standard di cura nell'ambito del diritto alla salute nonché del principio di eguaglianza.

La seconda sfida che l'attuazione comporta è *garantire concretamente un'adeguata tutela della riservatezza e dei dati personali* sanitari oggetto di trattamento. La questione riguarda sia il trattamento dei dati sanitari elettronici nell'ambito del loro uso primario sia il trattamento per l'uso secondario.

Le questioni che si aprono sono evidentemente diverse.

Per l'uso primario è fondamentale garantire un'applicazione coerente tra GDPR e Regolamento EHDS. Vi sono aree di sovrapposizione e di integrazione che devono essere identificate con cura. A livello generale, il Regolamento EHDS interviene anche in aree come quella, ad esempio, del trattamento dei dati genetici in cui il GDPR consentiva agli Stati membri un significativo margine di azione nazionale. Vi sono nuovi diritti dell'interessato che il Regolamento EHDS riconosce e diritti preesistenti garantiti dal GDPR che sono oggetto di integrazione o specificazione. È evidente che qui non può essere messo in discussione il ruolo delle Autorità di protezione dei dati personali, le quali inevitabilmente vedono allargarsi il loro raggio d'azione in un'ottica più orientata alla circolazione che alla protezione. A tale allargamento non può che conseguire un aumento delle risorse sia in termini di risorse economiche sia in termini di risorse di personale.

Per l'uso secondario, il percorso attuativo è, se possibile, ancora più complesso perché prevede che gli Stati individuino gli organismi responsabili dell'accesso ai dati chiamati a concedere le prescritte autorizzazioni e garantire l'osservanza gli obblighi regolamentari. Per l'Italia, il primo grande nodo da sciogliere riguarda l'assetto istituzionale: sarà opportuno istituire un unico organismo nazionale chiamato a dialogare con i titolari dei dati a livello regionale e locale o piuttosto un sistema decentrato con un organismo per ogni Regione ed un organismo di coordinamento? Nonostante a prima vista la soluzione unitaria parrebbe preferibile per garantire la complessa attuazione d'altra parte occorre considerare che la struttura regionale e locale del sistema sanitario potrebbe spingere per una diversa soluzione.

La terza sfida fondamentale che l'attuazione del Regolamento EHDS pone riguarda la transizione digitale sotto il profilo della *formazione* e dell'*informazione* con particolare riferimento non solo agli operatori sanitari ma pure pazienti. Il profilo della cd. literacy è presente in tutti gli atti regolamenti con cui l'UE pretende di disciplinare la società digitale[31]. La presenza di tali riferimenti si spiega con la consapevolezza che il cambio di paradigma sociale è talmente

[31] Il Regolamento dedica due norme (artt. 83 e 84) specificamente alla formazione del personale sanitario e dei pazienti. Sulla questione generale della formazione in ambito sanitario v. il contributo F.G. PIZZETTI, *La "health literacy": compito della Repubblica, e diritto e dovere del cittadino?* in A. LAMBERTI (a cura di) *Scuola, università e ricerca: diritti, doveri e democrazia nello "Stato di cultura"*, Napoli, 2024, 993 ss.

repentino e profondo da poter ingenerare un effetto di straniamento nei cittadini e nelle categorie professionali di volta in volta coinvolte.

Ciò è ancor più vero nel contesto sanitario in cui occorre preservare con ogni mezzo il rapporto fiduciario tra il medico e il paziente. Un rapporto che, occorre osservare, appare già oggi in crisi e su cui sono destinate ad incidere le nuove tecnologie dell'IA. È evidente che l'inserimento dell'intelligenza artificiale nel rapporto tra medico e paziente richiede un ampio sforzo formativo e informativo di entrambe le parti del rapporto.

Infine, occorre essere realisti sul fatto che una tale trasformazione dei sistemi sanitari in senso digitale potrebbe ingenerare – almeno in una prima fase - un considerevole aumento di attività a carico degli operatori sanitari: è noto in proposito che l'aumento dei compiti burocratici produca sempre una forte resistenza al cambiamento. Per questo è necessario predisporre le opportune misure per accompagnare la transizione digitale in ambito sanitario sia con piani di formazione del personale sanitario ed amministrativo sia con l'arricchimento degli organici amministrativi con persone dotate di competenze tecnologiche e giuridiche adeguate.

In conclusione, è innegabile che il percorso di attuazione dell'EHDS – e più in generale di affermazione della *Digital Health* – si presenta assai difficile e richiede interventi e piani straordinari di ammodernamento. In assenza di questi, la transizione che le nuove norme richiedono potrebbe rivelarsi paradossalmente controindicata. Non c'è, infatti, per i cittadini nulla di più dannoso del sottoutilizzo tecnologico che un maldestro utilizzo delle nuove tecnologie.