federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

4 DICEMBRE 2024

Gestione e conservazione dei dati sanitari. Il *vulnus* normativo che impatta su sicurezza e *data protection*

di Elisa Sorrentino
Consiglio Nazionale delle Ricerche
Istituto di Informatica e Telematica

e Anna Federica Spagnuolo
Consiglio Nazionale delle Ricerche
Istituto di Informatica e Telematica

Gestione e conservazione dei dati sanitari. Il *vulnus* normativo che impatta su sicurezza e *data protection*[*]

di Elisa Sorrentino
Consiglio Nazionale delle Ricerche
Istituto di Informatica e Telematica

e Anna Federica Spagnuolo
Consiglio Nazionale delle Ricerche
Istituto di Informatica e Telematica

Abstract [It]: La mancanza di regole chiare per l'affidabilità, autenticità, integrità, leggibilità e reperibilità dei dati mette a rischio il loro valore legale nel tempo. Questo vulnus normativo impatta negativamente sulla loro sicurezza e sulla privacy dei cittadini. L'analisi normativa sul tema della governance dei dati suggerisce di favorire l'apertura dei dati personali nel rispetto dei principi FAIR e di estendere il concetto di data retention a quello di data preservation.

Title: Management and storage of health data. The regulatory breach impacting security and data protection
Abstract [En]: The lack of clear rules for data reliability, authenticity, integrity, readability, and accessibility undermines their legal value over time. This regulatory gap negatively affects their security and citizen privacy. The legal analysis on data governance suggests promoting the openness of personal data in compliance with FAIR principles and extending the concept of data retention to data preservation.

Parole chiave: Conservazione dei dati, sicurezza dei dati, dati sanitari, principi FAIR
Keywords: Data preservation, data security, health data, FAIR principles

1. Introduzione

La capacità di accedere, elaborare e condividere i dati sanitari[1] rappresenta una risorsa strategica di primaria importanza per il progresso e l'innovazione del comparto sanitario, tanto in ambito europeo che

[*] Articolo sottoposto a referaggio.

[1] L'articolo 4 paragrafo 15 del Regolamento (UE) 2016/679 (GDPR) definisce i dati sanitari come "qualsiasi informazione relativa alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivela informazioni relative al suo stato di salute". Questa definizione include anche i dati relativi alla prevenzione, diagnosi, cura o trattamento di malattie o condizioni fisiche, nonché i dati relativi alla salute dei singoli o di gruppi di persone. Si veda a tal proposito di M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, n. 1, pp. 165-190, di P. GUARDA, *I dati sanitari,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo,* Giappichelli, Torino, 2019, p. 594; di F. CAGGIA, *Il trattamento dei dati dei dati sanitari sulla salute, con particolare riferimento all'ambito sanitario,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali,* Giappichelli, Torino, 2007, pp. 407-410. Una parte della dottrina ha sottolineato come manchi effettivamente una definizione di dato sanitario, riconducendo tale scelta alla finalità di «lasciare una libertà al singolo operatore pratico di individuare di volta in volta quale informazione possa essere idonea a fornire indicazioni sullo stato di salute di un soggetto… guardando probabilmente più che al contenuto delle informazioni, alle finalità cui essa è destinata».

su scala nazionale. La possibilità di sfruttare appieno questo prezioso patrimonio informativo è imprescindibile per garantire un'assistenza sanitaria maggiormente mirata e personalizzata, promuovere lo sviluppo di innovative soluzioni terapeutiche e tecnologiche, nonché supportare la definizione di politiche sanitarie più incisive ed efficaci. Tale cruciale rilevanza, come vedremo, è stata ampiamente riconosciuta e valorizzata a livello comunitario a partire dalla Strategia Europea dei Dati[2] che ha posto le basi per l'adozione di un approccio integrato e coordinato alla gestione dei dati, inclusi quelli del settore sanitario. Durante l'emergenza pandemica generata dal Covid-19, l'esigenza di accedere, scambiare e sfruttare rapidamente i dati sanitari si è resa ancora più evidente per fronteggiare la crisi e garantire un'assistenza adeguata. Tuttavia, in gran parte del territorio nazionale[3] la mancanza di criteri uniformi di raccolta e trasmissione, insieme alla carenza di trattamento adeguato in termini di formazione e conservazione[4], ha reso complessa la trasformazione dei dati in informazioni utili[5], mettendo spesso a repentaglio la sicurezza dei dati stessi. Tali criticità persistono ancora oggi e hanno effetti importanti anche sul Fascicolo Sanitario Elettronico (FSE) [6] che, attraverso gli interventi previsti dal Piano Nazionale

[2] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a European Strategy for data, Brussels, 19.2.2020 COM (2020) 66 final

[3] Si veda a tal proposito di G. CARULLO, P. PROVENZANO (a cura di), *Le Regioni alla prova della pandemia da Covid-19, dalla Fase 1 alla Fase 2*, vol. I e II, Editoriale Scientifica, Napoli, 2020.

[4] V. PAGNANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in S. CALZOLAIO (a cura di), *Ubi Data, Ibi Imperium: Il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, 3(1), 2021, p. 15. L'autrice fa espresso riferimento al modello di gestione della pandemia della Regione Veneto che, pur nella complessità delle questioni giuridiche che ha sollevato, pare essere stato, almeno in una prima fase, un esempio di utilizzo efficace delle banche dati nel contenimento dell'emergenza sanitaria.

[5] Si veda a tal proposito di D.U. GALETTA *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013,* in federalismi.it, 5, 2016, p. 9. L'autore specifica un distinguo tra la definizione di dato e quella di informazione asserendo che «mentre il "dato" è sempre un elemento conoscitivo, la "informazione" ha una connotazione in qualche maniera soggettiva, in quanto è quello che l'utente di volta in volta ricava dall'aggregazione dei dati che può ottenere consultando un database». Sulla stessa linea, con specifico riferimento ai dati sanitari altra parte della dottrina rileva l'interrelazione tra il concetto di dato e di informazione. In particolare, ci si interroga se la nozione di dato sanitario debba essere interpretata in senso stretto, limitandola ai soli dati che attestano una patologia, o se diversamente possa intendersi nella più ampia accezione di informazioni che possono far sospettare la presenza di un disturbo o patologia. Si veda quanto osservato sul punto da G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Zanichelli Bologna, 2012, pp. 57-61. Sul concetto di "dato" come rappresentazione digitale dell'informazione si veda di A. IANNUZZI, *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act*, in P. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024.

[6] Il FSE è definito all'art. 12 del d.l. 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*" (convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221). Il già menzionato decreto istituisce il FSE demandandone l'attuazione alle Regioni e alle Province Autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali. Successivamente, il d. l. 21 giugno 2013, n. 69 fisserà al 30 giugno 2015 il termine per l'attivazione del FSE presso le Regioni e le Province Autonome. Il 29 settembre 2015 viene pubblicato il D.P.C.M. n. 178 recante *Regolamento in materia di fascicolo sanitario elettronico*, che disciplina il FSE e ne detta i contenuti. Il recente art. 21 (Misure in materia di fascicolo sanitario elettronico e governo della sanità digitale) del d.l. 27 gennaio 2022 n. 4[6], convertito in legge n. 25 il 28 marzo 2022, rubricato *Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico*, apporta modifiche all'art 12 del d.l 18 ottobre 2012, n. 179, con l'obiettivo di favorire il raggiungimento degli obiettivi del PNRR in materia di sanità digitale e di garantirne la piena implementazione. Il testo della legge n. 25

di Ripresa e Resilienza (PNRR)[7], dovrebbe divenire pietra angolare per i servizi sanitari digitali e la valorizzazione dei dati clinici nazionali[8].

è consultabile sul sito della Gazzetta Ufficiale. Tra gli interventi più significativi finalizzati ad attuare il nuovo governo della sanità digitale si segnalano le ulteriori funzioni attribuite all'Agenas - Agenzia nazionale per i servizi sanitari regionali - per garantire, tra l'altro, l'interoperabilità dei Fascicoli sanitari elettronici, d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, e la realizzazione, a cura del Ministero della salute, del nuovo Ecosistema dei Dati Sanitari (EDS), in accordo con l'Agenzia per la cybersicurezza nazionale. Sono inoltre previste norme di coordinamento per l'attuazione del nuovo impianto di governo del FSE e, infine, la possibilità per Agenas e Ministero della salute di avvalersi della Sogei per la gestione dell'Ecosistema dati sanitari e per la messa a disposizione alle strutture sanitarie e sociosanitarie di specifiche soluzioni software, senza nuovi o maggiori oneri per la finanza pubblica. Le nuove disposizioni apportano importanti novità in materia di disponibilità e condivisione dei dati e l'istituzione dell'EDS avrebbe un ruolo determinante. L'EDS andrebbe difatti a raccogliere ed elaborare i dati trasmessi dalle strutture sanitarie e sociosanitarie, dagli enti del Servizio Sanitario Nazionale, e da quelli resi disponibili tramite il sistema Tessera Sanitaria, al fine di garantire il coordinamento informatico e assicurare servizi sanitari omogenei su tutto il territorio nazionale. Il Ministero della Salute ha poi successivamente emanato il Decreto ministeriale 18 maggio 2022, relativo all'integrazione dei dati essenziali che compongono i documenti del Fascicolo Sanitario Elettronico e il 20 maggio 2022, emana le nuove Linee Guida nazionali di concerto con il Ministero per l'innovazione tecnologica e la transizione digitale e il Ministro dell'economia e delle finanze. Le Linee Guida ampliano le tipologie di documenti che andranno ad alimentare il FSE e, estendendo anche ai dati strutturati degli episodi ambulatoriali, di ricovero, PSS, e così via, con l'obiettivo di ampliare il patrimonio informativo a disposizione di cittadini, operatori e del Sistema Sanitario Regionale (SSR). Le Linee Guida andranno inoltre a definire le regole tecniche per garantire la raccolta, la conservazione, la consultazione e l'interscambio di dati sanitari da parte degli enti del SSN e dei soggetti pubblici e privati che erogano prestazioni sanitarie e sociosanitarie agli assistiti. Il Decreto del Ministro della Salute del 7 settembre 2023, pubblicato nella Gazzetta Ufficiale Serie Generale del 24 ottobre 2023, va a stabilire i contenuti e le modalità di accesso del Fascicolo Sanitario Elettronico (FSE) 2.0, emanato in attuazione delle disposizioni di cui al comma 7 dell'art. 12 del d.l n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni. Questo decreto definisce i dati e i documenti presenti nel FSE, i limiti di responsabilità dei soggetti coinvolti nella sua implementazione, le garanzie di sicurezza per il trattamento dei dati personali e le modalità di accesso differenziate. Sullo strumento, G. POLIFRONE, *Sanità digitale. Prospettive e criticità di una rivoluzione necessaria*, Edizioni LSWR, Milano, 2019, p. 11 e ss; G. COMANDÈ, L. NOCCO, V. PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Riv. it. med. leg.*, 2012, p. 105 e ss. Sul tema dell'accessibilità ai documenti contenuti nel FSE si veda anche E. SORRENTINO, M.T. GUAGLIANONE, E. CARDILLO, M.T. CHIARAVALLOTI, A.F. SPAGNUOLO, G.A. CAVARRETTA, *La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico*, in *Riv. it. Di informatica e diritto*, 2020, p. 35 e ss. Sull'uso dello strumento in fase di emergenza da Sars Covid si veda di E. SORRENTINO, A. F. SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in federalismi.it, Fascicolo n. 30/2020, pp. 242-254, si veda ancora di N. POSTERARO, *The digitalization of the healthcare sector in Italy: the Electronic Health Record*, in M.A. SANDULLI, F. APERIO BELLA (a cura di), *Shaping the Future of Health Law: Challenges for Public Law*, in *federalismi.it*, 17 novembre 2021, p. 10 ss.

[7] Cfr. *Piano Nazionale di Ripresa e Resilienza* (PNRR) consultabile sul sito del Governo. Il PNRR è stato definitivamente approvato in sede europea il 13 luglio 2021, con Decisione di esecuzione del Consiglio a seguito della proposta della Commissione. Più dettagliatamente, la Missione n. 6, dedicata alla salute, prevede, tra i suoi settori d'intervento, l'innovazione, la ricerca e la digitalizzazione del Servizio Sanitario Nazionale (SSN) e in tali ambiti rientra il potenziamento, la diffusione, l'omogeneità e l'accessibilità del FSE da parte degli assistiti e degli operatori sanitari su tutto il territorio nazionale. Nello specifico, il PNRR prevede "la piena integrazione di tutti i documenti sanitari e tipologie di dati, la creazione e implementazione di un archivio centrale, l'interoperabilità e piattaforma di servizi, la progettazione di un'interfaccia utente standardizzata e la definizione dei servizi che il FSE dovrà fornire. Si veda di N. POSTERARO, *Il fascicolo sanitario elettronico*, in V. BONTEMPI (a cura di), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, RomaTrE-Press, Roma, 2022, p. 187 ss.

[8] Cfr. *PNRR*, *op. cit.*, p. 17.

Sono diversi i *gap* ancora da colmare in relazione al FSE[9] e, più ampiamente, in materia di dati sanitari soprattutto in relazione al loro uso secondario[10]. In questo lavoro, ci concentreremo principalmente sulla carenza di regole uniformi e puntuali finalizzate a garantire che i dati, contenuti e trasportati dai documenti clinici, mantengano nel tempo le caratteristiche di affidabilità, autenticità, integrità, leggibilità e reperibilità[11] assicurandone in tal modo la permanenza del pieno valore legale. Tale mancanza a nostro avviso si configura come un importante *vulnus* normativo che, in assenza di interventi puntuali, rischia di inficiare la possibilità di tracciare dettagliatamente la storicità di un percorso clinico e ottenere così un ritorno in termini di efficienza dell'intero *setting* assistenziale[12] oltre che una perfetta aderenza alle *policy* di *privacy* e sicurezza[13].

[9] Il FSE non è ancora implementato in modo uniforme su tutto il territorio nazionale. Alcune Regioni hanno sviluppato e adottato il sistema in modo più completo rispetto ad altre, creando disparità nell'accesso e nella gestione delle informazioni cliniche. Inoltre, i documenti clinici inseriti nel FSE sono spesso costituiti da dati non strutturati, il che rende più complessa l'interpretazione e l'utilizzo delle informazioni contenute. Sono diversi i fattori di disallineamento e tra questi si possono annoverare la mancanza di una diffusione uniforme dei servizi digitali in ambito sanitario, le difficoltà di alcune strutture nel collegare i propri sistemi informativi al FSE, l'utilizzo improprio dei documenti e mancata indicizzazione, che ne compromette l'accessibilità e l'interoperabilità, la comunicazione non regolare dei flussi di dati, la carenza di regole di codifica standardizzate, la pluralità di sistemi architetturali utilizzati.

[10] L'uso secondario dei dati sanitari è riferibile al trattamento di dati personali sanitari per scopi diversi da quelli per cui sono stati originariamente raccolti. Ci si riferisce all'uso di dati anonimizzati provenienti da cartelle cliniche, registri di sanità pubblica, sperimentazioni cliniche ecc. per finalità di interesse collettivo come la protezione della salute pubblica, la produzione di statistiche ufficiali, la ricerca scientifica e lo sviluppo di algoritmi di intelligenza artificiale. Tutto questo richiede un approccio equilibrato che valorizzi il potenziale dei dati sanitari a beneficio di tutti i soggetti coinvolti, nel rispetto dei diritti e delle libertà fondamentali dei cittadini. Si veda a tal proposito di A. CABRIO, *La seconda vita dei dati. luci e ombre della normativa privacy in materia di secondary data use*, in F. FRATTINI, F. MASSIMINO (a cura di), *I dati. Il futuro della sanità: strumenti per una reale innovazione*, Edra, 2022, pp. 25-30. Si veda ancora di R. BECKER, D. CHOKOSHVILI, G. COMANDÉ, *Secondary use of Personal Health Data: when is it "Further Processing" under the GDPR, and What Are the Implications for Data Controllers?, in European Journal of Health Law,* 2022, p. 29; G. MAGLIO, *L'uso dei dati nella Sanità: difficoltà procedurali e legislative*, 2023, consultabile sul sito di Agenda Digitale.

[11] L'art. 44, comma 1-ter, del d.lgs. n. 82/2005, *Codice dell'amministrazione digitale* (CAD), afferma che "il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità", secondo le modalità indicate nelle Linee guida, le quali confermano la natura del sistema di conservazione quale insieme di regole, procedure e tecnologie strutturate in modo tale da garantire tali caratteristiche dei documenti informatici singoli o organizzati all'interno di fascicoli, serie o interi archivi. Inoltre, esse specificano, per quanto riguarda i modelli organizzativi, che la conservazione potrà essere realizzata all'interno o all'esterno della struttura organizzativa titolare degli oggetti da conservare.

[12] In ambito sanitario un corretto processo di conservazione è di fondamentale importanza, poiché solo se tutti i documenti clinici e amministrativi continuano a mantenere nel tempo le caratteristiche di affidabilità, autenticità, integrità, leggibilità e reperibilità è possibile tracciare la storicità di un percorso clinico e ottenere contestualmente un immediato ritorno in termini di efficienza dell'intero setting assistenziale. A tal proposito si veda di E. SORRENTINO, M. T GUAGLIANONE, E. CARDILLO, M. T. CHIARAVALLOTI, A. F. SPAGNUOLO, G. A CAVARRETTA, *La conservazione dei documenti, op.cit.* Si veda ancora di A. ALFIER, *Gli archivi sanitari nell'epoca della sanità elettronica: una sfida ai paradigmi tradizionali della scienza archivistica?* in S. PIGLIAPOCO (a cura di), *Documenti e archivi nella sanità elettronica*, EUM Edizioni Università di Macerata, luglio 2016, pp. 137-195.

[13] Un'approfondita analisi in tema di sicurezza è offerta da S. STALLA-BOURDILLON, *Privacy vs Security… Are We Done Yet?* in S. STALLA-BOURDILLON, G. PHILLIPS, M. D. RYAN (a cura di), *Privacy vs. Security*, SpringerBriefs in Cybersecurity, Springer, London, 2014, p. 62: "It is therefore inappropriate to try to oppose the values of privacy and security in general terms. Going further it is crucial to precisely identify the type and seriousness of the security threat at stake in order to properly identify the needs of the democratic society implicated. In this line it becomes necessary to distinguish, to the extent possible, between different, though closely related, concepts and in particular between the concepts of national security, public security and the prevention of crimes. Indeed, when "only" the prevention of

Ampliando il discorso e, dunque, analizzando i riferimenti normativi e le linee guida sui dati aperti a livello europeo e nazionale, e considerando in particolare gli sviluppi recenti in tema di principi FAIR[14], si potrebbe ipotizzare un'interpretazione estensiva di tali percorsi anche ai dati sanitari ed iniziare a configurare una politica di corretta gestione e conservazione che vada ad aumentare significativamente la sicurezza dei dati, minimizzando il rischio di violazioni.

2. Nuova Governance europea dei dati sanitari: impatti e prospettive

La Strategia europea per i dati[15] presentata dalla Commissione europea nel 2020 rappresenta un punto di svolta nell'approccio comunitario all'accesso e alla condivisione dei dati. Riconoscendo il valore strategico di questo patrimonio informativo per il progresso, l'innovazione e la ricerca[16], la Strategia getta le basi per

crimes is at stake it should be more difficult to justify interferences to the right to respect of private life". Si veda ancora di O. POLLICINO, G. DE GREGORIO, M. BASSINI, *Internet law and protection of fundamental rights*, Stampa Università Bocconi, Milano, 2022. Gli autori presentano i diritti e le libertà in relazione sia alle opportunità che alle sfide delle tecnologie digitali, soffermandosi su come l'avvento delle tecnologie digitali abbia impattato su contenuti e dati, esplorandone gli effetti in termini di tutela della libertà di espressione, diritto alla *privacy* e protezione dei dati. In particolare, la terza parte (pp. 169-268) del libro analizza l'ambito della *privacy* e protezione dei dati guardando alle loro radici storiche, al ruolo del GDPR, incentrandosi specificamente anche sulla conservazione e sul trasferimento dei dati. Si veda inoltre di A. FIASCHI, *Fascicolo Sanitario Elettronico: i rischi per la data protection delle politiche di sanità integrata*, in *Cybercecurity360.it*.

[14] I principi FAIR sono stati elaborati nel 2014 per ottimizzare la riutilizzabilità dei dati della ricerca. Essi rappresentano un insieme di linee guida e migliori pratiche sviluppate per garantire che i dati, o qualsiasi oggetto digitale, siano *Findable*/Rintracciabili, *Accessible*/Accessibili, *Interoperable*/Interoperabili e *Reusable*/Riutilizzabili. Rintracciabili: per poter rendere i dati riutilizzabili occorre che siano per prima cosa rintracciabili dagli esseri umani e dalle macchine. Il recupero automatico e affidabile di set di dati dipende dagli identificatori persistenti (PID) utilizzati, quali ad esempio DOI, *Handle* o URN, e dai metadati descrittivi attribuiti ai dati, che devono essere registrati in "cataloghi" o in *repository* indicizzabili anche dalle macchine. Accessibili: i dati o almeno i loro metadati devono poter essere accessibili dagli esseri umani e dalle macchine anche attraverso sistemi di autenticazione e autorizzazione (non è necessario che i dati depositati siano open access) mediante l'uso di protocolli standard. I dati e i loro metadati devono essere depositati in archivi o repository che li rendano possibilmente persistenti nel tempo e rintracciabili in rete. Almeno i metadati dovrebbero rimanere sempre disponibili anche quando i dati non sono in open access. Interoperabili: i dati devono poter essere combinati e utilizzati insieme con altri dati o strumenti. Il formato dei dati deve pertanto essere aperto e interpretabile da vari strumenti, compresi altre basi di dati. Il concetto di interoperabilità si applica anche ai metadati. Ad esempio, i metadati dovrebbero utilizzare un linguaggio standardizzato e condiviso a livello internazionale dai diversi servizi di indicizzazione. Riutilizzabili: sia i metadati, sia i dati devono essere descritti e documentati nel migliore dei modi, a garanzia della loro qualità e perché possano essere replicati e/o combinati in contesti diversi. Il trattamento dei dati dovrebbe conformarsi agli standard o ai protocolli riconosciuti dalle comunità scientifiche di riferimento. Il riutilizzo dei metadati e dei dati dovrebbe essere dichiarato con una/o più licenze aperte chiare ed accessibili. A tal proposito è possibile consultare i principi sul sito FORCE11.

[15] La Strategia è finalizzata a rendere l'UE una società aperta e inclusiva, all'interno della quale i dati potranno circolare in maniera transsettoriale, a beneficio di tutti in pieno rispetto delle norme europee, in particolare sulla tutela della vita privata e sulla protezione dei dati, sul diritto della concorrenza, sull'accesso ai dati e al loro utilizzo. Si veda di S. CORSO, *Una strategia europea per i dati, anche sanitari*, in *Responsabilità medica*, 7 marzo 2021.

[16] La Commissione europea, nella Comunicazione sulla strategia per i dati, ha evidenziato che «Nel corso degli ultimi anni le tecnologie digitali hanno trasformato l'economia e la società, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei. I dati sono un elemento centrale di tale trasformazione, che non fa che cominciare. L'innovazione guidata dai dati genererà benefici enormi per i cittadini, ad esempio tramite il miglioramento della medicina personalizzata, le nuove soluzioni di mobilità e il suo contributo al Green Deal europeo. In una società in cui è in costante aumento la quantità di dati generati dai singoli cittadini, la metodologia di raccolta e utilizzo di tali dati deve porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europei. I

l'istituzione di spazi comuni europei di dati, specifici per dominio, in cui siano garantiti a livello transfrontaliero (ed extra europeo) elevati livelli di *data security e data privacy*[17]. Inizia a prendere forma un quadro normativo finalizzato a rendere l'UE *leader* nella capacità di promuovere una società aperta e inclusiva, basata sulla disponibilità generale di dati e ad innalzare la soglia di fiducia dei cittadini nell'ambiente digitale. Nel solco tracciato dalla Strategia, il Regolamento n. 868/2022 noto come *Data Governance Act (DGA)* [18], rappresenta il primo atto normativo adottato in ambito comunitario per disciplinare la *governance* dei dati. Entrato in vigore il 23 settembre 2023, il Regolamento delinea un quadro orizzontale di principi e regole applicabili trasversalmente a diversi settori. Il riutilizzo dei dati pubblici, i servizi di intermediazione di dati e l'altruismo dei dati[19] rappresentano i tre pilastri su cui, a norma del

cittadini daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati. Allo stesso tempo, il volume crescente di dati industriali non personali e di dati pubblici in Europa, unito ai cambiamenti tecnologici riguardanti le modalità di conservazione ed elaborazione dei dati, costituirà una potenziale fonte di crescita e innovazione che è opportuno sfruttare». Si veda European Commission, *Communication from the Commission*, *cit.*

[17] Il documento richiama il pieno rispetto al GDPR, al regolamento sulla libera circolazione dei dati non personali (Regolamento (UE) 2018/1807), al regolamento sulla cybersicurezza (Regolamento (UE) 2019/881) e alla direttiva sull'apertura dei dati (Direttiva (UE) 2019/1024).

[18] Parlamento Europeo e il Consiglio dell'Unione Europea, *Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*, consultabile sul sito della Gazzetta ufficiale dell'Unione europea. Il *Data Governance Act* si sviluppa lungo quattro ben precise direttrici: il riutilizzo di determinati dati detenuti da soggetti pubblici (Capo II); l'attività di intermediazione dei dati (Capo III); la messa a disposizione dei dati per fini altruistici (Capo IV) e, non da ultimo, l'istituzione di un nuovo sistema di *governance* dei dati e di sanzioni (Capo V e Capo VI). Sul tema dell'altruismo dei dati si richiama F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Annali AISDUE*, 2021. L'autrice mette in rilievo che *"Le autorità competenti incaricate del monitoraggio e dell'attuazione del quadro di notifica per i fornitori di servizi di condivisione dei dati e per gli enti che praticano l'altruismo dei dati sono nominate dagli Stati membri (Capo V della proposta). Le autorità avranno il potere di monitorare il rispetto del regolamento stesso, di imporre sanzioni finanziarie "dissuasive" e di "richiedere la cessazione o il rinvio" della fornitura del servizio. I titolari dei diritti in questione possono presentare un reclamo all'autorità nazionale competente nei confronti di un fornitore di servizi di condivisione dei dati o di un'entità iscritta nel registro in parola. Peraltro, gli intermediari saranno sottoposti a un obbligo di notifica per accrescere la fiducia consentendo un monitoraggio sui requisiti per l'esercizio delle funzioni condotto delle autorità nazionali competenti. Relativamente alla sicurezza, la proposta indica di implementare tutte le misure, inclusa la cifratura, per impedire l'accesso ai sistemi in cui sono conservati i dati"*. Si veda ancora di E. SALERNO, *Il Data Governance Act, il nuovo Regolamento europeo per il mercato unico dei dati rischia di non essere abbastanza e favorire i grandi della tecnologia*, in *Privacy e Cybersecurity*, 26 febbraio 2021, p. 7; A. SOLA, *Primi cenni di regolazione europea nell'economia dei dati*, in *MediaLaws*, 2021, n. 3, p. 194 ss. Dalla lettura del Regolamento si evince la necessità di garantire uno sviluppo equilibrato e armonioso in tre ambiti chiave: facilitare l'accesso ai dati, in particolare quelli detenuti dal settore pubblico, rimuovendo gli ostacoli legali che ne impediscono il riutilizzo; tutelare il diritto degli utenti di condividere i dati generati dai prodotti connessi con terzi fornitori di servizi, promuovendo la concorrenza e l'innovazione; consentire alle autorità pubbliche di accedere a dati detenuti da privati in casi eccezionali, ad esempio per rispondere prontamente a emergenze, nel rispetto di specifici requisiti come la dimostrazione della necessità e l'esclusione di oneri per le PMI. Su questi specifici aspetti si veda di D. POLETTI, *Gli intermediari dei dati. Data Intermediaries, in European Journal of Privacy Law & Technologies*, 2022/1. Si veda ancora di A. TROJSI, *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *federalismi.it*, 2023, 4: 276-306. Per ciò che attiene la dottrina d'oltralpe si veda di B. CASSAR, *Gouvernance des données, répertoire IP/IT et Communication*, Dalloz, mars 2022; P MOUSSIER, *Les conséquences pour les personnes publiques du Data Governance Act,* in *International Journal of Digital and Data Law/Revue internationale de droit des données et du numérique*, 2023, 9, pp. 57-72.

[19] Sull' altruismo dei dati si veda di E. CREMONA, *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso,* in *Rivista italiana di informatica e diritto*, 2023, 5.2: pp. 111-130. Sulla condivisione dei dati per finalità di sviluppo e ricerca si veda di A. IANNUZZI, *I regolamenti intersettoriali, cit.*

DGA, deve fondarsi la condivisione dei dati (personali e non personali). Questi principi costituiranno il basamento dei successivi atti normativi per l'accesso e l'utilizzo dei dati, compresi quelli sanitari. In linea di continuità, il 3 maggio 2022 la Commissione europea, proponendosi di tradurre in realtà il diritto dei cittadini di accedere e condividere i propri dati sanitari in un contesto transfrontaliero, pubblica una proposta di Regolamento per l'istituzione dell'*European Health Data Space* (EHDS)[20]. L'intento del legislatore comunitario è di garantire ai cittadini la portabilità e il pieno diritto di accesso ai propri dati sanitari personali in modo da facilitare l'assistenza sanitaria ovunque si trovino[21], attraverso regole rigorose per l'uso di dati sanitari opportunamente anonimizzati o pseudonimizzati[22]. Quel che si prospetta, dunque, è la possibilità di predisporre una *governance* dei dati sanitari finalizzata ad abilitare nuovi modelli di cura, migliorare la prevenzione attraverso l'individuazione di percorsi sanitari mirati nonché indirizzata allo sviluppo, alla ricerca e alla definizione di *policy* governative e normative basate sull'evidenza.

Da elemento statico e conoscitivo, il dato sanitario acquisisce un valore aggiunto in forza del suo potenziale "utilizzo e riutilizzo"[23] rendendo necessario un corrispondente e proporzionale rafforzamento delle misure di tutela. È esattamente sulla base di tali presupposti che il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD) esprimono un parere

[20] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, Strasbourg, 3.5.2022 COM (2022) 197 final, consultabile sul sito dell'Unione Europea. Si veda a tal proposito di S. CORSO, *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *federalismi.it*, 10 agosto 2022. estano aperti i temi legati al consenso dell'interessato come principale presupposto per il trattamento dei dati relativi alla salute per finalità di ricerca. Il Regolamento EHDS non specifica, difatti, se il consenso del paziente debba essere obbligatorio o se sia sufficiente un meccanismo di opt-out (possibilità di opporsi all'utilizzo dei propri dati).

[21] Il Regolamento alla sezione 2 del Capo II, art. 12 prevede l'obbligo di designazione da parte di ciascuno Stato membro di un "punto di contatto nazionale per la sanità digitale" che dovrà collegarsi con gli altri "punti di contatto nazionali" designati dagli altri Stati membri attraverso la piattaforma centrale per la sanità digitale "MyHealth@EU.

[22] L'anonimizzazione è un processo che rimuove in modo definitivo e irreversibile qualsiasi collegamento tra un dato personale e l'identità della persona a cui si riferisce. Una volta anonimizzato, un dato non può più essere ricondotto al soggetto originario e perde quindi la sua natura di dato personale. Diversamente la pseudonimizzazione è una tecnica che consente di dissociare un dato personale dall'identità dell'interessato, senza però eliminare completamente questo legame. Il dato viene modificato in modo da non poter essere attribuito a una persona specifica senza l'utilizzo di informazioni aggiuntive. Queste informazioni, chiamate "chiave di pseudonimizzazione", permettono di ristabilire il collegamento originario tra il dato e l'identità dell'interessato rendendoli solo temporaneamente non attribuibili a una persona identificata o identificabile. Si veda a tal proposito di E. PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, p. 360 ss.; C. IRTI, *Personal data, non-personal data, anonymised data, pseudonymised data, de-identified data*, in R. SENIGAGLIA, C. IRTI, A. BERNES (a cura di), *Privacy and Data Protection in Software Services,* Springer, Berlino, 2022, p. 49 ss.

[23] Si veda European Commission, *Communication from the Commission*, *cit.*, all'interno della quale si precisa che "il valore dei dati risiede nel loro utilizzo e riutilizzo". La possibilità di ricavare informazioni dalla loro analisi consente di godere di indiscutibili vantaggi in termini di potere e di controllo. Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 34 ss.; S. RODOTÀ, *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2019, 1, pp. 9 ss.; A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.*, 2012, p. 135 ss.; S. ZUBOFF, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, in *Journal of Information Technology* (2015) 30, pp. 75–89.

congiunto[24], in merito alla succitata proposta di Regolamento. Le due Autorità, pur accogliendo favorevolmente l'idea di rafforzare il controllo delle persone[25] sul trattamento dei propri dati sanitari personali, pongono un freno[26] all'uso secondario[27] degli stessi richiamando una maggiore attenzione alle disposizioni del GDPR[28], a norma del quale i dati sanitari, in quanto dati particolari, devono poter beneficiare di una tutela rafforzata[29]. Pertanto, benché siano innegabili le opportunità derivanti dall'uso secondario dei dati sanitari digitali in termini di cura, ricerca e obiettivi governativi, è altrettanto evidente che tale pratica richiede di affrontare, preliminarmente, una serie di sfide e questioni cruciali, soprattutto in termini di tutela dei diritti e delle libertà dei cittadini, in un contesto in cui i dati sanitari sono preda di attacchi cibernetici,[30] anche in ragione del pregiudizio esponenziale derivante dalla paralisi dei servizi sanitari[31]. Rispetto a tale scenario di riferimento, il cauto approccio delle autorità competenti in materia di protezione dei dati personali non può che leggersi come una richiesta di maggior tutela per i diritti fondamentali dei cittadini. La prudenza indotta dal parere dell'EDPB e del GEPD è infatti legata alla vulnerabilità che contraddistingue i dati digitali, caratteristica che può avere conseguenze molto gravi, soprattutto, in contesti di sanità digitale giacché, oltre a favorire la possibilità di alterare e modificare i documenti che li trasportano generando errori diagnostici e terapeutici, può consentire anche con

[24] European Data Protection Board, *EDPB-EDPS Joint Opinion03/2022 on the Proposal for a Regulation on the European Health Data Space*, Adopted on 12 July 2022, consultabile sul sito dell'EDPB.

[25] L'articolo 3 dell'European Health Data Space contiene una lista di diritti in relazione all'uso primario dei dati sanitari elettronici, come il diritto di accesso o di ottenere una copia elettronica dei dati. Gli operatori sanitari che avranno accesso ai dati sanitari elettronici delle persone fisiche in cura presso di loro dovranno garantire che i dati sanitari elettronici delle persone assistite siano aggiornati con informazioni relative ai servizi sanitari prestati (articolo 4 proposta EHDS)

[26] Secondo EDPS e EDPB, il trattamento dei dati attraverso le applicazioni per il benessere comporta rischi reali per la *privacy,* soprattutto quando avviene un incrocio con altri dati.

[27] Il Capo IV del Regolamento sullo Spazio Europeo dei dati sanitari, dagli artt. 33 a 58, dedica ampio spazio all'*uso secondario* di dati sanitari elettronici. In particolare, l'art. 33 definisce la tipologia di dati che possono essere impiegati per le finalità specifiche individuate dall'art. 34 ed all'art. 35 elenca le finalità vietate. Sull'argomento si veda di S. CORSO, *Lo spazio europeo dei dati sanitari: la CommissioneEuropea presenta la proposta di regolamento*, in *federalismi.it*, 10 agosto 2022.

[28] Si veda a tal proposito di F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, 121; S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica,* in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. 101/2018,* Giuffrè, Milano, 2019, p. 585 e ss. Gli autori mettono in luce come sul piano pubblicistico la tutela ha ad oggetto: «interessi pubblici perseguiti da soggetti deputati istituzionalmente al raggiungimento di finalità di programmazione, gestione, valutazione e controllo dell'assistenza sanitaria».

[29] L'articolo 9 del GDPR dispone per i dati sanitari una protezione rafforzata: il criterio generale è che il trattamento di questo tipo di dati è vietato, fatte salve le eccezioni previste dalla norma.

[30] Per come si evince dal Rapporto CLUSIT 2024, consultabile sul sito dell'Associazione CLUSIT, gli attacchi cibernetici sono in crescita e i sistemi informativi sanitari restano quelli a maggior rischio di accesso indebito, alterazione, manipolazione, anche in ragione del pregiudizio esponenziale derivante dalla paralisi dei servizi sanitari. In particolare, il settore sanitario nel 2023 è il quarto più colpito dagli attacchi informatici di successo e di pubblico dominio, secondo quanto riportato in Hackmanac *Global Cyber Attacks Report* 2024.

[31] Garante per la protezione dei dati personali, *Sicurezza del dato sanitario e condivisione* - Intervento di Pasquale Stanzione – Panorama, consultabile sul sito del Garante privacy.

maggiore facilità la mappatura e con essa la ricostruzione dell'*identikit* della persona[32]. Alle molteplici incertezze si aggiungono inevitabilmente anche le perplessità derivanti dalle nuove modalità di calcolo e di analisi, dalle loro maggiori capacità di raccolta, di elaborazione e conservazione che di fatto rinnovano completamente il concetto stesso di tutela della *privacy*[33].

All'interno di uno scenario così complesso, il delicato percorso normativo non può però ignorare la volontà politica di incoraggiare un mercato comune per la condivisione dei dati (personali e non). Per tale ragione, dopo mesi di negoziati, il 15 marzo 2024 il Consiglio dell'UE e il Parlamento europeo raggiungono l'accordo [34] sul regolamento EHDS, con il precipuo scopo di contribuire in modo significativo allo sviluppo di un mercato unico anche per i servizi e i prodotti di sanità digitale. L'ecosistema dovrà, difatti, aprire nuove frontiere per la ricerca e l'innovazione, favorendo la creazione di *dataset* di dimensioni consistenti e facilitare così la conduzione di studi multicentrici su scala europea.

Nell'articolato mosaico normativo, delineato dalla Strategia Europea dei dati, il *Data Act*[35] integra il *DGA* completando il quadro regolatorio di riferimento e sancendo nuovi obblighi e specifici diritti sull'accesso ai dati. In particolare, mentre la legge sulla *governance* dei dati ha posto come obiettivo quello di aumentare la fiducia nei meccanismi volontari di condivisione, la legge sui dati fornisce specifici dettagli sull'uso e il riuso dei dati. Sulle fondamenta già gettate dal DGA inizia così a concretizzarsi, la costruzione dei "*data spaces*"[36]. Resta, tuttavia, da capire quale sarà, nelle fasi di recepimento, il livello di *compliance* al GDPR nonché agli *standard* per i processi di corretta gestione e conservazione dei dati, e, dunque, se sicurezza e integrità delle informazioni potranno essere garantite secondo un approccio totalmente *privacy by design* e *by default*[37].

---

[32] E. BRUGIOTTI, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Dirittifondamentali.it,* n.2/2013. Cfr. G. FINOCCHIARO, *Corpo digitale e informazioni nella sanità elettronica,* in *Salute e Società*, n.2/2017.

[33] Cfr. L. CALIFANO, *Come si governa la tecnologia digitale?*, in *Cultura giuridica e diritto vivente,* Vol. 8(2021), p.2.

[34] Si veda il Comunicato stampa del Consiglio dell'Unione europea 15 marzo 2024 01:10. Restano ancora oggi aperti i temi legati al consenso dell'interessato come principale base giuridica per il trattamento dei dati relativi alla salute per finalità di ricerca. Il Regolamento EHDS non specifica, difatti, se il consenso del paziente debba essere obbligatorio o se sia sufficiente un meccanismo di *opt-out* (possibilità di opporsi all'utilizzo dei propri dati).

[35] *Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 recante norme armonizzate sull'accesso e l'utilizzo equi dei dati e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (legge sui dati)* – (GU L del 22.12.2023).

[36] A tal proposito si veda di A. IANNUZZI, *I regolamenti intersettoriali, cit.*

[37] *Privacy by design* e *by default* implica la realizzazione di un ambiente digitale, che fin dalla fase di progettazione, deve essere concepito come un insieme di strutture e meccanismi che garantiscano il diritto fondamentale alla protezione dei dati personali degli utenti. L'architettura e l'organizzazione dello spazio digitale devono essere pensate e realizzate in modo da rispettare e tutelare questo principio sin dalle basi. In altre parole, la *privacy* si assume come requisito imprescindibile da incorporare fin dall'inizio della progettazione di qualsiasi sistema, servizio o applicazione digitale. Un approccio proattivo e preventivo alla tutela della privacy essenziale per garantire che i diritti e le libertà delle persone siano salvaguardati in un mondo sempre più digitalizzato e interconnesso. Solo così si può costruire un ambiente *online* affidabile, trasparente e rispettoso della dignità degli individui. Per approfondimenti si veda A. CAVOUKIAN, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian*, in S. MCGUINNESS, B.J. KOOPS, E. ASSCHER (a cura di), *Identity in the Information Society*, Volume 3, SpringerLink, pp. 247–251, (2010); J.B. KOOPS, R.E. LEENES, *Privacy*

3. Il parere del Garante Privacy su EDS

In ottemperanza ai dettami europei anche il nostro legislatore ha definito uno schema di decreto prevedendo la realizzazione dell'Ecosistema Dati Sanitari (EDS) all'interno della riforma del FSE[38] che ha però visto il parere negativo del nostro Garante Privacy. In particolare, il Garante sostiene che l'ecosistema "comporta di fatto la duplicazione di dati e documenti sanitari già presenti nel FSE e determina la costituzione della più grande banca dati sulla salute del nostro Paese". Un tale *database,* continua l'Autorità, "raccoglierebbe a livello centralizzato, senza garanzie di anonimato per gli assistiti, dati e documenti sanitari relativi a tutte le prestazioni sanitarie erogate sul territorio nazionale" [39].

Il Garante sottolinea l'esigenza di un previo parere dell'Agenzia per la Cybersicurezza Nazionale in relazione alla valutazione di adeguate misure di sicurezza per il trattamento dei dati sanitari. L'Autorità, inoltre, evidenzia alcuni profili di non conformità al GDPR. In particolare, menziona profili di contenuto (non essendovi chiarezza circa i dati trasmessi all'EDS dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria); di alimentazione (dovendosi chiarire i soggetti e le modalità di alimentazione dell'EDS); di rispetto dei principi generali legati al trattamento (il Garante riscontra carenze in termini di garanzie per gli interessati, rilevando l'impatto del mancato aggiornamento dei dati ai principi generali del trattamento dei dati personali sanciti dall' art. 5 del GDPR) e di valutazione del rischio (i trattamenti previsti nell'EDS richiedono una preventiva valutazione di impatto ai sensi dell'art. 35 del GDPR, al fine di individuare le misure idonee a tutelare i diritti e le libertà fondamentali degli interessati e garantire il rispetto dei principi generali del Regolamento. Tra i principali rischi da analizzare vi sono quelli di re-identificazione dell'interessato, di accessi abusivi illeciti, di integrità ed esattezza dei dati, di perdita e distruzione dei dati, di utilizzo per finalità non compatibili, nonché di trattamenti automatizzati con possibili ricadute sul singolo).

---

regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data protection law, in *International Review of Law, Computers & Technology* (2), p. 159-171; S. CALZOLAIO, *Digital (and privacy) by default. L'identità costituzionale dell'amministrazione digitale*, in *Giornale di storia costituzionale*, 31, I, 2016, pp. 185-20; G. BINCOLETTO, *La privacy by design. Un'analisi comparata nell'era digitale*, Aracne, Roma, 2019; A. CAVOUKIAN, S. KINGSMILL, *Privacy by Design Setting a New Standard for Privacy Certification*, Deloitte, Toronto, 2016; S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in federalismi.it, 24 (2017) pp. 1-21; F. BRAVO, *Data Management Tools and Privacy by Design and by Default*, in R. SENIGAGLIA, C. IRTI, A. BERNES (a cura di), *Privacy*, *cit.*, p. 85 ss.

[38] Decreto legge 27 gennaio 2022, n. 4, convertito con modificazioni dalla L. n. 25 del 28.03.2022, al cui art. 21 definisce le misure in materia di FSE e governo della sanità digitale, consultabile sul sito della Gazzetta Ufficiale.

[39]Garante per la protezione dei dati personali, *Parere al Ministero della Salute sullo schema di decreto da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sull'Ecosistema Dati Sanitari (EDS)* - 22 agosto 2022 [9802752], consultabile sul sito del Garante privacy.

Contestualmente, al fine di favorire e migliorare l'implementazione a livello nazionale del FSE, il Garante suggerisce una serie di correzioni su un secondo schema di decreto[40] ritenuto non pienamente conforme all'art.12 del d.l n. 179/2012 e non perfettamente allineato ai decreti del Ministero della Salute attesi ai sensi del d.l. n. 34/2020 oltre che ai requisiti e alle prescrizioni normative di cui agli articoli 6, comma 3 (sulla base giuridica e la finalità del trattamento dei dati di particolare natura) del GDPR e di cui all'articolo 2-*sexies* del Codice della privacy (sui trattamenti delle categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g) del GDPR).

L'intervento dell'Autorità è perfettamente in linea con il parere espresso dalle omologhe Autorità europee. Non mira, difatti, ad ostacolare o rallentare l'introduzione di strumenti digitali per lo sviluppo e l'innovazione dei servizi sanitari per i cittadini, piuttosto mette perentoriamente in luce l'importanza del rispetto del GDPR. Il Garante, in altri termini, richiama il legislatore ad operare un'armonizzazione dell'impianto normativo con le regole poste a tutela della *privacy* e a bilanciare, dunque, le esigenze di digitalizzazione, trasparenza e apertura con il diritto fondamentale alla protezione dei dati personali, tutelando l'individuo come utente e cittadino[41] ma ancor prima come persona.

In merito alle carenze riscontrate dal nostro Garante per ciò che attiene l'aderenza ai principi generali del trattamento dei dati personali sanciti dall'art. 5 del GDPR, è ancora una volta necessario richiamare l'importanza di un adeguato processo di gestione e conservazione delle informazioni, nonché il richiamo

[40]Garante per la protezione dei dati personali, *Parere al Ministero della Salute sullo schema di decreto, da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sul Fascicolo Sanitario Elettronico (FSE) - 22 agosto 2022 [9802729]*, consultabile sul sito del Garante privacy. In particolare, viene esaminata la gestione dei diritti degli interessati le questioni inerenti alla titolarità di alcuni trattamenti in ambito FSE (su Profilo Sanitario Sintetico, PSS, Taccuino Personale; Dossier Farmaceutico), alle informative sul trattamento prive degli elementi di trasparenza fondamentali, alla necessità di diversificazione del consenso dell'interessato in relazione alle diverse finalità del trattamento, onde correttamente alimentare la cosiddetta Anagrafe dei consensi, fino alla impostazione non conforme dei trattamenti per profilassi internazionale, governo sanitario, diagnosi, cura e riabilitazione e prevenzione. L'8 giugno 2023 sulla intervenuta modifica del decreto, il Garante ha poi espresso parere favorevole ponendo però come condizione: l'introduzione nello schema di decreto dei tempi entro cui gli interessati dovranno ricevere informazioni sul trattamento dei propri dati attraverso il FSE, l'avvio di campagne volte a comunicare agli interessati l'integrazione automatica dei propri dati con il FSE e la possibilità di opporsi. Il Garante ha inoltre richiamato l'attenzione del legislatore sulla necessità che le disposizioni attuative della medicina predittiva, dell'interconnessione dei sistemi sanitari e delle funzionalità del Sistema TS, nonché la disciplina della telemedicina, nella parte in cui prevedono la condivisione di dati e documenti con il FSE, siano conformi alla disciplina sulla protezione dei dati personali e coerenti con l'assetto e le misure di garanzia individuate nello schema di decreto sul FSE. Manca inoltre, sempre a parere del Garante, la DPIA (da allegarsi al decreto) sui rischi che l'Autorità aveva individuato ai fini dell'*assessment* in sede di Valutazione di Impatto (dal rischio di re identificazione dell'interessato a quello di accesso abusivo e illecito ai dati; dal rischio per l'integrità, esattezza e aggiornamento dei dati del FSE a quello di perdita e distruzione dei dati, utilizzo dei dati per finalità non compatibili; fino ai rischi connessi all'utilizzo delle tecnologie basate su logiche algoritmiche e sull'Intelligenza Artificiale, con i trattamenti automatizzati che possono avere ricadute sul singolo interessato. Il Parere è consultabile sul sito del Garante privacy.

[41] F. FAINI, *Governo dei dati personali nell'impiego dell'intelligenza artificiale e della blockchain da parte della sanità pubblica,* in *Diritto Mercato Tecnologia*, 2023 p. 34.

alle regole di *data storage* poste dal GDPR[42] per garantire completezza, esattezza, aggiornamento e sicurezza dei dati personali lungo tutto il loro ciclo di vita[43].

Solo attraverso un approccio olistico e sistemico, che tenga conto anche di tutti gli aspetti legati alla gestione e conservazione delle informazioni, in linea con gli *standard* e le *best practice* internazionali sarà possibile realizzare una *governance* dei dati[44] *compliance* al GDPR anche in prospettiva di un *data space* sanitario.

4. Verso una possibile regolamentazione in materia di gestione e conservazione dei dati

Secondo la normativa vigente i dati personali e non devono essere conservati per lo stesso periodo temporale stabilito per il documento clinico in cui sono contenuti[45], rispettando il principio di limitazione della conservazione dettato dall'articolo 5, paragrafo 1 lettera e) del GDPR[46] che impone di conservare i

[42] V. PAGNANELLI, *Conservazione dei dati e sovranità digitale.*, *cit.,* pp. 11-26. L'autrice fa espresso riferimento al GDPR e ai principi di data storage dei dati personali che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati), esatti e, se necessario, aggiornati (principio di esattezza), conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di limitazione della conservazione), e trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di integrità e riservatezza).

[43] La completezza dei dati implica la raccolta di tutte le informazioni necessarie e pertinenti rispetto alle finalità del trattamento, evitando lacune o omissioni. L'esattezza, invece, presuppone l'adozione di accorgimenti per prevenire errori o inesattezze, attraverso processi di verifica e correzione. L'aggiornamento richiede l'implementazione di meccanismi che consentano di mantenere le informazioni costantemente allineate con la realtà cui si riferiscono. Infine, la sicurezza impone l'adozione di misure tecniche e organizzative adeguate a proteggere i dati da trattamenti non autorizzati o illeciti, nonché da perdita, distruzione o danno accidentale.

[44] Si veda a tal proposito di E. SORRENTINO, A. F. SPAGNUOLO, *Dati sanitari: aperti, accessibili e riutilizzabili*, in *MediaLaws*, 2022, pp. 170-182. Nel testo si mette in risalto l'importanza di una *governance* che valorizzi la condivisione dei dati pubblici, gestiti interamente in digitale, in maniera aperta e in aderenza a principi e standard condivisi.

[45] I riferimenti sono:

1. la circolare del Ministero della sanità del 19 dicembre 1986 n. 900;
2. l'articolo 5 del d.m. del 18 febbraio 1982;
3. l'articolo 4 del d.m. del 14 febbraio 1997.

Nella Circolare dicembre 1986 n. 900, "*le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario*". Deve invece essere conservata, a cura del medico visitatore, per almeno cinque anni, la documentazione inerente agli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica (art. 5, d.m. 18/02/1982). La documentazione iconografica radiologica deve essere conservata per un periodo non inferiore a dieci anni (art. 4, d.m. 14 febbraio 1997). Più complessa è l'individuazione del tempi di conservazione per alcuni documenti sanitari per i quali non ci sono indicazioni in disposizioni normative, come, ad esempio, accade per le cartelle cliniche di strutture private non convenzionate; si deve, quindi far riferimento al Regolamento UE 2016/679.In questo caso, il titolare del trattamento, in virtù del principio di responsabilizzazione previsto per tutti i trattamenti, dovrà individuare tale periodo in modo che i dati siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati (principio di limitazione della conservazione, art. 5, par. 1, lett. e del Regolamento) e indicare tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato ai sensi dell'art 13, par.2, lett. a), GDPR.

[46] Il GDPR all'art. 5, paragrafo 1, lettera e) detta il principio di limitazione della conservazione: «I dati sono […] conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati […]». Agli artt. 13 par. 2 lett. a) e 14 par. 2 lett. a) del GDPR si

dati personali per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti, salvo esigenze di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

All'interno del panorama nazionale, non sono tuttavia rinvenibili disposizioni organiche che specifichino chiaramente, così come previsto per i documenti, le modalità e/o processi grazie ai quali anche ai dati si possa garantire, autenticità, integrità, affidabilità, leggibilità, validità legale e reperibilità nel tempo attraverso un corretto processo di conservazione[47].

recita che il Titolare del trattamento, nel rendere l'informativa all'interessato, deve indicare anche il periodo di conservazione dei dati oppure, se ciò non è possibile, quali sono i criteri utilizzati per determinare tale periodo; si tratta quindi di una informazione che è necessario fornire prima che il trattamento abbia luogo. Il Considerando 39, art. 5 lett. e) disciplina che: "i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica". Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario […]. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. In termini di *data retention* la conservazione è consentita fino a quando non si sono esaurite le finalità per le quali il dato stesso è stato raccolto o altrimenti trattato (art. 17 e Considerando 65 del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali).

[47]Il CAD all'art. 20, comma 5-bis richiama gli obblighi di conservazione e di esibizione di documenti informatici, precisando che questi si intendono soddisfatti a tutti gli effetti di legge se le procedure utilizzate sono conformi alle "*Linee guida sulla formazione, gestione e conservazione dei documenti informatic*i" (d'ora in poi Linee guida) emanate il 10 settembre 2020 dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'ex art. 71 del CAD e successivamente modificate a maggio 2021. Il CAD ha subito modifiche e integrazioni, apportate (in ordine cronologico): dal d.lgs. 26 agosto 2016, n. 179; dal d.lgs.13 dicembre 2017, n. 217; dal d.l. 28 settembre 2018, n. 109, convertito con modificazioni dalla Legge 16 novembre 2018, n. 130; dal d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12; dalla Legge 30 dicembre 2018, n. 145 e, infine, dal d.l. 26 ottobre 2019, n. 124. Le nuove Linee guida dell'AgID aggiornano le attuali regole tecniche in base all'art. 71 del CAD. Esse, inoltre, abrogano il d.p.c.m. 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici", abrogano (in parte per la sezione sulle Regole tecniche per il protocollo informatico) il d.p.c.m. 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione", e uniformano la normativa in materia attraverso la creazione di un testo unico di base per la formazione, gestione e conservazione di tutti i documenti informatici. Il Glossario (Allegato1) delle Linee Guida AgID definisce la 'conservazione' come 'l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti'.

Se, però, analizziamo la normativa di riferimento sugli *open data*[48] e i recenti sviluppi in tema di principi FAIR[49], si potrebbe ipotizzare un'interpretazione estensiva di tali percorsi anche ai dati sanitari ed iniziare a configurare una politica di corretta gestione e conservazione che vada ad aumentare significativamente la sicurezza dei dati, minimizzando il rischio di violazioni. In altri termini, applicare i principi *open data* e FAIR ai dati sanitari, in una prospettiva di completa apertura e condivisione, potrebbe risultare funzionale all'implementazione di una solida politica di conservazione, aumentando al contempo la valorizzazione di questa preziosa risorsa informativa nonché i livelli di sicurezza.

È la natura pubblica del patrimonio informativo che eleva i dati al rango di bene comune imponendo che siano resi aperti, fruibili e disponibili[50]. Questo principio è sancito dalla sopracitata Strategia Europea sui Dati e dalla Direttiva (UE) 2019/1024 cosiddetta Direttiva *Open Data*[51] che introduce, al Considerando 16, il concetto di "apertura fin dalla progettazione e per impostazione predefinita"[52], richiamato altresì

[48] Il quadro normativo di riferimento per la disciplina degli *open data* è dato dal CAD che al Capo V detta le disposizioni riguardanti la disponibilità, la fruibilità e la sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni. In particolare, l'art. 50 si occupa della disponibilità e fruibilità dei dati della pubblica amministrazione, mentre l'art. 52 riguarda l'accesso telematico ai dati e ai documenti delle amministrazioni pubbliche introducendo il principio dell'*open by default*, in base al quale "i dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza […], si intendono rilasciati come dati di tipo aperto. L'art. 68 fornisce le definizioni di formato di tipo aperto e di dati di tipo aperto. Per una panoramica sulla letteratura scientifica di riferimento si veda di B. COCCAGNA, G. ZICCARDI, *Open data, trasparenza elettronica e codice aperto*, in M. DURANTE, U. PAGALLO (a cura di), *Manuale di informatica giuridica e di diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, p. 403 ss.; V. PAGNANELLI, *Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, in *Giornale di storia cost.*, 2016, vol. 31, p. 205; F. SCIACCHITANO, *Disciplina e utilizzo degli Open Data in Italia*, in *MediaLaws*, 2018, pp. 281- 314.

[49] I principi FAIR sono stati elaborati nel 2014 per ottimizzare la riutilizzabilità dei dati della ricerca. Essi rappresentano un insieme di linee guida e migliori pratiche sviluppate per garantire che i dati, o qualsiasi oggetto digitale, siano *Findable*/Rintracciabili, *Accessible*/Accessibili, *Interoperable*/Interoperabili e *Reusable*/Riutilizzabili. Rintracciabili: per poter rendere i dati riutilizzabili occorre che siano per prima cosa rintracciabili dagli esseri umani e dalle macchine. Il recupero automatico e affidabile di set di dati dipende dagli identificatori persistenti (PID) utilizzati, quali ad esempio DOI, *Handle* o URN, e dai metadati descrittivi attribuiti ai dati, che devono essere registrati in "cataloghi" o in *repository* indicizzabili anche dalle macchine. Accessibili: i dati o almeno i loro metadati devono poter essere accessibili dagli esseri umani e dalle macchine anche attraverso sistemi di autenticazione e autorizzazione (non è necessario che i dati depositati siano open access) mediante l'uso di protocolli standard. I dati e i loro metadati devono essere depositati in archivi o repository che li rendano possibilmente persistenti nel tempo e rintracciabili in rete. Almeno i metadati dovrebbero rimanere sempre disponibili anche quando i dati non sono in open access. Interoperabili: i dati devono poter essere combinati e utilizzati insieme con altri dati o strumenti. Il formato dei dati deve pertanto essere aperto e interpretabile da vari strumenti, compresi altre basi di dati. Il concetto di interoperabilità si applica anche ai metadati. Ad esempio, i metadati dovrebbero utilizzare un linguaggio standardizzato e condiviso a livello internazionale dai diversi servizi di indicizzazione. Riutilizzabili: sia i metadati, sia i dati devono essere descritti e documentati nel migliore dei modi, a garanzia della loro qualità e perché possano essere replicati e/o combinati in contesti diversi. Il trattamento dei dati dovrebbe conformarsi agli standard o ai protocolli riconosciuti dalle comunità scientifiche di riferimento. Il riutilizzo dei metadati e dei dati dovrebbe essere dichiarato con una/o più licenze aperte chiare ed accessibili. A tal proposito è possibile consultare i principi sul sito FORCE11.

[50] E. SORRENTINO, A. F. SPAGNUOLO, *cit.*, 2022, si veda ancora A. F. SPAGNUOLO, E. SORRENTINO, *Open data per l'e-democracy*, in *Rivista italiana di informatica e diritto*, 4, 1 (mag. 2022), pp. 273-282.

[51] La Direttiva è consultabile in Gazzetta ufficiale dell'Unione europea.

[52] Il Considerando 16 della *Direttiva*, *Ibid.*, chiarisce che "il concetto di apertura dei dati si intende generalmente riferito a dati in formati aperti che possono essere utilizzati, riutilizzati e condivisi liberamente da chiunque e per qualsiasi finalità", funzionali all'ampia "disponibilità (...) dell'informazione del settore pubblico a fini privati o commerciali, con

anche dal Considerando 9 del *DGA*[53]. I principi *open data by design* e *by default* guidano anche il Piano Triennale per l'Informatica 2024/2026[54] indirizzando, in tale direzione, anche il nostro panorama normativo nazionale. Questo orientamento si arricchisce ulteriormente con la stesura delle Linee Guida *Open Data*[55], un documento che evidenzia espressamente la stretta correlazione tra le politiche di apertura e le politiche di conservazione dei dati. Le linee Guida sottolineano, esplicitamente l'importanza di adottare *standard* di riferimento e di rispettare i principi FAIR per garantire l'interoperabilità, la reperibilità, l'accessibilità e la riutilizzabilità dei dati e metadati in linea con il modello OAIS[56].

Se il quadro normativo internazionale e sovranazionale sta evolvendo verso politiche di maggiore apertura e condivisione dei dati pubblici, gli sviluppi in merito all'apertura dei dati nel campo della ricerca scientifica[57] evidenziano espressamente come la condivisione del patrimonio informativo possa ampliare l'orizzonte delle conoscenze e migliorare la qualità della ricerca.

Nel 2018 la Commissione europea, nell'ambito del *framework H2020*, definisce i progetti denominati *Open Research Data Pilot* (ORD)[58] con l'obiettivo di rendere i dati di ricerca aperti, "*as open as possible, as closed as necessary*". Il progetto pilota, già esteso a tutte le aree tematiche di *Horizon 2020*, a partire dal *Work programme* 2017[59] presenta due pilastri principali: sviluppare un piano di gestione dei dati (*Data Management Plan*[60]) e, se possibile, fornire l'accesso aperto e il riutilizzo dei dati digitali della ricerca secondo i principi FAIR.

---

vincoli minimi o in assenza di ogni vincolo di natura legale, tecnica o finanziaria", per favorire "la circolazione di informazioni non solo per gli operatori economici ma principalmente per il pubblico" e "promuovere l'impegno sociale nonché avviare e favorire lo sviluppo di nuovi servizi basati su modi innovativi di combinare tali informazioni tra loro e di usarle". Il considerando precisa, inoltre, che nell'attuare il principio di apertura sin dalla progettazione e per impostazione predefinita, gli Stati "dovrebbero (...) assicurare la protezione dei dati personali anche là dove le informazioni in un insieme di dati individuale possono non presentare un rischio di identificazione o di individuazione di una persona fisica, ma possono, se associate ad altre informazioni disponibili, comportare un siffatto rischio".

[53] Il Considerando n. 9 del Regolamento (UE) 2022/868 nello specifico stabilisce: "Al fine di facilitare la protezione dei dati personali e riservati e accelerare la messa a disposizione di tali dati per il riutilizzo ai sensi del presente regolamento, gli Stati membri dovrebbero incoraggiare gli enti pubblici a creare e mettere a disposizione i dati in conformità del principio dell' «apertura fin dalla progettazione e per impostazione predefinita» di cui all'articolo 5, paragrafo 2, della direttiva (UE) 2019/1024 e promuovere la creazione e la raccolta di dati in formati e strutture che facilitino l'anonimizzazione in tal senso".

[54] Agenzia per l'Italia Digitale, *Piano Triennale per l'informatica*, consultabile sul sito dell'Agenzia per l'Italia Digitale.

[55] Agenzia per l'Italia Digitale, *Linee Guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*, versione 1.0, consultabile sul sito dell'Agenzia per l'Italia Digitale.

[56] L'*Open Archival Information System* è un modello concettuale per la conservazione digitale. Online è possibile consultare la versione 2014, pubblicata dal Consultative Committee for Space Data Systems (CCSDS).

[57] Sull'approccio alla scienza aperta in riferimento al settore sanitario si veda: P. AURUCCI, *Legal issues in regulating observational studies: the impact of the GDPR on Italian biomedical research*, in *European Data Protection Law Review*, 5, 2019, 197-208.

[58] Unione Europea, *Open Research Data (ORD) — l'adozione nell'ambito di Orizzonte 2020*, Aggiornato: 19.04.2018, consultabile sul sito dell' Unione Europea.

[59] European Commission, *Data management*, consultabile sul sito dell'European Commission.

[60] Il Data Management Plan (DMP) è lo strumento chiave per pianificare la conservazione e la sostenibilità a lungo termine dei dati assicurandone l'accessibilità, l'interoperabilità e il riutilizzo secondo i principi FAIR. Da tempo obbligatorio negli ambienti scientifici anglosassoni, il DMP è obbligatorio anche nei progetti Horizion 2020 così per

Su questi presupposti si sviluppa il progetto *FAIR4Health* che, riunendo competenze in vari settori (ricerca sanitaria, gestione dei dati, informatica medica e legale), arriva a promuovere l'applicazione dei principi FAIR anche ai dati della ricerca clinica europea[61]. Nel campo della ricerca scientifica si consolida la stretta correlazione tra apertura, condivisione e una solida politica di conservazione. Recentemente, si è iniziato ad ipotizzare l'associazione dei principi FAIR ai principi TRUST[62] *(Transparency, Responsibility, User Focus, Sustainability, Tecnology)* per l'implementazione di *repository* in grado di conservare i dati di ricerca a lungo termine[63]. L'idea è che l'utilizzo dei principi FAIR sin dalla progettazione del sistema di raccolta (FAIR *by design*) e la valutazione di quali dati riutilizzare sulla base di un'analisi dei metadati[64] associati ad un set di dati personali identificati attraverso identificatori univoci e persistenti rappresenta la soluzione per rendere i dati facilmente identificabili e rintracciabili *(Findable)*[65], accessibili in modo aperto e ben descritti (*Accessible*) oltre che interoperabili (*Interoperable)* e riutilizzabili (*Reusable*).

come si evince dalle Linee Guida per il trattamento dei dati personali nei progetti H2020 "*Project management e rendicontazione*" che definiscono il DPM un documento formale che indica nel dettaglio come devono essere gestiti i dati sia durante un progetto di ricerca che dopo il suo completamento. Scopo del DMP è fornire informazioni sulla Data Management Policy che si intende adottare per rendere disponibili i dati della ricerca in Open Access, ovvero una analisi e una descrizione dei dati stessi, degli standard, delle tecniche e dei workflow che li caratterizzano e delle politiche di accesso, riuso e preservazione. Le Linee Guida sono consultabili sul sito APRE. Per la compilazione esistono linee guida consolidate e strumenti online, come ad esempio quelli del Digital Curation Centre [DCC, 2013].

[61] L'obiettivo principale del progetto è quello di trasformare i dati grezzi in dati FAIR, rendendoli reperibili, accessibili, interoperabili e riutilizzabili. Per affrontare le sfide del progetto, è stata condotta un'analisi preliminare dei requisiti legali, etici e tecnici per la condivisione e il riutilizzo dei dati sanitari. Successivamente, sono state raccolte specifiche tecniche e requisiti per lo sviluppo, garantendo che la soluzione tecnica rispettasse i principi FAIR e l'architettura tecnologica. Le specifiche possono essere consultate sul sito FAIR4Health.

[62] Rilasciati il 14 maggio 2020, su Scientific Data e risultanti da mesi di consultazione e discussione della comunità di ricerca nell'ambito della Research Data Alliance (RDA), i principi TRUST sono stati sviluppati al fine di facilitare l'adozione di best practices per la gestione dei repositories. Il primo giugno 2020 l'Open Preservation Foundation (OPF), organismo tra i più attivi in contesto europeo per l'elaborazione di strumenti e linee guida per la conservazione digitale, ha accolto questo set di principi, consultabili sul sito dell'Open Preservation Foundation. Si veda sull'argomento di D. LIN, J. CRABTREE, I. DILLO et al., *The TRUST Principles for digital repositories*, in *Sci Data* **7**, p. 144 (2020) https://doi.org/10.1038/s41597-020-0486-7; F. MARTI, *Digital preservation "FAIRness" and "TRUSTworthiness": i principi FAIR e TRUST nei contesti di conservazione digitale.* Raccolta degli abstract estesi della 10ª conferenza nazionale *AIUCD 2021-DH* per la società: eguaglianza, partecipazione, diritti e valori nell'era digitale. Volume degli abstract estesi della 10a conferenza nazionale. *AIUCD-Ass. per l'informatica umanistica e la cultura digitale*, 2021. Si veda ancora di C. BETTELLA, Y. CARRER, G. TURETTA, *La valutazione FAIRness di un archivio digitale certificato: tra principi teorici e azioni pratiche*, in *DigItalia*, *17*(1), pp. 113-133.

[63] Questo concetto è definito dal modello OAIS come un arco di tempo abbastanza ampio perché l'evoluzione tecnologica possa determinare un impatto sulle risorse digitali, oltre che sulla comunità di riferimento.

[64] E.T. INAU, J. SACK, D. WALTEMATH, A. A. ZELEKE, *Initiatives, Concepts, and Implementation Practices of FAIR (Findable, Accessible, Interoperable, and Reusable) Data Principles in Health Data Stewardship Practice: Protocol for a Scoping Review, JMIR Research Protocols,* 2021 Feb 2;10(2): e22505.

[65] Il principio FAIR "*Findable*" si collega con lo standard OAIS poiché entrambi sottolineano l'importanza di rendere i dati facilmente rintracciabili. OAIS fornisce linee guida per l'organizzazione e l'indicizzazione dei dati in modo che siano facilmente individuabili all'interno di un archivio. L'accessibilità dei dati è un punto chiave sia nei principi FAIR che nello standard OAIS. Mentre FAIR si concentra sull'accesso aperto ai dati, OAIS definisce protocolli per garantire che i dati siano accessibili nel tempo, anche attraverso la descrizione dei servizi di accesso. L'interoperabilità dei dati è promossa sia dai principi FAIR che da OAIS. FAIR enfatizza la necessità che i dati siano strutturati in modo da poter essere combinati con altri dataset, mentre OAIS stabilisce standard per garantire che i dati siano leggibili e utilizzabili a lungo termine. Il concetto di riutilizzabilità dei dati è centrale sia nei principi FAIR che nello standard OAIS. FAIR

In parallelo, un sistema di *repository* TRUST *by design* accresce la fiducia degli utenti fornendo informazioni chiare sui contenuti, sui servizi e sulle condizioni d'uso del repository (*Transparency*), rispettando gli standard di metadati e curatela attraverso servizi di accesso e gestione di diritti e sicurezza (*Responsibility*), rispondendo ai bisogni degli utenti con strumenti più semplici di ricerca, esplorazione e comprensione dei dati (*User Focus*), assicurando l'accesso continuo con una gestione efficace delle emergenze, dei rischi, dei finanziamenti e della *governance* per la conservazione a lungo termine (*Sustainability*) e garantendo l'affidabilità dell'infrastruttura tecnica del *repository* con tecnologie sicure e di qualità (*Technology*). I principi FAIR e TRUST, in altri termini, garantiscono una corretta gestione e conservazione dei dati nel lungo termine attraverso l'implementazione di *repository* funzionali e durevoli nel tempo[66] all'interno dei quali anche i dati sanitari se trattati in forma anonima possono essere liberamente condivisibili per l'uso secondario senza che ciò presenti rischi per la sicurezza degli individui[67].

5. Conclusioni

I dati sanitari oggi rappresentano informazioni preziose, ma se vogliamo che lo siano soprattutto per finalità di cura, di ricerca o per esigenze di sanità pubblica devono essere correttamente gestiti e conservati nel pieno rispetto delle *policy* in materia di *privacy* e sicurezza. Tale assioma può trovare la sua massima esplicazione all'interno di un quadro regolatorio armonizzato, in cui il diritto sia integrato, in via preventiva, nella tecnologia, contemplando clausole, misure correttive e strumenti rimediali proattivi e reattivi[68], anche grazie ad una puntuale analisi dei rischi. In tal senso sarebbe auspicabile che la questione sulla conservazione dei dati andasse oltre l'esclusivo concetto di *data retention* e, per una maggiore completezza tecnico normativa, rientrasse anche nel paradigma della *data preservation*. In altri termini,

promuove la creazione di metadati ricchi per facilitare il riutilizzo dei dati, mentre OAIS si concentra sulla conservazione a lungo termine dei dati in modo che possano essere recuperati e utilizzati anche in futuro. A tal proposito è d'uopo evidenziare che il modello OAIS non fa riferimento esplicito ai documenti ma piuttosto all'importanza di trattare le informazioni come entità che richiedono una conservazione accurata e documentata per garantirne l'integrità e l'affidabilità nel tempo. L'OAIS rimarca, difatti, la necessità di conservare informazioni che devono essere gestite in modo appropriato ed essere oggetto di regolamentazione e pianificazione. Lo standard «si propone come quadro concettuale unitario per descrivere oggetti, processi, strategie e tecniche finalizzati alla conservazione digitale a lungo termine, nonché per comprendere le loro reciproche relazioni e per analizzare e confrontare soluzioni conservative diverse. Il modello si basa su un'idea dinamica della conservazione, intesa come processo permanente e mai concluso di monitoraggio del contesto in cui sono immersi gli oggetti; e disegna una complessa architettura di funzioni e oggetti informativi fondata sull'individuazione delle risorse necessarie per ricostruire il significato degli oggetti, assumendo il bit come unità minima del sistema concettuale». Si veda di G. MICHETTI, *Il modello OAIS*, in *DigItalia*, 3(1), pp. 32–49. Recuperato da https://digitalia.cultura.gov.it/article/view/441.

[66] F. MARTI, *Digital preservation" FAIRness", cit.*; M. BOECKHOUT, G. A. ZIELHUIS, A. L. BREDENOORD, *The FAIR guiding principles for data stewardship: fair enough?,* in *European Journal of Human Genetics,* 26(7), 2018, p. 931 ss., nature.com; A. F. SPAGNUOLO, E. SORRENTINO, *Open data, cit.*

[67] O. GRABER-SOUDRY, T. MINSSEN, D. NILSSON, M. CORRALES, J. WESTED, B. ILLIEN, (2021), *Legal interoperability and the FAIR data principles*, *An X-officio study commissioned by the EOSC FAIR Working Group*. EOSC Secretariat & X-officio.

[68] F. FAINI, *Governo dei dati*, *cit.*, p. 36.

partendo dai contesti di produzione e di gestione, i dati dovrebbero essere formati e, dunque, trattati in maniera adeguata e in funzione della loro conservazione, avendo chiaro l'obiettivo di preservarne nel tempo anche le caratteristiche di integrità, autenticità e accuratezza. L'ideale sarebbe la progettazione di sistemi nonché la definizione di procedure e processi affidabili attraverso i quali i dati possano essere gestiti all'interno di file contenitori corredati da metadati che li rendano autoconsistenti e indipendenti dall'ambiente di produzione[69]. Siamo ancora distanti dal poter prefigurare l'implementazione di soluzioni totalmente *open* per i dati particolari ma l'obiettivo non può che essere quello di accelerare il passo verso una completa trasformazione digitale in cui anche i dati sanitari possano essere considerati beni comuni aperti e interoperabili.

6. Riconoscimenti

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambe le Autrici ed è stato parzialmente realizzato nell'ambito delle attività del progetto "SEcurity and RIghts in the CyberSpace – SERICS (PE00000014)" - Piano Nazionale di Ripresa e Resilienza MUR finanziato dall'Unione Europea – NextGenerationEU, CUP B53C22003950001.

[69] P. A. MARZOTTI, *Metadata profiles for interoperability. The E-ARK specifications for e-archiving*, in *JLIS.it* 12, 3 (September 2021), pp. 105−118.