LA GOVERNANCE MULTILIVELLO DELLO SPAZIO EUROPEO DEI DATI SANITARI (*EHDS*): STANDARDIZZAZIONE, USO E INTEROPERABILITÀ DEI DATI TRA *AI ACT* E *GDPR*[*]

di Alessia Sciamanna[**]

Sommario. 1. Introduzione: La digitalizzazione sanitaria come «stress test» costituzionale. – 2. La costruzione giuridica dell'*EHDS*: la tensione tra funzionalizzazione del dato e tutela della salute. – 3. Le antinomie del sistema: la triangolazione normativa tra *EHDS*, *GDPR* e *AI Act*. – 3.1. Il cambio di paradigma: dalla *data protection* alla *data valorisation* nell'uso secondario. – 3.2. L'Intelligenza Artificiale in sanità: il paradosso applicativo tra qualificazione «ad alto rischio» e necessità di *data quality*. 3.3. «*Compliance* sistemica»: coerenza normativa tra uso del dato e legittimità costituzionale 4. L'attuazione differenziata del Regolamento: asimmetrie istituzionali e *governance* multilivello. – 4.1. Il «caso Italia»: il conflitto tra programmazione pubblica e *privacy* nel regionalismo sanitario. – 5. Dinamiche globali e convergenze regolative: il dibattito internazionale e le sue ricadute. – 6. Conclusioni.

1. Introduzione: la digitalizzazione sanitaria come* «stress test» *costituzionale. La digitalizzazione costituisce una delle principali sfide e opportunità per i sistemi sanitari europei. Non rappresenta più una mera evoluzione tecnologica o un processo di efficientamento amministrativo, bensì si configura come una delle più profonde trasformazioni strutturali del *welfare state* contemporaneo, definendo una nuova dimensione dell'agire pubblico che la dottrina ha efficacemente descritto come condizione *Onlife*[1]. In tale contesto si colloca lo Spazio europeo dei dati sanitari (*European Health Data Space*, d'ora in avanti *EHDS*[2]), che rappresenta il primo intervento organico dell'Unione europea volto a costruire un ecosistema[3] sanitario digitale integrato[4]. Il suo obiettivo è garantire l'interoperabilità dei dati sanitari e l'accesso a cure di qualità su base transfrontaliera, superando la frammentazione dei sistemi informativi nazionali e favorendo una più efficiente circolazione delle informazioni cliniche.

---

[*] *Sottoposto a referaggio.*

[**] Dottoranda di ricerca in Equity, Diversity & Inclusion – Università Telematica Pegaso.

[1] L. Floridi, *The Onlife Manifesto: Being Human in a Hyperconnected Era,* Cham, 2015; Id., *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Milano, 2017.

[2] Reg. UE 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 relativo allo Spazio europeo dei dati sanitari e che modifica la dir. 2011/24/UE e il reg. (UE) 2024/2847.

[3] Comunicazione della Commissione, *Una strategia europea per i dati*, COM(2020) 66 final.

[4] L'*EHDS* mira a fornire una cornice giuridica unitaria per la raccolta, la condivisione e l'utilizzo dei dati sanitari, sia per finalità primarie di cura, sia per scopi secondari legati a ricerca, innovazione e *policy making,* e a disciplinare gli *standard* tecnici della infrastruttura tecnologica sottesa a tale disciplina.

Alla luce dell'esperienze apprese durante la crisi pandemica da COVID-19, che ha agito da potente acceleratore di processi latenti, l'integrazione delle tecnologie digitali nei percorsi di cura pone sfide inedite che investono direttamente le categorie fondanti del diritto pubblico e costituzionale coinvolte nel trattamento ed uso del dato[5].

Tali evidenze, emerse con vigore durante la crisi pandemica, hanno palesato come l'assenza di interoperabilità, la disomogeneità dei formati e la difficoltà di utilizzare in modo coordinato i dati disponibili possano tradursi in inefficienze sistemiche e in diseguaglianze sostanziali nell'accesso alle cure[6].

In tale ottica, l'indagine analizza la costruzione dell'*EHDS* quale fulcro di una complessa triangolazione normativa con il *Regolamento generale sulla protezione dei dati* (d'ora in avanti *GDPR*) e il *Regolamento sull'intelligenza artificiale* (d'ora poi *AI Act*), soffermandosi sulle tensioni scaturite dal passaggio paradigmatico verso la valorizzazione dei dati per finalità di interesse pubblico. Il percorso di ricerca si snoda attraverso la disamina delle aporie del caso italiano e delle dinamiche internazionali per dimostrare come l'interoperabilità dell'informazione costituisca oggi un presupposto di adeguatezza della sussidiarietà, volto a inquadrare il dato sanitario come «*Data for Public Good*» per la sostenibilità del *welfare*, destinato ad incidere sulle modalità di erogazione delle prestazioni e sulla concreta azionabilità del diritto alla salute.

L'*EHDS* si configura, infatti, come condizione abilitante del Fascicolo sanitario elettronico transfrontaliero e come strumento attuativo del diritto alla salute[7] sancito dalla Carta dei diritti fondamentali dell'Unione europea[8], contribuendo alla costruzione di una cittadinanza sanitaria europea[9] e alla rimozione di ostacoli strutturali all'esercizio di tale diritto in condizioni di uguaglianza sostanziale. Esso può essere qualificato, al tempo stesso, come *framework* giuridico e come infrastruttura abilitante, nel senso di un insieme coordinato di norme, *standard* tecnici e assetti di *governance* multilivello[10] volto a rendere operazionali i dati sanitari per finalità di cura, programmazione, ricerca e *policy making*, nel rispetto dei diritti fondamentali.

In questa prospettiva, la digitalizzazione sanitaria supera la dimensione del processo tecnico-organizzativo mettendo alla prova la tenuta dei principi di proporzionalità e sussidiarietà degli Stati membri nel «transito dal mondo degli atomi a quello dei *bit*[11]» e diventando un vero e proprio «stress test» per gli assetti costituzionali, chiamati a confrontarsi con una nuova forma di integrazione funzionale fondata sul dato[12]. La centralità del dato sanitario, inteso

---

[5] M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione svolta alla Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta, 2013.

[6] Per un'analisi del rapporto tra pandemia e *governance* dei dati si veda F. S. Marini, G. Scaccia (a cura di), *Emergenza Covid-19 e ordinamento costituzionale*, Torino, 2020. Sul ruolo dell'art. 35 Carta dei diritti fondamentali dell'Unione europea quale base del diritto alla salute si veda L. Uccello Barretta, *Il diritto alla salute nello spazio europeo: la mobilità sanitaria alla luce della direttiva 2011/24/UE*, in *Federalismi.it*, 19, 2014.

[7] Corte cost., sent. 22 giugno 1990, n. 307, punto 2 del *Considerato in diritto*, ove la Corte definisce la salute come un fondamentale diritto dell'individuo e interesse della collettività.

[8] Art. 35 Carta dei diritti fondamentali dell'Unione europea.

[9] Sulla nozione di cittadinanza sanitaria europea si veda N. Pasini, *Cittadinanza sanitaria, nuove finalità della medicina, società multietniche*, in *Salute e Società*, 3, 2, 2004, 49 ss. e G. Fares, *La tutela della salute del cittadino europeo: diritto o libertà?*, in *Dirittifondamentali.it*, 2, 2019.

[10] S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Le Nuove Leggi Civili Commentate*, 3, 2025, 563 ss.

[11] O. Pollicino, *Judicial protection of fundamental rights in the transition from the world of atoms to the word of bits: the case of freedom of speech*, in *European Law Journal*, 25, 2, 2019, 155 ss.

[12] Sul carattere trasformativo della digitalizzazione dei sistemi sanitari si veda D. Morana, *Diritto alla salute, ricerca tecnico-scientifica e innovazioni tecnologiche,* in G. Ferri (a cura di), *Diritto costituzionale e nuove tecnologie,* Napoli, 2022, 321 ss.

non più soltanto come informazione clinica individuale ma come risorsa strategica nelle varie dimensioni della pianificazione strategica sanitaria, impone una rilettura sia dei tradizionali confini tra tutela dei diritti fondamentali ed interesse pubblico alla salute che della sostenibilità dei sistemi sanitari[13]. Dalla capacità sistemica di bilanciamento di queste dimensioni del diritto alla salute dipende, infatti, la sostenibilità dei sistemi di *welfare*, che vivono oggi una profonda crisi identitaria alla luce delle continue sfide imposte dai mutevoli contesti socioeconomici, sotto la pressione anche dell'impatto della tecnologia in tutti i campi.

La riflessione sulla digitalizzazione della sanità si inserisce più ampiamente nel dibattito sulla trasformazione digitale come mutamento strutturale dei presupposti dell'azione pubblica. Il passaggio da sistemi analogici a sistemi informazionali non comporta una mera trasposizione tecnica di procedure esistenti, ma incide sulle categorie giuridiche tradizionali, sollecitando una riconsiderazione dei rapporti tra persona, tecnologia e potere pubblico. In questa prospettiva, la gestione dei dati sanitari assume un rilievo paradigmatico, in quanto coinvolge diritti fondamentali, assetti istituzionali e modelli di *welfare*, configurandosi come uno dei principali terreni di sperimentazione della «società *Onlife*», nella quale dimensione digitale e dimensione fisica risultano sempre più intrecciate[14].

In questo scenario, particolarmente delicato risulta il tema della *governance* dell'ecosistema digitale salute in cui la gestione, il trattamento e la condivisione dei dati sanitari, informazioni che afferiscono al nucleo più intimo della dignità umana e dei diritti fondamentali[15], come protetti dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea, diventano precondizione per l'esercizio stesso del diritto alla salute.

Alla luce di tali criticità, l'analisi che segue si interroga sulla tenuta del costituzionalismo digitale europeo e della cittadinanza sanitaria europea[16], inquadrando l'*EHDS* non solo come strumento tecnico, ma come leva giuridica per la riorganizzazione della *governance* multilivello e condizione abilitante per la tutela effettiva del diritto alla salute[17].

2. La costruzione giuridica dell'EHDS: la tensione tra funzionalizzazione del dato e tutela della salute. Dal punto di vista giuridico, lo Spazio europeo dei dati sanitari[18] si fonda su una combinazione articolata di basi normative che riflettono la natura trasversale del dato sanitario. Il Regolamento costituisce un tornante decisivo nella strategia normativa dell'Unione europea per il decennio digitale[19] e trova il proprio fondamento nell'art. 114 del Trattato sul funzionamento dell'Unione europea (d'ora in avanti TFUE), quale misura volta a garantire l'armonizzazione legislativa ai fini del corretto funzionamento del mercato interno, nell'art. 16 TFUE, che riconosce la protezione dei dati personali come diritto fondamentale e competenza

[13] Sulla natura dei dati sanitari quale infrastruttura critica si veda E. Sorrentino, A. F. Spagnuolo, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 29, 2024, 137 ss. Il dato sanitario, infatti, è anche risorsa strategica per la gestione delle emergenze e per l'adozione di decisioni pubbliche basate su dati verificabili e accurati.

[14] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Milano, 2017, cit.

[15] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014.

[16] Si veda G. De Gregorio, *Digital Constitutionalism in Europe*, Cambridge, 2022, Torino, 2016.

[17] Per un inquadramento sul ruolo della protezione dei dati personali nell'articolazione multilivello della legislazione nazionale ed europea, si veda F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016.

[18] Proposta di regolamento sullo Spazio europeo dei dati sanitari, COM (2022) 197 final, 3 maggio 2022.

[19] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030.

dell'Unione, e nell'art. 168 TFUE[20], che attribuisce all'Unione un ruolo di coordinamento e sostegno in materia di sanità pubblica[21].

Questa pluralità di basi giuridiche[22] consente al legislatore europeo di intervenire simultaneamente su circolazione transfrontaliera dei dati, tutela dei diritti fondamentali e organizzazione dei sistemi sanitari nazionali. Al tempo stesso, essa rende visibile una tensione strutturale che attraversa l'intero impianto dell'*EHDS*: quella tra la protezione della riservatezza e dell'autodeterminazione informativa, espressione di una posizione individuale che tende a collocare il diritto alla salute in una dimensione prevalentemente privatistica, e l'interesse pubblico alla corretta programmazione sanitaria, alla sostenibilità del *welfare* e all'equità di accesso alle cure, che richiama invece una concezione pubblicistica e collettiva della salute[23].

In altri termini, l'*EHDS* rende esplicito un problema di bilanciamento tra diritti fondamentali e interessi pubblici primari, che non può essere risolto né attraverso una prevalenza automatica della logica individuale del dato, né mediante una funzionalizzazione[24] illimitata della risorsa informativa. Il dato sanitario, pur rimanendo oggetto di una tutela rafforzata, viene progressivamente inserito in un circuito di utilizzi[25] che travalicano la relazione individuale di cura, assumendo una funzione infrastrutturale per finalità di ricerca, innovazione e programmazione delle politiche sanitarie.

Questa estensione funzionale del dato sanitario segna un punto di discontinuità rispetto all'impostazione tradizionale della protezione dei dati personali[26], sollevando interrogativi rilevanti[27] in termini di proporzionalità, finalità del trattamento e legittimazione dell'intervento pubblico.

---

[20] Tale scelta non è neutra: ancorando la sanità digitale alle logiche del mercato unico, la Commissione espande *de facto* le proprie competenze in un settore, quello della sanità pubblica, dove i Trattati le riserverebbero un ruolo di mero supporto. Si veda in proposito A. Alemanno, *Towards a European Health Union: Time to Level Up, in European Journal of Risk Regulation*, 11, n. 4, 2020, 721 ss.

[21] Questa tensione competenziale richiama la storica giurisprudenza della Corte di Giustizia sui limiti dell'armonizzazione tecnica quando impatta sulla salute pubblica Corte Giust., 5 ottobre 2000, C-376/98, *Germania c. Parlamento europeo e Consiglio*. Da un lato, l'*EHDS* impone *standard* uniformi per l'interoperabilità dei sistemi di cartella clinica elettronica (*EHR*); dall'altro, incide profondamente sull'organizzazione dei sistemi sanitari nazionali, introducendo una *governance* centralizzata nella definizione degli *standard* ma decentrata nell'attuazione. Sul punto R. Balduzzi, D. Servetti, *Regionalismo differenziato e materia sanitaria,* in *Rivista AIC,* 2, 2019. Ciò rischia di creare frizioni con gli assetti costituzionali interni, specialmente in ordinamenti a regionalismo differenziato come quello italiano, già provati dalla gestione emergenziale. Si veda M. Cavino, *Covid-19. Una prima lettura dei provvedimenti adottati dal Governo,* in *Federalismi.it*, in *Osservatorio Emergenza Covid-19,* 2020.

[22] Sulle implicazioni istituzionali delle basi giuridiche composite si veda R. Adam, A. Tizzano, *Manuale di Diritto dell'Unione europea*, Torino, 2024, 475ss.

[23] Sul significato sistemico della combinazione tra basi giuridiche e fra dimensione privatistica e dimensione pubblicistica del diritto alla salute nel trattamento dei dati sanitari, si veda S. Corso, *Il trattamento dei dati personali in ambito sanitario*, in *Rivista italiana di informatica e diritto*, 7, 2, 2025, 205 ss.

[24] Sul rischio di funzionalizzazione del dato sanitario si veda G. Resta, *Diritti fondamentali e diritto privato nel contesto digitale*, in F. Caggia, G. Resta (a cura di), *I diritti fondamentali in Europa e il diritto privato*, Roma, 2019, 117 ss. Si veda anche A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, 2017, 144 ss.

[25] Nel disciplinare il cd. uso secondario, il Regolamento legittima il riutilizzo di vaste moli di dati anche in assenza del consenso del paziente, basandosi su una presunzione di interesse pubblico prevalente esplicitata nei considerando del Regolamento, in particolare il Considerando 54.

[26] Si veda reg. (UE) 2016/679 (*GDPR*), artt. 5 e 9. Il *GDPR* è infatti costruito intorno alla centralità dell'autodeterminazione informativa.

[27] Sulle riserve delle autorità europee si consulti *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*.

Non a caso il regolamento introduce gli *Health Data Access Bodies*[28], autorità preposte al controllo dell'accesso ai dati per usi secondari, chiamate a valutare la legittimità delle richieste e a garantire il rispetto di misure quali pseudonimizzazione, auditabilità e trasparenza. La previsione di tali organismi riflette il tentativo di costruire una *governance* pubblica del dato sanitario che consenta di conciliare l'esigenza di valorizzazione informativa con la tutela dei diritti fondamentali, evitando che l'apertura all'uso secondario si traduca in una deregolazione sostanziale[29].

Un precedente metodologico utile per inquadrare la tensione tra esigenze privatistiche di tutela individuale e interesse pubblico di tutela collettiva è rappresentato dall'evoluzione del diritto amministrativo in materia di accesso e trasparenza. Anche in quel contesto, a partire dall'introduzione della l. 241/1990[30], le pubbliche amministrazioni si sono trovate a confrontarsi con il dilemma del bilanciamento tra il diritto alla riservatezza e l'interesse pubblico alla conoscibilità e al controllo democratico dell'azione amministrativa. Nel tempo, attraverso l'elaborazione giurisprudenziale e regolatoria, il bilanciamento è divenuto la tecnica ordinaria per evitare che la tutela della *privacy* si trasformasse in un limite assoluto e paralizzante, o che la trasparenza degenerasse in una diffusione sproporzionata di dati personali[31]

Pur non trattandosi di accesso in senso tradizionale, ma di uso secondario (accesso funzionale) e *governance* del dato, il parallelismo non è meccanico, ma pare calzante sul piano costituzionale; l'*EHDS*, infatti, in quanto primo quadro europeo organico di disciplina di un intero ecosistema, impone alle autorità competenti di metabolizzare logiche di bilanciamento strutturate, basate su principi giuridici e garanzie tecniche e procedurali tassative[32], che si configurano come condizioni necessarie ma non sufficienti per legittimare l'accesso stesso al dato. La letteratura ha mostrato come il bilanciamento tra diritti fondamentali non possa essere affidato a soluzioni rigide, ma richieda valutazioni ragionevoli e proporzionate[33], coerenti con l'impostazione della giurisprudenza costituzionale[34].

La dottrina costituzionalistica ha, inoltre, da tempo evidenziato come il diritto alla salute presenti una struttura intrinsecamente «bifronte», nella quale la dimensione individuale della pretesa si intreccia con una dimensione collettiva e organizzativa, affidata all'intervento pubblico[35]. In tale prospettiva, il dato sanitario non può essere considerato esclusivamente come proiezione dell'autonomia individuale, ma anche come elemento funzionale all'attuazione di politiche sanitarie efficaci, capaci di garantire uguaglianza sostanziale

---

[28] Sulla costruzione degli *Health Data Access Bodies*, si veda ancora la *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, 2022, cit.

[29] Sul ruolo di tali organismi nel bilanciamento tra innovazione e diritti si veda P. Quinn, E. Ellyne, C. Yao, *Will the GDPR restrain health data access bodies under the European Health Data Space (EHDS)?,* in *Computer Law & Security Review*, 54, 2024.

[30] L. 241/1990, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*.

[31] D.lgs. 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*, come modificato dal d.lgs. 97/2016. Si veda anche ANAC, Determinazione n. 1309 del 28 dicembre 2016. *Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, c. 2, d.lgs. 33/2013*, adottate d'intesa con il Garante.

[32] Tra i principi ricordiamo la proporzionalità, necessità e finalità determinate e tra le garanzie tecniche e procedurali tassative la pseudonimizzazione, tracciabilità, auditabilità e supervisione.

[33] C. Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *Federalismi.it*, 14, 2020. C. Della Giustina, *Alla ricerca di un ragionevole equilibrio tra principio di trasparenza e tutela della riservatezza*, in *Nomos*, 1, 2020.

[34] Si veda Corte cost., sent. n. 20/2019 sulla necessità di un bilanciamento proporzionato tra finalità di trasparenza e tutela dei dati personali, con valorizzazione appunto del principio di proporzionalità.

[35] In dottrina, sulla doppia dimensione dell'art. 32 Cost., riferimento essenziale è M. Luciani, *Il diritto costituzionale alla salute*, in *Diritto e Società*, 1980.

nell'accesso alle cure, riconducendo nuovamente alla duplice natura del diritto alla salute[36] nelle sue dimensioni di fondamentale diritto dell'individuo e di interesse della collettività, che discende dall'art. 32 della Cost. Il bilanciamento tra tutela della riservatezza e interesse pubblico alla salute si configura, pertanto, non come un'eccezione, ma come una tecnica ordinaria di governo dei diritti sociali in contesti complessi[37].

L'adozione di strumenti di proporzionalità e ragionevolezza consente di evitare sia una concezione assolutizzata della *privacy*, sia una funzionalizzazione indiscriminata del dato, preservando diritti fondamentali e, al contempo, l'effettività dell'azione pubblica ricomponendo le tensioni strutturali tra valori di pari rango[38].

La difficoltà delle autorità di controllo nel ricalibrare le proprie categorie interpretative appare in parte fisiologica nelle fasi iniziali di riforme strutturali; tuttavia, tale prudenza non può tradursi in una paralisi stabile dell'azione pubblica quando siano in gioco diritti sociali fondamentali e obiettivi di interesse generale. Anche le istituzioni europee hanno sottolineato la necessità di garantire che l'uso dei dati sanitari per finalità pubbliche avvenga nel rispetto dei diritti fondamentali, ma senza compromettere l'efficacia delle politiche sanitarie e la sostenibilità dei sistemi di *welfare*[39].

Non è di poco conto osservare che proprio la disciplina nazionale in materia di protezione dei dati personali, pur formalmente armonizzata al *GDPR* a seguito del d.lgs. 101/2018[40], continua a presentare margini di difformità interpretativa che incidono sulla concreta attuazione dell'*EHDS* e sulla possibilità di valorizzare il dato sanitario in funzione dei diritti sociali, come si vedrà nel prosieguo.

3. Le antinomie del sistema: la triangolazione normativa tra EHDS, GDPR e AI Act.

La standardizzazione del dato sanitario costituisce il presupposto tecnico e giuridico per la realizzazione dello Spazio europeo dei dati sanitari. L'*EHDS* mira a superare la storica frammentazione dei sistemi informativi sanitari[41] nazionali attraverso l'introduzione di formati comuni per il Fascicolo sanitario elettronico, requisiti minimi di qualità e sicurezza del dato e protocolli condivisi di interoperabilità.

La standardizzazione assume un rilievo che va oltre la dimensione tecnologica, configurandosi come infrastruttura costituzionale e strumento di integrazione europea sostanziale[42], in quanto condizione per garantire parità di trattamento tra cittadini e continuità delle cure oltre i confini nazionali[43]. La mancata interoperabilità dei sistemi sanitari nazionali costituisce l'ostacolo

---

[36] Sulla complessa dialettica tra dimensione individuale e collettiva del diritto alla salute, si veda A. Baldassarre, (voce) *Diritti sociali*, in *Enc. Giur.*, Roma, 1989, nonché, più recentemente, L. Chieffi, *La tutela del diritto alla salute tra prospettive di regionalismo differenziato e persistenti divari territoriali*, in *Nomos*, 1, 2020.

[37] S. Rodotà, *Il diritto di avere diritti*, Bari, 2013; G. Fares, *La tutela della salute del cittadino europeo: diritto o libertà?*, in *Dirittifondamentali.it*, 2, 2019, cit.

[38] M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione svolta alla Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta, 2013, cit.

[39] Ancora *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, cit., per la parte sui rilievi su proporzionalità, finalità e garanzie nel trattamento di dati sanitari su larga scala.

[40] D.lgs. 101/2018, *Disposizioni per l'adeguamento della normativa nazionale al Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (sull'armonizzazione del Codice privacy).

[41] Sulla frammentazione dei sistemi sanitari nazionali si veda Censis, italiadecide, *Il sistema della salute in Italia*, 2024.

[42] Sull'effetto armonizzatore indiretto del diritto dell'Unione si veda S. Cassese (a cura di), *La nuova costituzione economica*, Bari, 2021.

[43] Sulla tensione tra standardizzazione e autonomia nazionale si veda L. Torchia, *Lo stato digitale*, Bologna, 2023.

strutturale[44], alla realizzazione della mobilità sanitaria e della programmazione pubblica e, di riflesso, dello spazio europeo della salute.

La costruzione dello Spazio europeo dei dati sanitari si inserisce in un contesto normativo europeo già fortemente stratificato, nel quale coesistono regimi giuridici differenti, ispirati a logiche regolative non sempre convergenti[45]. In particolare, l'*EHDS* si colloca all'intersezione tra il *GDPR* e l'*AI Act*, dando luogo a una complessa triangolazione normativa[46] che incide in modo significativo sulla disciplina del dato sanitario.

Il *GDPR* ha storicamente rappresentato il fulcro della tutela dei dati personali nell'ordinamento europeo, qualificando i dati relativi alla salute come categorie particolari soggette a un regime di protezione rafforzata. L'*AI Act*, dal canto suo, introduce un approccio basato sulla gestione del rischio, classificando le applicazioni di intelligenza artificiale (d'ora in poi *AI*) in ambito sanitario tra i sistemi ad alto rischio[47] (art. 9) e subordinandone l'uso al rispetto di requisiti stringenti di trasparenza (art. 13), tracciabilità, qualità dei dati[48](art. 10), e supervisione umana significativa[49] (art. 14).

L'*EHDS* si innesta su questo quadro introducendo una disciplina funzionale alla circolazione e al riutilizzo dei dati sanitari, anche per finalità diverse dalla cura. Ne deriva un sistema nel quale, come evidenziato, coesistono senza una piena gerarchizzazione, logiche di protezione, di valorizzazione e di gestione del rischio, con il pericolo di antinomie latenti[50] non soltanto applicative, ma strutturali[51]. Il dato sanitario diviene così il punto di frizione tra esigenze di tutela individuale, obiettivi di innovazione tecnologica e interessi pubblici alla sostenibilità dei sistemi di *welfare*.

La dottrina ha messo in luce come la stratificazione delle fonti in materia di dati ed *AI* abbia prodotto un sistema normativo policentrico, nel quale la coesistenza di regimi differenti rischia di generare sovrapposizioni e incoerenze applicative. In particolare, è stato osservato che la disciplina europea della protezione dei dati, pur orientata alla tutela della persona, non può essere interpretata in modo avulso dalle esigenze di funzionamento dei sistemi pubblici complessi, pena la trasformazione delle garanzie in fattori di inerzia istituzionale[52].

3.1. Il cambio di paradigma: dalla data protection alla data valorisation nell'uso secondario. Uno degli elementi più innovativi, e al contempo più problematici, dell'*EHDS* riguarda la disciplina dell'uso secondario dei dati sanitari. Accanto al trattamento primario, funzionale alla cura del paziente, il Regolamento legittima l'accesso ai dati per finalità di ricerca

---

[44] Sulla dimensione infrastrutturale del dato sanitario si veda *WHO*, *Global Strategy on Digital Health 2020-2025*, Ginevra, 2021 e la sua recente estensione di due anni nella versione *Global Strategy on Digital Health 2020-2027*, Ginevra, 2025.

[45] Le diverse *rationes* delle norme, ovvero la tutela statica del dato, la sicurezza del prodotto e la libera circolazione, faticano a trovare una sintesi operativa. Si veda G. Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019.

[46] Sull'interazione tra *EHDS*, *GDPR* e altri regolamenti nel più ampio quadro di sanità digitale in cui si innesta l'*AI Act*, si veda C. Stancanelli, *Governance dei dati sanitari: il ruolo incrociato di EHDS e DGA*, in *Agenda Digitale*, 2025.

[47] Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 (*AI Act*). Capo III, artt. 6-14; sul punto v. anche Allegato III.

[48] Sui requisiti di qualità e rappresentatività dei *dataset* si consulti *European Commission*, *AI Act Explanatory Memorandum*, 2021 alla Proposta di Regolamento.

[49] Sul ruolo della supervisione umana significativa si veda S. Rodotà, *Tecnologie e diritti*, Bologna, 2021.

[50] F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

[51] Si veda ancora *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, cit.

[52] G. Finocchiaro, *Privacy e protezione dei dati personali*, Bologna, 2012; F. Pizzetti (a cura di), *La protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021.

scientifica, innovazione tecnologica, elaborazione delle politiche pubbliche e valutazione delle prestazioni dei sistemi sanitari, anche in assenza del consenso dell'interessato.
Questo passaggio segna un mutamento paradigmatico rispetto all'impostazione tradizionale del *GDPR*, fondata sulla centralità del consenso e sulla rigida delimitazione delle finalità del trattamento[53], che nel caso dell'utilizzo primario dei dati sanitari, ovvero per finalità di cura, aveva tutto sommato trovato un suo equilibrio. Il dato sanitario viene ora progressivamente sottratto a una dimensione esclusivamente individuale per essere inserito in un circuito di valorizzazione informativa a fini sistemici, a partire dalla esigenza di stratificazione della popolazione[54], divenuta sempre più pressante negli ultimi decenni di programmazione sanitaria a causa della crisi demografica del Paese[55] ed emersa con drammatica urgenza durante la pandemia da COVID-19[56]. In tale prospettiva, la protezione dei dati non scompare, ma viene ricalibrata attraverso specifici strumenti di mitigazione del rischio, quali la pseudonimizzazione[57], l'accesso controllato, la limitazione delle finalità e l'auditabilità dei trattamenti.
La tensione che ne deriva non è soltanto tecnica, ma costituzionale, poiché pone il problema della compatibilità[58] tra la crescente funzionalizzazione[59] del dato sanitario e il principio personalistico che informa la tutela dei diritti fondamentali nell'ordinamento europeo[60]. Il

[53] Si veda reg. (UE) 2016/679 (*GDPR*), cit., art. 5, par. 1, lett. b) e art. 9.
[54] Ministero della Salute, *Piano Nazionale della Cronicità*, 15 settembre 2016, Parte I, C), 1 che individua nella stratificazione del rischio lo strumento cardine per la presa in carico differenziata del paziente. Tale approccio è stato istituzionalizzato dal d.m. 77/2022 *Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*, che all'Allegato 1, cap. 3 pone la stratificazione della popolazione a fondamento del nuovo modello di sanità territoriale.
[55] ISTAT, *Rapporto annuale 2023. La situazione del Paese*, Roma, 2023, cap. 1, 37 ss. L'Istituto evidenzia come l'invecchiamento progressivo della popolazione, con oltre il 24% di residenti *over* 65, configuri una situazione demografica «sconosciuta», che pone seri dubbi sulla tenuta del sistema di protezione sociale. Tale scenario impone la necessità di ripensare la programmazione del Servizio sanitario nazionale il cui attuale assetto, in assenza di strumenti predittivi di allocazione delle risorse, rischia di diventare insostenibile. Si veda Corte Conti, *Rapporto 2023 sul coordinamento della finanza pubblica*, Roma, 2023, *Sintesi e conclusioni*, 33, par. 89, ove la magistratura contabile ammonisce che, in relazione all'invecchiamento della popolazione, «non si può assecondare, senza rischi per la tenuta del sistema, che un quarto degli investimenti annualmente necessari sia finanziato attingendo a risorse correnti».
[56] Si pensi al Piano strategico nazionale dei vaccini per la prevenzione delle infezioni da SARS-CoV-2 adottato dal Ministero della Salute con d.m. 2 gennaio 2021 e al successivo aggiornamento tramite d.m. 12 marzo 2021, recante le *Raccomandazioni ad interim sui gruppi target della vaccinazione anti-SARS-CoV-2/COVID-19*, che ha reso necessaria l'elaborazione massiva e l'incrocio proattivo di dati sanitari per individuare le categorie di «elevata fragilità» a cui garantire priorità di accesso, operazione resa complessa proprio dalla frammentazione dei *database* regionali.
[57] Per un approccio alla pseudonimizzazione come misura di sicurezza, si veda in senso più ampio A. Mantelero, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law & Security Review*, 32, 2, 2016, 238 ss., che tratta della ricalibratura della protezione dei dati attraverso strumenti di mitigazione del rischio.
[58] Sulla tensione tra valore economico-sociale del dato e tutela della personalità, si veda A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, 2017, 144 ss., cit. che evidenzia i limiti del consenso di fronte alla potenza predittiva dei *Big Data*.
[59] Sul rischio di patrimonializzazione del dato si veda anche, in termini più generali, V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss.
[60] Sul principio personalistico nella dimensione digitale e sulla costruzione del diritto alla protezione dei dati come diritto fondamentale autonomo di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione europea, imprescindibile è il riferimento a S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli,* Bari, 2014, cit., che definisce la protezione dei dati come componente essenziale della dignità umana, teorizzando la declinazione del concetto di *habeas data* come proiezione inviolabile della persona nello spazio digitale. Sul punto anche P.

rischio è che la logica della *data valorisation* finisca per prevalere sulla logica della *data protection*, trasformando il dato sanitario in una risorsa collettiva sganciata da un adeguato presidio di garanzie sostanziali.
La crisi del consenso come base esclusiva del trattamento dei dati sanitari è stata ampiamente evidenziata soprattutto con riferimento agli usi secondari del dato per finalità di ricerca e programmazione. In tali ambiti, il consenso individuale risulta spesso inadeguato a fondare trattamenti su larga scala, rendendo necessario il ricorso a basi giuridiche di natura pubblicistica, accompagnate da garanzie procedurali e istituzionali idonee a tutelare i diritti degli interessati[61].

3.2. L'Intelligenza Artificiale in sanità: il paradosso applicativo tra qualificazione «ad alto rischio» e necessità di data quality. Come anticipato, l'impiego dell'intelligenza artificiale in ambito sanitario accentua ulteriormente le antinomie[62] del sistema poiché l'*AI Act*, qualificando le applicazioni di *AI* utilizzate per finalità diagnostiche, terapeutiche e decisionali come sistemi ad alto rischio, presuppone la disponibilità di *dataset* sanitari ampi, rappresentativi, aggiornati e interoperabili[63], senza i quali le applicazioni di *AI* non possono garantire affidabilità, accuratezza e assenza di *bias*[64]. In questo senso, l'*EHDS* si configura come prerequisito indispensabile per l'attuazione stessa dell'*AI Act* in ambito sanitario.
Si determina così un paradosso regolativo: da un lato, l'ordinamento europeo impone vincoli stringenti all'uso dell'*AI* per tutelare i diritti fondamentali[65]; dall'altro, rende necessario un ampliamento dell'accesso ai dati sanitari per garantire la qualità dei sistemi algoritmici. Questo equilibrio instabile espone il sistema al rischio di una tutela meramente formale dei diritti, qualora la qualità dei dati non sia effettivamente garantita o la supervisione umana risulti solo nominale[66].
La letteratura ha sottolineato come l'impiego dell'intelligenza artificiale in sanità sollevi questioni che travalicano la dimensione tecnologica, investendo temi quali la responsabilità, la

Stanzione (a cura di), *La privacy dell'era digitale. Le Relazioni dei Presidenti dell'Autorità Garante 1997-2022*, Torino, 2022.

[61] Sul crescente *gap* informativo e il suo impatto sul consenso si veda A. Lo Calzo, *Il consenso informato «alla luce della nuova normativa» tra diritto e dovere alla salute*, in *Diritto e salute*, 3, 2018.

[62] L'antinomia riguarda anche il principio di limitazione della finalità: l'*EHDS* estende l'elenco degli «usi compatibili», delegando agli *Health Data Access Bodies* una discrezionalità amministrativa che potrebbe variare significativamente da Stato a Stato, si veda L. Bolognini (a cura di), *Privacy e libero mercato digitale Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Milano, 2021, mettendo a rischio l'uniformità di tutela nello spazio giuridico europeo. Tale criticità si innesta sulla più ampia riflessione circa le deroghe al principio di finalità nel diritto UE, per la quale si veda anche M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 179 ss.

[63] Si genera qui una dipendenza circolare, che potremmo definire un «paradosso della qualità»: l'*AI Act* (art. 10) impone che i *dataset* di addestramento siano privi di errori e completi, obbligando di fatto ad attingere ai dati reali dell'EHDS. Si veda G. De Gregorio, F. Paolucci, *Dati e Intelligenza artificiale all'intersezione tra mercato e democrazia*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino 2022, 109 ss. Tuttavia, l'uso massivo di dati sanitari per l'addestramento algoritmico aumenta esponenzialmente il rischio di re-identificazione, entrando in rotta di collisione con i principi di minimizzazione. La soluzione tecnica degli «ambienti di trattamento sicuri» rischia di spostare la fiducia dalla norma all'infrastruttura, ponendo nuovi interrogativi in tema di responsabilità civile ed algoritmica. Si veda U. Ruffolo, (a cura di), *Intelligenza Artificiale e responsabilità*, Milano, 2017.

[64] Sulla non neutralità degli algoritmi V. Molaschi, *Algoritmi e discriminazione*, in *Fundamental Rights*, 2, 2022, 19 ss.

[65] *European Commission*, *Study on eHealth, interoperability of health data and artificial intelligence for health and care in the European Union. Lot 2: Artificial Intelligence for health and care in the EU. Final Study Report*, 2022.

[66] Sul concetto di responsabilità condivisa si veda A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D. U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020.

fiducia e la legittimazione delle decisioni pubbliche, in una dimensione sistemica di *governance* pubblica che implica anche una dimensione di rischio che va individuato e quanto più possibile mitigato[67]. In particolare, l'affidamento a sistemi algoritmici in ambito sanitario richiede un presidio giuridico rafforzato, capace di garantire trasparenza, spiegabilità e controllo umano effettivo, pena il rischio di opacizzazione dei processi decisionali e di erosione della fiducia dei cittadini nel sistema sanitario[68].

3.3. «Compliance sistemica»: coerenza normativa tra uso del dato e legittimità costituzionale. Alla luce delle antinomie evidenziate, emerge l'esigenza di una nozione di «*compliance* sistemica»[69] intesa non come mera conformità formale a singole disposizioni normative della singola entità preposta al governo di parte del sistema, ma come coerenza complessiva tra i diversi regimi giuridici che disciplinano il dato sanitario e attori istituzionali che intervengono a vario titolo nell'intero processo di raccolta, utilizzo e conservazione del dato. Tale gestione deve inoltre essere improntata al principio del buon andamento e imparzialità dell'azione amministrativa di cui all'art. 97 Cost, superando la logica della mera efficienza. Si consideri anche che, affinché la *compliance* sistemica sia davvero efficace, non è sufficiente un adempimento dei soli obblighi discendenti dalla normativa europea, ma occorre tenere in considerazione anche le specificità dei sistemi sanitari regionali e della normazione a livello regionale, nonché dei variegati modelli organizzativi che caratterizzano gli enti che erogano prestazioni sanitarie. Come è noto, l'inversione del riparto di competenze nell'attuazione del diritto alla salute che informa il novellato art. 117 della Cost. ha potenziato la autonomia delle Regioni contribuendo alla diversificazione del *range* delle prestazioni offerte, alla varietà dei modelli organizzativi ed anche alla libertà di selezione dei fornitori di servizi. In sintesi, prima di passare alle implicazioni del regionalismo con specifico riferimento ai dati sanitari del prossimo paragrafo, la legittimità costituzionale dell'*EHDS* e delle applicazioni di *AI* in sanità dipende dalla capacità del sistema di assicurare un allineamento sostanziale tra uso del dato, tutela dei diritti fondamentali e responsabilità istituzionale. In tale prospettiva, il coordinamento tra *EHDS*, *GDPR* e *AI Act* non può essere affidato esclusivamente a strumenti tecnici o procedurali, ma richiede un approccio interpretativo orientato ai valori costituzionali comuni agli Stati membri[70].
La previsione di meccanismi di *governance* multilivello, di autorità di accesso ai dati, di controlli *ex ante* ed *ex post* sui trattamenti e di obblighi di *accountability*[71] rappresenta un primo tentativo di costruire tale coerenza. Resta tuttavia aperta la questione se tali strumenti siano sufficienti a

[67] Sul rischio sistemico dei sistemi sanitari algoritmici si veda E. Vayena, A. Blasimme, *Health Research with Big Data: Time for Systemic Oversight*, in *Journal of Law, Medicine and Ethics*, 46, 1, 2018, 119 ss.
[68] *WHO Europe*, *Artificial intelligence is reshaping health systems: state of readiness across the European Union*, 2026.
[69] L'analisi delle aporie del sistema conduce a ritenere insufficiente l'attuale approccio alla *compliance*, che appare frammentato, a «silos», e più formale che sostanziale. Si veda P. Guarda, *I dati sanitari*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 591 ss.
[70] Sul principio di leale cooperazione, art. 4, par. 3, Trattato sull'Unione Europea (d'ora in avanti TUE).
[71] Sulla gestione del rischio, A. Mantelero, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Nuove leggi civili commentate*, 2017, 144 ss, cit.

prevenire derive funzionalistiche[72] del dato sanitario e a garantire un'effettiva tutela del diritto alla salute in un contesto di crescente automazione decisionale[73].

4. L'attuazione differenziata del Regolamento: asimmetrie istituzionali e governance multilivello. L'attuazione dello Spazio europeo dei dati sanitari richiede un articolato assetto di *governance* multilivello, nel quale interagiscono istituzioni europee, Stati membri, autorità indipendenti e livelli sub-statali. La Commissione europea definisce il quadro giuridico e tecnico di riferimento, anche attraverso atti delegati e di esecuzione; agli Stati membri spetta l'implementazione del Regolamento nei rispettivi ordinamenti; alle autorità nazionali competenti è affidato il compito di garantire il coordinamento tra *standard* europei e sistemi sanitari nazionali; mentre gli enti territoriali e le strutture sanitarie sono chiamati ad assicurare l'operatività concreta delle nuove infrastrutture digitali.

Questa architettura riflette una logica di integrazione funzionale che non incide formalmente sulle competenze sanitarie nazionali, ma ne condiziona in modo significativo l'esercizio. L'*EHDS* introduce infatti obblighi, *standard* e meccanismi di accesso ai dati che, pur presentandosi come strumenti di coordinamento, producono effetti sostanziali sugli assetti amministrativi[74] e sui modelli di *governance* sanitaria interna.

Ne deriva un'attuazione potenzialmente differenziata del Regolamento, nella quale la capacità[75] degli ordinamenti nazionali di recepire ed esercitare efficacemente le nuove funzioni[76] dipende da fattori istituzionali, infrastrutturali e organizzativi. In questo quadro, il rischio non è soltanto quello di una disomogeneità applicativa, ma di una frammentazione dell'effettività dei diritti connessi alla cittadinanza sanitaria europea, con conseguente ampliamento dei divari territoriali o un inasprimento delle disuguaglianze tra *targets*.

La *governance* multilivello dei dati sanitari richiama, più in generale, le riflessioni dottrinali sulla trasformazione dell'amministrazione europea[77], nella quale strumenti di coordinamento e standardizzazione producono effetti sostanziali sugli assetti interni degli Stati membri. In tale contesto, la gestione dei dati si configura come una nuova forma di esercizio del potere

---

[72] In merito all'insufficienza dei soli strumenti di *compliance* formale per arginare le «derive funzionalistiche» e predatorie sui dati, si veda A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 34, 4, 2018, 754 ss., il quale propone di integrare la *data protection* con valutazioni di impatto etico-sociale più ampie.

[73] Per alcuni esempi sulle sfide poste dall'automazione decisionale alla tutela dei diritti fondamentali e sul rischio che la tecnica algoritmica comprima la dimensione umana, si rinvia a A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, 63 ss.

[74] Sui profili costituzionali e di competenza sollevati dall'EHDS, si veda A. *Fiorentini, Stretching Constitutional Boundaries: The European Health Data Space Regulation and Its Impact on the Public Health Integration Process*, in *European Constitutional Law Review*, 2026.

[75] Si veda D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT),* in R. Cavallo Perin, D.U. Galetta (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale,* Torino, 2020, 85 ss. Le pubbliche amministrazioni, chiamate a operare come nodi periferici di una rete europea, scontano spesso ritardi strutturali nei processi di digitalizzazione. Si veda M. Clarich, *Manuale di diritto amministrativo*, Bologna, 2022.

[76] Capacità, oltre che essenziale per l'effettività dell'esercizio del diritto alla salute, anche discendente dal principio di leale cooperazione di cui all'art. 4, par. 3, TUE.

[77] Il riferimento sulla strutturazione amministrativa dell'Unione tramite organismi tecnici è E. Chiti, *Le agenzie europee. Unità e decentramento nelle amministrazioni comunitarie*, Padova, 2002. L'Autore vi teorizza il modello dell'amministrazione «composta», in cui agenzie e *network* fungono da cerniera tra livello sovranazionale e nazionale: un modello che l'*EHDS* oggi replica ed espande, attribuendo ai nuovi *Health Data Access Bodies* funzioni ibride di regolazione tecnica e tutela dei diritti.

pubblico[78], che richiede meccanismi di responsabilità, trasparenza[79] e leale collaborazione[80] tra livelli di governo.

4.1. Il «caso Italia»: il conflitto tra programmazione pubblica e privacy nel regionalismo sanitario. Il contesto italiano offre un esempio particolarmente significativo delle tensioni che possono emergere nell'attuazione dello Spazio europeo dei dati sanitari. Come è noto, il Servizio sanitario nazionale è caratterizzato da un elevato grado di regionalizzazione, rafforzato dalla riforma del Titolo V della Costituzione[81], che attribuisce alle Regioni competenze rilevanti in materia di organizzazione e programmazione sanitaria[82]. Tale assetto ha prodotto, nel tempo, una marcata eterogeneità anche dei sistemi informativi sanitari regionali[83], con differenze significative anche in termini di infrastrutture digitali, *standard* tecnici e livelli di interoperabilità. L'attuazione dell'*EHDS* in Italia deve pertanto misurarsi con le croniche asimmetrie del regionalismo sanitario[84], laddove la frammentazione dei sistemi informativi regionali riflette una più profonda disparità nell'esercizio del diritto alla salute, spesso condizionato dai vincoli di bilancio e dalle diverse capacità programmatorie dei singoli enti territoriali[85].

Nel quadro della digitalizzazione sanitaria, il Fascicolo sanitario elettronico (FSE) ha rappresentato uno degli strumenti principali per la raccolta e la circolazione dei dati clinici. Tuttavia, la sua implementazione ha evidenziato le criticità strutturali richiamate, legate alla frammentazione regionale e alla difficoltà di garantire una piena interoperabilità a livello

[78] Sulla gestione dei dati come nuova morfologia del potere amministrativo e sulla conseguente necessità di garanzie di *accountability* si veda A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 2018, cit.

[79] Sulla trasparenza come garanzia costituzionale si veda U. Galetta, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Rivista italiana di diritto pubblico comunitario*, 5, 2016, 1019 ss.

[80] Sul principio di leale collaborazione di cui all'art. 4, par. 3, TUE quale cardine dell'amministrazione europea integrata o «composta» si veda E. Chiti, C. Franchini, *L'integrazione amministrativa europea,* Bologna, 2003.

[81] Sull'assetto del riparto di competenze di cui all'art. 117, c. 3, Cost., che assegna alla potestà legislativa concorrente la «tutela della salute», si veda, tra i molti, M. Luciani, *Il diritto costituzionale alla salute*, in *Diritto e Società,* 1980, 769 ss., cit. Tale assetto ha cristallizzato un modello di regionalismo sanitario caratterizzato da una spiccata differenziazione che ha condotto, nei fatti, alla coesistenza di ventuno sistemi sanitari regionali tra loro non sempre comunicanti. Questa frammentazione si riflette in una profonda asimmetria territoriale, efficacemente descritta in dottrina come distribuzione «a macchia di leopardo» delle infrastrutture digitali e dei livelli di interoperabilità, che condiziona l'effettività del diritto alla salute in base alla localizzazione geografica dell'assistito. Il diritto alla salute, infatti, pur nella sua natura di diritto fondamentale, sconta il carattere di diritto «finanziariamente condizionato» (sul punto, si veda la fondamentale sentenza della Corte Cost. n. 455 del 1990; e più recentemente la pronuncia n. 62 del 2020 della stessa Corte), la cui attuazione è legata alla pianificazione delle risorse e alla ripartizione del Fondo Sanitario Nazionale. La circostanza per cui le Regioni possano garantire, con risorse proprie, prestazioni ulteriori rispetto ai Livelli Essenziali di Assistenza (LEA), finisce per esacerbare i divari territoriali, cristallizzando una «cittadinanza sanitaria a geometria variabile» in cui coesistono pazienti di «serie A» e di «serie B». Tale scenario appare in aperto contrasto con la logica di standardizzazione, coesione e circolarità informativa sottesa allo Spazio europeo dei dati sanitari, il quale richiede, al contrario, un'omogeneizzazione dei percorsi di cura che mal si concilia con le derive centrifughe del regionalismo eccessivamente differenziato.

[82] La Corte costituzionale ha più volte ribadito la necessità di bilanciare le competenze statali di coordinamento con l'autonomia gestionale delle Regioni; si veda Corte Cost., sent. 12 marzo 2021, n. 37.

[83] Sulla disomogeneità dei sistemi informativi regionali si è espressa la Corte Conti, Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato, Delib. n. 24/2025/G.

[84] Sulle criticità del regionalismo sanitario italiano si veda R. Balduzzi, *Cittadinanza, corti e salute*, Padova, 2007.

[85] La frammentazione dei sistemi informativi regionali rischia di minare l'uguaglianza nell'accesso alle cure; per una analisi delle sfide legate al FSE per il regionalismo italiano si veda A. Molfetta, *Dalle Disposizioni Anticipate di Trattamento al Fascicolo Sanitario Elettronico 2.0: nuove sfide e perduranti problemi per il regionalismo italiano*, in *Corti Supreme e Salute*, 2025, 3.

nazionale. L'accelerazione impressa dal PNRR ha ulteriormente intensificato tali tensioni, imponendo tempi rapidi di attuazione e obiettivi ambiziosi di digitalizzazione, non sempre accompagnati da un adeguato consolidamento delle garanzie giuridiche ed organizzative[86].
In questo scenario, il contesto italiano assume i tratti di un emblematico «laboratorio regolativo-attuativo» nel panorama continentale. L'ordinamento nazionale si trova, infatti, a gestire una frizione sistemica tra due spinte di segno opposto: da un lato, l'attuazione dello Spazio europeo dei dati sanitari, che impone un'armonizzazione centralizzatrice basata su *standard* tecnici rigorosi e su una logica di integrazione funzionale sovranazionale; dall'altro, l'attuale dibattito istituzionale sulle riforme del regionalismo differenziato di cui art. 116, c. 3, Cost., orientato a una maggiore autonomia organizzativa e programmatoria degli enti territoriali.

Si determina così un paradosso politico-giuridico di estremo interesse per il diritto costituzionale europeo e nazionale: proprio mentre il legislatore europeo richiede una «ricentralizzazione tecnica» del dato sanitario per garantirne la circolarità e l'interoperabilità, il sistema interno è lambito da dinamiche centrifughe che rischiano di cristallizzare ulteriormente le asimmetrie regionali. La sfida dell'*EHDS* in Italia non è dunque solo tecnologica, ma investe la capacità del modello di *governance* multilivello di ricomporre questa tensione, evitando che l'autonomia rivendicata dalle Regioni si traduca in un ostacolo strutturale alla costruzione di una cittadinanza sanitaria europea uniforme[87] e ad una effettiva omogeneità nell'erogazione dei servizi di salute, espressione di una maggiore coesione tra i territori. Il rischio, in assenza di un coordinamento forte e di un effettivo ricorso al principio di leale collaborazione, è che la digitalizzazione, da fattore di coesione, finisca per diventare l'ennesimo terreno di scontro tra Stato e Regioni, a discapito dell'effettività dei diritti fondamentali.
In questo contesto di spinte contrapposte, il ruolo del Garante per la protezione dei dati personali (d'ora in avanti, Garante) è stato centrale[88]. L'Autorità ha più volte richiamato l'attenzione sui limiti dei trattamenti centralizzati dei dati sanitari e sulla necessità di rispettare i principi di minimizzazione, proporzionalità e finalità del trattamento, garantendo una base giuridica chiara e puntuale per l'uso dei dati a fini diversi dalla cura[89]. L'intervento del Garante non si configura come una resistenza all'innovazione digitale, bensì come un tentativo di ricondurre la trasformazione tecnologica entro un quadro di legittimità costituzionale. L'attuazione dell'*EHDS* impone un superamento della visione tradizionale dell'autorità di controllo come «contropotere» isolato. Il Garante si trova oggi ad agire all'interno di un assetto

---

[86] Corte Conti, Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato, Delib. n. 24/2025/G., cit., ove si evidenziano le criticità nel rispetto delle milestone e dei target previsti per l'investimento M6C2I1.3.1.

[87] Sulla nozione di cittadinanza sanitaria europea si veda L. Busatta, *La cittadinanza della salute nell'Unione Europea: il fenomeno della mobilità transfrontaliera dei pazienti, dalla libera circolazione alla dimensione relazionale dei diritti*, in *DPCE Online*, 23, 3, 2015, 1 ss.

[88] Sul tema della cooperazione tra autorità indipendenti e organismi tecnici, che può leggersi come un pilastro di un'amministrazione policentrica, il riferimento si veda T. Spasari, P. Bailo, G. Pesel, G. D'Alessandro, G. Ricci, *Beyond Consent-Centred Protection in Digital Healthcare: Italy, Secondary Use of Health Data, and Governance-Based Safeguards for AI-Mediated Care*, in *Laws*, 2026, 15, 4, 76. In tale prospettiva, il ruolo del Garante per la protezione dei dati personali deve evolversi, nella lettura che qui si propone, da autorità di controllo «esclusiva» ad attore di un sistema di garanzia composito. Tale assetto richiede un'integrazione procedimentale tra funzioni di vigilanza e competenze tecniche, in cui il Garante è chiamato a dialogare costantemente con i nuovi *Health Data Access Bodies* e con le autorità sanitarie nazionali in una logica di co-regolazione del rischio informativo.

[89] Garante per la protezione dei dati personali, Provv. n. 243 del 7 luglio 2022, dove l'Autorità ha evidenziato come la pseudonimizzazione, nella specie il troncamento dell'indirizzo IP, non sia sufficiente a sottrarre il trattamento al perimetro del GDPR quando il rischio di ri-identificazione rimane elevato. Si veda anche Provv. 2 febbraio 2023, dove il Garante è intervenuto in via d'urgenza ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, per limitare il trattamento di dati privo di base giuridica idonea, in violazione degli artt. 5, 6, 8, 9 e 25 del Regolamento (caso Replika).

di attori composito, in cui la funzione di tutela del dato deve integrarsi con le competenze programmatorie e tecniche degli organismi sanitari e dei nuovi soggetti regolatori europei. Si delinea, dunque, un modello di *governance* policentrica[90], dove la legittimità dei trattamenti su larga scala non dipende da un singolo atto di assenso, ma dalla capacità di questi diversi attori di cooperare lealmente, trasformando il bilanciamento tra *privacy* e salute in un processo istituzionale condiviso e dinamico.

Tuttavia, gli interventi inibitori e sanzionatori adottati recentemente[91] nei confronti di alcune Regioni, anche in relazione al conferimento al Ministero della Salute[92] di dati pseudonimizzati nell'ambito di progetti pubblici finanziati con fondi europei[93], hanno prodotto un effetto potenzialmente paralizzante sulla capacità programmatoria del sistema[94], rendendo evidente una frizione profonda tra obiettivi di *governance* sanitaria e prassi di tutela della *privacy* di segno fortemente difensivo. L'intervento dell'Autorità Garante, pur muovendo da un necessario e rigoroso ancoraggio ai principi di minimizzazione e finalità, finisce per generare un effetto indiretto di inerzia programmatoria. Non si tratta di una aprioristica resistenza al cambiamento, ma dell'esito di un quadro normativo che ancora fatica a comporre la dimensione individuale della protezione dei dati con quella collettiva della sostenibilità sanitaria.

È proprio in questo snodo, infatti, che riemergono nella loro concreta dimensione le antinomie analizzate nel paragrafo precedente. La spinta verso una maggiore funzionalizzazione del dato sanitario, necessaria per finalità di programmazione, ricerca e innovazione, entra in tensione con un assetto istituzionale che assegna alle Regioni un ruolo centrale nella gestione della sanità e che affida alle autorità indipendenti il compito di presidiare i diritti fondamentali. Il rischio è che, in assenza di un coordinamento efficace, la *governance* del dato sanitario si trasformi in un terreno di conflitto tra livelli di governo e attori del sistema, con ricadute negative sull'effettività del diritto alla salute[95], e sulla fiducia dei cittadini nel sistema stesso[96].

---

[90] Sulle forme di *governance* policentrica nel diritto dell'UE si veda G. della Cananea, *L'Unione europea. Un ordinamento composito*, Bari, 2003.

[91] Sulla frizione tra tutela dei dati e programmazione sanitaria si vedano nel contesto del PNRR i pareri non positivi resi dal Garante per la protezione dei dati personali sugli schemi di decreto relativi al Fascicolo Sanitario Elettronico e all'Ecosistema Dati Sanitari: parere n. 294 del 22 agosto 2022; parere del 22 agosto 2022 sull'EDS; parere del 26 gennaio 2023, superati solo con il parere favorevole n. 256 dell'8 giugno 2023.

[92] Sul limite costituzionale del conferimento di dati sanitari allo Stato si veda Corte cost., sent. n. 169/2017. In tale occasione, la Consulta, in ordine alla complessa dialettica tra esigenze di monitoraggio centrale e tutela della riservatezza, ha precisato che il conferimento di flussi informativi sanitari dalle Regioni allo Stato non può tradursi in un'acquisizione automatica o indiscriminata di dati sensibili. Pur riconoscendo la legittimità della raccolta dati per finalità di coordinamento della finanza pubblica e monitoraggio dei livelli essenziali di assistenza (LEA) di cui all'art. 117, c. 2, lett. *m)*, Cost., la Corte ha ribadito che l'esercizio di tali prerogative deve conformarsi al principio di leale collaborazione e al canone di proporzionalità. La sentenza sottolinea come l'acquisizione di dati individualizzati debba essere strettamente correlata a finalità pubbliche specifiche e assistita da garanzie tecniche idonee a prevenire un'esorbitante intrusione nel nucleo della dignità umana. Tale pronuncia costituisce il riferimento giurisprudenziale cardine per l'approccio «difensivo» delle autorità nazionali, segnalando il rischio che una funzionalizzazione illimitata della risorsa informativa possa compromettere l'autodeterminazione del singolo.

[93] Sul ruolo del Garante e le sue recenti sanzioni in ambito sanitario si consulti Garante per la protezione dei dati personali, Provv. n. 65 del 24 febbraio 2022.

[94] Il provvedimento, sanzionando il conferimento del dato nell'ambito dello sviluppo di un prototipo di un sistema predittivo di stratificazione, ha precluso la possibilità di sfruttare le potenzialità dei sistemi di *AI* per stratificare adeguatamente la popolazione e, conseguentemente, per allocare più efficientemente il Fondo Sanitario Nazionale.

[95] M. Luciani, *Diritti sociali e livelli essenziali delle prestazioni pubbliche nei sessant'anni della Corte costituzionale*, in *Rivista AIC*, 3, 2016. Si veda anche Corte cost., sent. n. 275/2016.

[96] L. Sciolla, *Fiducia e relazioni politiche*, in *Parolechiave*, 42, 2009.

La paralisi che talora ne deriva non è imputabile a un eccesso di potere, bensì a una asimmetria interpretativa tra i livelli di governo e le autorità di controllo. In assenza di una cornice normativa che riconosca al dato sanitario la natura di «infrastruttura di servizio», il Garante è costretto a una postura difensiva che, per eccesso di garanzia sul singolo, rischia di compromettere l'efficacia delle cure per la collettività.

La stasi istituzionale nell'utilizzo dei dati sanitari pseudonimizzati incide in modo particolarmente grave sulla possibilità di effettuare una corretta stratificazione della popolazione, elemento imprescindibile per una programmazione sanitaria fondata sui bisogni concreti dei destinatari delle prestazioni, sia in termini demografici sia in termini socio-sanitari. La disponibilità di dati aggregati e stratificati consente infatti di individuare profili di fragilità, cronicità e diseguaglianze territoriali, orientando l'offerta assistenziale in modo mirato.

Tale stratificazione non risponde a una logica meramente statistica, ma costituisce il presupposto operativo per l'attuazione del principio di sussidiarietà verticale[97], nella misura in cui permette ai livelli di governo più prossimi ai cittadini di programmare l'erogazione dei servizi sanitari in modo proporzionato e coerente con i bisogni effettivi delle comunità locali. L'impossibilità di conferire e processare dati sanitari, anche in forma pseudonimizzata e per finalità pubbliche di programmazione, compromette dunque la funzione allocativa del sistema sanitario, impedendo una distribuzione razionale delle risorse e una modulazione dell'offerta assistenziale in termini sia quantitativi sia qualitativi. Ne deriva una programmazione indifferenziata, incapace di cogliere le specificità territoriali e sociali, che si traduce in inefficienze strutturali e in un utilizzo subottimale del Fondo Sanitario Nazionale.

Le ricadute di questo «corto circuito»[98] non sono neutre sul piano dei diritti. Una programmazione inefficiente contribuisce al persistere di liste di attesa elevate, che costringono i cittadini a ricorrere a forme di mobilità sanitaria verso Regioni con bilanci più sani e modelli organizzativi più efficienti, in grado di offrire una gamma più ampia di prestazioni. Tali mobilità, oltre a incidere sull'equità nell'accesso alle cure, rappresentano una complessità organizzativa che ha un costo per il sistema nel suo complesso, sottraendo risorse che potrebbero essere reinvestite in una redistribuzione più efficiente delle economie nel riparto

[97] Sul principio di sussidiarietà in materia sanitaria, inteso come criterio dinamico di riparto delle funzioni tra i diversi livelli di governo, oltre alla più volte citata fondamentale ricostruzione di M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione svolta alla Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta, 2013, cit., si veda per un inquadramento sistematico nel Titolo V, B. Caravita, *Lineamenti di diritto costituzionale federale e regionale*, Torino, 2009. In ambito sanitario, la sussidiarietà verticale di cui all'art. 118 Cost. deve essere letta in combinato disposto con i principi di adeguatezza e differenziazione: il conferimento delle funzioni ai livelli di governo più prossimi al cittadino, ovvero Regioni e Aziende sanitarie, è costituzionalmente legittimo solo se tali enti sono posti in condizione di esercitare la propria missione programmatoria in modo efficace. In tale prospettiva, l'interoperabilità dei dati sanitari si configura come un «presupposto di adeguatezza»: senza una base informativa strutturata e predittiva, il livello locale rimane «cieco», rendendo la sussidiarietà un mero simulacro burocratico anziché uno strumento di tutela della salute. Al contempo, la sussidiarietà opera anche in senso europeo, si veda art. 5, par. 3, TUE, legittimando l'intervento dell'Unione, anche attraverso l'*EHDS,* laddove la frammentazione informativa degli Stati membri pregiudichi l'uniformità dei diritti e la sicurezza delle cure transfrontaliere. La stratificazione dei dati, dunque, lungi dall'essere una pratica puramente gestionale, diviene il vettore di quella che si può qui definire come «sussidiarietà cognitiva», non nel senso, generico, della prossimità conoscitiva del livello di governo più vicino al cittadino, ma come specifico presupposto informativo-strutturale indispensabile per coniugare l'autonomia territoriale con il dovere di un esercizio effettivo della funzione programmatoria regionale in sanità e di garantire l'eguaglianza sostanziale dei cittadini nell'accesso alle prestazioni di cui all'art. 3, c. 2, Cost.

[98] Il «corto circuito» istituzionale è stato già rilevato dagli organismi di rilievo costituzionale. Si veda CNEL, *Relazione del CNEL sui livelli e la qualità dei servizi erogati dalle pubbliche amministrazioni centrali e locali a imprese e cittadini*, 2024.

del Fondo Sanitario stesso e in un conseguente miglioramento dell'offerta sanitaria regionale nella sua dimensione aggregata.

Il mancato utilizzo dei dati per una programmazione efficace a causa di un approccio ipergarantista alla *privacy* rischia quindi, paradossalmente, di comportare una violazione indiretta di diritti sociali fondamentali, non perché formalmente compressi, ma perché resi di fatto non azionabili[99], in particolare l'equo accesso alle cure e la continuità assistenziale, mettendo così in pericolo non solo l'effettività del diritto alla salute ma, astrattamente, lo stesso diritto alla vita.

La tensione tra il dettato della norma europea e l'incapacità di attuazione del nostro Paese denota un contrasto latente tra livelli di normazione, alimentato anche dalla persistenza di letture interpretative ancorate a una logica pre-funzionale della *privacy*, nonostante l'armonizzazione formale del Codice *privacy* al *GDPR* operata dal d.lgs. 101/2018.

Il caso italiano evidenzia così come la difficoltà di articolare il diritto alla salute attraverso il digitale non derivi da un *deficit* normativo europeo, bensì da un'insufficiente integrazione tra livelli di governo e da una lettura difensiva delle garanzie *privacy*, che non valorizza adeguatamente il ruolo del dato quale strumento di attuazione della sussidiarietà[100] e di promozione dell'uguaglianza sostanziale.

In questa prospettiva, l'attuazione dell'*EHDS* in Italia può essere letta come un banco di prova della capacità del regionalismo sanitario e del livello centrale di evolvere verso modelli cooperativi, fondati su *standard* comuni[101], responsabilità condivise[102] e meccanismi di leale collaborazione. La sfida non consiste soltanto nell'adeguamento tecnico alle prescrizioni europee, ma nella costruzione di una *governance* del dato sanitario che sappia conciliare programmazione sanitaria, tutela della *privacy* e garanzie costituzionali in un contesto istituzionale complesso e differenziato, fino al livello delle aziende sanitarie, che possono incidere ulteriormente sulla frammentazione scegliendo autonomamente soluzioni *software* e

---

[99] Si configura, infatti, non tanto una negazione del titolo giuridico, quanto una sua compressione funzionale e sostanziale: il diritto alla salute rimane formalmente garantito dall'ordinamento, ma viene privato della possibilità di esplicarsi nel pieno delle proprie potenzialità evolutive. In assenza delle leve tecnologiche e informative necessarie a una programmazione proattiva, la tutela rischia di degradare a mera proclamazione astratta, precludendo ai cittadini l'accesso a quelle forme di assistenza personalizzata, preventiva e predittiva che la valorizzazione del dato potrebbe, e dovrebbe, rendere effettive.

[100] Il richiamo al principio di sussidiarietà estrinseca appieno in questo contesto la sua peculiare polivalenza semantica, operando sulla già enunciata duplice dimensione, europea e nazionale. Sotto il profilo del diritto dell'Unione, la sussidiarietà di cui all'art. 5, par. 3, TUE, legittima l'intervento del legislatore europeo laddove l'obiettivo di uno spazio armonizzato di dati sanitari non possa essere perseguito dai singoli Stati membri a causa della frammentazione tecnica e normativa; in tal senso, l'*EHDS* configura una forma di «sussidiarietà digitale attiva», atta a colmare i deficit di interoperabilità transfrontaliera; si veda G. Cerrina Feroni, *Ricerca scientifica e protezione dei dati personali alla luce dell'EHDS: un equilibrio necessario*, in *Corti Supreme e Salute*, 2025. Sotto il profilo interno, il riferimento è alla sussidiarietà verticale di cui all'art. 118 Cost., intesa non solo come riparto di funzioni, ma come principio di adeguatezza: il dato sanitario, adeguatamente valorizzato, diviene lo strumento procedimentale che permette ai livelli di governo più prossimi al cittadino di programmare l'offerta assistenziale in modo mirato e predittivo. Tale dinamica alimenta quella che la dottrina più recente definisce «solidarietà europea attraverso il dato», intesa come superamento dell'egoismo informativo nazionale in favore di un ecosistema di mutuo soccorso scientifico e clinico. Sul nesso tra digitalizzazione e solidarietà, si veda *G. Proietti, Tutela e valorizzazione dei dati nei mercati digitali*, Milano, 2025. In questa prospettiva, la sussidiarietà smette di essere un mero criterio di riparto di competenze per divenire leva di promozione dell'eguaglianza sostanziale, garantendo che l'innovazione tecnologica non accresca i divari territoriali ma si faccia veicolo di coesione sociale e continuità delle cure.

[101] Sull'esigenza di *standard* nazionali uniformi e di coordinamento tra livelli di governo nell'attuazione dell'EHDS si veda la dottrina sulla leale collaborazione tra Stato e Regioni in materia sanitaria, che individua in tale principio lo strumento per bilanciare uniformità della tutela del diritto alla salute e autonomia organizzativa regionale, tra cui C. E. Gallo, *Leale collaborazione tra Stato e Regioni e patti per la salute*, Centro Studi di Diritto Sanitario, SPISA, 2021.

[102] Sul potere sostitutivo e i suoi limiti si veda Corte cost., sent. n. 43/2004.

fornitori. In questo senso il divario digitale, esacerbato da tale frammentazione, rischia di generare ulteriori fratture nell'esercizio del diritto alla salute.

5. Dinamiche globali e convergenze regolative: il dibattito internazionale e le sue ricadute. La complessità delle dinamiche nazionali fin qui descritte trova un necessario termine di paragone nelle evoluzioni maturate in ambito internazionale, dove il dibattito sul EHDS, lungi dallo svilupparsi in un vuoto normativo, si colloca all'interno di dinamiche globali caratterizzate da modelli regolativi differenti ma convergenti in materia di *governance* dei dati e digitalizzazione dei sistemi sanitari. L'approccio europeo[103] delineato dall'*EHDS* si distingue per il tentativo di conciliare la valorizzazione del dato sanitario come infrastruttura del *welfare* con un elevato livello di tutela dei diritti fondamentali, ponendosi in una posizione intermedia rispetto a modelli maggiormente orientati al mercato o, al contrario, a modelli basati su un controllo pubblico centralizzato dei dati.

In tale prospettiva, l'*EHDS* si configura come parte della strategia europea, richiamata in apertura, volta a promuovere sistemi sanitari *data-driven*, nei quali l'utilizzo sistematico dei dati costituisce uno strumento essenziale per migliorare la qualità delle cure, rafforzare la sostenibilità finanziaria e ridurre le diseguaglianze di accesso. Questa impostazione trova riscontro nelle più recenti elaborazioni dell'Organizzazione mondiale della sanità (d'ora in poi *WHO)*[104], in particolare nell'ambito delle politiche di *WHO Europe* dedicate alla *governance* dei dati e alla sanità digitale, che riconoscono il valore dei dati sanitari come risorsa pubblica, a condizione che il loro utilizzo sia incardinato in quadri normativi chiari e orientati ai diritti. Secondo l'approccio sviluppato da *WHO Europe*, i sistemi informativi sanitari rappresentano una componente strutturale[105] dei moderni sistemi di *welfare*, in quanto consentono di supportare decisioni basate sull'evidenza, di migliorare la programmazione dei servizi e di promuovere l'equità sanitaria[106]. In tale quadro, la *governance* dei dati sanitari è concepita come un processo istituzionale continuo[107], che richiede trasparenza, responsabilità e fiducia, piuttosto che come una mera questione tecnica o tecnologica.

---

[103] J. de Barros et al., *The EU-funded action to strengthen health information systems*, Copenhagen, 2024. Il contributo descrive l'azione strategica finanziata dall'Unione europea e implementata dal *WHO Regional Office for Europe*, finalizzata al potenziamento strutturale dell'uso e del riuso dei dati sanitari attraverso l'adozione di modelli di *data governance* armonizzati a livello nazionale e transfrontaliero.

[104] *WHO, Global Strategy on Digital Health 2020–2025,* Ginevra, 2021, cit.

[105] *WHO Regional Office for Europe*, *Regional digital health action plan for the WHO European Region 2023–2030,* Copenhagen, 2023, dove si sottolinea come la trasformazione digitale non sia un fine tecnologico, ma un fattore abilitante per il rafforzamento dei sistemi di protezione sociale. Il documento definisce i quadri strategici (*strategic frameworks*) e le linee guida politiche (*policy guidance*) per il rafforzamento dei sistemi informativi sanitari nazionali attraverso una *governance* del dato armonizzata. Il documento fornisce un inquadramento sistematico della funzione dei sistemi informativi sanitari quali pilastri per una *governance* pubblica trasparente e per il potenziamento dell'efficacia dei moderni sistemi sanitari nazionali.

[106] *WHO Regional Office for Europe*, *Health data governance in the age of artificial intelligence: policy imperatives for the WHO European Region*, Copenhagen, 2025. Il documento analizza l'intersezione tra la disponibilità di basi dati strutturate e l'efficacia predittiva dei sistemi di IA, ponendo la qualità del dato come precondizione per la tutela dell'equità nei sistemi sanitari e della trasparenza nei processi decisionali automatizzati, che sostanziano il decision-making algoritmico.

[107] *WHO Regional Office for Europe*, *Digital Health in the WHO European Region: the ongoing journey to commitment and transformation*, Copenhagen, 2023. In questo documento, il *WHO* evidenzia la necessità del passaggio dalla gestione tecnica del dato alla sua *governance* istituzionale, attraverso dati standard, interoperabilità e un sistema di qualità nella gestione degli stessi. Partendo dai dati sullo stato di attuazione della *digital health* in Europa, individua margini di miglioramento in un processo di miglioramento continuo per garantire l'interoperabilità dei dati e sulla *governance* dei dati sanitari contribuendo alla resilienza dei sistemi sanitari europei.

Un elemento centrale delle più recenti pubblicazioni di *WHO Europe* riguarda proprio il nesso tra uso dei dati, equità e salute pubblica e conferma quanto dedotto sinora. Il *WHO* indica infatti che i dati sanitari, se correttamente raccolti, integrati e analizzati, consentono di individuare diseguaglianze strutturali, bisogni sanitari emergenti e fattori di rischio legati a determinanti sociali e demografici, orientando le politiche sanitarie verso una maggiore equità sostanziale. In questa prospettiva, la digitalizzazione non è un fine in sé, ma uno strumento funzionale alla realizzazione del diritto alla salute in una dimensione collettiva.

In particolare, *WHO Europe* ha sottolineato il ruolo della *population stratification* come strumento chiave per il *population health management*, evidenziando come la disponibilità di dati sanitari aggregati e pseudonimizzati consenta di programmare interventi mirati in funzione dei bisogni concreti delle popolazioni di riferimento[108]. La stratificazione della popolazione, basata su indicatori clinici, demografici e socioeconomici, è indicata come condizione essenziale per una programmazione sanitaria efficace e per la riduzione delle diseguaglianze territoriali e sociali[109].

L'urgenza di una trasformazione digitale basata sui dati non risponde soltanto a logiche di efficientamento amministrativo, ma si pone come risposta necessaria al mutamento strutturale della domanda di salute negli ultimi decenni, determinata dall'aumento della vita media e dei cd. grandi anziani, e la conseguente aumentata necessità di servizi di salute legati alla maggiore incidenza di cronicità e fragilità. Questa esigenza è particolarmente sentita in Italia, dove i dati Istat evidenziano una tendenza demografica particolarmente dirompente, anche rispetto alla media europea[110]: nei prossimi vent'anni la quota di popolazione over-65 supererà la soglia del 34%[111], con una proiezione di crescita della multicronicità che rischia di rendere insostenibile l'attuale assetto finanziario del Servizio Sanitario Nazionale.

In questo scenario, l'adozione di modelli predittivi fondati sulla *population stratification* cessa di essere una mera opzione gestionale per configurarsi come un presupposto essenziale per garantire l'effettività del diritto alla salute. Solo attraverso una programmazione proattiva, capace di anticipare i bisogni assistenziali e di allocare le risorse in modo mirato, è possibile

---

[108] *WHO Regional Office for Europe*, *Population health management in primary health care: a proactive approach to improve health and well-being: primary heath care policy paper* series, Copenhagen, 2023. Il *policy paper* assume uno specifico rilievo rispetto alla programmazione sanitaria della gestione della cronicità. Su questo tema si consultino anche i documenti di indirizzo (*technical briefs*) sulla *population stratification* quali strumenti per l'allocazione efficiente delle risorse, basata sui bisogni reali della popolazione, e il superamento dei divari territoriali nell'accesso alle cure.

[109] In questo senso si veda anche, per i principi generali a livello globale, il documento *OECD, Health Data Governance: Privacy, Monitoring and Research*, Parigi, 2015. Il documento approfondisce il nesso inscindibile tra la gestione dei dati di popolazione e l'equità sanitaria, analizzando il valore dei dati sanitari per l'«interesse pubblico» (*public interest*): una risorsa collettiva il cui valore risiede nella capacità di generare benefici sociali diffusi attraverso la ricerca e la programmazione, a condizione che sia governata da una cornice etica e giuridica capace di bilanciare la valorizzazione informativa con la rigorosa tutela della dignità umana. Viene sottolineato come una *governance* del dato orientata all'interesse pubblico sia condizione imprescindibile per una programmazione sanitaria efficace e per la riduzione strutturale delle diseguaglianze.

[110] Per un raffronto con la media dei Paesi membri, si vedano le rilevazioni Eurostat, in particolare *Ageing Europe – looking at the lives of older people*, 2020 ed., che confermano il primato demografico negativo dell'Italia: l'indice di vecchiaia e la quota di ultrasessantacinquenni nel nostro Paese risultano sensibilmente superiori alla media UE-27, configurando una sfida di sostenibilità del sistema sanitario più acuta rispetto al resto del continente.

[111] Si veda ancora ISTAT, *Rapporto annuale 2023. La situazione del Paese*, Roma, 2023, cit., in particolare il cap. 2 (Cambiamenti nel mercato del lavoro e investimenti in capitale umano), dove si evidenzia il progressivo l'invecchiamento della popolazione e il suo impatto sul sistema paese. Sull'impatto economico della cronicità si consulti anche Ministero della Salute, *Piano Nazionale della Cronicità*, 2016, cit., e il più recente d.m. 77/2022 *Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*, cit., sulla riorganizzazione della sanità territoriale, che pone la stratificazione della popolazione a fondamento del nuovo modello di assistenza primaria, basato sul principio della prossimità territoriale, in attuazione del principio di sussidiarietà.

preservare il carattere universalistico del sistema di *welfare* ed evitare che l'incremento della spesa sanitaria si traduca in una progressiva erosione degli indefettibili Livelli Essenziali di Assistenza (LEA), a scapito delle fasce di popolazione più vulnerabili, sia dal punto di vista sociosanitario che socioeconomico.

Queste elaborazioni internazionali trovano un significativo punto di contatto con l'impostazione dell'*EHDS*, che legittima l'uso secondario dei dati sanitari per finalità di interesse pubblico, quali la ricerca scientifica, la valutazione delle politiche sanitarie e la programmazione dell'offerta assistenziale. L'uso dei dati per tali finalità non è concepito come una deroga alla tutela della *privacy*, ma come un ambito che richiede garanzie specifiche, proporzionate e alternative al consenso individuale, in linea con i principi di necessità e proporzionalità.

In questo senso, le posizioni espresse dalle autorità europee di protezione dei dati convergono con l'approccio *WHO*, nel riconoscere che l'interesse pubblico alla salute può costituire una base giuridica autonoma per il trattamento dei dati sanitari, purché accompagnata da adeguate garanzie. La *Joint Opinion* di *EDPB* ed *EDPS* sulla proposta di *EHDS* ha infatti richiamato esplicitamente la necessità di assicurare coerenza sistemica tra protezione dei dati, interesse pubblico e funzionamento dei sistemi sanitari, valorizzando gli strumenti di tutela già richiamati diversi dal consenso, quali la essenziale pseudonimizzazione, il controllo degli accessi e la supervisione istituzionale[112].

La convergenza tra il quadro europeo e il dibattito internazionale conferma che la questione centrale non introduce un'eccezione alla protezione dei dati, ma richiede un salto di qualità nella capacità degli ordinamenti di praticare un bilanciamento maturo, riguardando non la legittimità astratta dell'uso dei dati sanitari, bensì la costruzione di condizioni di legittimità sostanziale, nelle quali la valorizzazione del dato sia funzionale alla tutela dei diritti fondamentali e alla promozione della salute pubblica. In assenza di tali condizioni, la digitalizzazione rischia di tradursi in un fattore di diseguaglianza e di inefficienza, piuttosto che in uno strumento di rafforzamento dei sistemi sanitari[113].

6. Conclusioni. L'analisi dello Spazio europeo dei dati sanitari mette in evidenza come la digitalizzazione della sanità rappresenti oggi uno dei banchi di prova più avanzati per il diritto pubblico europeo. L'*EHDS* non si limita a introdurre nuovi obblighi tecnici o *standard* di interoperabilità, ma incide profondamente sulle modalità di esercizio del diritto alla salute, sollecitando una ridefinizione dei rapporti tra tutela dei diritti fondamentali, organizzazione dei sistemi sanitari e responsabilità istituzionale[114].

Le tensioni emerse nel corso dell'analisi, tra protezione della *privacy* e interesse pubblico alla salute, tra valorizzazione del dato e garanzie dei diritti, tra integrazione europea e attuazione nazionale differenziata, non appaiono contingenti, accidentali, ma strutturali. Esse riflettono la complessità dei diritti sociali nell'era digitale e l'esigenza di strumenti giuridici capaci di governare tale complessità senza ricorrere a soluzioni semplificatrici o a letture rigidamente difensive delle garanzie.

---

[112] Si veda ancora *EDPB-EDP Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, cit.

[113] Sul punto ancora S. Rodotà, *Tecnologie e diritti*, Bologna, 2021, cit.

[114] Tale approccio richiede l'adozione di strumenti di *governance ex ante*, come valutazioni d'impatto che analizzino congiuntamente i rischi per la *privacy* e quelli derivanti dall'uso dell'*AI*, evitando duplicazioni burocratiche. Sul tema A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in BioLaw Journal, 2019, cit. Fondamentale sarà inoltre l'istituzionalizzazione del principio di *accountability* lungo tutta la catena del valore del dato, per garantire che la responsabilità non si disperda nelle pieghe della *governance* multilivello. Si veda reg. (UE) 2016/679 (*GDPR*), cit., art. 5, par. 2.

In questo contesto, il bilanciamento si conferma come la tecnica ordinaria attraverso cui articolare il diritto alla salute nello spazio digitale, secondo criteri di proporzionalità, ragionevolezza e sussidiarietà. L'*EHDS* richiede di superare concezioni statiche della protezione dei dati, promuovendo una lettura dinamica della *privacy* come diritto da tutelare mediante garanzie adeguate alle finalità pubbliche legittime perseguite.

In tale prospettiva, la dottrina ha sottolineato come la tutela dei diritti fondamentali nell'ambiente digitale non possa essere affidata a divieti generalizzati o a una concezione meramente difensiva delle autorità di controllo, ma richieda istituzioni capaci di assumersi la responsabilità delle scelte allocative e programmatorie, governando il rischio anziché neutralizzarlo astrattamente[115].

L'*EHDS* impone di governare conflitti strutturali, non di negarli. *Privacy* e salute pubblica non sono alternative: richiedono bilanciamenti dinamici. Il caso italiano mostra i rischi di approcci difensivi, che possono trasformare le garanzie in ostacoli all'effettività dei diritti.

In previsione della piena entrata in vigore dell'*EHDS*, è necessaria un'armonizzazione interpretativa che riconosca il dato sanitario come leva di attuazione del diritto alla salute in un quadro multilivello responsabile. Per tale ragione, appare necessario rafforzare il coordinamento interpretativo ed operativo tra le autorità coinvolte nella *governance* del dato sanitario, promuovendo una lettura sistemica delle norme europee e nazionali che valorizzi l'uso dei dati per finalità pubbliche legittime, senza compromettere la tutela della persona. In particolare, l'attuazione dell'*EHDS* richiede orientamenti chiari e coerenti capaci di distinguere tra usi necessari e proporzionati del dato per la programmazione sanitaria e trattamenti eccedenti o non giustificati, evitando che la garanzia si trasformi in un fattore di veto permanente.

Il caso italiano mostra in modo emblematico come l'assenza di tale coordinamento possa tradursi in un rallentamento dell'azione pubblica, con effetti indiretti ma significativi sull'effettività del diritto alla salute. Come argomentato nel corso del contributo, l'impossibilità di utilizzare dati sanitari pseudonimizzati per la stratificazione della popolazione e la programmazione dell'offerta può parzialmente compromette la capacità di ridurre le diseguaglianze territoriali, contenere le liste di attesa e garantire un equo accesso alle cure, incidendo su diritti sociali che restano formalmente riconosciuti ma sostanzialmente inattuabili.

In conclusione, lo Spazio europeo dei dati sanitari non è solo un regolamento tecnico: è un esperimento di sovranità digitale che mira a costruire una vera «Unione europea della salute»[116] e può costituire uno strumento decisivo per rafforzare il diritto alla salute in una prospettiva europea e multilivello, a condizione che il dato sanitario sia riconosciuto come leva di attuazione, e non di compressione, dei diritti fondamentali.

La credibilità di questo modello dipende dalla sua tenuta interna e dalla capacità di trasformare il conflitto normativo in un nuovo equilibrio costituzionale. La sfida per il giurista è garantire che l'innovazione tecnologica avvenga nel rispetto del nucleo essenziale dei diritti fondamentali, assicurando che la sanità digitale sia uno strumento di coesione e non di esclusione[117]. Siamo chiamati non a scegliere tra *privacy* e salute pubblica, ma a costruire un nuovo equilibrio, istituzionalmente responsabile e costituzionalmente orientato, capace di trasformare la digitalizzazione in un fattore di eguaglianza sostanziale e di sostenibilità del *welfare*[118] e di superare lo «stress test» costituzionale, assorbendo l'impatto dirompente della tecnologia su uno dei settori sensibili per eccellenza qual è quello della salute.

---

[115] G. De Gregorio, *Digital Constitutionalism in Europe*, Cambridge, 2022, cit., 74 ss.

[116] Comunicazione della Commissione, *Costruire un'Unione europea della salute*, COM(2020) 724 final.

[117] G. Ferri, *Diritto costituzionale e nuove tecnologie*, Napoli, 2022.

[118] Sulla necessità di un bilanciamento tra principi e sulla coesistenza di valori eterogenei nell'ordinamento costituzionale pluralista, si veda il contributo fondamentale di G. Zagrebelsky, *Il diritto mite*, Torino, 1992. La

Abstract. Il saggio analizza la costruzione dello Spazio europeo dei dati sanitari (*EHDS*) alla luce della complessa triangolazione normativa con il *GDPR* e l'*AI Act*. Inquadrando la digitalizzazione sanitaria come uno «stress test» per le categorie del diritto pubblico e il costituzionalismo europeo e nazionale, l'indagine si sofferma sul passaggio paradigmatico dalla *data protection* alla *data valorisation* in funzione dell'interesse pubblico, esaminando le tensioni con il diritto alla protezione dei dati personali e la conseguente necessità di nuovi bilanciamenti verso una «*compliance* di sistema». Attraverso l'analisi del «caso Italia», segnato dalle peculiarità del regionalismo e da un approccio improntato a un rigore garantista delle autorità di controllo, il contributo evidenzia come l'interoperabilità del dato costituisca oggi un presupposto di adeguatezza per l'esercizio della sussidiarietà e un vettore di solidarietà europea. Il riconoscimento del dato sanitario come «*Data for Public Good*» emerge, infine, come condizione necessaria per garantire l'eguaglianza sostanziale e la sostenibilità del *welfare* di fronte alle sfide demografiche delle aumentate prospettive di vita e della cronicità.

Abstract. This paper examines the development of the European Health Data Space (*EHDS*) within the complex regulatory framework of the *GDPR* and the *AI Act*. By framing the digitalization of healthcare as a «stress test» for public law categories and European and national constitutionalism, the study focuses on the paradigmatic shift from data protection to data valorisation for public interest purposes, examining the tensions with the right to personal data protection and the subsequent need for new balancing of interests towards a «systemic compliance». Through an analysis of the «Italian case», characterized by regionalist peculiarities and a highly protection-oriented approach by supervisory authorities, the article highlights how data interoperability has become a prerequisite for the effective exercise of subsidiarity and a driver of European solidarity. Finally, the recognition of health data as a «Data for Public Good» emerges as a necessary condition to ensure substantive equality and the sustainability of welfare systems in the face of the demographic challenges posed by increased life expectancy and chronic diseases.

Parole chiave. *EHDS* – *Governance* multilivello – *Compliance* di sistema – Bilanciamento tra *privacy* e uso del dato – Cittadinanza sanitaria europea

Key words. *EHDS* – Multilevel Governance – Systemic compliance – Balancing between privacy and data use – European health citizenship.

prospettiva del «diritto mite» appare particolarmente feconda per inquadrare la *governance* dello Spazio europeo dei dati sanitari, laddove la ricerca di un «equilibrio dinamico» tra protezione della riservatezza e tutela della salute collettiva richiede istituzioni capaci di comporre tensioni strutturali senza cedere alla «tirannia» di un valore sull'altro, preservando così la natura pluralista e inclusiva del sistema di *welfare*.