Università di Foggia

Corso di Dottorato in
Diritto e Sicurezza
XXXVIII ciclo

European Health Data Space: interoperabilità, sicurezza e tutela dei diritti.

Analisi delle sfide regolatorie del nuovo Spazio Europeo dei Dati Sanitari.

Tutor
Chiar.mo Prof. Onofrio Troiano

Dottoranda
Dott.ssa Miriam Incoronata
Nigro Di Gregorio

Firmato digitalmente da:
Onofrio Troiano
Data: 05/01/2026 20:48:53

Co-tutor

Anno Accademico 2024/2025

MIRIAM INCORONATA NIGRO DI GREGORIO

European Health Data Space: interoperabilità, sicurezza e tutela dei diritti.
Analisi delle sfide regolatorie del nuovo Spazio Europeo dei Dati Sanitari.

Indice

Introduzione

Il rapido avanzamento scientifico, la crescente digitalizzazione dei sistemi sanitari e le esigenze emerse durante la recente crisi pandemica costituiscono il contesto nel quale si è inserita la proposta della Commissione Europea relativa allo *European Health Data Space* (EHDS) che ha dato vita al Regolamento pubblicato nella Gazzetta ufficiale dell'Unione europea il 5 marzo 2025. Si tratta del primo spazio dati comune dell'Unione dedicato alla sanità, destinato a divenire un pilastro dell'Unione Europea della Salute.

Il regolamento definisce un quadro armonizzato per l'uso, lo scambio e il riutilizzo sicuro dei dati sanitari elettronici, con l'obiettivo di garantire interoperabilità, promuovere l'innovazione e favorire il buon funzionamento del mercato interno.

L'EHDS mira a rafforzare i diritti dei cittadini, assicurando accesso, controllo e condivisione dei propri dati sanitari anche oltre i confini nazionali, nonché a consentire il riutilizzo dei dati per finalità di ricerca, innovazione, politiche pubbliche e attività regolatorie.

Il regolamento integra i principali quadri normativi europei in materia di dati, tra cui il GDPR, prevedendo ulteriori tutele specifiche per il settore sanitario.

L'uso primario dei dati sarà orientato a garantire maggiore controllo ai pazienti, mentre l'uso secondario sarà subordinato a permessi rilasciati da enti dedicati e limitato a finalità chiaramente definite e prettamente annesse al settore della ricerca. L'elaborazione dei dati prevede l'elaborazione degli stessi in ambienti sicuri, nel rispetto dei più elevati standard di *privacy* e *cybersicurezza*, con divieti di ri-identificazione.

L'attuazione dell'EHDS prevede una pianificazione basata su una tempistica graduale: l'entrata in vigore è avvenuta nel 2025, con la successiva adozione degli atti attuativi entro il 2027 e l'avvio progressivo dello scambio transfrontaliero dei dati tra il 2029 e il 2035[*].

[*] Le informazioni relative al Regolamento sullo Spazio europeo dei dati sanitari sono fornite dal sito ufficiale dell'Unione Europea. (https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_it)

Le aspettative in termini di benefici sono significative: si prevede un miglioramento dell'efficienza dei sistemi sanitari, un rafforzamento della ricerca scientifica basata su dati di qualità e un impulso allo sviluppo del mercato europeo della salute digitale.

Nonostante le potenzialità, l'EHDS solleva rilevanti interrogativi in ordine alla tutela dei diritti fondamentali e alla sicurezza dei dati sanitari, considerata la particolare sensibilità delle informazioni trattate. La realizzazione effettiva degli obiettivi del regolamento richiede una collaborazione coordinata tra gli Stati membri, senza la quale il progetto rischierebbe di perdere efficacia.

Alla luce di quanto esposto, occorre interrogarsi se l'EHDS rappresenti un reale strumento di efficientamento del sistema sanitario europeo o un progetto di difficile attuazione. L'analisi che segue si propone di esaminare il complesso equilibrio tra diritto alla salute, progresso della ricerca medica e garanzie di sicurezza nella circolazione dei dati sanitari.

CAPITOLO I

L'INTEROPERABILITÀ NEL SISTEMA SANITARIO: L'UTILIZZO DELL'INFRASTRUTTURA NAZIONALE PER L'INTEROPERABILITÀ DEL FASCICOLO SANITARIO ELETTRONICO.

SOMMARIO: 1. La piattaforma digitale per l'efficienza dei servizi sanitari pubblici. – 2. Sanità digitale: integrazione, connessione e sviluppo. – 3. L'Infrastruttura Nazionale per l'Interoperabilità del Fascicolo Sanitario Elettronico. – 4. Continuità digitale dell'informazione sanitaria.

1. La piattaforma digitale per l'efficienza dei servizi sanitari pubblici.

L'interoperabilità è una proprietà dei sistemi informativi che consente a diverse piattaforme, attraverso apposite interfacce, di comunicare e scambiarsi dati in modo automatico, permettendo l'integrazione e la cooperazione tra sistemi differenti, rendendo possibile la condivisione delle informazioni[1]. Il suo utilizzo all'interno del sistema amministrativo trova fondamento nell'articolo 117, secondo comma, lett. r), della Costituzione, nella parte in cui attribuisce allo Stato la competenza legislativa esclusiva del "*coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale*"[2]. Questa previsione evidenzia la volontà costituzionale di promuovere un sistema informativo integrato e coerente, la cui realizzazione, oggi, si concretizza soprattutto attraverso lo scambio di dati in formato digitale[3].

---

[1] «*interoperabilità: caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi*.»: art. 1, comma 1, lettera d), d.lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale.

[2] «*Lo Stato ha legislazione esclusiva nelle seguenti materie: [...] r) pesi, misure e determinazione del tempo; coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale; opere dell'ingegno*;»: art. 117, comma 2, Costituzione.
Sul punto, v. G. C. FERONI, *Sanità digitale e assetti istituzionali. Una lettura costituzionalistica*, in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, G. C. FERONI, (a cura di) Bologna, 2022, 16 ss.

[3] M. MAGGIOLINI, *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari*, in *Rivista scientifica trimestrale di diritto amministrativo*, 2025, 389, 390, 391, 392 e 393.

Non a caso, il parametro utilizzato per la valutazione di un efficace operato della Pubblica Amministrazione è collegato alla semplificazione dell'attività amministrativa, attuata grazie alla circolazione delle informazioni correlate ai servizi erogati; i *database* di interesse nazionale rappresentano un sistema che considera il multilivello istituzionale e assicura l'utilizzo delle informazioni[4].

L'interoperabilità del dato viene attuata attraverso soluzioni tecnologiche dedicate, che assicurano lo scambio delle informazioni. Il loro utilizzo efficace è subordinato all'adozione di strumenti adeguati, ma anche alla regolamentazione degli stessi, così da assicurare un inquadramento normativo idoneo a prevenire eventuali abusi.

I dati immagazzinati e usati dalla Pubblica Amministrazione contengono numerose informazioni sensibili per le quali è indispensabile l'adozione di adeguate garanzie che ne promuovano un corretto utilizzo. Tale aspetto rileva in considerazione del fatto che la semplice conservazione del dato è stata superata da innumerevoli possibilità di utilizzo connesse, che accantonano l'individualità del soggetto a cui appartengono[5].

L'emergente rilevanza del concetto di interoperabilità trova conferma nelle "*Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni*"[6], che individuano le tecnologie e gli *standard* che le pubbliche amministrazioni sono tenute a considerare nella progettazione e nello sviluppo dei propri sistemi informatici, al fine di garantire l'integrazione e il coordinamento informativo e informatico dei dati[7].

---

[4] «*I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico*.»: art. 50, comma 1, d.lgs. 7 marzo 2005, n. 82.

[5] Per un'ampia riflessione relativa alle possibilità di utilizzo dei dati personali, con particolare riguardo alla patrimonializzazione degli stessi, v. N. PICA, *Una lettura giuspubblicistica del dibattito civilistico sulla patrimonializzazione dei dati personali,* in *Rivista di diritto amministrativo*, 2021, 497 ss.

[6] *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni,* Agenzia per l'Italia digitale, Versione 1.2, 2023, emanate ai sensi dell'art. 71, d. lgs. 7 marzo 2005, n. 82.

[7] Contribuiscono alla definizione del modello di interoperabilità delle pubbliche amministrazioni anche le *Linee Guida Tecnologie e standard per la sicurezza*

Tale coordinamento deve avvenire non solo tra le amministrazioni centrali, regionali e locali, ma anche con i sistemi dell'Unione Europea, i gestori di servizi pubblici e i soggetti privati coinvolti[8].

Anche le iniziative relative alla promozione di una Pubblica Amministrazione digitale[9], rientrante nel quadro del piano di rilancio *Next Generation EU*, attribuiscono centralità al principio di interoperabilità. In questo contesto si colloca la Piattaforma Digitale Nazionale Dati[10],un'infrastruttura tecnologica strategica che consente l'interoperabilità tra i sistemi informativi e le banche dati delle pubbliche amministrazioni e dei gestori di servizi pubblici, in coerenza con gli obiettivi delineati dal Codice dell'Amministrazione Digitale[11].

L'interoperabilità dei dati presenti nei registri pubblici riguarda anche le informazioni di natura sanitaria, la cui circolazione semplificata dovrebbe avvenire all'interno di un assetto istituzionale capace di valorizzarne l'utilizzo. L'introduzione di strumenti tecnologici dedicati all'archiviazione dei dati sanitari si è sviluppata in un contesto caratterizzato da una crescente pluralità di attori e da una mobilità sempre più accentuata dei pazienti[12]. Tale evoluzione ha accentuato i rischi di dispersione delle informazioni e di formazione di quadri clinici incompleti. La mancanza di dati aggregati e facilmente accessibili rischia infatti di generare una visione

---

dell'interoperabilità tramite API dei sistemi informatici, Agenzia per l'Italia digitale, Versione 2.0, 2022.

[8] Per ulteriori riflessioni sul punto, v. I. MACRÌ, *Digitalizzazione, innovazione e sicurezza nella P.A.,* Milano, 2022, 33 e ss.

[9] Per un ulteriore approfondimento, v. *Le misure previste per una PA protagonista della transizione digitale, PA digitale 2026*, Ministero per l'innovazione tecnologica e la transizione digitale, Dipartimento per la trasformazione digitale.

[10] Art. 50 *ter*, d. lgs. 7 marzo 2005, n. 82, introdotto dall'art. 45, d.lgs. 13 dicembre 2017, n. 217.

[11] Sul punto v., art. 50, d. lgs. 7 marzo 2005, n. 82.

[12] «*Con specifico riferimento alla sanità digitale si riconosce che la crisi causata dal Covid-19 dimostra l'importanza della trasformazione digitale della sanità e dell'assistenza e il suo valore nel rafforzamento della resilienza dei sistemi sanitari e della loro risposta alla pandemia, sottolineando le potenzialità insite nello sviluppo di uno spazio europeo dei dati sanitari nel favorire soluzioni efficaci in termini di prevenzione, diagnosi, trattamenti e cure, oltre che in termini di costi e di ottimizzazione del flusso dei lavori nell'assistenza sanitaria, conseguendo così migliori risultati sanitari per i pazienti e migliori sistemi di sorveglianza epidemiologica, con una conseguente maggiore resilienza dei sistemi sanitari.*»: I. MACRÌ, *Digitalizzazione, innovazione e sicurezza nella P.A.,* cit., 20.

parziale della situazione clinica, con potenziali ricadute negative sulla qualità dell'assistenza erogata[13].

2. Sanità digitale: integrazione, connessione e sviluppo

Tra sanità e digitalizzazione sussiste un'elevata interconnessione; il progressivo miglioramento dei servizi sanitari erogati si evolve e determina, proporzionalmente, lo sviluppo del Paese e dei cittadini coinvolti.
Tuttavia, un'efficiente evoluzione del sistema sanitario non è caratterizzata esclusivamente dall'innovazione dei modelli diagnostici adottati e dalla promozione della ricerca scientifica, ma richiede un'attenta valutazione dei numerosi aspetti coinvolti nel processo di digitalizzazione.
Sul punto rileva la vulnerabilità del dato sanitario, intesa sia come potenziale esposizione per il titolare, in caso di trattamento illecito o non appropriato[14], ma anche come rischio di alterazione delle informazioni, che potrebbe comportare errori diagnostici non irrilevanti[15].
Tutto questo serve per mettere in luce un ulteriore adempimento al quale deve prestare attenzione lo Stato erogatore di servizi sanitari che, per evitare l'evoluzione di un sistema basato sulla "malasanità", deve garantire la sicurezza dei dati e dei sistemi che li ospitano.

---

[13] M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, in *Informatica Giuridica*, (a cura di) G. ZICCARDI, P. PIERRI, Milano, 2019, 43 ss.

[14] La delicatezza delle informazioni legate al dato sanitario ha indotto alla definizione degli stessi come «*sensibilissimi*», in vista della forte correlazione con la sfera più intima e personale dell'individuo. Ciò implica l'esigenza di una tutela rafforzata, dal punto di vista normativo ma anche etico. Ma l'esigenza di protezione dei dati sanitari si confronta costantemente con il diritto alla salute e con gli interessi generali della sanità pubblica, inducendo all'adozione di criteri maggiormente flessibili, rispetto a quelli ordinariamente utilizzati in altri contesti.
Un esempio significativo è rappresentato dal d.l. 9 marzo 2020, n. 14 che per attuare un potenziamento del Servizio Sanitario Nazionale, al fine di contrastare il coronavirus, ha disposto una serie di deroghe alla normativa relativa alla protezione dei dati personali, anche per potenziare la circolazione delle informazioni tra le cliniche nazionali: sul punto, v. M. CIANCIMINO, *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, *I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, in *Quaderni della Rassegna di diritto civile* (a cura di) P. PERLINGIERI, Napoli, 2020, 15 e ss.; che cita a sua volta V. ZENO-ZENOCOVICH, Sub. art. 22, *Commento*, in *La tutela dei dati personali. Commentario alla L. n. 675 del 1966*, Padova, 1999, 276

[15] Ai fini di un'analisi più articolata della distinzione tra "*Dato relativo alla salute"* e "*dato sanitario*", v. G. AMARÙ, A. FAVA, M. FOSSI, F. MAINARDI, *La privacy del dato sanitario, Manuale per operatori e professionisti che trattano dati relativi alla salute e per chi vuole saperne di più*, Milano, 2024, 91 ss.

Il settore sanitario è potenzialmente esposto a conseguenze rilevanti che necessitano di ingenti investimenti utili a garantire elevati livelli di sicurezza: innovazione tecnologica e garanzie devono essere caratterizzate da una evoluzione a specchio, o parallela, ove la progressione di una richiede l'avanzamento delle altre, per evitare pericolosi scompensi che darebbero vita a vuoti di tutela.

La digitalizzazione ha preso il sopravvento, sostituendo i tradizionali metodi di conservazione cartacea con sistemi di archiviazione digitale. In ambito sanitario è venuta meno la cosiddetta "cartella locale" che prevedeva la conservazione delle informazioni sanitarie presso la struttura erogante e la consultazione esclusiva dello specialista direttamente coinvolto.

Nel tempo, l'affidamento da parte della medicina contemporanea sui sistemi informatici è aumentato: l'automazione di processi un tempo complessi e la delega di decisioni minori a intelligenze artificiali consentono di ottimizzare il lavoro degli operatori sanitari[16]. Ma per promuovere l'operato del sistema sanitario, serve un progresso coordinato tra innovazione tecnologica e tutele.

La condivisione delle informazioni cliniche all'interno di sistemi che ospitano la gestione dei flussi delle informazioni sanitarie, avviene tramite *datasets*. Ciò spinge ad affermare che il tema sicurezza deve essere considerato come elemento primario; la progettazione delle piattaforme informatiche, attraverso una strategia di preventiva valutazione dei modelli architetturali, dovrebbe garantire un adeguato livello di sicurezza[17].

Il mutamento del perimetro d'azione nella gestione dei dati, in generale, e del dato sanitario, in particolare, orienta verso l'obiettivo di soddisfare l'esigenza di garantire riservatezza e integrità[18] delle informazioni incluse

---

[16] Cfr. ampiamente F. MATTEI, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie*, in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati,* G. C. FERONI, (a cura di), Bologna, 2022, 125 ss.

[17] M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, in *Informatica Giuridica*, cit., 2019, 1 ss.

[18] *«I dati personali sono: f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).*»: art. 5, Regolamento generale sulla protezione dei dati (UE) 2016/679, 27 aprile 2016, in G.U.U.E., 4 maggio 2016.

nei sistemi informativi, anche attraverso l'implementazione di un sistema di gestione della sicurezza delle informazioni[19].

In origine, le strutture dati venivano sviluppate separatamente, in contesti specifici e senza una visione unificata, portando alla nascita di sistemi isolati, ciascuno con proprie modalità di comunicazione e funzionalità, progettate dai singoli produttori.

Con il progressivo evolversi delle esigenze delle strutture ospedaliere, sono state integrate soluzioni più avanzate: dalla gestione delle cure, all'organizzazione del personale, fino alla condivisione sicura dei dati sensibili tra i reparti, superando l'uso della documentazione cartacea. Ogni azienda ospedaliera è dotata di sistemi informativi che archiviano e gestiscono un ampio spettro di dati, tra cui informazioni anagrafiche e diagnostiche dei pazienti.

Tutto ciò ha portato allo sviluppo di sistemi informativi più completi, in grado di organizzare in modo integrato tutte le fasi di trattamento, elaborazione e distribuzione dei dati, con l'obiettivo di connettere tra loro le diverse componenti del sistema sanitario. Tuttavia, tali progressi non hanno risolto il problema della compatibilità tra sistemi eterogenei: se ciascuno adotta codifiche o standard differenti, la comunicazione e lo scambio dei dati risultano di fatto impossibili.

Per superare questo ostacolo intervengono standard capaci di definire regole comuni per l'accesso, la strutturazione e l'utilizzo dei dati, così da renderli fruibili da qualsiasi dispositivo o sistema all'interno di una rete globale. Tra gli standard più diffusi per la gestione e la trasmissione dei dati

---

[19] «*L'infrastruttura definita come Sistema di Gestione della Sicurezza delle Informazioni (SGSI) include la struttura organizzativa, le politiche, le attività di pianificazione, le prassi, le procedure, i processi e le risorse dell'organizzazione. Il modello è previsto all'interno dello standard ISO/IEC ed è composto da due parti:*
1. requisiti del SGSI, la parte che garantisce l'efficacia del sistema di gestione. È la parte in cui si applicano i due approcci importanti: approccio per processi e approccio sistemico applicato alla gestione;
2. obiettivi e controlli che introduce un terzo approccio definito come Plan Do Check Act (PDCA) che viene applicato per strutturare i processi del sistema di gestione per la sicurezza delle informazioni»: così M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, in *Informatica Giuridica*, cit., 7 ss.

sanitari vi è il protocollo HL7[20], che svolge un ruolo fondamentale non solo nell'organizzazione delle informazioni cliniche e anagrafiche dei pazienti, ma anche nei processi amministrativi e contabili delle strutture sanitarie, nella gestione della logistica interna, del personale e degli ordini farmaceutici. Tale *standard* risulta altresì ampiamente utilizzato per favorire la comunicazione tra diverse strutture sanitarie e tra gli operatori del settore, quali medici di base, farmacisti, tecnici di laboratorio e personale amministrativo. Uno dei principali vantaggi del sistema HL7 è l'elevato grado di interoperabilità, che consente un'efficace integrazione tra piattaforme diverse e garantisce una maggiore fluidità nella circolazione delle informazioni. L'adozione di un'architettura basata su tecnologie web facilita ulteriormente l'accesso ai dati, permettendo una gestione più tempestiva delle risorse e una migliore operatività dei servizi[21].

La frammentazione dei linguaggi e dei formati utilizzati nei diversi sistemi può richiedere operazioni di conversione che, in alcuni casi, comportano perdita di informazioni rilevanti, generando lacune nella ricostruzione della storia clinica del paziente. Ciò rende evidente l'importanza di adottare sistemi fondati su "dati gemellati", ossia strutture informative tra loro affini e compatibili[22].

---

[20] «*HL7 FHIR is an open standard developed in 2010 to exchange health data among healthcare information systems. It innovates from previous monolithic model-based HL7 versions by defining "resources" that represent clinical concepts that can be "profiled" to support complex healthcare scenarios. HL7 FHIR resources are used to store, exchange, and process data, supporting healthcare providers in making better informed decisions*. »: così R. GAZZARATA, J. ALMEIDA, L. LINDSKOLD, G. CANGIOLI, E. GAETA, G. FICO, C. E. CHRONAKI, *HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: Scoping review, in International Journal of Medical Informatics*, 2024, 2 ss.

[21] Per ulteriori approfondimenti sui benefici e sull'impatto applicativo dello *standard*, v. V. LAVECCHIA, DEFINIZIONE *e caratteristiche dello standard HL7 (Health Level 7)*, in *Informatica e Ingegneria Online*, (https://vitolavecchia.altervista.org/lo-standard-hl7-health-level-7/)

[22] «*Currently in healthcare, there is a need to exchange health related data for clinical care, quality measures, and research. Early attempts resulted in unique interfaces that are not standards based, leading to higher costs, inconsistencies in data, and over time, loss of system transparency. The standardized approach to healthcare data exchange has many benefits. The importance and relevance of the HL7 V3 messages is demonstrated through several use cases describing the need for exchanged messages supporting transfer of care, querying of records, and continuity of care.* »: così W. GOOSSEN, L. HEERMANN LANGFORD, *Exchanging care records using HL7 V3 care provision messages, J Am Med Inform Assoc*, 2014, 364 ss.

La facilitazione dello scambio di dati rappresenta il principale obiettivo dello *standard*, che consente la compatibilità comunicativa tra sistemi differenti considerando diversi linguaggi di programmazione e sistemi, garantendo l'utilizzo di supporti esterni. In questo modo vengono superate le barriere imposte da infrastrutture eterogenee, un elemento imprescindibile in un contesto caratterizzato dalla diffusione di strumenti digitali e di tecnologie di comunicazione che richiedono modalità di trasmissione dei dati armonizzate tra tutti i soggetti coinvolti.

L'interoperabilità, infatti, consiste nella capacità dei sistemi di "dialogare" attraverso la condivisione delle informazioni. Una struttura comunicativa compatibile è quindi indispensabile per il confronto e l'utilizzo dei dati clinici generati, consentendo una visione più completa e integrata della situazione sanitaria[23].

Tutto questo produce benefici a vantaggio dell'utente finale, ossia del paziente, facilitando l'accesso e contribuendo a migliorare l'efficienza e l'accuratezza dell'intervento medico, mirando anche alla riduzione della probabilità di errore umano e ottimizzando, o quantomeno provando a ottimizzare, l'*iter* di cura del paziente.

Le diverse versioni di HL7 hanno condotto allo sviluppo del FHIR (*Fast Healthcare Interoperability Resource*), una nuova architettura pensata per creare messaggi strutturati compatibili sia con le precedenti versioni di HL7 e, allo stesso tempo, adattabili alle tecnologie più moderne, come le applicazioni mobili, le cartelle cliniche elettroniche e i servizi *cloud*[24].

In sintesi, lo *standard* HL7 rappresenta una tecnologia abilitante fondamentale per garantire l'interoperabilità tra i sistemi digitali in ambito

---

[23] LEHNE M., SASS J., ESSENWANGER A., LEHNE M., SCHEPERS J. e THUN S., *Why digital medicine depends on interoperability*, in *Digit Med*, 2019, 79

[24] «*Fast Health Interoperability Resources (FHIR, pronounced Bfire) can be thought of as HL7 (Health Level 7) version 4.0, but that is where any resemblance to other HL7 standards ends*»: così M. A. HUSSAIN, S. G. LANGER E M. KOHLI, *Learning HL7 FHIR Using the HAPI FHIR Server and Its Use in Medical Imaging with the SIIM Dataset, Journal of Digital Imaging*, 2018, 334.

Cfr. ampiamente M. AYAZ, M. F. PASHA, M. Y. ALZAHRANI, R. BUDIARTO, D. STIAWAN, *The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities,* in *JMIR Medical Informatics*, 2021.

sanitario, condizione essenziale per il funzionamento efficace del Fascicolo Sanitario Elettronico[25].

[25] HL7 Italia, costituita nel 2003 come sezione nazionale di HL7 *International*, è incaricata dell'adattamento e dell'applicazione dello standard HL7 al contesto sanitario italiano. In un'ottica più ampia, l'associazione promuove il coinvolgimento attivo delle realtà regionali e nazionali nello sviluppo dello *standard*, contribuendo al processo di innovazione e digitalizzazione dell'infrastruttura tecnologica sanitaria del Paese. Per ulteriori approfondimenti relativi ai vantaggi e all'impatto dello *standard* HL7 sull'interoperabilità dei sistemi sanitari, si rinvia alla documentazione ufficiale, v. Realm Italiano, *Specifiche, Guide e White Paper di HL7 Italia*, (Realm Italiano – HL7 Italia)

3. L'Infrastruttura Nazionale per l'Interoperabilità dei Fascicolo Sanitario Elettronico.

In Italia è stata realizzata una piattaforma tecnologica nazionale volta a garantire l'interoperabilità tra i Fascicoli Sanitari Elettronici regionali, facilitando lo scambio standardizzato delle informazioni sanitarie sull'intero territorio nazionale. In questo quadro si colloca l'Infrastruttura Nazionale per l'Interoperabilità (INI), che rappresenta il canale di comunicazione centrale attraverso cui avviene l'interconnessione tra le diverse piattaforme regionali[26].

L'evoluzione normativa e tecnologica intervenuta negli anni ha reso necessario un aggiornamento continuo sia dell'architettura sia delle funzionalità dell'infrastruttura. Tuttavia, per comprendere pienamente le logiche di funzionamento attuali, risulta utile esaminare la versione originaria del documento progettuale del 2017. Questo approccio consente di individuare le basi concettuali e operative su cui il sistema è stato costruito, offrendo una chiave interpretativa essenziale per leggere e comprendere le successive evoluzioni. L'analisi della prima versione permette infatti di evidenziare con maggiore chiarezza il disegno architetturale iniziale e i meccanismi di interoperabilità che, pur essendo stati oggetto di aggiornamento, costituiscono le fondamenta del sistema attuale[27].

---

[26] *«INI», l'Infrastruttura nazionale per l'interoperabilità fra i FSE, parte del Sistema FSE, istituita ai sensi del comma 15-ter dell'art. 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, realizzata dal Ministero dell'economia e delle finanze attraverso l'infrastruttura del Sistema Tessera Sanitaria realizzato in attuazione dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito con modificazioni, dalla legge 24 novembre 2003, n. 326»:* art. 1, comma 1, lettera q), Decreto 7 settembre 2023, *Ministero della salute, Fascicolo sanitario elettronico 2.0, in G.U. n. 249, 2023*; cfr. con precedente versione «d*)«INI», l'Infrastruttura nazionale per l'interoperabilità fra i FSE, istituita ai sensi del comma 15-ter del predetto art. 12,realizzata dal Ministero dell'economia e delle finanze, della quale lo stesso assume la titolarità del trattamento dei dati, sulla base di quanto previsto dall'art. 22 del presente decreto*»: art. 1, comma1, lettera d), d.m., 4 agosto 2017, *Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)*, ai sensi dell'art. 12, comma 15-ter, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, l. 17 dicembre 2012, n. 221, in G.U. n. 195, 22 agosto 2017.

[27] Di recente pubblicazione: *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.2, 31.07.2025 e *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle*

L'infrastruttura del fascicolo sanitario elettronico si basa su un modello funzionale ed è utilizzata per garantire l'interoperabilità dei dati clinici attraverso una rete regionale[28].

Ogni sistema regionale rende disponibile un modello architetturale che si occupa della gestione del contenuto del fascicolo sanitario e dell'accesso consentito al soggetto in cura, ai medici o pediatri e ai restanti soggetti coinvolti nel processo di cura[29].

Ogni regione e provincia autonoma adotta un proprio sistema o, in via sussidiaria, usufruisce delle funzionalità messe a disposizione dall'Infrastruttura Nazionale. In ogni caso, l'interoperabilità tra i sistemi delle singole regioni è assicurata tramite l'interazione con l'Infrastruttura Nazionale per l'Interoperabilità (INI).

Regioni In Sussidiarietà, Versione 2.6.2, 23.09.2025. L'ultima versione ha introdotto le seguenti novità: nel servizio di ricerca documenti è stata modificata la lunghezza del campo TipologiaDocumentoAlto (valido per tutte le regioni in sussidiarietà). Inoltre, sono stati introdotti nuovi campi relativi al taccuino: nel servizio di comunicazione metadati sono stati aggiunti TaccuinoTitolo, TaccuinoDescrizione, TaccuinoNomeMedico e TaccuinoNomeFile, esclusivamente per la regione Campania. Infine, nella risposta del servizio di ricerca documenti, in caso di dati provenienti dal taccuino, sono stati aggiunti i campi TaccuinoTitolo, TaccuinoDescrizione e TaccuinoNomeMedico, validi per tutte le regioni.

[28] «*tale Infrastruttura nazionale ha il compito di garantire l'interoperabilità dei FSE regionali, l'identificazione dell'assistito attraverso l'allineamento con l'Anagrafe Nazionale degli Assistiti (ANA), l'interconnessione dei soggetti previsti per la trasmissione telematica dei dati per le regioni che ne faranno richiesta entro il 31 marzo 2017, la gestione delle codifiche nazionali e regionali stabilite e rese disponibili dalle Amministrazioni e dagli enti che le detengono*.»: Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12, comma 15-ter, D.L. 179/2012)*, circ. n. 4, 2017, 6.

[29] «*Il FSE contiene i seguenti dati e documenti, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale, i cui contenuti sono riportati, in sede di prima applicazione, nell'allegato A al presente decreto: a) dati identificativi e amministrativi dell'assistito (esenzioni per reddito e patologia, contatti, delegati); b) referti, inclusi quelli consegnati ai sensi del decreto del Presidente del Consiglio dei ministri 8 agosto 2013, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 243 del 16 ottobre 2013; c) verbali pronto soccorso; d) lettere di dimissione; e) profilo sanitario sintetico, di cui all'art. 4; f) prescrizioni specialistiche e farmaceutiche; g) cartelle cliniche; h) erogazione farmaci a carico SSN e non a carico SSN; i) vaccinazioni; j) erogazione di prestazioni di assistenza specialistica; k) taccuino personale dell'assistito, di cui all'art. 5; l) dati delle tessere per i portatori di impianto; m) lettera di invito per screening*.»: art. 3, d.m. 7 settembre 2023, *Fascicolo sanitario elettronico 2.0,* in G.U. n. 249, 2023.

Infatti, oltre a garantire la generica interconnessione dei sistemi adottati all'intero della singola regione o provincia autonoma, è utilizzata dalle regioni e province che non hanno creato soluzioni proprie[30].

Le componenti principali del modello architetturale sono il *repository* che garantisce memorizzazione e accesso dei documenti clinici prodotti e il *registry* che consente l'indicizzazione dei documenti mediante metadati aggregati[31].

La documentazione viene archiviata nei *repository* digitali che possono essere organizzati a livello regionale, in forma centralizzata, o localizzati presso i differenti organismi sanitari che li hanno prodotti. L'architettura del sistema prevede una struttura ripartita, gestita autonomamente dalla singola regione o provincia autonoma[32]. Il *repository* è finalizzato alla conservazione dei documenti sanitari.

Un registro regionale, *registry*, fungendo da supporto dei *repository*, conserva i metadati associati ai documenti, agevolandone l'individuazione e il recupero[33].

Al fine di garantire il corretto perseguimento dell'interoperabilità è indispensabile la verifica dei dati anagrafici degli assistiti che si sottopongono a una prestazione sanitari da parte di un dominio regionale[34].

---

[30] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 10.

[31] Gli organismi che si occupano della redazione e produzione dei documenti sanitari hanno la titolarità degli stessi.

[32] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit., 12*

[33] A titolo esemplificativo i metadati comprendono la tipologia e l'autore del documento, l'identificativo del paziente cui esso si riferisce e l'ubicazione del *repository* che contiene il documento originario.

[33] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 9 e 10.

[34] «*1. Per rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, è istituita, nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze in attuazione di quanto disposto dall'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, l'Anagrafe nazionale degli assistiti (ANA).*

2. L'ANA, realizzata dal Ministero dell'economia e delle finanze, in accordo con il Ministero della salute in relazione alle specifiche esigenze di monitoraggio dei livelli essenziali di assistenza (LEA), nel rispetto delle previsioni di cui al comma 5 dell'articolo 62 del presente Codice, subentra, per tutte le finalità previste dalla normativa vigente, alle anagrafi e agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, ai

Il modello architetturale dell'infrastruttura nazionale per l'interoperabilità prevede che ogni regione di assistenza[35] memorizzi all'interno di un proprio registro indice tutti i metadati associati ai documenti sanitari dei propri assistiti, tenendo conto sia dei documenti prodotti all'interno del perimetro regionale, sia di quelli prodotti all'esterno. Nel caso in cui la regione sia

sensi dell'articolo 7 della legge 7 agosto 1982, n. 526, che mantengono la titolarità dei dati di propria competenza e ne assicurano l'aggiornamento.
3. L'ANA assicura alla singola azienda sanitaria locale la disponibilità dei dati e degli strumenti per lo svolgimento delle funzioni di propria competenza e garantisce l'accesso ai dati in essa contenuti da parte delle pubbliche amministrazioni per le relative finalità istituzionali, secondo le modalità di cui all'articolo 60, comma 2-bis, del presente Codice.
4. Con il subentro dell'ANA, l'azienda sanitaria locale cessa di fornire ai cittadini il libretto sanitario personale previsto dall'articolo 27 della legge 23 dicembre 1978, n. 833. È facoltà dei cittadini di accedere in rete ai propri dati contenuti nell'ANA, secondo le modalità di cui al comma 1 dell'articolo 6 del presente Codice, ovvero di richiedere presso l'azienda sanitaria locale competente copia cartacea degli stessi.
5. In caso di trasferimento di residenza del cittadino, l'ANA ne dà immediata comunicazione in modalità telematica alle aziende sanitarie locali interessate dal trasferimento. L'azienda sanitaria locale nel cui territorio è compresa la nuova residenza provvede alla presa in carico del cittadino, nonché all'aggiornamento dell'ANA per i dati di propria competenza. Nessun'altra comunicazione in merito al trasferimento di residenza è dovuta dal cittadino alle aziende sanitarie locali interessate.
6. L'ANA assicura al nuovo sistema informativo sanitario nazionale realizzato dal Ministero della salute in attuazione di quanto disposto dall'articolo 87 della legge 23 dicembre 2000, n. 388, con le modalità definite dal decreto del Presidente del Consiglio dei ministri di cui al comma 7, l'accesso ai dati e la disponibilità degli strumenti funzionali a garantire l'appropriatezza e l'efficacia delle prestazioni di cura erogate al cittadino, nonché per le finalità di cui all'articolo 15, comma 25-bis, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135.
7. Entro il 30 giugno 2014, con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della salute e del Ministro dell'economia e delle finanze, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le province autonome di Trento e di Bolzano, sono stabiliti:
a) i contenuti dell'ANA, tra i quali devono essere inclusi le scelte del medico di medicina generale e del pediatra di libera scelta, il codice esenzione e il domicilio;
b) il piano per il graduale subentro dell'ANA alle anagrafi e agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, da completare entro il 30 giugno 2015;
c) le garanzie e le misure di sicurezza da adottare, i criteri per l'interoperabilità dell'ANA con le altre banche dati di rilevanza nazionale e regionale, nonché le modalità di cooperazione dell'ANA con banche dati già istituite a livello regionale per le medesime finalità, nel rispetto della normativa sulla protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e delle regole tecniche del sistema pubblico di connettività, ai sensi del presente Codice.»: art. 62 ter, d.lgs. 7 marzo 2005, n. 82

[35] *«RdA», la regione o provincia autonoma ovvero SASN di assistenza dell'assistito, ovvero, per gli assistiti per i quali non risulta associata una RdA, il titolare del Portale nazionale FSE»*: art. 1, comma 1, lettera j), Decreto 7 settembre 2023, *Ministero della salute, Fascicolo sanitario elettronico 2.0, in G.U. n. 249, 2023;* cfr. con precedente versione *« t) «RdA», la regione o provincia autonoma ovvero SASN di assistenza dell'assistito»* art 1, comma 1, lettera t), d.m., 4 agosto 2017.

sprovvista di un sistema di FSE, i metadati confluiranno all'interno del FSE dell'assistito[36], previo consenso all'alimentazione dello stesso[37].

I consensi degli individui acquisiti da regioni e province autonome confluiscono all'interno dell'infrastruttura nazionale. Le interazioni tra i sistemi regionali relativi al fascicolo sanitario elettronico avvengono tramite l'infrastruttura nazionale per l'interoperabilità, che reindirizza la richiesta alla regione di riferimento.

Al fine di garantire l'adeguato funzionamento del sistema, soprattutto in riferimento alla verifica della regione di assistenza e del consenso dell'assistito, la singola regione avvia appositi processi, tramite l'infrastruttura nazionale che svolge le opportune verifiche. Quest'ultima, a seguito di tali verifiche svolte con il sistema anagrafico, comunica alla stessa regione richiedente di essere competente e di proseguire autonomamente il processo all'interno del proprio dominio, oppure, inoltra la richiesta alla regione di assistenza corretta, restituendo l'esito ottenuto alla regione richiedente.

I possibili scenari illustrati sono due: l'assistito è all'interno della propria regione di assistenza oppure all'esterno; in entrambi i casi è la regione richiedente ad avviare il processo, innescando l'interazione con l'infrastruttura nazionale di interoperabilità che verifica il codice fiscale e individua la regione di assistenza corretta. Con l'intermediazione degli strumenti utilizzati per le verifiche anagrafiche, ha luogo l'accertamento del consenso prestato e l'invio della richiesta alla regione di assistenza competente. Nel caso in cui la regione di assistenza coincida con quella richiedente, il processo prosegue interamente nella regione in questione, sempre previa verifica del consenso dell'interessato[38].

---

[36] *«Assistito», il soggetto presente nell'Anagrafe nazionale degli assistiti, disciplinata dal decreto di cui al comma 7 dell'art. 62-ter del CAD*»: art. 1, comma 1, lettera c), Decreto 7 settembre 2023, *Ministero della salute, Fascicolo sanitario elettronico 2.0, in G.U. n. 249, 2023;* cfr. con precedente definizione *«n) «assistito», il soggetto che ricorre all'assistenza sanitaria nell'ambito del Servizio sanitario nazionale»:* art. 1, comma 1, lettera n), d.m. 4 agosto 2017.

[37] Per una riflessione relativa al ruolo del consenso, v. A. GHIGLIA, *La pandemia tra rischi e opportunità,* in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, G. C. FERONI (a cura di), Bologna, 2022, 113 ss.

[38] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 18, 19 e 20.

La maggiore efficienza, alla base della creazione dell'Infrastruttura Nazionale per l'Interoperabilità del Fasciolo Sanitario Elettronico, era intesa come obiettivo da conseguire anche attraverso la centralizzazione, a livello nazionale, della gestione dei consensi espressi dagli assistiti promuovendo un alleggerimento degli oneri delle singole regioni, poiché il consenso o il diniego espresso dall'assistito assume validità a livello nazionale, comprendendo un perimetro più ampio e non limitato al contesto regionale. L'infrastruttura mette a disposizione un apposito servizio per la ricezione e la conservazione dei consensi raccolti, garantendone la facile accessibilità ai fini delle verifiche.

Il consenso riveste un ruolo centrale per l'attivazione del fascicolo sanitario elettronico; ogni paziente deve necessariamente manifestare la propria volontà, con possibilità di aggiornamento dello stesso, ammettendo l'indicizzazione dei documenti sanitari prodotti e la consultazione dei documenti da parte del personale preposto.

In realtà, è prevista anche la possibilità di attuare un'indicizzazione preventiva, con l'obiettivo di rendere immediatamente disponibile la storia clinica del paziente, sempre previa emissione del consenso all'alimentazione dello strumento di archiviazione[39].

Anche in tal caso viene distinto l'assistito fuori dalla regione di assistenza dall'assistito all'interno della stessa.

Nel primo caso, la regione che eroga il servizio avvia il processo di gestione dei consensi, richiedendo all'infrastruttura nazionale lo storico dei consensi già prestati dall'assistito, l'informativa di riferimento utilizzata in passato e quella attualmente utilizzata nella regione di assistenza, accompagnata da una modulistica necessaria per la raccolta di nuovi consensi e revoche. L'utente autenticato può attivare il processo tramite il nodo regionale, che inoltra la richiesta all'infrastruttura nazionale. Quest'ultima risponde

[39] I consensi relativi all'alimentazione, alla consultazione e all'accesso vengono archiviati in modo centralizzato all'interno dell'Infrastruttura Nazionale per l'Interoperabilità: per l'illustrazione del processo v. stessi, v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* figura 6, 22

fornendo lo stato attuale dei consensi - alimentazione, consultazione, pregresso- le informative passate e aggiornate e la relativa modulistica.
A seguito della presa visione della documentazione da parte del paziente, la regione trasmette all'infrastruttura nazionale le informazioni aggiornate. Quest'ultima procede con l'archiviazione delle stesse nel proprio *repository* e avverte la regione di assistenza dell'aggiornamento effettuato[40].
Quando l'assistito si trova nella regione di assistenza, il processo di gestione dei consensi viene attivato dalla stessa regione del paziente, che richiede all'infrastruttura nazionale i consensi eventualmente già espressi, insieme all'informativa precedentemente utilizzata e all'ultima versione aggiornata dell'informativa e della modulistica per raccogliere nuovi consensi o revoche. Un soggetto già autenticato avvia tale procedura tramite il nodo regionale.
Dunque, l'infrastruttura nazionale fornisce alla regione richiedente[41] lo stato attuale dei consensi, l'informativa originaria e quella aggiornata, con la relativa modulistica. A seguito della presa visione dell'informativa, la regione invia all'infrastruttura i nuovi consensi espressi, che vengono memorizzati in modo sicuro all'interno del *repository* nazionale[42].
Ogni regione e provincia autonoma è tenuta a fornire specifici servizi finalizzati alla funzionalità di ricerca dei dati contenuti nel fascicolo sanitario elettronico[43]. Tale previsione si estende anche all'infrastruttura

---

[40] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit., 25.*
[41] *«RdE», la regione o provincia autonoma ovvero SASN di erogazione di una prestazione sanitaria»*: art. 1, comma 1, lettera k), d.m. 7 settembre 2023; cfr. con precedente versione «*s) «RdE», la regione o provincia autonoma ovvero SASN di erogazione di una prestazione sanitaria*»: art 1, comma 1, lettera s). d.m. 4 agosto 2017.
[42] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 33.
[43] «*Ciascuna regione o provincia autonoma espone verso le altre regioni e province autonome servizi specifici a supporto dell'interoperabilità del FSE al fine di garantire almeno le seguenti funzionalità: a) la ricerca dei documenti del FSE di cui all'articolo 2*»: art. 25, comma 1, lett. a), D.P.C.M. n. 178 del 2025; v. anche art. 27, comma 1, lettera c).
Ma sul punto appare rilevante sottolineare che «*Il decreto del Presidente del Consiglio dei ministri 29 settembre 2015, n. 178, pubblicato nella Gazzetta Ufficiale della Repubblica italiana 11 novembre 2015, n. 263, cessa di avere efficacia dal giorno dell'entrata in vigore del presente decreto, ad eccezione dei Capi III e IV, che rimangono in vigore fino all'adozione, con successivi decreti ai sensi del comma 7 dell'art. 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, di specifiche disposizioni per i trattamenti dei dati e dei*

nazionale per l'interoperabilità che, ancora una volta, interviene in modalità diversificata a seconda dei casi.

Per un soggetto al di fuori della regione di assistenza, la funzione di ricerca consente a un operatore o a un professionista di inviare una richiesta di metadati relativi ai documenti di interesse, nel rispetto di specifici parametri di ricerca e delle politiche di accesso previste.

L'infrastruttura nazionale favorisce la realizzazione della fase di ricerca semplificando l'interazione tra la regione di erogazione e la regione di assistenza di riferimento, occupandosi dell'attuazione di specifici controlli, tra cui quello relativo alla verifica della prestazione del consenso per la consultazione dei documenti, fornito dall'assistito.

Nel caso in cui l'assistito abbia precedentemente fornito il consenso alla consultazione, ha luogo l'inoltro della richiesta alla regione di assistenza o, in caso contrario, l'invio di un messaggio di errore alla regione di erogazione.

Se invocata, la regione di assistenza fornisce i metadati che riguardano il paziente, contenuti nel fascicolo elettronico di riferimento. In ultimo, l'infrastruttura nazionale inoltra i metadati alla regione di erogazione[44].

Nel caso in cui il processo di ricerca dei documenti avvenga all'interno della regione di appartenenza dell'assistito, l'infrastruttura nazionale favorisce la realizzazione dell'intero processo, semplificando l'interazione fra la regione di assistenza e la regione di erogazione. In presenza di precedente consenso fornito dall'assistito in merito alla consultazione documentale, l'infrastruttura nazionale invia l'esito positivo alla regione di assistenza o, al contrario, un messaggio di errore. Nel caso di esito positivo, il processo di ricerca documentale prosegue nella regione di assistenza che si occupa della ricerca dei metadati nel proprio indice, con successiva presentazione dei

documenti del FSE per le finalità di ricerca e di Governo.»: art 27, comma 5, d.m. 7 settembre 2023.

[44]Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 41.

propri risultati di ricerca[45]. Notiamo che in questo secondo schema la regione di erogazione non è presente nella fase di ricerca documentale.

Le specifiche tecniche disciplinano anche un processo relativo al recupero dei documenti che coinvolge una nuova figura: la regione che contiene il documento.

Nel caso di assistito al di fuori della regione di assistenza il processo di recupero del documento viene fatta da un operatore sanitario o professionista che opera fuori dal perimetro di appartenenza dell'assistito. In questo caso sussiste una diramazione mediante l'esecuzione di un sottoprocesso di ricerca documentale basata sullo schema della ricerca dei documenti descritta in precedenza.

A seguito dei controlli effettuati, ha luogo l'inoltro della richiesta ricevuta dalla regione di erogazione del servizio alla regione contenente il documento, che fornisce un riscontro. A seguito del recupero, l'infrastruttura nazionale inoltra una notifica alla regione di assistenza[46].

Quando la richiesta di recupero di un documento avviene all'interno della stessa regione in cui il paziente è assistito, la procedura risulta semplificata perché la fase di ricerca del documento è già stata svolta in precedenza.

Gli assistiti, i professionisti o gli operatori sanitari possono inoltrare la richiesta di recupero tramite *software* o portali *web*. A quel punto, l'infrastruttura nazionale riceve la richiesta e la inoltra alla regione in cui si trova il documento[47].

Il sistema posto alla base del funzionamento del fascicolo sanitario elettronico regionale individua e recupera il documento, che viene poi

---

[45] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 49.

[46] Le interfacce necessarie per la realizzazione del processo di Recupero Documento sono recupero documento (INI e RCD) e notifica recupero documento (RDA). Per ulteriori approfondimenti grafici v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 55 ss.

[47] «*L'INI, dopo aver ricevuto il messaggio dalla RDA, effettua i seguenti controlli: i) verifica la correttezza del messaggio di richiesta; ii) valida il paziente e verifica se è stato espresso il consenso alla consultazione dallo stesso. A seguito del superamento dei controlli, la INI inoltra il messaggio alla RCD.*»: Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 62

restituito all'infrastruttura nazionale. Infine, quest'ultima provvede a inviare il documento al sistema di archiviazione che ha originato la richiesta, completando così il processo.

Il documento di progetto dell'infrastruttura nazionale per l'interoperabilità disciplina anche un processo strutturato di comunicazione dei metadati, articolato in tre categorie distinte: la comunicazione di nuovi dati, l'aggiornamento dei metadati relativi a documenti esistenti e la cancellazione dei metadati associati a un documento. Ciascuna di queste aree è disciplinata da un processo specifico, definito in base alle finalità e alle modalità operative previste dall'infrastruttura stessa.

Il processo di comunicazione relativo alla creazione documentale relativa ad un assistito fuori dalla regione di assistenza consente ad un operatore o professionista della regione di erogazione di comunicare alla regione di assistenza, mediante l'infrastruttura nazionale, la creazione *ex novo* di un documento che confluisce nel fascicolo sanitario elettronico.

La richiesta è indirizzata all'infrastruttura nazionale che svolge una verifica dell'identità dell'assistito, con successiva individuazione della regione di appartenenza e controllo relativo al precedente consenso prestato dallo stesso, relativo all'alimentazione del fascicolo sanitario elettronico. Nel caso in cui sussista il consenso, l'infrastruttura nazionale provvede alla trasmissione dei metadati del nuovo documento da inserire nell'indice del fascicolo elettronico, alla regione di assistenza. In caso contrario, avviene la trasmissione di un messaggio di errore. L'ultimo passaggio prevede che la regione di assistenza, restituisca all'infrastruttura nazionale l'esito dell'operazione, il quale viene successivamente reso disponibile dalla regione di erogazione[48].

Nel caso di paziente all'interno della regione di assistenza, l'avvio parte da un operatore sanitario della regione in questione, che invia una richiesta all'infrastruttura nazionale, che procede con la verifica della presenza del consenso dell'assistito. Solamente in caso di esito positivo, l'infrastruttura

[48] Per una illustrazione del processo descritto, v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 71 ss.

nazionale richiede al sistema della regione di assistenza di procedere con l'inserimento dei metadati relativi al nuovo documento all'interno del fascicolo elettronico[49].

Anche il processo di comunicazione dei metadati relativi all'aggiornamento di un documento prevede due scenari distinti. Nel caso in cui l'operazione viene avviata all'interno della regione di assistenza, il sistema regionale richiede all'infrastruttura nazionale la verifica della validazione dell'assistito, sempre relativa alla scheda anagrafica, e la valutazione della sussistenza del precedente consenso. Tali verifiche anticipano la fase successiva dedicata all'aggiornamento dei metadati di un documento contenuto nel fascicolo elettronico del paziente. Solo in presenza di esito positivo, si procede con l'aggiornamento dei metadati del documento presente nel fascicolo sanitario elettronico dell'assistito, che viene memorizzato dal sistema regionale della medesima regione di assistenza[50].

Qualora il processo di comunicazione dei metadati avvenga al di fuori della regione di assistenza, l'infrastruttura assume il ruolo di intermediario: la richiesta, originata dalla regione che detiene il documento, viene trasmessa all'infrastruttura nazionale, che provvede a inoltrarla alla regione di assistenza di riferimento[51].

Il processo di cancellazione dei metadati, nel caso in cui l'assistito si trovi al di fuori della regione di assistenza, prevede l'invio di una richiesta da parte di un'altra regione finalizzata alla cancellazione dei metadati associati a un documento presente nel fascicolo elettronico del paziente coinvolto. Anche in questo scenario, l'infrastruttura nazionale svolge un ruolo centrale di

---

[49] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici,* 76 e 77.

[50] Per ulteriori approfondimenti sul punto, v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit., 88 ss., con particolare riferimento al* paragrafo 4.6.2.1.2.2.

[51] «*La RCD deve preliminarmente ottenere i riferimenti dei metadati da aggiornare eseguendo il processo di Recupero Riferimenti Documento, descritto nel seguito del documento. L'INI svolge una serie di attività di controllo sulla validità della richiesta di comunicazione di aggiornamento (quali validazione e recupero RDA dell'assistito mediante ANA), prima di inoltrare la richiesta al sistema di FSE della RDA dell'assistito. Al termine dell'operazione, la RCD riceve dall'INI una risposta contenente l'esito della stessa, ottenuta dalla RDA*.»: Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit., 83, 84.*

intermediazione tra i sistemi regionali coinvolti, garantendo la corretta gestione del flusso informativo e il rispetto delle regole di interoperabilità.
Una preliminare fase di controllo svolta dall'infrastruttura nazionale relativamente alla validità della richiesta di aggiornamento e alla verifica dell'identità dell'assistito, anticipa l'inoltro della richiesta alla regione di assistenza. In caso di esito positivo, la regione di assistenza riceve la richiesta e provvede alla cancellazione logica[52].
Nel caso in cui il processo di cancellazione avviene all'interno della stessa regione di assistenza del soggetto, il dialogo tra l'infrastruttura nazionale e la regione serve per verificare l'identità dell'assistito, tramite il sottoprocesso di ricerca documenti. In estrema sintesi, in questo scenario l'interazione con l'infrastruttura nazionale ha la funzione di verificare che i metadati da aggiornare siano effettivamente riferiti a un assistito in carico alla regione di assistenza. Ottenuta tale conferma, quest'ultima può procedere con l'aggiornamento dei metadati all'interno del proprio *registry*.
L'interazione con l'infrastruttura nazionale costituisce quindi un passaggio essenziale per la validazione dell'assistito e per garantire la coerenza del processo di aggiornamento[53].
Il processo di recupero dei riferimenti del documento è funzionale ai tre processi precedentemente descritti: comunicazione dei metadati, aggiornamento del documento e cancellazione dei metadati, nei casi in cui l'assistito si trovi al di fuori della propria regione di assistenza. A differenza del processo di ricerca documentale, tale procedura non prevede la verifica del consenso alla consultazione da parte dell'assistito.
In questo contesto, la regione che detiene il documento avvia la richiesta di recupero dei riferimenti, coinvolgendo l'infrastruttura nazionale e la regione di assistenza del paziente che è titolare dei metadati da aggiornare o cancellare. L'infrastruttura nazionale svolge un ruolo di intermediazione,

[52]Il documento parla di cancellazione logica in vista del possibile recupero delle informazioni rimosse. La cancellazione in questione non è definitiva: v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 93 ss.
[53] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 100 ss.

garantendo la corretta trasmissione delle informazioni tra i sistemi regionali coinvolti[54].

Ciascuna regione e provincia autonoma, e anche l'infrastruttura nazionale per l'interoperabilità, devono mettere a disposizione servizi che siano in grado di supportare l'interoperabilità del fascicolo sanitario elettronico, tenendo particolarmente conto dell'aspetto relativo alla comunicazione e alla gestione dei metadati relativi ai documenti che compongono il fascicolo stesso.

Il processo seguito in caso di modifica della regione di assistenza sanitaria prevede il trasferimento integrale dell'indice documentale, ovvero di tutti i metadati afferenti ai documenti clinici contenuti nel fascicolo elettronico del paziente, dalla regione di assistenza originaria alla nuova regione. Nella fase di passaggio, nel caso in cui non sia ancora chiara l'identificazione della nuova regione di assistenza del paziente, l'intero indice viene conservato dall'infrastruttura nazionale che, in questa fase di intermediazione, garantisce la continuità dei servizi connessi al fascicolo elettronico.

Il documento illustra due differenti scenari: il primo riguarda i casi in cui non è possibile individuare immediatamente la nuova regione di assistenza, generando una situazione di incertezza nella gestione dei flussi informativi; il secondo scenario si riferisce al subentro di una nuova Azienda Sanitaria Locale appartenente a una regione diversa, che ha formalmente preso in carico l'assistito.

Il processo che prevede il trasferimento all'infrastruttura nazionale è avviato tramite una comunicazione da parte dell'anagrafe nazionale degli assisiti che informa l'infrastruttura della temporanea assenza di una regione di riferimento per il paziente.

Successivamente, l'infrastruttura nazionale formula una richiesta alla regione di provenienza dell'assistito al fine di ottenere la trasmissione dell'indice documentale di riferimento. La regione chiamata provvede all'invio di quanto richiesto.

---

[54] Per un ulteriore approfondimento di tale processo si rinvia ad Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 110 ss.

Una volta completata questa fase, la regione precedente di assistenza è tenuta alla cancellazione dei metadati dal proprio sistema informativo, al fine di garantire la coerenza e l'integrità del processo di trasferimento[55].
A seguito dell'attribuzione di una nuova regione a un assistito, si rende necessario il trasferimento di tutti i metadati precedentemente gestiti da un diverso sistema regionale. La nuova regione di assistenza avvia quindi una richiesta di trasferimento dell'indice documentale all'infrastruttura nazionale. Quest'ultima, dopo aver verificato l'identità dell'assistito, accerta se l'indice risulti già disponibile nei propri archivi oppure se debba essere richiesto alla regione di provenienza. Nel primo caso, l'infrastruttura provvede direttamente alla trasmissione dell'indice alla nuova regione di assistenza; nel secondo, inoltra la richiesta alla regione precedentemente competente, affinché proceda all'invio dei metadati necessari.
A seguito della ricezione dei metadati associati all'assistito, la regione ora competente, formula richiesta all'infrastruttura nazionale, affinché provveda alla cancellazione dei dati medesimi[56].

4. Continuità digitale dell'informazione sanitaria.

Entro il 31 marzo 2017 le regioni e le province autonome hanno manifestato la volontà di utilizzare, in tutto o in parte, i servizi messi a disposizione dall'Infrastruttura Nazionale di Interoperabilità per la realizzazione del Fascicolo Sanitario Elettronico destinato agli assistiti rientranti nella rispettiva area di competenza. Tale infrastruttura, come illustrato nel paragrafo precedente, si fonda su processi articolati e consente la gestione federata delle informazioni sanitarie[57].

---

[55] Per ulteriori approfondimenti sul punto, v. Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit.,* 17.
[56] Agenzia per l'Italia Digitale (AgID), *Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici, cit., 123 ss.*
[57] «*1. Entro il 31 marzo 2017, le regioni e province autonome comunicano al Ministero dell'economia e delle finanze e al Ministero della salute la richiesta di volersi avvalere di tutti o parte dei servizi FSE-INI di cui all'articolo 19 per la realizzazione del FSE per gli assistiti SSN di propria competenza. 2. Entro il 31 marzo 2017, il Ministero della salute comunica al Ministero dell'economia e delle finanze l'eventuale richiesta di volersi avvalere di tutti o parte dei servizi FSEINI di cui all'articolo 19 per la realizzazione del*

L'infrastruttura rende disponibili diversi servizi, descritti nella circolare dell'Agenzia per l'Italia digitale[58], finalizzati al perseguimento degli obiettivi previsti[59]. Le strutture standardizzate dei dati utilizzate per lo scambio informativo tra i sistemi regionali e il sistema centrale, i cosiddetti tracciati, costituiscono moduli digitali che identificano le informazioni da trasmettere, ne definiscono il formato e disciplinano le modalità di comunicazione attraverso specifiche tecniche. Tali moduli sono impiegati per l'erogazione dei servizi di sussidiarietà, destinati alle regioni e alle province autonome che hanno scelto di non realizzare un proprio Fascicolo Sanitario Elettronico e che delegano la relativa gestione all'infrastruttura nazionale. In questi casi l'interazione avviene direttamente tra l'attore e l'infrastruttura, senza intermediari.

FSE per gli assistiti SASN.»: art. 20, d.m.4 agosto 2017, *Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)*, ai sensi dell'art. 12, comma 15-ter, del D.L. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221, in G.U., n. 195, 22 agosto 2017.

[58]«*L'Agenzia per l'Italia digitale promuove l'innovazione nel Paese e l'utilizzo delle tecnologie digitali per organizzare la pubblica amministrazione anche nei rapporti con cittadini e imprese, secondo principi di legalità, imparzialità e trasparenza e criteri di efficienza, economicità ed efficacia, collaborando con le istituzioni europee e adempiendo agli obblighi assunti dall'Italia a livello internazionale nel settore della digitalizzazione (art. 14-bis, comma 1, CAD). In collaborazione con le comunità digitali regionali AGID promuove la cultura digitale e la ricerca. Uno dei compiti chiave svolti dall'AGID riguarda l'emanazione di linee guida in materia di digitalizzazione, con l'esclusione della sicurezza informatica, attualmente di competenza della nuova Agenzia per la cybersicurezza nazionale (ACN52). Si tratta di un'attività fondamentale perché attraverso le linee guida si dà concretezza alle norme contenute nel CAD, che diventano così applicabili. E proprio sull'attuazione e sul rispetto del CAD AGID svolge funzioni di indirizzo, vigilanza e controllo, adottando anche atti su specifiche materie (agenda digitale, digitalizzazione della pubblica amministrazione, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea*).»: I. MACRÌ, *Digitalizzazione, innovazione e sicurezza nella P.A.,* cit., 45.

[59] «*In sede di prima applicazione delle disposizioni del presente decreto, le regioni e province autonome assicurano:*
a) disponibilità dei servizi per l'accesso dell'assistito al proprio FSE;
b) disponibilità dei servizi per il collegamento e l'abilitazione all'accesso e all'alimentazione del FSE da parte dei MMG/PLS, nonché delle strutture sanitarie;
c) disponibilità dei servizi a supporto dell'interoperabilità del FSE, in conformità alle disposizioni di cui all'articolo 25;
d) disponibilità dei servizi per la gestione dei referti di laboratorio. I dati essenziali che compongono il referto di laboratorio sono individuati nel disciplinare tecnico;
e) disponibilità dei servizi per la gestione del profilo sanitario sintetico.»: art. 27, D.P.C.M. 29 settembre 2015, n. 178, *Regolamento in materia di fascicolo sanitario elettronico*, in G.U., n. 263, 11 novembre 2015.

I tracciati svolgono anche una funzione di traduzione di linguaggio: le regioni che non hanno aderito alla sussidiarietà e che hanno sviluppato un proprio FSE regionale interagiscono con l'infrastruttura nazionale tramite servizi dedicati, utilizzati unicamente dalla regione e non dai singoli attori, in modo da assicurare l'allineamento tecnico tra sistemi diversi. In tali circostanze, i servizi utilizzati come traduzione di linguaggio sono svolti unicamente dalla regione che si collega all'infrastruttura nazionale e non dai singoli attori, prevedendo una diretta interazione con la struttura regionale dedicata[60], mediante un'autenticazione effettuata attraverso un certificato *client*[61].

Per le regioni che invece hanno aderito alla sussidiarietà è previsto che gli attori accedano al fascicolo sanitario elettronico mediante autenticazione sull'infrastruttura nazionale, attraverso l'utilizzo di differenti strumenti di identificazione, come la tessera sanitaria o la carta d'identità digitale[62].

I servizi disponibili sono organizzati in tre macrocategorie funzionali: consenso, per la gestione dell'inserimento e della visualizzazione dei consensi previsti dal fascicolo sanitario elettronico; metadati, per l'indicizzazione e l'aggiornamento dei documenti all'interno dell'indice del fascicolo; e documenti, per le operazioni di ricerca, recupero e trasferimento delle informazioni sanitarie.

In dettaglio, il servizio di comunicazione dell'informativa permette alle regioni e alle province autonome di Trento e Bolzano di trasmettere all'infrastruttura nazionale i documenti contenenti le regole che disciplinano l'attivazione del fascicolo sanitario elettronico da parte degli assistiti. Questa funzionalità non è prevista per le regioni che aderiscono ai servizi in modalità di sussidiarietà, essendo riservata esclusivamente a quelle che utilizzano il servizio come "traduttore di linguaggio", finalizzato

---

[60] Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 7.

[61] Se la regione non è in possesso dovrà seguire la procedura prevista dal sistema TS (Tessera sanitaria) per il rilascio: Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 8.

[62] Per un approfondimento relativo alla carta d'identità digitale, v. I. MACRÌ, *Digitalizzazione, innovazione e sicurezza nella P.A.,* cit., 162 ss.

a garantire l'interoperabilità tra sistemi differenti. L'informativa, inviata tramite documentazione in formato PDF, deve contenere puntuali riferimenti relativi alla normativa relativa al trattamento dei dati personali[63] e al fascicolo sanitario elettronico, al fine di rendere chiaro il funzionamento, il contenuto e le modalità di consultazione.

Inoltre, deve essere predisposta apposita modulistica per la raccolta del consenso del soggetto interessato. Tutte le regioni e le province autonome sono tenute a trasmettere all'infrastruttura nazionale la propria informativa, al fine di consentire agli assistiti di esprimere validamente il proprio consenso[64].

È previsto anche il servizio di recupero dell'informativa, che permette a un attore del processo abilitato di acquisire i documenti forniti dalle regioni e province autonome[65].

La comunicazione dei consensi consente a un attore autorizzato di esprimere le diverse tipologie di consenso previste[66]. Ogni manifestazione di consenso viene trattata come una nuova espressione: non è possibile

---

[63] «*1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.*»: art. 2-*sexies*, D.lgs. 30 giugno 2003, n. 196

[64] Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 10.

[65] Per un ulteriore approfondimento sulle specifiche tecniche v. Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 11.

[66] «*Le tipologie di consenso che possono essere espresse dall'assistito sono: 1. all'alimentazione del FSE: per inserire nuovi documenti, aggiornarli oppure cancellarli; 2. alla consultazione del FSE: per leggere i documenti del FSE; 3. al pregresso: per far confluire nel FSE i documenti prodotti in precedenza, ossia nei periodi in cui non era espresso il consenso all'alimentazione del FSE. Tutte le tipologie di consenso agiscono sull'intero FSE del cittadino e per ciascun tipo di consenso può essere espressa la relativa revoca. Di seguito viene riportato il contenuto della banca dati dell'anagrafe dei consensi e delle revoche. Tali consensi e revoche sono trasmessi e aggiornati attraverso il FSE istituito presso la regione o provincia autonoma di assistenza, ovvero il SASN.*»: allegato B, d.m. 4 agosto 2017, *Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE) di cui all'art. 12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179*, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, in G.U. n. 195, 2017.

modificare parzialmente o integralmente le scelte precedenti, ma è necessario indicare nuovamente tutti i consensi richiesti, che sostituiscono integralmente quelli già registrati[67]. La previsione del rinnovo del consenso favorisce la tutela del soggetto coinvolto.

Inoltre, attraverso questo tipo di integrazione, gli attori abilitati possono consultare i consensi di un assistito, conformemente a quanto stabilito dalla normativa regionale[68].

Il servizio di comunicazione dei metadati consente, previa autorizzazione, di procedere all'indicizzazione di un documento mediante la trasmissione dei relativi metadati. Tale comunicazione viene effettuata, per il tramite dell'indice nazionale delle interoperabilità, da parte di soggetti afferenti alla regione di erogazione e destinata alla regione di assistenza competente.

Le regioni che operano in modalità "sussidiarietà" e utilizzano il servizio di comunicazione dei metadati devono trasmettere, oltre ai metadati necessari per l'indicizzazione, anche eventuali allegati. Al contrario, le regioni che impiegano il servizio come "traduttore di linguaggio" devono inviare solo i metadati per l'indicizzazione, poiché il documento di riferimento è già disponibile nei loro sistemi[69].

Il servizio di cancellazione dei metadati è riservato esclusivamente al soggetto processuale che risulta essere l'autore del documento. Tale soggetto può eliminare i metadati precedentemente associati, utilizzando il servizio di comunicazione previsto[70].

Il servizio di ricerca documenti consente a un attore del processo, abilitato all'utilizzo di tale funzionalità, di richiedere i documenti appartenenti ad un

---

[67] Per un ulteriore approfondimento sulle specifiche tecniche v. Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 12 e 13.

[68] Per un ulteriore approfondimento sulle specifiche tecniche v. Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 14 e 15.

[69] Per ulteriori approfondimenti di natura tecnica v. Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 16 e ss. Fino a 27.

[70] Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 28 e 29.

assistito relativamente a un determinato periodo di tempo, sotto forma di lista di metadati[71].

È inoltre previsto un servizio che consente a un attore del processo di recuperare un documento; deve trattarsi di un soggetto abilitato all'utilizzo di tale servizio. La ricerca del documento si basa sulla lista di metadati ottenuta come esito del servizio di "ricerca documenti"[72].

Attraverso il servizio denominato "esito caricamento documenti", il soggetto legittimato nel processo, e precedentemente abilitato all'uso della specifica funzionalità, riceve un riscontro sull'esito dei controlli effettuati dal sistema FSE-INI[73] in relazione a un documento trasmesso.

L'accesso al suddetto servizio è riservato esclusivamente alle regioni che operano in regime di *sussidiarietà*. Sono pertanto escluse le regioni che utilizzano il sistema FSE-INI unicamente con funzione di "traduttore", poiché, in tali casi, i documenti risultano archiviati nei sistemi informativi regionali di rispettiva competenza[74].

Il servizio di trasferimento degli indici consente il passaggio dei metadati documentali indicizzati relativi a un assistito da una regione di assistenza a un'altra, nel caso in cui intervenga un cambiamento nella competenza territoriale.

---

[71] Per ulteriori approfondimenti di natura tecnica v. Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 30, 31 e 32.

[72] Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, Versione 2.6.1, 16 maggio 2025, 33 e 34.

[73] «e*) «FSE-INI», infrastruttura e servizi telematici dell'INI per le regioni e province autonome che, ai sensi del comma 15-ter, punto 3) del predetto art. 12, comunicano al Ministero dell'economia e delle finanze e al Ministero della salute di volersi avvalere dell'INI ai sensi del comma 15 del citato art. 12*»: art 1, comma 1, lettera e), d.m. 4 agosto 2017.

[74] L'esito dell'elaborazione trasmesso dal sistema può essere di tre tipi. Se il documento è privo di errori e viene accettato dal sistema FSE-INI, l'esito sarà "OK". In caso contrario, se il documento presenta errori o non è conforme ai requisiti richiesti, viene respinto con l'esito "KO". Esiste anche una terza possibilità: "ELAB", che indica che il documento è ancora in fase di elaborazione da parte del sistema e non ha ancora ricevuto un esito definitivo: sul punto, v. Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, cit., 36.

In particolare, il processo può essere attivato secondo due differenti modalità operative: *pull* e *push*[75].

Le interazioni tra il sistema dell'infrastruttura nazionale e i *registry* regionali o nazionali, anche in caso di coincidenza tra regione di assistenza e regione di erogazione, sono state definite dalle specifiche previste per il Fascicolo Sanitario Elettronico 2.0 e sono finalizzate alla gestione dei metadati documentali. Nello specifico, si articolano in quattro scenari operativi: indicizzazione di un nuovo documento, aggiornamento dei metadati, sostituzione dell'indice e cancellazione logica dell'indice del documento.

L'attivazione di ciascuno di questi scenari avviene tramite l'invocazione, da parte dei sistemi produttori o pubblicatori, dei servizi esposti mediante il *gateway*[76], componente tecnologica prevista dal d.m. n. 7 del 2023[77].

A seguito del cambiamento di contesto architetturale introdotto dalle Linee Guida di attuazione del FSE 2.0, tutte le interazioni con i *registry* sono

---

[75] A seguito della variazione della Regione di Assistenza (RDA) dell'assistito, il trasferimento degli indici documentali associati al Fascicolo Sanitario Elettronico (FSE) può avvenire secondo due distinte modalità, disciplinate dal *framework* "*dataset*" definito da AgID. Nella modalità denominata "*pull*", il procedimento è attivato dalla regione subentrante (nuova RDA), la quale assume la responsabilità della tempestiva acquisizione degli indici relativi a tutti i documenti sanitari dell'assistito, ivi compresi quelli qualificati come oscurati e/o deprecati. Tale modalità è riservata esclusivamente alle Amministrazioni regionali che operano avvalendosi del Sistema INI nella qualità di "traduttore", restando pertanto inapplicabile alle regioni operanti in regime di "sussidiarietà". La nuova RDA è responsabile dell'intera sequenza procedimentale, che comprende: il reperimento dei metadati, il completamento della prima fase di acquisizione e, solo successivamente, l'attivazione del servizio di cancellazione dei metadati, al fine di evitare la perdita irreversibile di informazioni documentali prima dell'avvenuto trasferimento. In alternativa, nella modalità "*push*", il sistema INI attiva autonomamente il procedimento non appena riceve notifica di variazione della RDA da parte del sistema ANA. Anche tale modalità è riservata alle regioni che operano in modalità "traduttore". In questa ipotesi, il sistema INI cura l'intero flusso operativo, articolato in: recupero e trasferimento degli indici in area temporanea; cancellazione dei metadati subordinata alla corretta acquisizione degli stessi; trasferimento definitivo all'interno dell'indice documentale della nuova RDA, subordinatamente alla conferma di quest'ultima ovvero alla risoluzione di eventuali conflitti derivanti dalla pluralità di regioni precedenti di appartenenza: v. Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, cit., 37,38 e 39.

[76] Cfr. ampiamente A. N. DUEÑAS, P. A. TIFFIN, G. M. FINN, *Understanding gateway to medicine programmes,* in *Clean Teach,* 2021.

[77] Tutti i dettagli relativi ai flussi di interoperabilità, ai *dataset* scambiati e agli esempi di messaggi inviati tra il sistema produttore, il *gateway* e i sistemi di pubblicazione sono illustrati nel documento tecnico "*Specifiche di integrazione ai servizi gateway*" disponibile al seguente link: (https://github.com/ministero-salute/it-fse-support/tree/main/doc/integrazione-gateway#1-introduzione).

gestite esclusivamente tramite il *gateway*. In questo contesto, l'Infrastruttura Nazionale trasmette alla regione di assistenza, operante in regime di sussidiarietà, i metadati relativi a documenti generati sia internamente che esternamente alla stessa regione, tramite la nuova infrastruttura.

Lo scenario relativo all'indicizzazione di un nuovo documento basato sulla pubblicazione del documento da parte dell'attore competente, opera nel dominio regionale in regime di sussidiarietà, mediante invocazione del servizio esposto dal *gateway*.

Una volta ricevuta la richiesta, il *gateway* recupera i metadati presenti sia nel *token* sia nella richiesta stessa, integrandoli con quelli già estratti dal documento. Successivamente, il *gateway* valida la richiesta e costruisce la relativa asserzione di attributo, ossia un documento digitale strutturato che attesta, secondo formati standardizzati, una o più caratteristiche qualificanti dell'utente.

Completata questa fase, il processo prosegue attraverso diverse interazioni tra gli attori coinvolti: il *gateway* trasmette l'asserzione di attributo al servizio dell'infrastruttura nazionale dedicato alla comunicazione dei metadati. Il sistema nazionale, una volta validata la richiesta, archivia le informazioni contenute nell'asserzione, utili per notificare alla regione erogatrice l'avvenuta registrazione. Contestualmente, l'infrastruttura nazionale verifica l'identificativo dell'assistito tramite il sistema anagrafico, ottenendo informazioni relative alla regione di assistenza di riferimento e agli identificativi associati, anche se non più validi.

Se tutte le verifiche hanno esito positivo, l'infrastruttura nazionale trasmette la richiesta di comunicazione dei metadati al servizio di sussidiarietà del *registry* regionale, qualora dal sistema anagrafico emerga una regione di assistenza diversa. In caso di verifica negativa, l'infrastruttura nazionale risponde al *gateway* con un messaggio di errore, interrompendo il flusso.

Il servizio di sussidiarietà regionale fornisce quindi un riscontro all'Infrastruttura Nazionale, confermando l'avvenuta registrazione o trasmettendo un messaggio di errore. In caso di esito positivo,

l'Infrastruttura Nazionale notifica la comunicazione anche alla regione erogatrice, indipendentemente dal fatto che coincida o meno con la regione di assistenza[78].

Qualora un soggetto autorizzato proceda alla modifica di uno o più metadati associati a un documento, senza intervento diretto sul documento coinvolto, si configura lo scenario di aggiornamento metadati.

Una volta completate le operazioni preliminari, si avvia una sequenza di interazioni tra i diversi attori coinvolti nel processo[79].

Sono previsti anche lo scenario di sostituzione dell'indice di un documento[80] e quello di cancellazione logica dello stesso, nel caso in cui un documento

---

[78] Infine, l'INI inoltra al *gateway* il messaggio ricevuto dal servizio di sussidiarietà, sia in caso di esito positivo che negativo: Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, 42.

[79] Il *gateway* costruisce un'asserzione di attributo e procede a recuperare, tramite l'infrastruttura centrale, il riferimento al documento oggetto di aggiornamento attraverso il servizio dedicato. Qualora non sia possibile reperire tale riferimento, il flusso viene interrotto e viene restituito un errore al sistema chiamante. Successivamente, il *gateway* recupera i metadati associati al documento individuato, impiegando a tal fine il servizio di ricerca documenti o il servizio di sussidiarietà. Anche in questo caso, l'impossibilità di ottenere la lista dei metadati comporta l'interruzione del processo e la comunicazione di un errore al sistema invocante.
Una volta ottenuti i metadati esistenti, il *gateway* procede al loro aggiornamento integrando i dati provenienti dal *token* e quelli presenti nel corpo della richiesta, estratti precedentemente dal documento. Viene quindi generata una nuova asserzione di attributo, che, attraverso il servizio di comunicazione metadati o quello di sussidiarietà, viene trasmessa all'infrastruttura nazionale. Quest'ultimo provvede alla validazione della richiesta ricevuta, conservando l'informazione contenuta nell'attributo *organization-id*, utile alla successiva notifica verso la regione di erogazione dell'avvenuto aggiornamento. Dopo aver consultato il sistema anagrafe per identificare la regione di assistenza competente, l'infrastruttura nazionale inoltra la richiesta al *registry* regionale individuato, al relativo servizio di sussidiarietà oppure, in assenza di una regione di assistenza associata, al *registry* nazionale. Qualora anche una sola delle verifiche dia esito negativo, il processo viene interrotto e il *gateway* riceve una risposta di errore.
Il *registry* destinatario, sia esso regionale, nazionale o in sussidiarietà, restituisce all'infrastruttura nazionale l'esito dell'operazione, che può consistere in una conferma dell'avvenuto aggiornamento o in un messaggio di errore. In caso di esito positivo, l'infrastruttura nazionale provvede a inviare notifica di avvenuta comunicazione alla regione di erogazione competente, anche qualora quest'ultima coincida con la regione di assistenza.
L'infrastruttura nazionale provvede all'inoltro al *gateway* del messaggio ricevuto dal *registry* regionale, dal Servizio di sussidiarietà per il *registry* regionale o dal *registry* nazionale sia in caso di avvenuta registrazione dei metadati che in caso di errore: Dipartimento per la trasformazione digitale*, Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà,* cit., 44.

[80] Ogniqualvolta il documento originario venga rimpiazzato con una nuova versione. In tale contesto, l'attore designato all'interno del dominio regionale in regime di sussidiarietà (quale ad esempio un *repository* o *middleware* regionale) attiva il servizio di sostituzione documento offerto dal *gateway*: Dipartimento per la trasformazione digitale*, Specifiche*

venga eliminato, rendendo necessaria la rimozione dei relativi metadati. Tale operazione è avviata dall'attore preposto nel dominio regionale, mediante l'invocazione del servizio di cancellazione esposto dal *gateway*.

Dopo il completamento delle attività preliminari, il *gateway* interagisce con l'Infrastruttura Nazionale per ottenere il riferimento del documento da eliminare. Se il documento non viene individuato, il processo si interrompe e viene restituito un messaggio di errore. Qualora il documento sia reperito, il *gateway* ne recupera i metadati tramite l'infrastruttura nazionale; se anche questi risultano irreperibili, il flusso viene arrestato.

Una volta recuperate le informazioni, il *gateway* costruisce una nuova asserzione e invia la richiesta di cancellazione dei metadati all'infrastruttura nazionale, che procede alla validazione. Successivamente, interagisce con il sistema anagrafico per individuare la regione di assistenza e inoltrare la richiesta al registro competente.

Nel caso in cui una delle verifiche fallisca, il processo si blocca e viene restituito un messaggio di errore. Se la cancellazione va a buon fine, l'infrastruttura nazionale informa la regione di erogazione e comunica l'esito al *gateway*[81].

Le operazioni di aggiornamento e cancellazione dei documenti sanitari contenuti nel FSE 2.0, effettuate tramite portale *web*, avvengono quando un utente autorizzato invia un nuovo documento sanitario attraverso un *form* dedicato disponibile sul portale.

Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà, cit., 45 e 46.; per ulteriori approfondimenti relativi alla definizione dei principi per la conformità dei middleware regionali con FSE 2.0. consultare il sito (https://github.com/ministero-salute/it-fse-support/tree/main/doc/middleware-regionale)

[81] Il *gateway* costruisce un'asserzione e chiede all'infrastruttura nazionale il riferimento del documento da sostituire. Se il documento non viene trovato, il processo si interrompe. In caso contrario, il *gateway* crea una nuova asserzione e invia all'infrastruttura nazionale i metadati del nuovo documento insieme a quelli del documento da rimpiazzare.
L'infrastruttura nazionale valida la richiesta, conserva l'*organization-id* e verifica l'identità dell'assistito tramite il sistema anagrafe. Se tutte le verifiche vanno a buon fine, la richiesta viene trasmessa al registro competente. Il registro restituisce un riscontro, confermando l'avvenuta sostituzione oppure segnalando un errore. Infine, l'infrastruttura nazionale notifica la regione di erogazione e comunica al *gateway* l'esito dell'operazione: Dipartimento per la trasformazione digitale, *Specifiche Tecniche Dell'Infrastruttura Nazionale di Interoperabilità (INI) ad uso delle Regioni In Sussidiarietà*, 47 e 48.

In questo contesto, il portale assume a tutti gli effetti il ruolo di produttore di documenti, al pari degli altri attori abilitati, e deve seguire l'iter di accreditamento presso il *gateway*, conformemente alle specifiche di integrazione previste per i servizi del FSE 2.0.

Una volta accreditato, il portale deve avvalersi dei servizi forniti dal *gateway* e utilizzare quelli descritti in precedenza per le operazioni di aggiornamento ed eliminazione dei documenti e dei relativi metadati, in conformità con le disposizioni procedurali e tecniche definite nel modello architetturale del FSE 2.0.

L'analisi condotta finora delinea un quadro chiaro dell'evoluzione tecnico-organizzativa del fascicolo sanitario elettronico, evidenziando come l'Infrastruttura Nazionale, gli standard di interoperabilità (come HL7) e i meccanismi di gestione federata delle informazioni costituiscono i pilastri di una sanità che si è inteso architettare come efficiente e sicura.

Per valorizzare appieno il potenziale di questi strumenti, è necessario inquadrarli in un contesto più ampio, capace di superare i confini nazionali e di promuovere la circolazione transfrontaliera dei dati sanitari. In tale prospettiva si colloca lo Spazio Europeo dei Dati Sanitari[82], la cui normativa, fortemente intrecciata con la disciplina della tutela dei dati personali, sarà oggetto di approfondimento nei capitoli successivi[83].

---

[82] Regolamento sullo spazio europeo dei dati sanitari (UE) 2025/327, 11 febbraio 2025, in G.U.U.E., 5 marzo 2025

[83] «*Today nearly 30% of the world's data are generated by the healthcare industry.1 These data are typically collected for administrative purposes and are often proprietary. Moreover, data on factors that influence health (such as social determinants) increasingly are captured outside of the healthcare system. Although big healthcare data have the potential to improve patient outcomes and ultimately reduce healthcare costs, much of these data are siloed in disparate systems and platforms, making it difficult to access by researchers in both the health economics and outcomes research (HEOR) and health services research fields. In addition, in many jurisdictions, access to personal data is regulated by data privacy legislation. Although confidentiality and antidiscrimination efforts are necessary, there is a direct trade-off between assuring data privacy and allowing access to deidentified data to support health research aimed to improve population health. To leverage health data for research purposes, interoperability—that is, the ability to access, integrate, and cooperatively use data in a coordinated way both within and across different information systems, devices, and countries—is essential.* »: C. D. MULLINS, M. F. DRUMMOND, *Data Privacy and Health: How Do We Achieve the Right Balance?*, in *Value Heal*th, 2023.

CAPITOLO II

LA DIGITALIZZAZIONE DEI DATI SANITARI: SFIDE GIURIDICHE E PROSPETTIVE EUROPEE.

SOMMARIO:1. Lo spazio digitale come oggetto giuridico. 2. L'evoluzione della tutela dei dati personali nell'UE: dal consenso alla protezione preventiva. 3. La sicurezza dei dati sanitari: dal GDPR allo *European Health Data Space*. 4. Pseudonimizzazione: interpretazione alla luce di una recente pronuncia della Corte di Giustizia europea.

1. Lo spazio digitale come oggetto giuridico.

La digitalizzazione ha dato vita a numerose problematiche giuridiche che rappresentano una sfida cruciale per il diritto contemporaneo e impongono una revisione dei paradigmi tradizionali. Tra queste si evidenziano: la crisi del binomio territorio-sovranità e la conseguente difficoltà di garantire la protezione dell'individuo nel dominio informatico, la necessità di bilanciare i diritti fondamentali e l'esigenza di ridefinire lo spazio digitale come oggetto giuridico.

L'innovazione tecnologica incide direttamente sulla tutela dei diritti fondamentali, imponendo un aggiornamento della regolamentazione ordinaria. Il diritto è chiamato a adattarsi alle evoluzioni di natura tecnica e sociale, continuando ad assicurare l'ordinaria funzione di garanzia per la convivenza civile[84]. Tuttavia, la rapidità della transizione tecnologica ha spesso reso tardivi gli interventi normativi, creando un contesto in cui la riflessione giuridica fatica ad anticipare le implicazioni etiche e sociali dell'innovazione. Le questioni controverse che scaturiscono dalla

[84] La I Conferenza La.Ne.T. è stata incentrata sul tema delle transizioni digitali, affrontato mediante strumenti giuridici e con un approccio interdisciplinare, evidenziando come la digitalizzazione, pur nascendo nel contesto delle discipline STEM (*Science, Technology, Engineering e Mathematics*), presenti profonde implicazioni normative e costituisca una sfida cruciale per il diritto contemporaneo. La conferenza ha valorizzato il dialogo tra giuristi e studiosi di altre discipline, tentando di superare la frammentarietà degli approcci e offrendo una visione sistemica del fenomeno.

digitalizzazione sono numerose e mettono in discussione i paradigmi evolutivi tradizionali, inducendo una marcata revisione del ruolo del diritto stesso.

Uno dei primi nodi critici riguarda la crisi del tradizionale legame tra territorio e sovranità: la rete digitale si sottrae ai confini giuridici dello Stato, rendendo più difficile l'applicazione delle garanzie previste dall'ordinamento. Ne deriva una condizione di vulnerabilità per l'individuo, esposto a poteri non sempre soggetti a limiti e obblighi giuridici.

In questo scenario si impone una ricostruzione del sistema delle garanzie capace di estendersi anche ai nuovi spazi virtuali. L'identità della persona è messa in discussione dall'uso pervasivo delle piattaforme digitali[85], che attraverso strumenti di profilazione e tracciamento, riducono la capacità di autodeterminazione dell'individuo, trasformandolo in un oggetto di analisi algoritmica[86].

---

[85] L'adozione di una Dichiarazione dei diritti in Internet, quale forma sui generis di regolamentazione fondata non sulla previsione di regole e sanzioni, ma sul bilanciamento degli interessi coinvolti, rappresenta l'obiettivo della Commissione di studio istituita nel 2014 e presieduta da Stefano Rodotà. Tale documento non nasce come atto normativo vincolante, bensì come strumento di orientamento per il legislatore, volto a promuovere scelte normative centrate sui diritti in rete e sulle loro peculiarità: P. FALLETTA, *Lezioni di diritto pubblico del digitale*, CEDAM, 2024, 7 e 8, anche in *One legale*.

L'idea alla base del progetto è quella di una rete caratterizzata da un perimetro ampio, una sorta di spazio autonomo nel quale è necessario garantire la tutela dei diritti fondamentali, considerati i potenziali abusi che possono diffondersi rapidamente su larga scala. L'ambizioso tentativo di delineare un quadro giuridico per la tutela dei diritti digitali investe numerosi ambiti, dal diritto alla protezione dei dati sino alla necessità di programmi dedicati all'educazione digitale, con particolare attenzione alla consapevolezza del ruolo dell'anonimato. Tuttavia, l'aspetto maggiormente problematico della Dichiarazione riguarda la prospettiva eccessivamente individualista, che trascura la dimensione collettiva dei diritti digitali, nonostante il potenziale aggregativo delle tecnologie: per una riflessione critica, v. A. MORELLI*, I diritti e la rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet,* in *Federalismi.it*, 2015, 12 e ss.

Un cenno alla Dichiarazione dei diritti in Internet offre l'occasione per riaffermare la centralità degli ordinamenti nazionali nella creazione di spazi digitali inclusivi, in un momento storico caratterizzato da profonde trasformazioni tecnologiche. Già nel 2014 era stata avanzata l'idea di fondare costituzionalmente i diritti digitali in una dimensione sovranazionale, pur tra molte incertezze metodologiche. Sebbene appaia condivisibile la concezione della portata globale della rete e la consapevolezza che molte difficoltà non possano essere risolte mediante il solo diritto nazionale, non può tuttavia essere trascurata la necessità di interventi all'interno dei quadri regolatori interni. Le divergenze tra Stati in occasione dell'adozione di trattati internazionali — si pensi al trattato di Dubai del 2012 — dimostrano la difficoltà di giungere a una governance armonizzata della rete, a causa della pluralità degli interessi in gioco: A. MORELLI, *I diritti e la rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet,* cit., 17 e ss.

[86] F. DE SIMONE, L. DI MAJO, M. RUSSO*, Le transizioni digitali*, in *Rivista di Diritto dei Media*, 2025, 16 e ss.

Da ciò deriva l'esigenza di qualificare giuridicamente lo spazio digitale. Esso si configura come una rete materiale di trasmissione di energia e di dati in cui le informazioni digitali possono essere considerate "beni" ai sensi degli articoli 813 e 814 del Codice civile, in quanto oggetto di diritti e dotati di valore economico[87].

Le tecnologie emergenti hanno così modificato le coordinate spazio-temporali delle relazioni giuridiche, imponendo una revisione delle categorie dogmatiche tradizionali, sia in ambito privatistico che internazionale[88].

La diffusione delle tecnologie dell'informazione ha dato vita a numerose nuove opportunità, ma ha anche generato criticità legate alla tutela della riservatezza e l'aumento dell'uso di strumenti digitali, nuovi e preesistenti, ha posto al centro del dibattito giuridico la necessità di bilanciare diritti fondamentali, come il diritto alla salute con quello alla protezione dei dati personali[89].

---

[87] Gli articoli 813 e 814 c.c. assumono rilievo in questo contesto: il primo estende le disposizioni sui beni mobili a tutti gli altri diritti, mentre il secondo include tra i beni mobili le energie naturali aventi valore economico.

[88] Un esperimento concettuale particolarmente interessante approfondisce il rapporto tra spazio digitale, tempo e tecnologia, analizzando le conseguenze giuridiche della trasformazione spazio-temporale nella società digitale. Tale esperimento evidenzia che la tecnologia digitale agisce in dimensioni fisiche misurabili, mostrando come tempo e spazio siano variabili influenzate da fattori esterni. La tecnologia non si limita a occupare lo spazio, ma lo genera, creando nuovi ambienti di azione sempre più complessi. Lo spazio digitale si configura così come fenomeno giuridicamente rilevante, sia per la sua infrastruttura immateriale, sia per la capacità di produrre effetti normativi. Tale complessità impone una revisione delle categorie dogmatiche tradizionali e l'elaborazione di una teoria generale del diritto digitale capace di cogliere la natura dinamica della tecnologia: v. A. GORASSINI, *Lo spazio digitale come oggetto di un diritto reale?*, in *Rivista di diritto dei media*, 2, 2018, 60 e 61.

Tra i numerosi esempi pratici, emerge il tema della protezione dei dati personali e della *privacy* nel Metaverso, che obbliga il giurista a ripensare molte categorie tradizionali alla luce della trasformazione digitale. Il Metaverso, inteso come rete interoperabile che consente l'interazione tra utenti mediante avatar digitali, solleva questioni rilevanti per quanto riguarda la raccolta e il trattamento di dati biometrici e comportamentali, spesso effettuati tramite dispositivi immersivi senza piena consapevolezza dell'utente. Garantire il diritto alla riservatezza nel suo significato originario risulta particolarmente complesso. Il Metaverso impone quindi una profonda riflessione sul rapporto tra tecnologia, identità e libertà: v. A. ROSANÒ, *Tra Neuromanti e pecore elettriche: Metaverso e tutela dei dati personali e della privacy*, *in Rivista di Diritto dei Media*, 2025, 1, 84 e ss.

[89] «*Sebbene in periodi di crisi socio-sanitaria come quello attuale, ogni bilanciamento tra la protezione del diritto alla vita e il diritto inviolabile alla tutela dei dati personali diviene "ineguale", in quanto quest'ultimo diritto diviene recessivo davanti al superiore bene che è la vita stessa, messa in discussione dall'emergenza, il potenziale utilizzo dei dati personali su larga scala pone un tema di diritto costituzionale, determinando una*

Tale esigenza è emersa con particolare forza durante la pandemia da COVID-19, quando il diritto alla salute, sancito dall'articolo 32 della Costituzione, ha assunto un ruolo prevalente, giustificando limitazioni alla libertà di circolazione[90] e l'adozione di nuovi strumenti digitali per la gestione dell'emergenza. In questo contesto, la tecnologia è stata impiegata per dematerializzare strumenti di medicina ordinaria, ridurre il contatto fisico e ottimizzare l'erogazione delle cure[91], stravolgendo il perimetro di azione delle norme.

La dialettica tra vantaggi e criticità dell'innovazione tecnologica si sviluppa lungo due direttrici: da un lato, la tecnologia come potenziale minaccia da contenere per proteggere i diritti fondamentali; dall'altro, come strumento di espansione e, in taluni casi, di creazione di nuovi diritti. Questa tensione si riflette nella necessità di bilanciare divieti di ingerenza, diritti di difesa e diritti emergenti, in un contesto giuridico in continua evoluzione, con un confronto costante tra esigenze di evoluzione e tutela[92]. In questo quadro, assume particolare rilievo il bilanciamento tra la tutela della salute e la protezione dei dati sensibili[93] ove la transizione digitale impone una ricostruzione del sistema delle garanzie per adattarlo al nuovo contesto globale, nel quale la persona esige tutela anche nei nuovi spazi virtuali[94].

Questa riflessione si colloca nel più ampio contesto delle sfide poste dall'entrata in vigore del Regolamento sullo Spazio europeo dei dati sanitari, che mira a creare un sistema normativo basato sull'interoperabilità e sulla protezione dei diritti fondamentali anche nello spazio digitale. Questo è un

---

potenziale ingerenza nella qualità della vita del soggetto stesso»: F. COVINO, *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in *federalismi.it*, 2021, 44.

[90] Come stabilito dall'art. 16 Cost., la libertà di circolazione può essere limitata solo per motivi di sanità o sicurezza.

[91] L'analisi approfondita degli strumenti di archiviazione clinica digitalizzati, come il fascicolo sanitario elettronico e il dossier sanitario, è stata inserita nel Capitolo III*: "Regolamento sulla creazione dell'EHDS: il problema dell'interoperabilità dei dati sanitari".*

[92] A. GORASSINI, *Lo spazio digitale come oggetto di un diritto reale?*, in *Rivista di diritto dei media*, cit., 56 e ss.

[93] G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati*, cit., 110 e ss.

[94] F. DE SIMONE, L. DI MAJO, M. RUSSO, *Le transizioni digitali*, in *Rivista di Diritto dei Media*, cit., 11 e ss.

caso in cui la regolamentazione ambisce a rafforzare un nuovo spazio giuridico digitale che richiede un potenziamento delle misure di tutela, già complesse da garantire nella realtà ordinaria.

2. L'evoluzione della tutela dei dati personali nell'UE: dal consenso alla protezione preventiva.

Per rispondere alle criticità connesse alla protezione dei dati personali, l'ordinamento europeo ha dato vita a strumenti normativi volti a conciliare la tutela dei diritti fondamentali, la sicurezza dei trattamenti e la responsabilizzazione dei soggetti interessati: dal punto di vista del diritto, i dati personali non vengono considerati semplicemente come informazioni neutre, ma come elementi strettamente legati alla dignità e ai diritti fondamentali dell'individuo[95].

I principali approfondimenti emersi nel processo di analisi della regolazione riguardano la distinzione tra riservatezza e protezione dei dati come diritto fondamentale, le tensioni tra diritti di pari rango e la necessità di bilanciamento, i limiti della disciplina previgente e l'innovazione introdotta dal GDPR in termini di tutela preventiva, sicurezza e centralità dell'interessato.

La protezione dei dati si distingue dalla tradizionale nozione di riservatezza, configurandosi come diritto dinamico e in costante espansione, dotato di specifiche regole e strumenti di controllo riconosciuti all'interessato. La sua rilevanza deriva dal ruolo centrale che i dati rivestono nello sviluppo della personalità e nell'identificazione dell'individuo nel contesto sociale, rendendo la protezione dei dati inseparabile dalla tutela della dignità umana[96].

---

[95] V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista,* in *Rivista di diritto dei media*, 2, 2018, 33 e ss.

[96] La Carta dei diritti fondamentali dell'Unione sancisce all'art. 8 il diritto alla protezione dei dati personali che va letto congiuntamente all'art. 16 TFUE, il quale , a seguito delle modifiche subite, conferisce alle persone il diritto alla protezione dei propri dati personali: « *Si trascorre, per dirla con Stefano Rodotà, dalla tutela statica e negativa della riservatezza, che, costruita sul modello della proprietà privata, si esaurisce nell'esclusione delle interferenze altrui — in un* right to be let alone *— alla protezione dei dati personali, provvista altresì di una tutela dinamica, composta di regole rigorose che delineano le*

Nel tempo, la concezione classica di riservatezza ha ceduto il passo a modelli fondati sulla responsabilizzazione del soggetto interessato e sull'interazione tra diritti fondamentali di pari rango, spesso in tensione reciproca. La ricerca di un equilibrio tra tali diritti ha ispirato la direttiva 95/46/CE, che ha introdotto principi cardine in un contesto caratterizzato da una spiccata disomogeneità normativa. Essa ha colmato il vuoto regolatorio presente in ordinamenti privi di una disciplina organica, come quello italiano, e ha garantito la libera circolazione dei dati[97].

Tuttavia, la disciplina fondata sul consenso dell'interessato ha mostrato nel tempo limiti strutturali, soprattutto con l'emergere di pratiche come la profilazione, il *data mining* e la *dataveillance*[98]. Pur prevedendo principi di pertinenza e proporzionalità, la direttiva non ha impedito la frammentazione normativa e l'incertezza giuridica.

Il GDPR, successivo alla direttiva, rappresenta un *corpus* normativo volto a disciplinare il trattamento dei dati personali nell'ordinamento europeo. Esso si fonda su un sistema di controllo e intervento da parte dell'interessato, mediante diritti oppositivi come la cancellazione, la

modalità del trattamento e conferiscono poteri di controllo e di intervento alla persona interessata» M. G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, *Europa e Diritto Privato*, 2016, p. 1249, che a sua volta richiama S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2012, 397.

[97] In alcuni ordinamenti, a seguito della Convezione di Strasburgo sono stati effettuati interventi ad hoc: pensiamo al *Data Protection Act* inglese: *Regolamento (UE) 2854, 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828*, in GUUE 22.12.2023.

[98] In particolare, l'art. 15 della Direttiva stabiliva che: «*gli Stati membri riconoscono ad ogni persona il diritto a non essere sottoposta ad una decisione che produca effetti giuridici o che abbia effetti significativi nei suoi confronti, fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento e così via*». Tuttavia, l'attuazione di tale previsione si è rivelata particolarmente complessa, nonostante numerosi tentativi che traevano origine anche da alcune direttive settoriali come la n. 66 del 15 dicembre 1997 e la direttiva n. 58 del 12 luglio 2002, rispettivamente relative al settore della telecomunicazione e al settore delle comunicazioni elettriche, caratterizzate da un prudente approccio tra i diritti individuali, gli interessi economici e le esigenze pubblicistiche, con particolare riferimento alla sicurezza.
Sul punto rileva il contributo decisivo offerto dalla Corte di giustizia dell'Unione europea che hanno contribuito alla delineazione di una tutela rafforzata della *privacy*, v. pronunce: Corte giustizia UE, 8 aprile 2014, (causa C-293/12), nota come *Digital Rights Ireland*, Corte giustizia UE, 13 maggio 2014, (C-131/12), nota come *Google Spain (Costeja González*); Corte di giustizia UE, 6 ottobre 2015, (C-362/14), nota come *Schrems*.

rettifica e la limitazione del trattamento, che costituiscono strumenti di tutela contro trattamenti illeciti.

Pur perseguendo l'unificazione della disciplina, il regolamento ha riconosciuto agli Stati membri un margine di intervento normativo, consentendo l'introduzione di disposizioni nazionali per evitare lacune applicative. L'intervento materiale del Regolamento (UE) 2016/679 è stato ampliato rispetto alla direttiva 95/46/CE: il concetto di trattamento è stato esteso anche ad operazioni automatizzate e non automatizzate riferite a dati contenuti o destinati a figurare in un archivio[99].

Particolarmente rilevante è l'espansione della nozione di "dati personali" che include nuove categorie identificative come i dati relativi all'ubicazione, dati biometrici e genetici e dati identificativi online[100]. Il regolamento ha inoltre esteso il concetto di trattamento, includendo operazione come la strutturazione, l'uso e la limitazione, e ha introdotto la definizione di

---

[99] «*trattamento di dati personali*» («*trattamento*»): *qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione , l'elaborazione o la modifica , l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*.»: Articolo 2, lettera b), *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in GUUE L 281 del 23.11.1995.
«*trattamento*»: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*» : Articolo 4, Regolamento 679/2016 GDPR.

[100] Il concetto di identificabilità viene fornito dal considerando n. 26 che chiarisce che essa va valutata in base ai mezzi disponibili per il titolare e per i terzi. «*Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.*»: Considerando 26, Regolamento (UE) 2016/679 (GDPR).

"profilazione" quale trattamento automatizzato volto alla valutazione di aspetti afferenti alla sfera personale del soggetto[101].

Elemento distintivo del GDPR è l'abbandono dell'approccio meramente riparatorio adottato dalla direttiva, sostituito da una tutela preventiva fondata su strumenti come la valutazione d'impatto sulla protezione dei dati personali[102] e i principi di *privacy by design e privacy by default*[103]. L'articolo 25 del regolamento codifica tali concetti, imponendo al titolare l'adozione di misure tecniche e organizzative sin dalla fase di progettazione, nel rispetto del principio di minimizzazione, che impone un trattamento strettamente pertinente alla finalità prevista[104].

Il Regolamento (UE) 2016/679 conferisce alla sicurezza un ruolo centrale, elevandola a principio cardine. Essa assume efficacia diretta nei rapporti tra titolare, responsabile e interessato, imponendo un controllo sin dall'origine del trattamento e garantendo un monitoraggio costante. Così declinata, la

---

[101] «*profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*»: Articolo 4, Regolamento 679/2016 GDPR.

[102] La valutazione d'impatto è obbligatoria quando un trattamento presenta una forte possibilità di rischio elevato per i diritti e le libertà fondamentali.
«*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.»*: Articolo 35, paragrafo 1, Regolamento (UE) 2016/679 (GDPR).

[103] In particolare, il concetto di *privacy by design* fa riferimento all'integrazione di misure di protezione dei dati personali già nella fase di progettazione. Tale scelta trae origine dal fallimentare approccio meramente riparatorio adottato dalla precedente Direttiva 95/46, accantonato e sostituito da un'impostazione normativa preventiva.
Il concetto di *privacy by default* è strettamente correlato al principio di minimizzazione che rende chiaro il perimetro di riferimento del trattamento, meglio inteso come raccolta ed elaborazione dei dati strettamente necessari per la funzionalità richiesta. In sintesi, l'utente non deve adottare una condotta attiva per proteggere la propria *privacy*, avviene in automatico: Per un ulteriore approfondimento, v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, Milano, 2018, 53 e ss.

[104] «*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*»: Articolo 25, paragrafo 2, Regolamento (UE) 2016/679 (GDPR).

sicurezza si traduce nel diritto autonomo dell'interessato a un trattamento sicuro, volto alla protezione delle vulnerabilità e alla minimizzazione dei rischi. L'approccio basato sulla *privacy by design e by default*, la valutazione d'impatto e le misure di sicurezza previste dall'art. 32 rafforzano il ruolo della sicurezza che funge da principio informatore dell'intera disciplina[105].

Tra le nuove misure di protezione del GDPR figurano la pseudonimizzazione[106], trattamento che impedisce l'identificazione diretta dell'interessato, mediante la separazione e protezione delle informazioni aggiuntive, e l'anonimizzazione, che garantisce la non identificabilità della persona correlata al dato anonimizzato.

In sintesi, il diritto dell'Unione europea, con l'introduzione del GDPR, ha inteso rafforzare in modo strutturale il contenuto del diritto alla *privacy*, contrastando i rischi di svuotamento derivanti dalle tecnologie pervasive. Il cittadino europeo è posto al centro del sistema, mediante l'integrazione di meccanismi di tutela preventiva che, tuttavia, alla luce della continua evoluzione digitale, mostrano limiti e richiedono un costante aggiornamento interpretativo e applicativo[107].

Tali strumenti - anonimizzazione, pseudonimizzazione, valutazione d'impatto, *privacy by design e by default* - pur richiedendo un costante aggiornamento interpretativo per fronteggiare le evoluzioni tecnologiche, rappresentano una risposta concreta alle primissime sfide poste dalla digitalizzazione.

3. La sicurezza dei dati sanitari: dal GDPR allo *European Health Data Space*.

[105] M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali, Responsabilità Civile e Previdenza,* 2020, 1343 e ss.

[106] *«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*»: Articolo 4, Regolamento (UE) 2016/679 (GDPR).

[107] M. G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, cit., 1249 e ss.

Nel solco delle riflessioni precedenti, è necessario soffermarsi sulla categoria specifica dei dati sanitari, che rappresentano una delle forme più sensibili e maggiormente tutelate all'interno dell'ordinamento europeo. La progressiva digitalizzazione del settore sanitario e l'ambizione del legislatore sovranazionale di promuovere l'interoperabilità e la condivisione dei dati attraverso lo *European Health Data Space* impongono un approfondimento specifico sulle garanzie applicabili alla storia clinica dell'individuo, trattandosi di dati che incidono in modo diretto e profondo sulla sua sfera più intima.

È noto che alcune categorie di dati personali sono tradizionalmente considerate meritevoli di particolare protezione, in ragione degli effetti discriminatori che la loro divulgazione può comportare: tra esse rientrano, in posizione preminente, le informazioni relative allo stato di salute e alla vita sessuale.

La disciplina vigente in materia di protezione dei dati personali, fondata sul Regolamento n. 679 del 2016, ha introdotto un quadro uniforme a livello europeo, finalizzato a garantire un elevato livello di tutela dei diritti e delle libertà fondamentali della persona fisica. In tale quadro, assumono rilievo le "categorie particolari di dati", la cui natura intrinsecamente sensibile impone l'adozione di misure rafforzate di protezione. Il trattamento di tali dati è ammesso esclusivamente in presenza di condizioni tassative e per finalità legittime, tra cui gestione dei servizi sanitari, continuità dell'assistenza, tutela della sicurezza sanitaria e attività di ricerca scientifica[108].

[108] «*Le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica. Pertanto, il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a*

La protezione rafforzata attribuita a tali categorie si fonda su un divieto generale di trattamento, derogabile unicamente in circostanze specifiche. Quando il trattamento è effettuato da professionisti soggetti al segreto professionale, la liceità deriva da finalità di medicina preventiva, medicina del lavoro, diagnosi, assistenza o terapia sanitaria e sociale, gestione dei sistemi sanitari o motivi di pubblico interesse nel settore della sanità[109].

Questa attenzione normativa evidenzia una consapevolezza precoce rispetto all'impatto dell'evoluzione tecnologica sul settore sanitario, anticipando le implicazioni derivanti dalla crescente digitalizzazione dei processi clinici e assistenziali[110].

Il considerando 35 del GDPR offre una definizione ampia di dati personali relativi alla salute, includendo dati genetici, biometrici e quelli derivanti da esami clinici, campioni biologici, diagnosi, trattamenti e informazioni sullo stato fisiologico o biomedico, indipendentemente dalla fonte che li genera[111].

Il regolamento sancisce un divieto generale di trattamento dei dati sensibili, tra cui rientrano i dati genetici, biometrici, sanitari, volto a tutelare la dignità e la riservatezza della persona, prevedendo tuttavia deroghe in casi

---

esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.»: Considerando 53, Regolamento (UE) 679/2016 GDPR.

[109] G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, cit., 10 e 11.

[110] Cfr. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, cit., 1 e ss.

[111] *«Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio (1); un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.»*: Considerando 35, Regolamento (UE) 679/2016 GDPR.

specifici: consenso esplicito, tutela di interessi vitali, finalità sanitarie, sanità pubblica, interessi pubblici rilevanti e ricerca scientifica[112].

Con l'adozione del Regolamento 679/2016, si è affermata una distinzione significativa tra dato sensibile e dato sanitario, con quest'ultimo che ha acquistato una propria autonomia concettuale e normativa. L'articolo 4 qualifica come dati relativi alla salute «*dati personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di*

[112]«*1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.*»: Articolo 9, paragrafi 1 e 2, Regolamento (UE) 679/2016 GDPR.

assistenza sanitaria, che rivelano informazioni relative al suo stato di salute»[113]. A ciò si affianca il principio di *privacy by design*, inteso come protezione dei dati sin dalla fase di progettazione dei sistemi e dei processi. Questo principio assume particolare rilievo nel contesto delle piattaforme digitali che gestiscono i dati sanitari, imponendo una progettazione che includa un'analisi preventiva dei rischi possibili per i diritti e le libertà degli interessati[114]. A ciò si affianca il principio di "responsabilizzazione" conosciuto come *accountability* che attribuisce a titolari e responsabili il compito di dimostrare l'adozione di misure idonee ad assicurare la conformità alla normativa[115].

In ambito sanitario, ciò si traduce nella necessità di definire con precisione le modalità, i limiti e le garanzie del trattamento, nonché di assicurare che le informazioni relative allo stato di salute siano comunicate all'interessato o a terzi esclusivamente sulla base di un presupposto giuridico valido o

---

[113] Articolo 4, paragrafo 15, Regolamento (UE) 679/2016 GDPR; Sul punto, v. G. CAPILLI, *Diritto sanitario privato*, 2022, Pisa, 45 ss.

[114] «*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*»: Articolo 35, paragrafo 1, Regolamento (UE) 679/2016 GDPR.

[115] Il cambio di prospettiva tra la vecchia disciplina italiana e il nuovo Regolamento coinvolge anche l'introduzione del concetto di *accountability*.
Precedentemente era sufficiente che il titolare del trattamento si attenesse alle regole previste, al fine di evitare responsabilità, ma con il Regolamento 679/2016, viene riconosciuta allo stesso l'attuazione delle pratiche più adeguate, necessarie per ottimizzare il trattamento dei dati, garantendo elevati standard di sicurezza.
Inoltre, tale principio sancisce un generale flusso di comunicazione tra il titolare e gli altri soggetti coinvolti, tra cui rientrano anche la struttura interessata e l'autorità di controllo al fine di rendere concreta una gestione dei dati basata sul concetto di *privacy*, trasparenza, sicurezza e responsabilizzazione.
Non a caso, il principio di *accountability* trae origine da un contesto in cui si intendeva assicurare un operato trasparente, in maniera specifica facendo riferimento al contesto dell'amministrazione pubblica. Sembra opportuno ricordare che, in realtà tale concetto nell'ambito salute non è del tutto nuovo; già nel 2011 il Ministero della salute fornì una definizione di accountability così delineata: «*esistenza di regole sulla pubblicazione dei piani, relazioni (report), codici di comportamento, rendiconti economici, effettiva pubblicazione, disponibilità e ampia diffusione in una forma comprensibile, programmi sistematici di audit interno, fornitura di linee-guida (per garantire la qualità tecnica), campagne di comunicazione e rendicontazione sociale*»: All. 1, Decreto del ministero della salute, 4 agosto 2011, in G.U., 31 ottobre n. 241.
Sul punto, v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, cit., p. 47 e ss.; si vedano anche Considerando 74, Considerando 75 e Considerando 77, Regolamento (UE) 679/2016 (GDPR).

previa autorizzazione dell'interessato. Su tali presupposti si fonda l'obbligo, gravante sulle strutture sanitarie, di adottare misure tecniche e organizzative volte a prevenire comunicazioni indebite a soggetti non autorizzati.

A ciò si collega il fenomeno del *data breach*, ovvero una violazione della sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'acceso ai dati, con potenziali impatti significativi sulla riservatezza, l'integrità e la disponibilità delle informazioni. Le cause possono essere molteplici: attacchi informatici, errori umani, carenze nei sistemi di aggiornamento e manutenzione[116]. In caso di violazione, il titolare del trattamento è tenuto a notificare l'evento all'autorità di controllo competente[117], mentre la comunicazione agli interessati è obbligatoria quando il rischio per i loro diritti e libertà risulti elevato[118].

---

[116] C. C. GIARDINA, *Il data breach in ambito sanitario: l'importanza di una corretta policy per evitare sanzioni da parte del garante della privacy*, in *Azienditalia*, 2021, 1062 e ss.

[117] In particolare gli obblighi informativi prevedono che il titolare è tenuto a notificare l'evento all'autorità entro 72 ore dalla conoscenza: «*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.»: Articolo 33, Regolamento (UE) 2016/679 (GDPR).

[118] «*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la*

Alla luce di quanto esposto, risulta evidente come il processo di digitalizzazione del settore sanitario, pur costituendo una rilevante occasione di innovazione, richieda una particolare attenzione alla protezione dei dati personali. La delicatezza del trattamento dei dati sanitari ha reso necessari, nel tempo, numerosi interventi da parte del Garante per la protezione dei dati personali, volti a rafforzare le garanzie e a mitigare i rischi connessi[119]. Il settore sanitario, infatti, è tra i più esposti a rischi e violazioni, poiché gestisce una mole ingente di informazioni sensibili, spesso vitali per la persona[120]. Tale vulnerabilità è aggravata dalla crescente digitalizzazione dei servizi e dalla centralità che i dati sanitari rivestono nella gestione dell'assistenza[121].

In questo scenario, le strutture sanitarie assumono un ruolo fondamentale: esse devono dotarsi di sistemi tecnologici adeguati e garantire una formazione continua del personale, poiché il fattore umano rappresenta spesso l'anello debole della sicurezza e una delle principali cause di incidenti e fughe di dati.

A fronte di queste complessità, il legislatore europeo ha avviato un processo di revisione e adattamento dei diritti fondamentali dell'interessato, già riconosciuti dal Regolamento Generale sulla Protezione dei Dati, per rispondere alle specificità del trattamento dei dati sanitari elettronici. In Italia, l'adeguamento dell'ordinamento interno al quadro europeo è stato realizzato mediante il decreto legislativo n. 101 del 2018, che ha modificato il Codice in materia di protezione dei dati personali. Tra le innovazioni maggiormente rilevanti, si segnala il superamento dell'obbligo di acquisizione del consenso per il trattamento dei dati sanitari effettuato per

---

violazione all'interessato senza ingiustificato ritardo.»: Articolo 34, paragrafo 1, Regolamento (UE) 679/2016 GDPR.
Inoltre, il medesimo articolo prevede che la comunicazione deve essere effettuata adottando un linguaggio semplice: Articolo 34, paragrafo 2, Regolamento (UE) 679/2016 GDPR.

[119] Per un approfondimento di alcuni provvedimenti adottati dal Garante *Privacy*, si rinvia al Capitolo III del presente elaborato.

[120] Fra i tanti, si segnala l'attacco subito dall'ASL 1 Avezzano Sulmona L'Aquila e il conseguente provvedimento adottato dal Garante: v, *Garante per la protezione dei dati personali, Provvedimento dell'8 giugno 2023*, [9896217].

[121] Per un riferimento specifico relativo al *Data breach* nel dossier sanitario, v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, cit., 209.

finalità di diagnosi e cura, previsto dall'articolo 2-septies del Codice *privacy*[122].

Tale intervento normativo ha determinato il passaggio da un modello fondato sulla legittimazione del trattamento mediante consenso, a un sistema che impone una valutazione contestuale della finalità perseguita, al fine di verificare se il trattamento rientri tra quelli esenti da consenso, come diagnosi, cura, ricerca scientifica e monitoraggio clinico[123]. Le modifiche introdotte chiariscono il perimetro del trattamento lecito dei dati sanitari per finalità di tutela della salute dell'interessato, di terzi e della collettività. Il consenso diventa solo una delle possibili basi giuridiche, non più la principale. Il titolare del trattamento, medico, struttura sanitaria, ente di ricerca, deve valutare la finalità del trattamento e verificare se ricade in una delle eccezioni previste dall'art. 9, par. 2 del GDPR che ammette l'esclusione del consenso.

All'interno dello *European Health Data Space,* il concetto di consenso deriva dal Regolamento (UE) 679/2016[124], che non impone un unico modello, ma riconosce e rispetta la diversità delle normative e delle prassi nazionali[125]. È significativo, e forse preoccupante, che nel testo dell'EHDS il

---

[122] «*In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.*
2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale e tenendo conto:
a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.»: Articolo 2-septies, paragrafi 1 e 2, Codice Privacy.

[123] Sul punto, v. G. CAPILLI, *Diritto sanitario privato*, cit., 47.

[124] «a) le definizioni di «dato personale», «trattamento», «pseudonimizzazione», «titolare del trattamento», «responsabile del trattamento», «terzo», «consenso dell'interessato», «dati genetici», «dati relativi alla salute» e «organizzazione internazionale» stabilite all'articolo 4, rispettivamente ai punti 1), 2), 5), 7), 8), 10), 11), 13), 15) e 26), del regolamento (UE) 2016/679»: Articolo 2, paragrafo 1, lettera a), Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[125] Anche se l'EHDS mira a creare uno spazio europeo unificato per la condivisione e l'uso dei dati sanitari, non entra nel merito delle regole nazionali che disciplinano la prima raccolta dei dati sanitari elettronici. Sul punto, v. Considerando 11, Regolamento

termine "consenso" compaia raramente[126], riflettendo un mutamento profondo nella concezione della gestione dei dati sanitari a livello europeo[127].

Tradizionalmente, il consenso informato costituiva il cardine della legittimazione del trattamento dei dati personali in ambito sanitario; nel nuovo contesto, invece, il consenso assume un ruolo secondario rispetto ad altri meccanismi autorizzativi.

Allo stato attuale, non è ancora possibile delineare con certezza l'equilibrio finale tra le esigenze di protezione dei dati personali e quelle di accessibilità e condivisione. È però evidente che la protezione dei dati sanitari non può essere ridotta a mero adempimento burocratico: essa rappresenta un elemento essenziale della qualità dell'assistenza e della fiducia tra cittadino e sistema sanitario. La *governance* dei dati sanitari richiede pertanto un approccio integrato, capace di coniugare responsabilità, competenza e progresso tecnologico[128].

L'analisi fin qui condotta evidenzia come la digitalizzazione del settore sanitario, pur offrendo notevoli opportunità di innovazione, imponga un ripensamento delle garanzie a tutela della persona: la natura sensibile dei dati, la vulnerabilità del contesto clinico e la complessità delle basi

---

In Italia, ad esempio, rimane valido il sistema previsto dal Codice *Privacy* e dal GDPR, con l'articolo 2-septies e il ruolo del Garante, che stabiliscono le condizioni e le misure di garanzia per la raccolta e il trattamento iniziale dei dati sanitari. Questo significa che il consenso può continuare a essere richiesto a livello nazionale per la registrazione iniziale, specie per dati altamente sensibili come quelli genetici.

[126] Sul punto, v. anche articolo 48, paragrafo 2, Regolamento (UE) 2025/327 relativamente all' interoperabilità delle applicazioni per il benessere con i sistemi di cartelle cliniche elettroniche.

[127] Sul punto si veda anche Considerando 52, Regolamento (UE) 2025/327 il quale sancisce che relativamente all'uso secondario dei dati, gli Stati membri non possono imporre condizioni aggiuntive, come l'obbligo del consenso, oltre a quelle previste dal Regolamento (UE) 679/2016, al fine di facilitare la condivisione dei dati a livello comunitario.

[128] Risulta di notevole rilevanza la lettura del manuale dedicato agli operatori sanitari, il quale dedica attenzione a tutti gli elementi chiave della disciplina. Il testo offre una prospettiva non solo teorica, ma anche pratica, si sofferma sulla posizione del Garante in merito al trattamento dei dati relativi alla salute in ambito sanitario e fornisce una spiegazione di diversi aspetti legati alla sicurezza informatica.
Il manuale consente di ripercorrere la breve analisi presentata in questo paragrafo, indispensabile per comprendere i capitoli successivi, dedicati al nuovo regolamento: G. AMARÙ, A. FAVA, M. FOSSI, F. MAINARDI, *La privacy del dato sanitario, Manuale per operatori e professionisti che trattano dati relativi alla salute e per chi vuole saperne di più*, cit.

giuridiche del trattamento richiedono un approccio trasparente e responsabile. Lo *European Health Data Space* si configura, in questa prospettiva, come un laboratorio normativo e operativo destinato a coniugare interoperabilità e protezione, accessibilità e riservatezza, nel difficile ma necessario equilibrio tra diritti individuali e interessi collettivi[129].

4. Pseudonimizzazione: interpretazione alla luce della recente pronuncia della Corte di Giustizia europea.

Le sfide poste dalla digitalizzazione impongono un costante lavoro interpretativo, come dimostra la recente pronuncia della Corte di Giustizia[130], che permette di cogliere in concreto le implicazioni dinamiche della disciplina sulla protezione dei dati, con evidenti ricadute anche nel settore sanitario.

Tale posizione offre un'occasione significativa per approfondire il tema della pseudonimizzazione, alla luce delle implicazioni giuridiche emerse e del suo impatto sullo *European Health Data Space*.

La decisione oggetto di analisi trae origine da una vicenda complessa relativa alla procedura di risoluzione di una banca spagnola, avviata dalle autorità europee per evitarne il fallimento. In tale contesto, il Comitato di risoluzione (SRB) unico aveva affidato a una società di consulenza l'incarico di valutare il danno subito da azionisti e creditori, pubblicando un invito ufficiale nella Gazzetta dell'Unione europea affinché i soggetti interessati potessero esercitare il diritto di essere ascoltati, ai sensi dell'articolo 41, par. 2, lett. a), della Carta dei diritti fondamentali dell'UE[131].

Nel corso della procedura, il Comitato di risoluzione unico aveva inoltre diffuso un'informativa in materia di protezione dei dati personali e

[129] Sul punto, v. A. MORACE PINELLI, *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in *Nuov. Giur. civ. comm.*, 2025, 1023 e ss.

[130] Corte di Giustizia UE, 4 settembre 2025, (C-413/23).

[131] *«1.Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione. 2.Tale diritto comprende in particolare: a) il diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio; […]»:* Articolo 41, *Carta dei diritti fondamentali dell'Unione europea*.

trasmesso alla società incaricata unicamente le osservazioni presentate dagli interessati nella fase di consultazione, associate a un codice alfanumerico. Soltanto il Comitato era in grado di collegare tali osservazioni agli autori, rendendoli di fatto identificabili. Alcuni azionisti e creditori avevano quindi presentato reclamo al Garante europeo per la protezione dei dati (GEPD), lamentando la mancata comunicazione della trasmissione dei loro dati a un soggetto terzo, in violazione dell'articolo 15 del Regolamento (UE) 2018/1725.

In un primo momento, il GEPD aveva ammonito il SRB; successivamente, però, aveva rivisto la propria decisione, riconoscendo che i dati trasmessi erano pseudonimizzati e che la società terza non era in grado di identificare direttamente gli interessati. Ciononostante, il Garante aveva ribadito che l'informativa sulla *privacy* avrebbe dovuto coprire l'intera procedura e indicare chiaramente tutti i destinatari dei dati personali.

La Corte di Giustizia è stata chiamata a pronunciarsi sulla controversia, a seguito dell'impugnazione della decisione del GEPD. A sostegno delle rispettive posizioni sono intervenuti la Commissione europea, favorevole al SRB, e il Comitato europeo per la protezione dei dati, favorevole al GEPD.

Dalla pronuncia emergono interessanti riflessioni anche in chiave comparativa, alla luce dell'imminente applicazione del nuovo regolamento sullo Spazio europeo dei dati sanitari. Ciò è particolarmente rilevante poiché tale regolamento non introduce una definizione autonoma di "dato personale", ma rinvia direttamente a quella contenuta nel Regolamento (UE) 2016/679[132].

La Corte ha anzitutto chiarito che la nozione di "dato personale", di cui all'articolo 3, punto 1, del Regolamento 2018/1725, coincidente con quella

[132] *«Ai fini del presente regolamento si applicano le definizioni seguenti: a) le definizioni di «dato personale», «trattamento», «pseudonimizzazione», «titolare del trattamento», «responsabile del trattamento», «terzo», «consenso dell'interessato», «dati genetici», «dati relativi alla salute» e «organizzazione internazionale» stabilite all'articolo 4, rispettivamente ai punti 1), 2), 5), 7), 8), 10), 11), 13), 15) e 26), del regolamento (UE) 2016/679»*: Articolo 2, paragrafo 1, lettera a), Regolamento (UE) 2025/327 *del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.*

del Regolamento (UE) 2017/679[133], comprende «*qualsiasi informazione concernente una persona fisica identificata o identificabile*»[134]. L'uso dell'espressione «*qualsiasi informazione*» dimostra la volontà del legislatore di attribuire alla nozione un significato ampio, includendo anche pareri, valutazioni e osservazioni intrinsecamente riferibili a una persona[135]. Nel caso di specie, le osservazioni espresse dai partecipanti, intrinsecamente riferibili agli stessi, costituivano dati personali[136]. La qualificazione di «dato personale» richiede infatti la riferibilità dell'informazione a una persona identificata o identificabile[137], tenendo conto di tutti i mezzi ragionevolmente utilizzabili per risalire alla sua identità[138].

---

[133] *«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*»: Articolo 4, paragrafo 1, Regolamento (UE) 679/2016 GDPR.
Definizione sostanzialmente analoga a Nuova quella già formulata nella Direttiva 95/46/CE, del 24 ottobre 1995: *« dati personali »: qualsiasi informazione concernente una persona fisica identificata o identificabile (« persona interessata »); si considera identificabile la persona che può essere identificata, direttamente o indirettamente , in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica , psichica , economica , culturale o sociale*»: Articolo 2, lettera a), *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in GUUE L 281 del 23.11.1995. Relativamente all'analogia della definizione per un'applicazione coerente del diritto
la Corte richiama i seguenti precedenti: Corte di Giustizia UE, VI sezione, 7 marzo 2024, (C 479/22); Corte di Giustizia UE, IV sezione, 7 marzo 2024, (C-604/22).
[134] Articolo 3, punto 1, del Regolamento 2018/1725
[135] Corte di Giustizia UE, sezione I, 4 maggio 2023, (C-487/21); Corte di Giustizia UE, (C-479/22), cit.; Corte di Giustizia UE, sezione I, 4 ottobre 2024, (C-200/23).
[136] A sostegno di tale interpretazione, la Corte ha richiamato una precedente sentenza, nella quale era stato stabilito che anche le valutazioni o correzioni fatte da un esaminatore in un test professionale erano dati personali, perché esprimevano il suo punto di vista: v. Corte di Giustizia UE, sezione II, 20 dicembre 2017, (C-434/16).
[137] Tale riflessione trae origine dal già citato articolo 3, paragrafo 1, Regolamento (UE) 2018/1725.
[138] La Corte ha affermato che tale tipo di interpretazione è rafforzata dal considerando 16 dello stesso regolamento, il quale stabilisce che «*è auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per*

Quanto alla pseudonimizzazione, la Corte ha affermato che non può esistere una regola generale secondo cui i dati pseudonimizzati siano automaticamente esclusi dalla categoria dei dati personali: occorre invece verificare in concreto se vi siano elementi che permettano la reidentificazione dell'interessato[139].

Ma i dati pseudonimizzati non possono essere considerati anonimi qualora sia possibile risalire all'identità dell'interessato mediante informazioni aggiuntive[140].

Richiamando il considerando 16 del Regolamento 2018/1725, la Corte precisa che i dati pseudonimizzati possono qualificarsi come personali solo quando siano attribuibili a una persona fisica attraverso informazioni aggiuntive e quando tale identificabilità sia concretamente possibile, valutata alla luce di criteri oggettivi quali costi, tempi e mezzi tecnici disponibili. La nozione di dato personale resta ampia, ma non illimitata: è necessario che la persona sia identificata o identificabile[141].

La Corte ha respinto l'interpretazione estensiva proposta del Garante europeo[142], affermando che gli obblighi di protezione si applicano esclusivamente ai soggetti che dispongono di strumenti realistici per identificare l'interessato. La responsabilità del trattamento non può essere

---

accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori oggettivi, tra cui i costi e il tempo necessari per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.» Considerando 16, Regolamento (UE) 2018/1725.

[139] La Corte ha chiarito che i dati pseudonimizzati non rientrano puntualmente nella definizione fornita dall'art. 3, punto 1, del Regolamento (UE) 2018/1725 ma sono disciplinati nel punto 6 dello stesso articolo che definisce la pseudonimizzazione come un trattamento che rende i dati non attribuibili direttamente al soggetto interessato in assenza dell'uso specifico di informazioni aggiuntive conservate separatamente.
Inoltre, la Corte ha richiamato per analogia la seguente pronuncia: Corte di Giustizia UE, 5 dicembre 2023, (C-683/21).

[140] Anche il considerando 17 del regolamento stabilisce che la pseudonimizzazione si limita a ridurre il rischio di correlazione diretta tra dati e identità, sul punto, v. Considerando 17, Regolamento (UE) 2018/1725.

[141] Articolo 3, paragrafo 1, Regolamento 2018/1725.

[142] Il Garante europeo sosteneva che poiché il Comitato unico poteva identificare le persone, anche la società terza poteva farlo.

attribuita a chi non dispone di strumenti per identificare la persona. Di conseguenza, un soggetto terzo che riceve dati pseudonimizzati non è tenuto ad applicare la disciplina sulla protezione dei dati se non possiede strumenti, né diretti né indiretti, per identificare gli interessati.

Ne deriva che un dato pseudonimizzato non è, per definizione, un dato personale in maniera assoluta: la sua qualificazione dipende dal contesto e dalle circostanze del trattamento. La pseudonimizzazione, infatti, può impedire a soggetti diversi dal titolare del trattamento di identificare l'interessato, con la conseguenza che tali soggetti possono legittimamente trattare tali informazioni come dati non personali.

Tuttavia, questa interpretazione solleva rilevanti criticità nel settore sanitario e, in particolare, nell'ambito dello *European Health Data Space*, in cui i dati sanitari vengono condivisi tra numerosi attori pubblici e privati. In tale contesto, la qualificazione giuridica dei dati pseudonimizzati assume un valore decisivo: se il destinatario non è in grado di identificare l'interessato, rischia infatti di operare al di fuori del perimetro normativo previsto per la protezione dei dati personali.

Ciò impone una valutazione rigorosa delle misure tecniche di pseudonimizzazione e delle concrete possibilità di reidentificazione, al fine di evitare zone grigie nelle quali i dati sanitari potrebbero essere trattati senza adeguate garanzie e, conseguentemente, con potenziali pregiudizi per i diritti fondamentali degli interessati.

In tale prospettiva, la Corte si è soffermata sulla nozione di "persona identificabile", precisando che la valutazione dell'identificabilità deve riferirsi alla posizione del titolare del trattamento, e non a quella di eventuali soggetti terzi che ricevono i dati. Questo chiarimento risulta fondamentale anche ai fini dell'obbligo informativo previsto dall'articolo 15, par. 1, lett. e), del Regolamento 2018/1725, che impone al titolare di comunicare in modo chiaro, al momento della raccolta, i destinatari cui i dati personali saranno comunicati[143].

[143] *«1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: […] d) gli eventuali destinatari o le eventuali categorie di*

La Corte ha ulteriormente osservato che, sebbene l'articolo 3, punto 1, del medesimo regolamento non specifichi da quale prospettiva debba essere valutata l'identificabilità, essa può riguardare sia il titolare sia il terzo destinatario. La valutazione deve comunque avvenire considerando le circostanze concrete del trattamento[144]. Resta fermo che l'obbligo informativo opera nella fase iniziale di raccolta dei dati, con la finalità di garantire la validità del consenso, la trasparenza del trattamento e la piena tutela dei diritti dell'interessato.

In tale contesto, la Corte ha rilevato un errore giuridico nell'interpretazione secondo cui l'identificabilità andrebbe considerata dal punto di vista dei destinatari terzi.

L'articolo 15, paragrafo 1, lettera d), del regolamento 2018/1725 conferma, infatti, che il titolare è tenuto a informare l'interessato, già al momento della raccolta, circa gli eventuali destinatari dei dati. Si tratta di un obbligo essenziale: qualora il trattamento si fondi sul consenso, quest'ultimo è valido solo se l'interessato ha ricevuto tutte le informazioni necessarie per effettuare una scelta libera e consapevole. L'omessa comunicazione dei destinatari incide negativamente sulla trasparenza e invalida il consenso, impedendo all'interessato di esercitare in modo pieno i propri diritti, incluso quello di opporsi alla trasmissione dei dati.

Su questo punto, la Corte di giustizia ha assunto una posizione che appare orientata al rafforzamento delle garanzie in materia di protezione dei dati personali, riaffermando la centralità dell'obbligo informativo quale presidio essenziale nella tutela dei diritti fondamentali. Una diversa interpretazione, che permetta ai destinatari terzi di trattare dati pseudonimizzati senza un chiaro quadro informativo, rischierebbe di produrre effetti distorsivi, soprattutto nel contesto dello *European Health Data Space*.

In ambito sanitario, la possibilità di compromettere il controllo effettivo degli interessati sui propri dati è particolarmente concreta, soprattutto ove

destinatari dei dati personali» Articolo 15, paragrafo 1, lettera d), Regolamento (UE) 2018/1725.

[144] In merito all'identificazione indiretta di una persona fisica, ai sensi dell'articolo 4, punto 1, del GDPR: Corte di Giustizia UE, Sezione II, 19 ottobre 2016, (C-582/14); Corte di Giustizia UE, (C-479/22), cit.

si consideri la condizione di vulnerabilità che caratterizza il paziente. A differenza della procedura considerata dalla Corte, nella quale l'interessato agisce volontariamente per esercitare un proprio diritto, nel contesto clinico la comprensione dell'informativa e del consenso può risentire di situazioni di urgenza, pressione emotiva o fragilità psicofisica.

Un'interpretazione eccessivamente estensiva della normativa rischierebbe, pertanto, di svuotare di significato le garanzie previste dal legislatore europeo. Pertanto, la posizione assunta dalla Corte risulta condivisibile nella misura in cui valorizza l'obbligo informativo e preserva la centralità della persona, offrendo una lettura della normativa coerente con l'evoluzione degli scenari tecnologici, ma senza sacrificare l'essenza della tutela individuale.

Un'ultima osservazione generale si impone. Nel caso esaminato dalla Corte, non emerge alcun interesse collettivo sufficientemente rilevante da giustificare una compressione dei diritti individuali. In assenza di un interesse pubblico prevalente, chiaramente identificato e giuridicamente fondato, come la tutela della salute collettiva, non è ammissibile derogare sistematicamente ai diritti fondamentali.

Nel contesto dello *European Health Data Space*, tuttavia, la prevalenza dell'interesse collettivo potrebbe assumere un ruolo decisivo, fino al punto di incidere sull'orientamento interpretativo volto a privilegiare la posizione dell'individuo. Proprio per questo motivo è indispensabile che ogni deroga sia sorretta da una motivazione stringente e rigorosa, evitando letture estensive che possano compromettere l'assetto delle garanzie predisposto dal legislatore europeo. Solo un bilanciamento potrà assicurare la coerenza e la legittimità del nuovo quadro regolatorio.

CAPITOLO III

REGOLAMENTO SULLA CREAZIONE DELL'EHDS: IL PROBLEMA DELL'INTEROPERABILITA' DEI DATI SANITARI

SOMMARIO: 1. L'evoluzione del diritto sanitario transfrontaliero. – 2. La dimensione sociale del diritto alla salute: progressione o abuso? – 3. *European Health Data Space* e gestione etica dei dati sanitari. – 4. L'interoperabilità delle informazioni cliniche. – 5. Il problema della divulgazione dei dati contenuti nei *dossier* sanitari. – 6. L'uso primario dei dati sanitari. – 7. Il diritto alla limitazione dell'accesso. – 8. Il diritto di esclusione riconosciuto alle persone fisiche e il problema del rilevamento dell'accesso ai dati.

1. L'evoluzione del diritto sanitario transfrontaliero.

La scelta di affrontare il tema del diritto sanitario in chiave sovranazionale nasce dalle pressanti esigenze di sicurezza sanitaria che si sono diffuse con la globalizzazione e l'internazionalizzazione del concetto di salute ha coinvolto temi ordinariamente valutati a livello nazionale. In origine, le questioni legate alla sanità vennero trattate a livello intergovernativo per coordinare misure legate alla gestione e prevenzione di malattie contagiose trasmissibili con il trasporto delle merci.
Successivamente, si manifestò la necessità di rendere armonico il controllo della diffusione delle malattie infettive e da tale esigenza sono state generate le prime fonti di diritto sanitario internazionale: in particolare furono indette conferenze internazionali dedicate al tema, la prima si tenne a Parigi nel 1851[145].

[145] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, 2022, Milano, 65 e 66.

Nel XX secolo si diffusero i primi Organismi[146] creati per fornire supporto agli Stati nel perseguimento dell'obiettivo di promozione della salute e dei suoi valori intrinseci. Con il passare del tempo, tali Organismi divennero vere Istituzioni alle quali i singoli Stati cedevano parte della propria sovranità. Benché la fine della Seconda guerra mondiale abbia generato un rafforzamento di tale cooperazione, la vera svolta si ebbe nel 1948 con la costituzione dell'OMS, ancora oggi considerata l'anello principale dell'organizzazione sanitaria a livello mondiale e dell'affermazione della *global health governance*[147].

L'assistenza sanitaria transfrontaliera rappresentava il principale obiettivo da raggiungere[148]: nel 1950 la Convenzione Europea dei Diritti dell'Uomo e nel 1965 la Carta sociale europea si occuparono del diritto alla salute, ma tali interventi non diedero vita ad una puntuale competenza in materia[149].

La protezione della salute venne concretizzata solamente con il Trattato di Maastricht del 1992[150]: cure sicure e accessibili e creazione di sistemi sanitari innovativi rappresentavano gli obiettivi previsti dal TFUE[151], che

---

[146] Occorre far riferimento al *pan-America Sanitary Bureau* istituito nel 1902 e all'*International office of Public Health* istituito con un accordo firmato a Roma nel 1907: sul punto v. P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 67.

[147] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 68.

[148] Per un ulteriore approfondimento sul tema v. P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 69 ss.

[149] L'art. 11 della Carta sociale europea ha sancito il diritto alla protezione della salute e ha imposto agli Stati firmatari obblighi individuali e di cooperazione finalizzati ad assicurare che ogni persona abbia la possibilità di utilizzare le risorse che consentono di godere di uno stato di salute ottimale.

[150] Originariamente, la salute pubblica non veniva tutelata in maniera completa ed esclusiva, bensì come deroga al divieto di limitazione delle restrizioni all'importazione e all'esportazione delle merci: sul punto, v. art. 36, Trattato sul funzionamento dell'Unione europea, 9 maggio 2008, Gazzetta ufficiale dell'Unione europea, C 115/47. Nel 2000, anche la Carta di Nizza si è occupata del tema della salute: l'art. 35 della Carta dei diritti fondamentali dell'Unione europea ha sancito la protezione della salute delle persone.

[151] «*1. Nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un livello elevato di protezione della salute umana. L'azione dell'Unione, che completa le politiche nazionali, si indirizza al miglioramento della sanità pubblica, alla prevenzione delle malattie e affezioni e all'eliminazione delle fonti di pericolo per la salute fisica e mentale. Tale azione comprende la lotta contro i grandi flagelli, favorendo la ricerca sulle loro cause, la loro propagazione e la loro prevenzione, nonché l'informazione e l'educazione in materia sanitaria, nonché la sorveglianza, l'allarme e la lotta contro gravi minacce per la salute a carattere transfrontaliero. L'Unione completa l'azione degli Stati membri volta a ridurre gli effetti nocivi per la salute umana derivanti dall'uso di stupefacenti, comprese l'informazione e la prevenzione.*

spingeva verso la realizzazione della cooperazione tra gli Stati per favorire la promozione della salute e la prevenzione delle malattie.

In particolare, l'obiettivo primario delineato dall'art. 168 del Trattato sul Funzionamento dell'Unione Europea riguardava l'esigenza di omogeneità della disciplina dell'assistenza sanitaria, escludendo tematiche all'epoca sconosciute come la digitalizzazione dei sistemi sanitari e l'elaborazione di piani strategici per la gestione di eventuali emergenze sanitarie su larga scala[152].

2. L'Unione incoraggia la cooperazione tra gli Stati membri nei settori di cui al presente articolo e, ove necessario, appoggia la loro azione. In particolare, incoraggia la cooperazione tra gli Stati membri per migliorare la complementarità dei loro servizi sanitari nelle regioni di frontiera. Gli Stati membri coordinano tra loro, in collegamento con la Commissione, le rispettive politiche ed i rispettivi programmi nei settori di cui al paragrafo 1. La Commissione può prendere, in stretto contatto con gli Stati membri, ogni iniziativa utile a promuovere detto coordinamento, in particolare iniziative finalizzate alla definizione di orientamenti e indicatori, all'organizzazione di scambi delle migliori pratiche e alla preparazione di elementi necessari per il controllo e la valutazione periodici. Il Parlamento europeo è pienamente informato.

3. L'Unione e gli Stati membri favoriscono la cooperazione con i paesi terzi e con le organizzazioni internazionali competenti in materia di sanità pubblica.

4. In deroga all'articolo 2, paragrafo 5, e all'articolo 6, lettera a), e in conformità dell'articolo 4, paragrafo 2, lettera k), il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale e del Comitato delle regioni, contribuiscono alla realizzazione degli obiettivi previsti dal presente articolo, adottando, per affrontare i problemi comuni di sicurezza: a) misure che fissino parametri elevati di qualità e sicurezza degli organi e sostanze di origine umana, del sangue e degli emoderivati; tali misure non ostano a che gli Stati membri mantengano o introducano misure protettive più rigorose; b) misure nei settori veterinario e fitosanitario il cui obiettivo primario sia la protezione della sanità pubblica; c) misure che fissino parametri elevati di qualità e sicurezza dei medicinali e dei dispositivi di impiego medico.

5. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale e del Comitato delle regioni, possono anche adottare misure di incentivazione per proteggere e migliorare la salute umana, in particolare per lottare contro i grandi flagelli che si propagano oltre frontiera, misure concernenti la sorveglianza, l'allarme e la lotta contro gravi minacce per la salute a carattere transfrontaliero, e misure il cui obiettivo diretto sia la protezione della sanità pubblica in relazione al tabacco e all'abuso di alcol, ad esclusione di qualsiasi armonizzazione delle disposizioni legislative e regolamentari degli Stati membri.

6.Il Consiglio, su proposta della Commissione, può altresì adottare raccomandazioni per i fini stabiliti dal presente articolo.

7. L'azione dell'Unione rispetta le responsabilità degli Stati membri per la definizione della loro politica sanitaria e per l'organizzazione e la fornitura di servizi sanitari e di assistenza medica. Le responsabilità degli Stati membri includono la gestione dei servizi sanitari e dell'assistenza medica e l'assegnazione delle risorse loro destinate. Le misure di cui al paragrafo 4, lettera a) non pregiudicano le disposizioni nazionali sulla donazione e l'impiego medico di organi e sangue»: art. 168, TFUE.

[152] F. CIMBALI, *La Governance della sanità digitale*, 2023, Milano, 61.

Tuttavia, il tentativo di armonizzazione dell'azione degli Stati fu insufficiente a causa della previsione di una mera competenza di supporto affidata all'Europa, priva di poteri normativi[153].

Nel tempo, la globalizzazione e la diffusione delle nuove tecnologie, la necessità di uniformare i sistemi di protezione della salute a livello sovranazionale e l'esigenza di garantire la progressione delle politiche sanitarie vennero poste in primo piano: così nacque la Direttiva 2011/24/UE che disciplinando l'assistenza sanitaria transfrontaliera, si è occupata della promozione della cooperazione fra gli Stati europei[154]. Tale sinergia venne creata per garantire l'accesso a cure sanitarie di alta qualità e per promuovere il rafforzamento della libertà di circolazione delle persone[155].

Ma la Comunicazione della Commissione europea[156] ha posto la promozione della sanità digitale al centro del dibattito, con particolare attenzione alla condivisione dei dati e al miglioramento dell'utilizzo degli stessi per soddisfare esigenza di ricerca[157]. L'emergenza sanitaria globale ha posto in evidenza le numerose conseguenze causate dalla frammentata disciplina adottata dagli Stati membri.

I diversi interventi hanno portato a risultati insufficienti e ciò ha spinto la Commissione europea a intervenire con differenti iniziative attuate mediante investimenti in ambito sanitario: il Programma *"EU4Health"*[158]*,*

---

153 P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 78.

154 Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, relativa all'applicazione dei diritti dei pazienti in materia di assistenza sanitaria transfrontaliera (GU L 88 del 4 aprile 2011), recepita nell'ordinamento giuridico italiano con il d.lgs. 4 marzo 2014, n. 38. Per un'analisi approfondita dei precedenti interventi normativi europei. Sul punto, v. P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 83 ss.

155 F. TRINCIA, *La tutela del diritto alla salute secondo la direttiva 2011/23/UE,* in *Lavoro Diritti Europa*, 2018, 6 ss.

156 *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana*, COM (2018) 233 final, Bruxelles, 2018.

157 P. GUARDA, G. BINCOLETTO, *Diritto comparato della* privacy *e della protezione dei dati personali*, Milano, 2023, 296.

158 Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio, del 24 marzo 2021, che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-

entrato in vigore il 26 marzo 2021, fra i diversi obiettivi, prevede il coordinamento degli Stati europei finalizzato all'implementazione dell'utilizzo della digitalizzazione e alla promozione di una legislazione comunitaria[159].

Attualmente l'adozione di un approccio coordinato e la necessità di far nascere un'interconnessione dei sistemi sanitari europei rappresentano esigenze indispensabili[160]. La tradizionale competenza di supporto dell'Unione in materia di sanità si sta trasformando in un ruolo sovranazionale principale[161].

La disciplina contenuta nel nuovo Regolamento relativo alla creazione dell'*European Health Data Space* mira alla realizzazione di una cooperazione efficace tra gli Stati, in grado di incentivare l'adozione di sistemi sanitari avanzati che diano vita ad una concreta evoluzione del sistema sanitario europeo con benefici tangibili su larga scala.

2. La dimensione sociale del diritto alla salute: progressione o abuso?

Appare opportuno sottolineare la fragilità intrinseca all'esercizio del diritto alla salute che, a differenze di altri diritti, racchiude una sorta di auto insufficienza che trae origine dalla mancata possibilità per l'individuo di garantire il soddisfacimento delle esigenze, meglio qualificate come necessità inderogabili, legate all'esercizio di tale diritto.

La salute dell'individuo è direttamente collegata alle cure che necessitano di servizi e strumenti erogati da personale qualificato, all'interno di apposite strutture: l'essenza della "fragilità" è radicata nell'impossibilità per il singolo

2027 («programma UE per la salute», EU4Health) e che abroga il Regolamento (UE) n. 282/2014, (GUUE L 107/1 del 26 marzo 2021).

[159] G. LOFARO, *Dati sanitari e e-Health europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *mediaLaws*, 2022, 199.

[160] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, 2022, cit., 82.

[161] Dall'analisi fin qui effettuata possiamo affermare che il tema salute, nel corso del tempo, è stato posto al centro dell'attenzione dell'Unione Europea. L'evoluzione del diritto alla salute trova un chiaro riscontro nel testo dell'art. 168 del Trattato sul Funzionamento dell'Unione Europea.

di provvedere autonomamente, in quanto sprovvisto degli strumenti necessari per proteggere tale sfera giuridica soggettiva[162].

L'articolo 32 della Costituzione fa riferimento a una visione unitaria "del bene salute" che rispecchia sia l'interesse individuale che quello collettivo. Già nel passato emerse una considerazione notevolmente importante, incentrata sulla consapevolezza della mutabilità del contenuto del diritto alla salute considerato come una condizione "di benessere" da conservare nel lungo periodo, con la conseguente necessità di applicazione di misure mutabili nel tempo a causa della diversificazione delle esigenze che caratterizzano il contesto all'interno del quale si evolve il concetto stesso del bene salute[163]: «*in questo senso la disposizione dell'articolo 32 Cost. si è dimostrata particolarmente "prestabile"*»[164].

Dunque, l'ordinamento costituzionale attribuisce valore non solo al diritto alla salute inteso come diritto appartenente all'individuo, ma anche come interesse della collettività «*secondo il principio per cui il proprio diritto trova limite nel reciproco riconoscimento e nell'eguale protezione del diritto degli altri*»[165].

La forte interazione che sussiste tra la salute del singolo e quella della collettività emerge dal comma secondo dell'articolo 32 della Costituzione, il quale stabilisce che un soggetto non può essere sottoposto obbligatoriamente a un trattamento sanitario, salvo che non sia disposto dalla legge[166]. La chiave di lettura di tale concetto potrebbe essere tradotta in questo modo: il sacrificio individuale, rispetto alla propria libertà di autodeterminazione nella scelta di sottoporsi a cure mediche o altro, è

---

[162] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 25 e 26.

[163] A. SIMONCINI E. LONGO, *Articolo 32 Costituzione*, R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, I, 2006, 656 e 657.

[164] «*D'altro canto se si muove dalla più attuale considerazione della salute come fondamentale bene unitario della persona e, quindi, requisito necessario – anche se non sufficiente – per la piena realizzazione della persona stessa, allora si comprende come l'eterogeneità della disposizione altro non sia che il riflesso della oggettiva complessità di questo bene giuridico, la cui tutela effettiva è affidata alla convergenza di una serie di molteplice di azioni e strumenti diversi e non da un unico ed assorbente meccanismo di garanzia.»:* così A. SIMONCINI E. LONGO, *Articolo 32 Costituzione,* cit., 658.

[165] Corte costituzionale, sentenza n. 218 del 1994.

[166] Articolo 32, comma 2, Costituzione.

legittimo nel momento in cui viene giustificato dalla presenza di rischi che possono riflettere conseguenze per lo stato di salute della collettività[167]. Ovviamente, occorre precisare che l'imposizione di trattamenti non dovrebbe dar vita a conseguenze negative per il singolo e la compromissione dell'autodeterminazione dovrà essere proporzionata al contesto di riferimento e all'esigenza di tutela della salute intesa come interesse della collettività, sulla base di un rapporto fondato sul bilanciamento tra i valori presi in considerazione[168].

Dunque, dall'analisi del diritto alla salute derivante dalla lettura dell'articolo 32 della Costituzione emerge non solo la centralità del ruolo dell'apparato pubblico ma anche quella delle scelte del singolo che ricadono sulla collettività[169].

La dimensione aggregata del diritto alla salute esula dalla tradizionale analisi dell'articolo citato, a suo sostegno vi è una valutazione che non fa riferimento esclusivamente al momento della cura ma anche alla prevenzione che pone forte attenzione alla necessaria consapevolezza e diligenza dell'individuo rispetto alla proiezione delle sue scelte sulla sfera giuridica collettiva[170].

La complessa analisi legata al contenuto dell'articolo 32 della Costituzione richiede necessariamente un approfondimento della giurisprudenza costituzionale, in particolare della pronuncia in cui la Corte ha affermato che «nessun diritto è tiranno»[171]. Tale principio sottolinea la necessità di

---

[167] A. SIMONCINI E. LONGO, *Articolo 32 Costituzione,* cit., 667, i quali citano COCCONI, 1998, 93. L'importanza della tutela dell'altrui salute come elemento che giustifica la sottoposizione a trattamenti obbligatori viene sottolineata particolarmente in C. Cost. 218/1994 (accertamenti sanitari dell'H.I.V. su determinate categorie di lavoratori).

[168] A. SIMONCINI E. LONGO, *Articolo 32 Costituzione,* cit., 667.

[169] L'autore parla di "salute aggregata" riferendosi alle scelte individuali discrezionali che incidono sulla salute degli altri: si pensi al soggetto che sceglie di sottrarsi a campagne vaccinali: P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 27.

[170] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 29.

[171] «*Tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile, pertanto, individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre «sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro» (sentenza n. 264 del 2012). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della*

evitare che un diritto, seppur fondamentale, venga esercitato in modo assoluto, sacrificando ingiustamente diritti o interessi di pari rilievo: nessun diritto può essere considerato in una valenza tanto forte da imporsi in maniera incontestabile sugli altri, dal momento che, a livello Costituzionale, non esiste una gerarchia rigida e formalmente definita di principi e diritti fondamentali.

Emerge la necessità di bilanciare i valori di pari rango, tenendo conto del contesto concreto e del bene giuridico prevalente in quella determinata situazione. Una definizione statica di criteri da adottare all'interno del sistema sanitario rischierebbe di comprometterne l'efficacia, a causa di numerosi fattori che mutano nel tempo[172]. Dunque, non esiste una concezione di diritto alla salute (del singolo) incondizionata e immutabile che ne garantisca l'assoluta preminenza[173].

L'emergenza sanitaria ha messo in evidenza il binomio salute - interesse della collettività, mettendo in secondo piano il modello individualistico[174] e ponendo l'attenzione anche su un interessante e complicato rapporto di intersezione fra il diritto alla salute, nella sua concezione collettiva, e la *privacy*, in un contesto in cui regna il progresso tecnologico e i dati personali fungono da protagonisti.

È emersa su larga scala una tendenza a privilegiare la riduzione della *privacy* al fine di fronteggiare le gravi conseguenze legate alla

---

persona.»: Corte Cost., 9 maggio 2013, n. 85, in *Giornale di diritto amministrativo*, 2013, con nota di P. CARLUCCIO E R. FINOCCHI GHERSI, *Il caso Ilva: tutela dell'ambiente, bilanciamento tra diritti fondamentali e riserva di giurisdizione*, 750 ss.

[172] P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 13.

[173]Appare necessario un piccolo riferimento ad una pronuncia della Consulta che con la sentenza n. 85 del 2013 ha stabilito che all'interno del sistema costituzionale il diritto alla salute non prevale a priori rispetto a tutti gli altri in quanto tutti i diritti tutelati hanno una integrazione reciproca e dunque non possiamo parlare di prevalenza assoluta: Corte Cost., 9 maggio 2013, n. 85, cit.

[174]«All'esito di questa accidentalità, quasi traendo origine da una pretesa alternativa, tuttavia assente nel testo costituzionale, si è sostenuto enfaticamente il tramonto del modello individualistico, in luogo dell'instaurazione di un sistema capace di superare i limiti e l'inadeguatezza dell'autodeterminazione, ignorando probabilmente che la prospettiva programmatica dell'art. 32 cost. non impone una logica di contrapposizione frontale dei criteri, ma, più pacificamente semmai, la temporanea prevalenza, attualmente, dell'interesse collettivo, senza che ciò comporti il superamento della dimensione soggettiva, ma solo una convivenza a primato alternato, in ragione del contesto di riferimento.»: così P. D'ONOFRIO, *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, cit., 6.

compromissione della salute pubblica. In particolare, si è affermata una significativa compromissione della sfera individuale, con particolare riferimento al diritto alla riservatezza, per far fronte ad esigenze collettive quali la sicurezza pubblica e la tutela della salute della collettività. In questo senso può essere richiamato il celebre brocardo ciceroniano «*Salus rei publicae suprema lex esto*», a evidenziare come la salvaguardia della collettività rappresenti la legge suprema della convivenza civile[175].

Il Regolamento (UE) 2016/679 sancisce un generale divieto di trattamento dei dati inerenti alla salute in quanto rientranti nelle cd. «categorie particolari di dati personali»[176], prevedendo delle possibili deroghe correlate al verificarsi di determinati eventi[177].

Occorre considerare che il Regolamento (UE) 2016/679 fa direttamente riferimento alle pandemie[178], stabilendo che in tali contesti il trattamento dei dati sarebbe legittimato dalla diretta correlazione con la necessità di salvaguardare gli interessi vitali dell'interessato, o di altra persona fisica, e nell'esigenza di realizzare un compito di pubblico interesse[179].

I principi che rappresentano i pilastri della protezione dei dati personali, in particolare liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza e responsabilizzazione, non devono essere posti in secondo piano anche in contesti estremi come quello dell'emergenza sanitaria globale vissuta[180].

---

[175]Cicerone, *De legibus,* III, 3.8: "*Salus rei publicae suprema lex esto*".

[176]Articolo 9, Regolamento (UE) 2016/679 (GDPR).

[177]La deroga alla regola generale che sancisce la tutela del dato trova diretta correlazione con il principio di matrice europea in base al quale la protezione dei dati personali si confronta con altri diritti importanti. Sul punto v. considerando 4 Regolamento (UE) 2016/679 (GDPR).

[178] Considerando 46, Regolamento (UE) 2016/679 (GDPR).

[179]Articolo 6, paragrafo 1, lettera d) ed e), Regolamento (UE) 2016/679. Sul punto v. L. PROSIA, *Privacy o salute pubblica? Un apparente dilemma*, D. MORANA, S. MABELLINI (a cura di), *L'emergenza pandemica e l'impatto sul diritto pubblico: innovazione e prospettive future*, 2022, 61, 62 e 63.

[180]«*1. I dati personali sono:*

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

Solamente, in questo modo, il bilanciamento degli interessi coinvolti assume sembianze elastiche in grado di adattarsi al contesto di riferimento ed evitare una totale compromissione della tutela dei diritti fondamentali[181]. Tale argomentazione necessita di un ulteriore riferimento: l'avvento della progressione tecnologica, se ben utilizzata, rappresenta un fiore all'occhiello per il miglioramento dei servizi e delle prestazioni erogate dallo Stato. Tuttavia, sebbene rappresenti un'opportunità straordinaria, costituisce al contempo un rischio significativo, soprattutto quando il suo impiego genera conseguenze che penalizzano i singoli individui. Questo accade in particolare nei casi in cui il bilanciamento tra diritti individuali ed esigenze collettive risulta squilibrato, anche a vantaggio di queste ultime.

Nell'operazione di bilanciamento oggetto della nostra analisi, che riguarda l'equilibrio tra l'interesse del singolo e le esigenze della collettività, è necessario evitare che queste ultime legittimino un vero abuso, tale da comportare l'annullamento totale delle garanzie poste a tutela dei diritti individuali coinvolti.

Tali riflessioni, aprono una vasta argomentazione sulle conseguenze legate all'inarrestabile utilizzo di strumenti tecnologici che hanno preso il sopravvento nella quotidianità e che, anche a seguito della conclusione della fase pandemica, non hanno avuto un freno all'interno del contesto clinico

---

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) 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 o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).»: Articolo 5, Regolamento (UE)2016/679 (GDPR).

[181]L. PROSIA, *Privacy o salute pubblica? Un apparente dilemma*, cit., 64.

sanitario. Ciò che inizialmente sembrava legittimo in nome della pubblica incolumità, ha progressivamente lasciato spazio ad una compromissione sempre più profonda della sfera privata dell'individuo. In particolare, stiamo assistendo a una notevole riduzione delle tutele in materia di protezione dei dati personali, giustificata sia da esigenze di cura direttamente riferibili al singolo paziente, sia, in altri casi, da finalità correlate ad esigenze della collettività legate all'avanzamento della ricerca medica. Queste ultime, seppur orientate all'interesse generale, incidono notevolmente sulla dimensione individuale, esponendo il soggetto a una invadente limitazione della propria riservatezza.

Assistenti virtuali, telemedicina e interoperabilità dei dati sono solo alcuni dei pilastri fondanti della progressione medica, che rappresentano il contesto all'interno del quale si inseriscono numerosi interrogativi legati all'individuazione di scelte strategiche che siano in grado di apportare reali benefici senza eccedere nella compromissione della sfera giuridica del singolo.

Gli eventi che hanno caratterizzato gli ultimi anni, nel macrocontesto del tema salute, hanno aperto numerose riflessioni che coinvolgono aspetti di rilievo costituzionale, direttamente collegati al contenuto dell'articolo 32 della Costituzione che apre una attenta riflessione rispetto alla valutazione della salute come interesse del singolo e interesse condiviso dalla collettività[182].

La centralità dei temi della sanità e del diritto alla salute, inserita nel contesto di una costante digitalizzazione, rende il dato sanitario protagonista di numerose riflessioni, contribuendo a delineare una visione *datacentrica* della sanità, caratterizzata da una forte interconnessione e dall'utilizzo di numerosi strumenti innovativi, come l'intelligenza artificiale[183].

[182] G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati*, cit., 15 ss.
[183] G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati,* cit, 19.

3. European Health Data Space e gestione etica dei dati sanitari.

L'esigenza di garantire la sicurezza nelle differenti fasi di diffusione dei dati personali rappresenta una conseguenza che entra in collisione con numerosi vantaggi derivanti dal progresso tecnologico e della speditezza della circolazione delle informazioni. Gli individui abitualmente autorizzano la trasmissione dei dati personali a soggetti privati o pubblici, che vengono trattati per finalità eterogenee. Nasce così la necessità di generare una solida e coerente disciplina in grado di garantire il controllo e la consapevolezza delle modalità di diffusione delle informazioni personali, tutelando i diritti dei singoli.

Le discordanze presenti nei differenti Stati europei non sono state superate tramite l'applicazione del Regolamento (UE) 2016/679[184] che, in compenso, ha generato il primo impulso verso la regolamentazione dell'interconnessione tra dati sanitari, ricerca e *privacy* [185]. Le differenti modalità di recepimento del Regolamento (UE) 2016/679 hanno generato un quadro normativo disomogeneo che ha ostacolato il raggiungimento di un approccio uniforme e coerente all'interno dell'Unione Europea: pur avendo introdotto principi cardine in materia di protezione dei dati personali, non ha dato vita a una struttura normativa realmente armonizzata [186].

La notevole disparità nella gestione delle pratiche operative è stata, nel tempo, causata dall'assenza di un quadro normativo unitario in cui accesso

[184] Il Regolamento in questione origina dalla Direttiva 95/46/CE, che rappresentava il pilastro fondante della volontà di superare il frazionamento della disciplina del flusso dei dati tra i singoli Stati membri. Dalla direttiva si è passati a un Regolamento, applicabile dal 2018, che non ha stravolto completamente la normativa precedente, ma ha apportato modifiche significative al d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), che continua ad essere oggetto di numerose variazioni.

[185] I. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?* in *Europa e Diritto Privato*, 2021, 301; sul punto v. G. SCORZA, *Disposizioni generali,* in *comm. GDPR e normativa privacy*, G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), 2018, Milano, 4.

[186] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, in GU L 119/1 del 4 maggio 2016.

e gestione delle informazioni cambiavano da un Paese all'altro, determinando la limitazione della cooperazione transfrontaliera.

Nella macrocategoria dei dati personali rientrano i dati sanitari, ovvero quelle informazioni personali raccolte in un contesto basato sull'interazione fra un individuo e un operatore sanitario, i quali nel campo degli studi osservazionali possono distinguersi in: «*a) Dati derivati da flussi informativi sanitari e sistemi di sorveglianza [...]; b) Dati rilevati per finalità di prevenzione, diagnosi e cura nell'ambito dei diversi servizi sanitari e centri clinici [...]; c) Dati raccolti in un data-base clinico.*»[187].

Il progetto normativo posto alla base del nuovo *European Health Data Space* nasce al fine di colmare le lacune presenti nella disciplina attuale[188], provando a dissolvere le numerose difficoltà annesse all'adeguato esercizio dei diritti che ruotano attorno al fenomeno della digitalizzazione dei dati sanitari.

L'avvento della tecnologia ha influenzato notevolmente il contesto sanitario, introducendo numerose vulnerabilità prima sconosciute: questo ha determinato l'urgenza di equilibrare tutele e benefici.

In un contesto di tal tipo appare indispensabile garantire l'implementazione della tutela dei soggetti coinvolti, per assicurare una visione accurata dei rischi e dei danni potenziali derivanti dalla strumentalizzazione dei dati sanitari: il nuovo Regolamento, nel complesso, si impone di valutare l'incidenza delle nuove tecnologie sul sistema sanitario, tentando di garantire una gestione etica delle informazioni raccolte.

Attraverso l'implementazione di regole chiare e condivise si cerca di creare un equilibrio tra innovazione e tutela, favorendo una sanità efficiente ed equa a livello europeo[189].

---

[187] *Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale,* documento CCNCE, 6 aprile 2023, p. 5-6.

[188] *Proposta di Regolamento (UE) n. 197 del Parlamento europeo e del Consiglio, 3 maggio 2022, sullo spazio europeo dei dati sanitari*, Strasburgo, 3.5.2022 COM (2022), 197 final 2022/0140 (COD).

[189] Cfr. A. CINQUE, *Privacy, big-data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute, Nuova Giurisprudenza Civile Commentata*, 2021, p. 957 ss.

La necessità di garantire un'assistenza medica efficace su tutto il territorio europeo e la scelta di creare l'*European Health Data Space* rappresenta una diretta conseguenza della digitalizzazione delle informazioni sanitarie, ove è centrale il binomio sanità-circolazione del dato. Questi due elementi sono uniti sotto molteplici aspetti: in particolare l'innovazione in materia di diagnosi, prevenzione e cura è fortemente dipendente dalla condivisione dei dati su tutto il territorio europeo, e non solo. In tal modo dovrebbero essere garantiti un notevole miglioramento delle prestazioni offerte e un sistema maggiormente innovativo e integrato, grazie all'utilizzo strategico delle risorse.

L'Istituzione europea promotrice del progresso legislativo ha elaborato una proposta di Regolamento che distingue due diverse modalità di utilizzo dei dati sanitari: uso primario e uso secondario[190].

I due pilastri sui quali si erige la creazione dell'*European Health Data Space* sono: controllo e condivisione del dato, ove l'interoperabilità transfrontaliera rappresenta il primario obiettivo, collegato al tentativo di attuazione di una maggiore tutela dei soggetti coinvolti[191].

Attualmente, la semplificazione dei dati sanitari calibrata ad un adeguato equilibrio tra sicurezza e *privacy* rappresenta un'esigenza indispensabile, legata alla pressante necessità di una visione unitaria dei sistemi di condivisione dei dati sanitari a livello europeo, con l'eliminazione delle discrepanze legate alla gestione individuale dei sistemi sanitari da parte di ogni Stato europeo[192].

La volontà di attuare una sinergia di questo tipo non rappresenta una novità: con *l'eHalt Digital Service Infrastructure* (eHDSI) i cittadini europei dovrebbero già avere la possibilità di non interrompere le proprie

---

[190] G. CAPILLI, *Diritto sanitario privato*, 2022, cit., 77 ss.

[191] Articolo 1, *Emendamenti del Parlamento europeo,* approvati il 13 dicembre 2023, alla proposta di Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari.

[192] Sul tema, di particolare rilevanza è il programma di finanziamento EU4Health, elaborato per garantire il rafforzamento dei sistemi sanitari nazionali a seguito della pandemia da Covid-19. Istituito tramite il Regolamento (UE) 2021/552 intende migliorare e promuovere la salute tramite iniziative sanitarie internazionali, garantire la protezione degli individui, l'accesso ai medicinali e ai dispositivi medici, mirando ad un generale rafforzamento dei sistemi sanitari.

cure quando viaggiano all'interno dell'Unione Europea o al di fuori di essa, tramite l'utilizzo della piattaforma *Myhealth@EU*[193]. Tuttavia, attualmente vengono garantiti solamente due servizi sanitari: la prescrizione elettronica di farmaci[194] e il *patient summaries*[195].

Il quadro di monitoraggio fornito dai KPI offre differenti mappe che presentano indicatori di *performance* relativi a molteplici servizi che dovrebbero essere erogati tramite *MyHealth@EU*. In particolare, dall'analisi relativa al numero di paesi europei con *National contact point eHealth* operativo è emerso che: nel 2019 solamente 6 Stati garantivano tale operatività, con l'incremento di un solo paese nel 2020, seguito dalla partecipazione di 9 paesi in totale nel 2021, fino al raggiungimento di 11 paesi nel 2022, una fase di stallo nel 2023 e un incremento di 4 paesi avvenuto nel 2024, senza incrementi nel 2025[196].

Il fatto che non si sia perfezionata la realizzazione del piano posto alla base della creazione dell'infrastruttura europea per l'utilizzo di servizi sanitari transfrontalieri elettronici, seppur basato su un'attività meno onerosa rispetto all'articolata previsione contenuta nella proposta di Regolamento, pone sotto i riflettori la grave possibilità che l'Europa non riesca a concretizzare quanto sperato. Per garantire l'efficace operatività dell'*European Health Data Space* è indispensabile che venga attuata una sinergia funzionale finalizzata alla promozione di una visione non individualista dei singoli Stati, che dovranno necessariamente collaborare e

---

[193] Informazioni consultabili sul sito *web* ufficiale dell'Unione europea (https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en).

[194] Tale servizio consente ai cittadini di acquistare medicinali in una farmacia sita in un altro paese dell'UE; per ulteriori approfondimenti v. *Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, ePrescription and eDispensation of Authorised Medicinal Products guidelines, Release* 3.1, novembre 2024.

[195] Tramite tale strumento è possibile ottenere informazioni inerenti allo stato di salute del singolo individuo. Fa riferimento ad informazioni essenziali come eventuali allergie o farmaci che il soggetto sta assumendo e rientra nella più ampia raccolta dati contenuta nella cartella clinica elettronica. L'aspetto fondamentale riguarda la circolazione delle informazioni mediante l'utilizzo della lingua di riferimento del medico interessato dal caso concreto, contrastando eventuali barriere legate alla difficoltà di comprensione delle informazioni catalogate utilizzando la lingua del paese di origine del paziente; sul punto sono state emanate le *Guidelines on Patient Summary, Release* 3.4, novembre 2024.

[196] Informazioni rilevabili nel quadro di monitoraggio MyHealth@Eu (KPI), (https://experience.arcgis.com/experience/77f459be23e545b48f46a79cfaf19423/page/1_1/).

progredire per garantire la corretta applicazione del nuovo Regolamento europeo.

4. L'interoperabilità delle informazioni cliniche.

Seppur l'*European Health Data Space* rappresenti un'innovazione significativa nel contesto della gestione e della condivisione dei dati sanitari a livello transfrontaliero, è opportuno sottolineare che già con il Fascicolo sanitario elettronico (FSE) c'è stato un tentativo di promozione della raccolta e della gestione dei dati sanitari dei singoli individui, con particolare attenzione all'interoperabilità dei sistemi, volta a garantire la continuità delle cure e la corretta fruizione dei servizi sanitari a livello nazionale. Pertanto, pur rappresentando una novità importante sul piano sovranazionale, il Regolamento sullo Spazio europeo dei dati sanitari si inserisce in un quadro normativo operativo avviato, ma poco efficace.
Il Fascicolo sanitario elettronico rappresenta una macro-elaborazione delle informazioni e dei documenti legati alle prestazioni erogate da strutture private e dal Servizio Sanitario Nazionale nel tentativo di riscrivere l'intera storia clinica di un individuo[197]. Completezza e interoperabilità delle informazioni ne rappresentano i pilastri.
Le finalità perseguite sono molteplici: all'interno di questo documento confluiscono prescrizioni farmaceutiche e mediche, referti clinici, certificati

[197] Con il d.l. 19 maggio 2020, n. 34 (Decreto Rilancio), la definizione di fascicolo sanitario elettronico (FSE) è stata ampliata per includere anche i documenti relativi alle prestazioni non erogate dal Servizio Sanitario Nazionale (SSN) ma fornite da strutture private. Esistono differenti definizioni di FSE: le *Linee guida in tema di fascicolo sanitario elettronico (FSE) e dossier sanitario*, 16 luglio 2009, n. 25, elaborate dal Garante per la protezione dei dati personali, parlano di «*condivisione informatica, da parte di distinti Organismi e professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e il più possibile completo un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica*». L'art. 12, comma 1, d.l. 18 ottobre 2012, n. 179 sancisce che «*Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni al di fuori del Servizio sanitario nazionale*». Infine, il sito dell'Agenzia per l'Italia Digitale spiega che il FSE «*è lo strumento attraverso il quale il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria, condividendola con i professionisti sanitari per garantire un servizio più efficace ed efficiente*». Sul tema cfr. S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, in *Nuove leggi civili commentate*, 2024, 334 ss.

e tutte le informazioni rilevanti per la ricostruzione dello stato di salute e dei processi di cura adottati, al fine di consentire la verifica delle prestazioni erogate, la prevenzione e la profilassi internazionale da parte del Ministero competente.

All'interno di questo ampio documento è inclusa la *patient summary*, che funge da sintesi delle informazioni cliniche più rilevanti, con lo scopo di ottimizzare il recupero rapido dei dati essenziali in situazioni di emergenza sanitaria, garantendo un intervento tempestivo ed efficace[198].

Il modello originario del FSE prevedeva un'infrastruttura che utilizzava una rete nazionale e delle architetture regionali[199] e, già da allora, le esigenze che si cercarono di soddisfare riguardavano non solo una interoperabilità nazionale, ma anche sovranazionale, finalizzata a un'ottimizzazione dei sistemi di cura[200]. Inizialmente ci fu solo una parziale attuazione di tale

---

[198] Articolo 3, D.P.C.M. 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico; v. anche *Fascicolo sanitario elettronico (FSE)*, 2024, disponibile sul sito del Garante per la protezione dei dati personali, (https://www.garanteprivacy.it/temi/fse).

[199] La scelta di dar vita ad un sistema in cui i documenti dei pazienti devono entrare a far parte del fascicolo sanitario elettronico, sin dal principio richiedeva la creazione di un apposito sistema di raccolta digitale e il Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica, la Presidenza del Consiglio dei Ministri e il Dipartimento ICT, all'inizio avevano dato vita ad un progetto, denominato "Infrastruttura tecnologica del Fascicolo Sanitario Elettronico", che prevedeva un architettura denominata inFSE in grado di svolgere le funzioni principali, necessarie per la gestione e i funzionamento del FSE, configurato secondo un modello federale.
In particolare, tale infrastruttura prevede l'erogazione di differenti servizi che possono essere suddivisi in una macroarea legata all'ottimizzazione delle funzioni per gestire il FSE e una che riguarda servizi volti a supportare l'interoperabilità dei sistemi territoriali.
Successivamente è stato elaborato un progetto denominato brevemente OpenInFSE, infrastruttura integrata con i sistemi di Fascicolo sanitario elettronico di Calabria, Campania e Piemonte che consente la ricerca e il recupero di documenti sanitari grazie all'interoperabilità dei sistemi territoriali di FSE.
Un altro importante progetto italiano IPSE, collegato al progetto europeo epSOS ha visto la partecipazione di Abruzzo, Emilia-Romagna, Friuli-Venezia Giulia, Lombardia, Molise, Sardegna, Toscana, Umbria, Veneto e la provincia autonoma di Trento, che hanno partecipato al fine di rendere le proprie soluzioni regionali di FSE in grado di coordinare e garantire uno scambio del patient summary. M. CIAMPI, M. SICURANZA, A. ESPOSITO, G. DE PIETRO, *Consiglio Nazionale delle Ricerche Istituto di Calcolo e Reti ad Alte Prestazioni, Progettazione e realizzazione di servizi per l'interoperabilità del Fascicolo Sanitario Elettronico mediante l'infrastruttura InFSE*, 2015, sul punto v. anche *InFSE: Infrastruttura tecnologica del Fascicolo Sanitario Elettronico Specifiche tecniche per l'interoperabilità dei sistemi territoriali di FSE, Presidenza del Consiglio dei Ministri Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica Consiglio Nazionale delle Ricerche Dipartimento di Ingegneria, ICT e Tecnologie per l'Energia e i Trasporti.*

[200] S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, cit., 336.

strumento sul territorio, caratterizzata da molte lacune che non garantivano l'efficacia del sistema: anche le Regioni che avevano adottato l'utilizzo di tale strumento non erano in grado di garantire l'omogeneità dell'alimentazione del FSE, compromettendo il perseguimento degli obiettivi di cura e interoperabilità[201].

La disciplina attuale prevede che il Fascicolo sanitario elettronico sia redatto e aggiornato dal medico di medicina generale o dal pediatra di libera scelta, che riassume la storia clinica dell'assistito e la situazione corrente conosciuta, per garantire continuità assistenziale[202].

Al fine di evitare ripercussioni negative nelle scelte adottate per elaborare modalità di cura e prevenzione, è indispensabile garantire che i dati utilizzati siano autentici, che le informazioni vengano costantemente aggiornate e, in generale, che la gestione avvenga in maniera omogenea[203].

La disciplina vigente prevede che tale strumento può essere alimentato sia da professionisti coinvolti nel processo di cura e sia dall'assistito. In particolare, tramite il "taccuino" il paziente può integrare le informazioni presenti sul supporto informatico[204]. In tal modo, possono essere inseriti dati rilevanti, come parametri relativi alla pressione arteriosa o alla glicemia, utili per definire un quadro esaustivo dello stato di salute dell'individuo, anche se le informazioni introdotte dal paziente sono considerate non certificate dal Servizio Sanitario Nazionale.

La previsione della possibilità di integrazione del fascicolo sanitario da parte degli individui comporta di primo acchito un favoreggiamento verso la realizzazione della possibilità di una completa redazione dello strumento

---

[201] Tale carenza è stata evidenziata nelle Linee guida per l'attuazione del Fse, adottate con decreto del Ministero della salute il 20 maggio 2022. Anche il monitoraggio trimestrale effettuato dall'Agenzia per l'Italia Digitale, visibile sul sito *web* dedicato (https://www.fascicolosanitario.gov.it/monitoraggio), ha dimostrato la carente risposta nazionale all'utilizzo di tale strumento nel 2022. Sul punto, v. S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, cit., 337.

[202] Rileva, dal punto di vista contenutistico, la differenza sancita dall'art. 2 del D.P.C.M. 29 settembre 2015, n. 178, il quale stabilisce una chiara distinzione fra il nucleo minimo dei dati e quelli integrativi, ove il nucleo minimo di dati è il medesimo per tutte le regioni e le province autonome, mentre gli ulteriori documenti integrativi sono determinati dalle scelte adottate dalla singola regione in materia di politica sanitaria e dal livello di digitalizzazione raggiunto.

[203] F. CIMBALI, *La governance della sanità digitale*, cit., 125.

[204] Articolo 4, D.P.C.M. 9 settembre 2015, n. 178.

clinico, in grado di contenere dati catalogati dal paziente stesso, con possibili riferimenti alla completezza del documento.
I vantaggi sono molteplici: in tal modo dovrebbe essere garantita la continuità e la completezza delle informazioni cliniche, con la possibilità di inserimento di sintomi, terapie o ulteriori informazioni non ancora inserite, con l'ulteriore inserimento di informazioni legate ad abitudini alimentari o parametri rilevabili tramite l'utilizzo di applicazioni e dispositivi utilizzati quotidianamente del paziente.
Tuttavia, dietro questa possibilità si celano differenti problematiche da non sottovalutare: il fatto che venga riconosciuta al paziente la possibilità di integrare le informazioni può comportare l'inserimento di dati imprecisi o difformi, causando la compromissione dell'affidabilità del documento clinico. Può verificarsi anche una disfunzione dell'efficacia dello strumento clinico causata da incongruenze tra precedenti indicazioni e valori inseriti dal personale medico qualificato e successivi dati non corrispondenti a quanto registrato dai medici.
Al fine di massimizzare e ottimizzare la previsione dello strumento di integrazione del FSE, anche in vista dell'entrata in vigore del nuovo Regolamento, sarebbe opportuno prevedere un sistema che consenta l'inserimento di informazioni ma mediante un vaglio antecedente attuato mediante controlli automatici che siano in grado di rilevare possibili incongruenze. La chiarezza del dato clinico è fondamentale, per tale motivo è necessario che vengano previste regole chiare per disciplinare l'integrazione, controlli costanti, con annessa interazione tra paziente e personale medico al fine di dar vita ad un utilizzo efficace dello strumento.
Occorre precisare che le informazioni inserite dal paziente non hanno la stessa validità di quelle introdotte dal personale addetto. Nella fase di valutazione delle informazioni contenute nel FSE, è indispensabile tener conto prevalentemente dei dati collocati dai professionisti. Gli altri parametri dovrebbero avere una valenza marginale, utili per la ricostruzione della storia clinica del paziente.
Appare legittimo domandarsi quale rilevanza va attribuita a questi dati soprattutto nel caso in cui un soggetto viene curato in uno stato estero; in

caso di difformità riscontrata tra le differenti informazioni inserite, con conseguente poca chiarezza del quadro clinico del paziente, sarebbe opportuno provvedere alla valutazione di un'anamnesi completa tramite la ripetizione di alcuni esami specifici. Anche se tale soluzione appare tardiva e non efficace in caso di urgenza. L'ultima parola spetterà alla discrezionalità del medico coinvolto, il quale dovrà adottare la soluzione maggiormente appropriata in relazione al caso concreto.

Nel corso del tempo sono stati numerosi i tentativi di modifica della disciplina posta alla base dell'utilizzo del Fascicolo sanitario elettronico, il quale attualmente viene identificato principalmente come mezzo utile alla PA per garantire un adeguato funzionamento del Sistema sanitario e non tanto più come elemento primariamente rivolto alla persona[205].

L'art. 12 del d.l. 18 ottobre 2012, n. 179, recante la definizione del FSE, ha subito numerose modifiche: con precisione parliamo di nove interventi[206]. Da ciò si desume il tentativo del legislatore di seguire le orme dell'evoluzione tecnologica, che tuttavia appare sempre parzialmente insufficiente[207]. Fra i tanti, significativo è l'intervento avuto con il c.d. Decreto rilancio, d.l. 19 maggio 2020, n. 34, il quale ha stabilito l'eliminazione della necessità di raccolta del consenso del paziente: a differenza della precedente disciplina, l'integrazione e la creazione del FSE avviene automaticamente[208].

In particolare, le linee guida del 2009 sancivano la forte rilevanza del principio di autodeterminazione del singolo che si evinceva dalla garanzia di scelta libera dell'individuo sulla creazione del fascicolo che ricostruiva la sua storia clinica[209].

---

[205] S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, cit., 338.

[206] In particolare, a seguito della crisi pandemica globale, tramite il d.l. 27 gennaio 2022, n. 4, è stata introdotta la lettera a-*ter* al secondo comma dell'art. 12, che ha aggiunto la finalità di profilassi internazionale. Nel corso del tempo, le finalità perseguite tramite l'utilizzo del Fse sono aumentate: oltre al principale fine legato alle esigenze di cura del paziente, è necessario far riferimento alle finalità che, se paragonate alla nuova disciplina dell'EHDS, possiamo definire secondarie, ossia quelle di studio e ricerca.

[207] S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, cit., 334 ss.

[208] Sul punto v. A. M. GAMBINO, E. MAGGIO E V. OCCORSIO*, La riforma del fascicolo sanitario elettronico*, in *Diritto mercato tecnologia*, 2020, 6 ss.

[209] *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario,*16 luglio 2009.

Il punto centrale riguardava anche la previsione di distinti consensi specifici, da parte dei singoli titolari del trattamento, e la possibilità di inserimento di pregressi eventi clinici rilevanti.

Il percorso seguito dal Garante con le linee guida del 2009 è stato via via superato, con una visione che sembrerebbe mettere in secondo piano il profilo soggettivo della persona, con prevalenza della tutela della salute collettiva. In particolare, viene stabilita l'obbligatoria costituzione del FSE, anche se originariamente l'art. 12 del d.l. n. 179/2012 continuava a prevedere la centralità dell'alimentazione di tale strumento solamente con la presenza del consenso del soggetto interessato. Tale previsione è stata eliminata mediante l'abrogazione del comma 3*bis* del citato articolo 12, mediante il d.l. 19 maggio 2020, n. 34, dando vita ad una significativa apertura verso la scelta di attuare una preferenza verso il pubblico interesse che supera quello individuale[210].

Il comunicato stampa dell'11 gennaio 2021 del Garante privacy ha stabilito dei punti chiavi per cercare di riequilibrare le previsioni che non mettevano più al centro della disciplina il consenso dell'interessato per l'integrazione del FSE[211].

La centralità del consenso non è stata accantonata rispetto alla consultazione del FSE per il perseguimento di finalità di diagnosi, cura e similari, rientranti nell'uso primario[212].

Anche il c.d. Decreto sostegni *ter*, convertito con l. 28 marzo 2022, n. 25 ha dato vita a significative modifiche: la più rilevante riguarda la previsione dell'integrazione del fascicolo sanitario elettronico con le prestazioni

---

[210] G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati,* cit., 27 e 28.

[211] In particolare, il Garante ha stabilito che l'integrazione di tale strumento con dati anteriori può avvenire solo quando ci sia stata un'adeguata campagna nazionale di informazione fornita ai cittadini per rendere chiare le novità inerenti all'alimentazione del Fascicolo sanitario elettronico, stabilendo un limite di 30 giorni, a favore dei singoli, per dar vita ad una opposizione. Solamente in presenza di queste precisazioni il FSE può essere alimentato con i dati pregressi del paziente.

[212] Articolo 12, comma 5, d.l. 18 ottobre 2012, n. 179, Mentre la consultazione del fascicolo sanitario elettronico per finalità rientranti nell'uso secondario deve avvenire a norma del comma 6 dell'art. 12 senza trattare i propri dati personali. Sul punto v. G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati,* cit., 30 e 31.

erogate dal SSN, ma anche da operatori privati, nei cinque giorni successivi all'erogazione stessa[213].

Attualmente la disciplina del Fascicolo sanitario elettronico è stata revisionata mediante il decreto del Ministero della salute del 7 settembre 2023 che disciplina il cd. fascicolo sanitario 2.0 che punta alla creazione di una infrastruttura ottimizzata in grado di garantire l'interoperabilità e lo scambio delle informazioni fra le diverse regioni.

In realtà già nel 2022 ci fu un tentativo di emissione di due Decreti Ministeriali collegati fra loro: uno riferito al FSE 2.0 e uno sulla creazione dell'Ecosistema dei Dati sanitari, entrambi oggetto di parere negativo da parte del Garante[214]. Quest'ultimo solamente con il provvedimento n. 256 dell'8 giugno 2023 ha espresso parere favorevole allo schema del decreto che disciplina il nuovo Fse 2.0[215].

Il d.m. in questione prevedeva originariamente il perseguimento di scopi legati alla cura, alla prevenzione, alla profilassi internazionale, alla ricerca scientifica e al governo sanitario, con particolare attenzione alla valutazione del grado di assistenza sanitaria offerto a livello nazionale. Ma con il nuovo Decreto Ministeriale, il Governo ha limitato la disciplina esclusivamente agli ambiti della cura, della prevenzione e della profilassi internazionale, escludendo così la ricerca scientifica e il governo sanitario. Questi ultimi aspetti continueranno a essere regolamentati dalla vecchia disciplina contenuta nel d.p.c.m. n. 178 del 2015[216].

---

[213] Art. 12, comma 1, d.l. 18 ottobre 2012, n. 179.

[214] V. 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, n 294, (doc. *web* n. 9802729); 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, n. 295 (doc. *web* n. 9802752).

[215] S. CORSO, *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, cit., 337 ss.

[216] In particolare, il D.P.C.M. 29 settembre 2015, n. 179 continuerà a disciplinare gli aspetti legati alle finalità di ricerca e di governo: continueranno ad essere applicati gli artt. 15, 16 e 17 e gli artt. 18, 19 e 20, fino all'adozione di ulteriori decreti. Il nuovo d.m. sul FSE 2.0 appare incompleto: sul punto, v. S. CORSO, *Il fascicolo sanitario 2.0: Spunti per una lettura critica*, cit., 339 ss.

Le numerose modifiche subite dal FSE hanno dato vita a un rilevante aumento della prevalenza delle funzioni dello Stato, diminuendo quello delle regioni[217].

La crisi sanitaria globale ha dato vita alla scelta di centralizzare le funzioni di gestione del Fascicolo sanitario elettronico: in particolare, il potere di coordinamento a livello centrale si evince dalla scelta di emissione delle Linee guida alle quali le singole regioni devono necessariamente adeguarsi, in quanto i piani adottati sono oggetto di valutazione da parte del Ministero della salute[218], anche se particolarmente rilevante è il d.m. Sanità del 7 settembre 2023 che, a differenze di quanto appena descritto, dà vita ad una sorta di controtendenza aprendo un parziale spiraglio di autonomia alle regioni che, assieme alle province autonome, possono occuparsi anche di gestioni specializzate dei dati personali motivate da interesse pubblico[219].

La circolazione dei dati sanitari rappresenta un macrocontesto in cui va assicurata la tutela del soggetto coinvolto, per questo motivo è indispensabile la creazione di un armonico sistema di condivisione che sia efficace e sicuro a livello regionale, nazionale e sovranazionale[220].

La centralità del controllo dell'interessato, seppur parziale, si manifesta tramite la possibilità di accesso e presa visione delle informazioni contenute nel fascicolo, nella possibilità di revoca del consenso, nel diritto di rettifica, nel diritto all'oscuramento[221] dei dati e nella possibilità di integrare i propri

---

[217]Appare opportuno far riferimento al fatto che la modifica apportata all'art. 12 del d.l. n. 179/2012 dal d.l. n. 4/2022 parla di "governo della sanità digitale" dimostrando la volontà di dar vita ad una gestione fortemente centralizzata. Così G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati,* cit., 21 ss.

[218]Si precisa che l'art. 12, comma 15-*bis,* d.l. 179/2012, introdotto dall'art. 21 d.l. 4/2022 sancisce che in caso adeguamento non conforme alle Linee guida si procederà all'esercizio del potere sostitutivo disciplinato dall'art. 117, comma 5 e 120, comma 2 della Costituzione. L'attuazione del PNRR conferma la scelta di accantonamento del ruolo preminente delle regioni. Per ulteriori approfondimenti v. G. C. FERONI, *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati,* cit., 24 ss.

[219]Articolo 13, d.m. 7 settembre 2023 (in Gazzetta ufficiale 24 ottobre 2023, n. 249)

[220]F. CIMBALI, *La governance della sanità digitale*, cit., 144.

[221] «*Il diritto di oscuramento può essere esercitato al momento dell'erogazione della prestazione, prima dell'alimentazione del FSE, direttamente nei confronti del soggetto che lo eroga, che è tenuto a informare in tal senso l'assistito, ovvero in qualunque momento successivo, tramite specifica istanza dell'assistito trasmessa al soggetto erogante.*

Nei casi in cui l'oscuramento di dati e documenti avviene successivamente all'alimentazione del FSE, l'assistito è informato del fatto che le informazioni del dato o documento oscurato possono essere state utilizzate prima dell'oscuramento per la

dati. Il minor peso attribuito all'autonomia decisionale del singolo risulta giustificato dall'esigenza di tutelarne la salute, attraverso la massimizzazione dell'interoperabilità delle informazioni cliniche, con l'obiettivo di garantire la centralità dell'ottimizzazione delle possibilità di cura[222].

Attualmente, la consultazione delle informazioni contenute nel FSE avviene solamente a seguito della prestazione di consenso da parte del soggetto interessato e con l'attento rispetto del segreto professionale da parte dei medici che lo hanno in cura, ad eccezione di specifici casi di emergenza sanitaria che prevedono procedure di rettifica rispetto alla regola generale. In particolare, l'accesso ha luogo tramite l'iter previsto dalla singola regione o provincia autonoma di riferimento.

---

realizzazione di altri documenti, quali il Profilo sanitario sintetico di cui all'art. 4, rispetto ai quali può autonomamente esercitare il medesimo diritto.
Il diritto di oscuramento può essere esercitato anche tramite una apposita funzionalità online resa disponibile nel FSE e, in tale caso, è garantito l'immediato oscuramento del dato o documento.
5. Nel caso in cui sia stato esercitato il diritto all'oscuramento, l'assistito può revocare in ogni momento l'oscuramento di un dato o documento con le medesime modalità previste per l'esercizio del diritto di oscuramento.
6. L'oscuramento di dati e documenti del FSE avviene con modalità tali da garantire che tutti i soggetti abilitati all'accesso al FSE per le finalità di cura, prevenzione e profilassi internazionale non possano venire automaticamente a conoscenza del fatto che l'assistito ha effettuato tale scelta e che tali dati esistano.
7. L'oscuramento delle prescrizioni, di cui all'art. 3, comma 1, lettera f), determina l'oscuramento automatico dei documenti relativi all'erogazione delle stesse, di cui all'art. 3, comma 1, lettere h) e
j), nonché' ai referti riferiti alle medesime prestazioni, di cui all'art. 3, comma 1, lettera b).» Articolo 9, Decreto 7 settembre 2023, *Ministero della salute, Fascicolo sanitario elettronico 2.0*; per un ulteriore approfondimento v. articolo 3, 17 ottobre 2024, *Min. Economia e Finanze*, *Modalità di messa a disposizione ai Fascicoli sanitari elettronici (FSE), tramite l'Infrastruttura nazionale per l'interoperabilità (INI), dei dati del Sistema tessera sanitaria e del consenso o diniego del Sistema informativo trapianti (SIT)*.

[222] L'utilizzo dei sistemi di archiviazione deve essere legato a adeguate previsioni che siano in grado di garantire l'effettiva protezione dei dati e delle informazioni inserite, al fine di mitigare rischi legati ad accessi abusivi, furto o smarrimento dei supporti di memorizzazione. Dovranno essere garantiti sistemi di autorizzazione idonei e procedure per la verifica periodica delle autorizzazioni fornite, l'utilizzo della crittografia per la comunicazione dei dati, la tracciabilità degli accessi e procedure di pseudonimizzazione. Anche in questo caso rileva la formazione del personale coinvolto che si occuperà della gestione dei dati. In particolare, La nuova disciplina prevede che i soggetti che concorrono all'alimentazione del FSE siano responsabili in caso di mancata, non tempestiva o non esatta alimentazione della documentazione. In particolare, ciò è stabilito dall'art. 12, comma 3, del decreto FSE 2.0, che si adegua alle indicazioni evidenziate dal Garante per la protezione dei dati personali nel provvedimento n. 294 del 22 agosto 2022, (doc. *web* n. 9802729). Sul punto, v. S. CORSO, *Il fascicolo sanitario 2.0: Spunti per una lettura critica*, cit., 343.

Attualmente, vengono utilizzati degli indicatori che consentono di monitorare l'andamento e lo stato di utilizzo del Fascicolo Sanitario Elettronico a livello nazionale. In particolare, il sito web dedicato al fascicolo sanitario utilizza differenti gruppi di indicatori: uno dedicato all'utilizzo e un altro alla disponibilità dei servizi e documenti.

I dati riferiti al 30 novembre 2024 dimostrano che i documenti che vengono inseriti nel FSE sono: verbale del pronto soccorso, referto specialistico ambulatoriale, referto di radiologia, referto di laboratorio, prescrizione specialistica, prescrizione farmaceutica e lettera di dimissione ospedaliera. In particolare, i grafici riportano la totale adesione da parte delle regioni in merito all'integrazione del FSE con i documenti sopra elencati.

Mentre solamente il 90% delle regioni provvede all'integrazione del FSE con il profilo sanitario sintetico[223], l'81% inserisce il referto di anatomia patologica[224], l'81% inserisce il documento di erogazione farmaci[225], 81% documento di erogazione di prestazioni di assistenza specialistica[226], 76% certificato vaccinale[227], 71% taccuino personale dell'assistito[228], 62% scheda singola vaccinazione[229], 24% lettera di invito per screening, vaccinazione o ad altri percorsi di prevenzione[230].

[223] In particolare, le regioni interessate sono: Abruzzo, Basilicata, Calabria, Campania, Emilia-Romagna, Friuli-Venezia Giulia, Lazio, Liguria, Lombardia, Marche, Molise, P.A. Bolzano, Piemonte, Puglia, Sardegna, Sicilia, Toscana, Umbria, Valle d'Aosta.

[224] In particolare, le regioni interessate sono: Abruzzo, Basilicata, Calabria, Campania, Friuli-Venezia Giulia, Lazio, Lombardia, Marche, Molise, P.A. Bolzano, P.A. Trento, Piemonte, Sardegna, Sicilia, Umbria, Valle d'Aosta, Veneto.

[225] In particolare, le regioni interessate sono: Abruzzo, Basilicata, Calabria, Campania, Emilia-Romagna, Friuli-Venezia Giulia, Lazio, Liguria, Molise, P.A. Bolzano, Piemonte, Puglia, Sardegna, Sicilia, Toscana, Umbria, Veneto.

[226] In particolare, le regioni interessate sono: Abruzzo, Basilicata, Calabria, Campania, Emilia-Romagna, Lazio, Liguria, Molise, P.A. Bolzano, P.A. Trento, Piemonte, Puglia, Sardegna, Sicilia, Toscana, Umbria, Veneto.

[227] In particolare, le regioni interessate sono: Abruzzo, Calabria, Campania, Emilia-Romagna, Friuli-Venezia Giulia, Lazio, Liguria, Lombardia, Molise, P.A. Trento, Piemonte, Sardegna, Sicilia, Toscana, Valle d'Aosta, Veneto.

[228] In particolare, le regioni interessate sono: Abruzzo, Calabria, Emilia-Romagna, Friuli-Venezia Giulia, Lazio, Liguria, Lombardia, Marche, Molise, P.A. Trento, Piemonte, Sardegna, Toscana, Valle d'Aosta, Veneto.

[229] In particolare, le regioni interessate sono: Abruzzo, Calabria, Campania, Emilia-Romagna, Lazio, Liguria, Molise, P.A. Bolzano, P.A. Trento, Piemonte, Sardegna, Sicilia, Toscana.

[230] In particolare, le regioni interessate sono: Basilicata, Emilia-Romagna, Lazio, Piemonte, Veneto.

Tali indicatori forniscono informazioni inerenti alla percentuale di regioni che hanno avviato l'alimentazione dei fascicoli dei propri assistiti[231].
Le difficoltà legate all'efficace utilizzo di tale strumento, la disomogenea adesione al modello da parte delle singole regioni e il fallimento della prima iniziativa di creazione di una disciplina sul FSE 2.0 nel 2022, che ha poi portato all'elaborazione di una nuova normativa incompleta rispetto al progetto originario, sollevano interrogativi rilevanti. Legittimo è chiedersi in che modo l'Italia, e tutti gli Stati europei, risponderanno alle prescrizioni sancite dal Regolamento che disciplina l'*European Health Data Space*. Una delle principali sfide riguarderà la capacità di garantire un'interoperabilità efficace dei dati sanitari a livello europeo, sia sotto il profilo della compatibilità tecnica tra gli strumenti adottati nei singoli Stati, sia in riferimento alla gestione delle informazioni cliniche redatte in lingue differenti. L'obiettivo sarà quello di assicurare continuità e adeguatezza delle cure su tutto il territorio europeo, garantendo elevati *standard* di coerenza e qualità nel trattamento dei dati clinici, con un occhio di riguardo per la tutela della riservatezza dei pazienti.

5. Il problema della divulgazione dei dati contenuti nei d*ossier* sanitari.

La digitalizzazione dei dati sanitari ha dato vita ad una progressiva dematerializzazione dei documenti utilizzati nelle diverse fasi di cura ove tutela della salute e tutela della *privacy* rappresentano i due poli di un bilanciamento che vacilla nell'inarrestabile ricerca di un giusto equilibrio. Anche in questo piccolo frangente della macroarea del tema della digitalizzazione della sanità, nasce la necessità di chiedersi se il raggiungimento di un giusto equilibrio rappresenti un obiettivo non perseguibile. Le riflessioni che seguono richiedono una maggiore attenzione se riferite alla gestione del dato su larga scala, compatibilmente a quanto previsto con la creazione dell'*European Health Data Space*.

[231] https://monitopen.fse.salute.gov.it/documentservices#documents

Dopo aver parlato del Fascicolo sanitario elettronico, l'attenzione va posta sul *dossier*: lo strumento utilizzato da una struttura che offre servizi sanitari che consente una parziale ricostruzione della storia clinica del paziente[232].
Diversi equivoci sono emersi, in particolare riferiti alle modalità di utilizzo degli stessi: numerosi provvedimenti sono stati comminati a causa dell'assenza di una chiara interpretazione della disciplina contenuta nel Codice *privacy*. Per tale motivo nel 2015 il Garante è intervenuto adottando le Linee guida in materia di *dossier* sanitario[233].
La necessità dell'intervento è stata spinta dall'esigenza di attuare un sistema di raccolta di informazioni chiare e attendibili, in grado di soddisfare i diritti degli individui coinvolti, tutelandoli sia come pazienti e sia come soggetti interessati ad un lecito trattamento dei dati personali.
Il *dossier* sanitario si differenzia dal FSE in quanto conserva gli eventi clinici di uno stesso soggetto, legati ad un'unica struttura sanitaria e, quindi, ad un unico titolare del trattamento, rappresentando una sorta di estensione dell'ordinaria raccolta dati. Nel caso isolato di trattamento, senza la presenza del *dossier* sanitario, il professionista deve utilizzare solo le informazioni fornite dal paziente, collegate all'evento clinico attuale. Mentre con il *dossier*, il personale coinvolto può accedere a tutte le informazioni ivi contenute, che rappresentano lo storico clinico del paziente, create in quella determinata struttura sanitaria. A differenza del FSE, il *dossier* è incompleto in quanto tutte le prestazioni sanitarie erogate altrove, non confluiscono al suo interno.
L'obiettivo principale della creazione del *dossier* sanitario riguarda il miglioramento del processo di cura del paziente, che può essere garantito solamente mediante un corretto inserimento delle informazioni cliniche e un monitoraggio volto ad evitare arbitrarie modifiche.
Le Linee guida del 2015 hanno chiarito che il titolare del trattamento è responsabile della comunicazione al soggetto in cura dell'utilità legata alla

[232] F. C. RAMPULLA, G. C. RICCIARDI, A. VENTURI, *Digitalizzazione delle amministrazioni e accesso ai dati e ai documenti informatici sanitari,* in *Federalismi.it*, 2, 2024, 139.
[233] In realtà già nel 2009 il Garante intervenne sul tema adottando con provvedimento del 16 luglio 2009 le *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*, in G.U. n. 178, 3 agosto 2009, (doc. *web* n. 1634116).

creazione dello strumento: ad esempio il miglioramento delle prestazioni erogate garantito dalla sinergia derivante dalla condivisione del dato con il personale coinvolto nel processo di cura.

Inoltre, deve essere specificato che il dissenso alla creazione o all'integrazione del *dossier* non comporta l'impossibilità di utilizzo delle cure; il consenso per la creazione del *dossier* sanitario conserva la sua autonomia, rispetto a quello necessario per l'ordinario trattamento dei dati collegati alla singola prestazione. Nel corso del tempo, non sarà necessario un rinnovo del medesimo: il personale sanitario coinvolto potrà direttamente accedervi sulla base della legittimazione creatasi con il consenso inizialmente conferito[234].

Il titolare del trattamento deve stabilire specifiche modalità di verifica dell'acquisizione del consenso[235]. Va riconosciuta particolare centralità all'informativa che deve essere fornita al soggetto interessato, al fine di garantire una scelta consapevole. In particolare, le Linee guida chiariscono che l'informativa può essere affissa nei locali della struttura coinvolta o pubblicata sul sito *web*[236].

La tutela della riservatezza del soggetto sottoposto alle cure rappresenta il principale elemento nella macroarea di bilanciamento degli interessi coinvolti: sul punto, il Garante ha chiarito l'importanza della tutela dell'anonimato dei soggetti affetti da HIV, che fanno uso di sostanze psicotrope o stupefacenti, che hanno subito violenza sessuale o donne che decidono di partorire in anonimato o interrompere la gravidanza. É indispensabile uno specifico consenso per l'inserimento di questa categoria "ultra sensibile" di dati nei *dossier*[237].

Inoltre, in situazioni di tal tipo, l'interessato può richiedere che tali informazioni siano accessibili ad una cerchia ristretta di professionisti. La

---

[234] Nei casi di legittimazione previsti, o in caso di consenso dell'interessato, al pari di ogni altra informazione che riguarda lo stato di salute di un individuo, le informazioni contenute nel *dossier* possono essere trattate per fini di ricerca: articolo 110, d.lgs. 30 giugno 2003, n. 196.

[235] Art. 79, comma 2, d.lgs. 30 giugno 2003, n. 196.

[236] *Linee guida in materia di Dossier sanitario*, 4 giugno 2015, (doc. *web* n. 4084632).

[237] S. MELCHIONNA, *Sanità digitale e innovazione*, in *Privacy e diritto dei dati sanitari*, L. BOLOGNINI, S. ZIPPONI (a cura di) 2024, Milano, p. 110.

scelta di generalizzare la possibilità di oscurare i dati inerenti a situazioni molto eterogenee, per natura e impatto sulle cure, appare discutibile. È infatti diverso consentire l'oscuramento di informazioni legate ad esperienze particolarmente sensibili, come episodi di violenza sessuale e interruzione volontaria della gravidanza, che quasi certamente non incideranno in modo diretto sull'efficacia delle cure, rispetto alla possibilità di nascondere dati clinici come la presenza di HIV[238]. Quest'ultima può avere conseguenze significative sulle scelte terapeutiche da adottare ma anche sulla sicurezza degli operatori sanitari coinvolti nel processo di cura.
In particolare, il Garante privacy ha chiarito che «*con riferimento alla raccolta di informazioni relative all'eventuale stato di sieropositività, è, dunque, compito del medico curante illustrare al paziente l'importanza di conoscere anche tale informazione in relazione al tipo di intervento o al piano terapeutico da eseguire. Qualora ritenga, infatti, che la conoscenza dello stato di sieropositività sia indispensabile in relazione al trattamento sanitario o terapeutico che intende realizzare, è suo compito illustrare al paziente le conseguenze che la mancata conoscenza di tale informazione potrebbe determinare*»[239].
Il personale sanitario coinvolto può raccogliere tali informazioni, solamente nel caso in cui il dato relativo alla sieropositività risulti necessario in funzione della prestazione medica da erogare, con la consapevole previsione che a seguito delle dovute informazioni fornite al paziente, quest'ultimo potrà scegliere di non comunicare al medico taluni eventi che lo riguardano[240].
Sul punto occorre evidenziare che la l. 30 giugno 1990, n. 135 stabilisce che la previsione del necessario consenso per la sottoposizione all'accertamento della presenza della sieropositività può essere derogata «per motivi di

[238] V. alla l. 5 giugno 1990, n. 135, con particolare riferimento all'art. 5 rubricato "*Accertamento dell'infezione*".
[239] Prescrizioni concernenti la raccolta d´informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie - 12 novembre 2009 (G.U. n. 289 del 12 dicembre 2009), Garante per la protezione dei dati personali, (doc. web n. 1673588).
[240] Prescrizioni concernenti la raccolta d´informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie - 12 novembre 2009 (G.U. n. 289 del 12 dicembre 2009), Garante per la protezione dei dati personali, (doc. web n. 1673588).

necessità clinica» del paziente stesso[241], evidenziando in modo chiaro la preminenza delle esigenze di cura connesse alla tutela della salute del paziente.

Seppur l'efficacia dell'interoperabilità viene messa in discussione, poiché l'omissione di informazioni clinicamente rilevanti rischia di compromettere la qualità e la continuità delle cure[242], non si può negare che l'oscuramento dei dati rappresenti una misura imprescindibile per garantire la tutela dei diritti e della riservatezza del soggetto coinvolto[243].

Le possibili conseguenze di tale scelta fanno riferimento al fatto che il *dossier*, che si presenta già come documento clinico incompleto, può subire ulteriori riduzioni. Sul punto appare rilevante il ruolo fondamentale del titolare del trattamento che deve fornire una corretta informativa volta a rendere consapevole il paziente dell'importanza della completezza del documento: nelle Linee del 2015, il Garante ha rilevato la diminuzione della percentuale dell'esercizio del diritto all'oscuramento, nei casi in cui è stata fornita corretta informativa sulle omissioni[244].

Anche se il medico è tenuto ad effettuare un'anamnesi dettagliata del paziente, illustrando l'importanza della completa raccolta dei dati personali, il soggetto interessato resta libero di scegliere[245].

---

[241] Articolo 5, comma 3, l. 30 giugno 1990, n. 135.

[242] In particolare occorre far riferimento alla disciplina sancita dal Regolamento (UE) 2016/679: l'articolo 9 disciplina il Trattamento di categorie particolari di dati personali, in tale categoria rientrano i dati relativi alla salute il cui trattamento è vietato salvo eccezioni, tra cui trattamento necessario per finalità di medicina preventiva o di diagnosi, erogazione di prestazioni sanitarie o gestione dei sistemi sanitari, (articolo 9, paragrafo 2, lettera h) e «consenso esplicito dell'interessato.» (articolo 9, paragrafo 2, lettera a). Sul tema rileva ulteriormente il contenuto dell'articolo 15 che disciplina il Diritto di accesso dell'interessato e stabilisce che quest'ultimo ha il diritto di sapere quali dati sono trattati, da chi, e per quali finalità. Rileva ulteriormente il contenuto degli artt. 16 e17 che sanciscono rispettivamente la rettifica e cancellazione e il Diritto alla cancellazione. Quest'ultimo rafforza il concetto di limitazione di utilizzo dei propri dati. Inoltre, occorre far riferimento alla disciplina contenuta nel Codice *privacy*, d.lgs. 196/2003 modificato dal d.lgs. 101/2018, ponendo particolare attenzione all'articolo 2-*septies* che disciplina le Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, all'art. 75 che disciplina specifiche condizioni in ambito sanitario.

[243]Tale garanzia era già presente nelle precedenti *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario,*16 luglio 2009.

[244] *Linee guida in materia di Dossier sanitario*, 4 giugno 2015.

[245] Occorre precisare che Nelle linee guida, il Garante stabilisce la legittimità dell'informativa tardiva, nel caso in cui il paziente si rechi presso la struttura sanitaria in gravi condizioni, senza la possibilità di esprimere la propria volontà.

La possibilità di non rendere visibili alcune informazioni deve essere attuata mediante un sistema che consenta di oscurare a sua volta tale scelta[246]. Dunque, all'interno di ogni struttura deve essere garantita una corretta gestione degli accessi, mediante l'utilizzo di barriere in grado di limitare la visibilità delle informazioni oscurate[247].

Sul punto, particolare attenzione va data al rischio legato all'accesso ai *dossier* sanitari, all'interno della medesima struttura, da parte di soggetti non direttamente coinvolti nell'attività di cura del paziente, per esigenze meramente esplorative. Ai pazienti è riconosciuto il diritto di poter richiedere la visione dell'elenco degli accessi effettuati.

Il rischio di un errato utilizzo delle informazioni contenute nel *dossier* sanitario è elevato, per tale motivo è necessario che il titolare del trattamento adotti l'utilizzo di sistemi di autenticazione adeguati.

A tal proposito, è importante una chiara definizione della cd. "profondità dell'accesso", intesa come previsione di differenti livelli di possibilità di visione del dato condiviso nel *dossier*. La profondità degli accessi deve essere modulata in base al ruolo dell'operatore coinvolto.

Inoltre, nelle linee guida viene specificata l'importanza della formazione del personale che utilizza i dati contenuti in tale supporto elettronico[248].

Inoltre, il soggetto interessato deve essere informato del fatto che il dossier può essere consultato nel caso in cui risulti indispensabile per la salvaguardia della salute di terzi o, in generale, della collettività: v. *Linee guida in materia di Dossier sanitario*, 4 giugno 2015.

[246] «*L'"oscuramento" dell'evento clinico (revocabile nel tempo) deve avvenire con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento")*»: *Linee guida in materia di Dossier sanitario*, 4 giugno 2015, p. 21.

[247] In vista della digitalizzazione dei sistemi, sul punto si rinvia alla lettura delle linee guida di riferimento, manuali e documenti tecnici per lo sviluppo e la gestione del Fascicolo Sanitario Elettronico (FSE), in particolare: *DM Comma 15-ter Specifiche tecniche per la gestione dell'oscuramento* e *Note tecniche per la gestione dell'oscuramento e il tracciamento delle operazioni*; Per un approfondimento delle modalità e dei meccanismi che consentono la presenza di barriere informative mediante le quali viene consentito l'oscuramento delle condizioni cliniche del paziente si rinvia ai documenti tecnici di riferimento: Il DM Comma 15-ter del 17 ottobre 2024, *Modalità di messa a disposizione ai Fascicoli sanitari elettronici (FSE), tramite l'Infrastruttura nazionale per l'interoperabilità (INI), dei dati del Sistema tessera sanitaria e del consenso o diniego del Sistema informativo trapianti (SIT),* definisce le regole per la gestione dell'oscuramento dei documenti del FSE.

[248] *Linee guida in materia di Dossier sanitario*, 4 giugno 2015.

Con l'intervento avvenuto nel 2015, il Garante ha assunto le sembianze del legislatore, a causa di una carenza normativa sul tema, chiarendo quali sono le misure di sicurezza da adottare per garantire una corretta gestione dei dati inseriti nel *dossier*. Nello specifico: sistemi di autenticazione e autorizzazione che consentono un accesso selettivo basato sul principio di indispensabilità del dato, tracciabilità degli accessi e delle operazioni effettuate[249], sistemi di *audit log* mediante l'attivazione di alert che siano in grado di individuare possibili anomalie[250] e, infine, separazione e cifratura dei dati[251].

La particolarità delle Linee guida adottate nel 2015 consiste nell'unicità della previsione relativa al diritto del soggetto interessato di prendere visione degli accessi al proprio *dossier*[252]: i titolari del trattamento devono fornire all'interessato l'indicazione delle informazioni che consentono di individuare chi ha effettuato l'accesso entro 15 giorni o, nei casi più complessi, entro 30 giorni.

---

[249] «*In particolare, i file di log devono registrare per ogni operazione di accesso al dossier effettuata da un incaricato, almeno le seguenti informazioni: il codice identificativo del soggetto incaricato che ha realizzato l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati. In ragione della particolare delicatezza del trattamento dei dati personali effettuato mediante il dossier è necessario che siano tracciate anche le operazioni di semplice consultazione (*inquiry*). Il titolare deve individuare un congruo periodo di conservazione dei log di tracciamento delle operazioni che risponda, da un lato, all'esigenza per gli interessati di venire a conoscenza dell'avvenuto accesso ai propri dati personali e delle motivazioni che lo hanno determinato e, dall'altro, alle esigenze medico legali della struttura sanitaria titolare del trattamento di dati personali. Alla luce dell'esperienza maturata in sede ispettiva, relativa all'enorme mole di accessi ai dossier sanitari che vengono effettuati all'interno delle strutture sanitarie giornalmente in modalità di sola consultazione, si ritiene congruo stabilire che i log delle operazioni siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.*»: Allegato A, *Linee guida in materia di Dossier sanitario*, 4 giugno 2015, p. 32-33.

[250] La gestione dei dati dovrà essere oggetto di un controllo periodico sulla liceità degli accessi, sull'integrità delle informazioni inserite e sulle procedure informatiche utilizzate, attuato da un'unità organizzativa diversa o da personale diverso rispetto a chi si occupa del trattamento dei dati: *Linee guida in materia di Dossier sanitario*, 4 giugno 2015.

[251] A titolo meramente esemplificativo potremmo pensare all'utilizzo di crittografia.

[252] Le linee guida adottate nel 2015 restano ugualmente utilizzabili nell'ottica di una corretta interpretazione della disciplina inserita nel Codice *privacy*, anche a seguito delle modifiche adottate con il d.lgs. del 2018, che ha adeguato il codice *privacy* alle disposizioni contenute nel GDPR. Il parziale superamento della disciplina fa riferimento alla notificazione al Garante nel caso di violazioni effettuate tramite il dossier, che ad oggi sembrano essere superate dal *data breach* disciplinato dall'art. 33 del Regolamento. Sul punto, v. S. MELCHIONNA, *Sanità digitale e innovazione*, op. cit., p. 106.

Il Garante ha emesso numerosi provvedimenti, a seguito di segnalazioni avviate da soggetti che avevano ricevuto una notifica relativa agli accessi illeciti[253] e, in particolare, è intervenuto con provvedimenti che hanno sanzionato la mancata adozione di adeguate precauzioni da parte di differenti aziende ospedaliere.

In particolare, prima della creazione delle Linee guida del 2015, una struttura sita in Friuli-Venezia Giulia utilizzava applicativi che consentivano il trattamento illecito di dati appartenenti a soggetti in cura, causato dall'assenza del consenso specifico per la raccolta delle informazioni all'interno del *dossier*. Nel caso di specie, il Garante ha evidenziato l'assenza di una informativa dettagliata fornita al paziente, la mancata previsione di puntuali limitazioni all'accesso da parte del personale sanitario e l'assenza della possibilità di esercizio del diritto all'oscuramento del dato clinico[254].

In un altro caso, a seguito di alcuni accertamenti ispettivi, è emersa l'assenza di limitazioni di accesso ai *dossier* di pazienti dimessi, privi di restrizioni temporali e limitazioni relative alla profondità di accesso del personale sanitario[255]. Anche l'utilizzo del *dossier* sanitario per lo svolgimento di funzioni amministrative legate al percorso di cura del paziente deve prevedere delle limitazioni[256].

Nonostante il tentativo di chiarimento della disciplina giuridica afferente all'utilizzo degli applicativi nell'ambito della sanità digitale, le strutture sanitarie hanno continuato a commettere illeciti.

Tuttavia, dall'analisi di un provvedimento emanato nel 2020 dal Garante emerge, a differenza di quanto accadeva antecedentemente, una maggiore consapevolezza dell'azienda ospedaliera coinvolta. Nel caso di specie, la struttura sanitaria ha segnalato tre differenti episodi di accesso non autorizzato ai *dossier* di soggetti che, oltre ad essere pazienti, erano anche

---

[253] Provvedimento del 21 aprile 2021, n. 155 (doc. *web* n. 9678507); Provvedimento del 22 febbraio 2024, (doc. *web* n. 10001279).

[254] Provvedimento 10 gennaio 2013, n. 3, (doc. *web* n. 2284708).

[255] In tale sede, il Garante ha rilevato un'anomalia in merito al consenso univoco per la raccolta dei dati all'interno dei dossier sanitari: l'azienda ospedaliera ha attuato tale previsione solamente da ottobre del 2014, raccogliendo dati in sistemi applicativi senza specifico consenso. Provvedimento del 22 giugno 2016, n. 273, (doc. *web* n. 5410033).

[256] Cfr. punto 6, *Linee guida in materia di Dossier sanitario*, 4 giugno 2015 e punto 4, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario* del 2009.

dipendenti dell'ente. Nel caso di specie l'azienda ospedaliera ha immediatamente avviato dei procedimenti disciplinari, per punire le condotte lesive dei propri dipendenti, etichettate come atti di mera curiosità, e ha dichiarato l'esplicita volontà di dar vita ad un'implementazione dei filtri utilizzati per limitare l'accesso del personale, specificando l'inserimento di un chiaro avvertimento sul tracciamento dell'accesso, volto a disincentivare l'utilizzo arbitrario dei sistemi[257].

Mentre con i primi provvedimenti[258] il Garante condannava anche la mancata raccolta del consenso e l'assenza di una corretta informativa, con il provvedimento del 2020 sono state riscontrate problematiche legate ai soli accessi[259]. Inoltre, nell'ultimo caso è stata riscontrata una maggiore consapevolezza dell'azienda ospedaliera che, benché non abbia preventivamente adottato delle misure idonee a prevenire accessi illeciti, ha dimostrato una maggiore prontezza verso la risoluzione e il progressivo raggiungimento di un adeguato sistema di controllo.

Appare chiara la sussistenza di un radicato analfabetismo da parte dei dipendenti[260]: la "mera curiosità" rappresenta una grave lesione degli artt. 5 e 9 del Regolamento europeo[261].

Le linee guida del 2015 sono state adottate al fine di fornire una visione chiara e univoca del *dossier* sanitario e per garantire un adeguato, sicuro e previdente trattamento dei dati personali. In particolare, l'attenzione del Garante è stata posta sull'inesatta convinzione di illimitata possibilità di accesso ai dati, legata al ruolo svolto all'interno di una delle articolazioni

---

[257] Provvedimento del 23 gennaio 2020, n. 18, (doc. *web*. n. 9269629), anche in *Azienditalia*, 2021, con commento di C.C. GIARDINA, *Il Data breach in ambito sanitario: l'importanza di una corretta policy per evitare sanzioni da parte del Garante della Privacy,* p. 1065.

[258] Provvedimenti del 10 gennaio 2013, n.3, (doc. *web* n. 2284708); Provvedimento del 22 giungo 2016, n. 273, (doc. *web* n. 5410033).

[259] Provvedimento del 23 gennaio 2020, n. 18, (doc. *web*. n. 9269629).

[260] Sul tema dell'accesso ai *dossier* da parte di personale sanitario non autorizzato, v. anche provvedimento del 21 aprile 2021, n. 155, (doc. *web* n. 9678507) ove si segnala l'accesso non autorizzato avvenuto per errore.

[261] *«Nell'ottica del perfezionamento dell'utilizzo di tale strumento, volto a garantire un trattamento dei dati lecito – in perfetta correlazione con il soddisfacimento del principio di accountability- deve necessariamente essere implementato un corretto sistema di formazione del personale coinvolto che accede e utilizza i dossier.»:* così S. MELCHIONNA, *Sanità digitale e innovazione*, cit., p. 108.

della struttura sanitaria. Ciò è errato. L'accesso ai *dossier* deve essere limitato, come più volte ribadito, dal punto di vista temporale alla fase di cura del paziente e dal punto di vista soggettivo in riferimento al personale effettivamente coinvolto[262].
Dall'analisi effettuata emerge, ancora una volta, la centralità della formazione del personale coinvolto, necessaria per dirimere i primissimi problemi legati alla corretta gestione del dato del paziente.

6. L'uso primario dei dati sanitari.

L'*European Health Data Space* disciplina l'uso primario e l'uso secondario dei dati sanitari. In particolare, l'uso primario, strettamente connesso alla regolamentazione delle modalità di accesso ai dati sanitari elettronici da parte di professionisti e alla definizione dei diritti delle persone fisiche, è disciplinato dal capo II. Il cardine della regolamentazione in oggetto è rappresentato dall'immediata disponibilità dei dati sanitari personali in formato elettronico, il cui accesso è garantito tramite servizi gratuiti, articolati su base nazionale, regionale o locale[263].
In particolare, le persone fisiche hanno la possibilità di accedere ai propri dati sanitari elettronici, rientranti nelle categorie prioritarie di cui all'art. 14[264], che sono trattati per l'erogazione di servizi di assistenza sanitaria. L'accesso è garantito a seguito della registrazione delle informazioni

[262] S. MELCHIONNA, *Sanità digitale e innovazione*, in Privacy e diritto dei dati sanitari, L. BOLOGNINI, S. ZIPPONI (a cura di), Milano, 2024, 104-105.
[263] Articolo 4, paragrafo 1, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.
[264] «Ai fini del presente capo, qualora i dati siano trattati in formato elettronico, le categorie prioritarie dei dati sanitari elettronici personali sono le seguenti: a) profili sanitari sintetici dei pazienti; b) prescrizioni elettroniche; c) dispensazioni elettroniche; d) esami diagnostici per immagini e relativi referti di immagini; e) risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti; e f) lettere di dimissione. Le caratteristiche principali delle categorie prioritarie di dati sanitari elettronici personali per uso primario sono indicate nell'allegato I. Gli Stati membri possono stabilire nel proprio del diritto nazionale l'accesso a categorie aggiuntive di dati sanitari elettronici personali per l'uso primario e il relativo scambio in conformità del presente capo.» Articolo 14, paragrafo 1, Regolamento

all'interno di un sistema di cartelle cliniche elettroniche in formato facilmente consultabile[265].

Il Regolamento prevede che, a prescindere dallo Stato di cura e di appartenenza, il personale sanitario avrà la possibilità di accedere ai dati dei pazienti in cura[266].

L'accesso da parte del personale sanitario sarà gratuito e avverrà mediante l'utilizzo di mezzi in grado di garantire l'identificazione elettronica del personale coinvolto[267] che dovrà occuparsi dell'aggiornamento delle informazioni cliniche relative al servizio prestato. L'integrazione avverrà anche in caso di dati registrati in uno Stato di cura differente da quello di affiliazione della paziente[268].

Tutte le attività di rettifica e inserimento dei dati prevedono l'individuazione del giorno, della data e del soggetto che ha effettuato l'aggiornamento o l'inserimento di nuove informazioni[269].

La centralità del ruolo e le nuove responsabilità riconosciute al personale sanitario fanno sorgere dei dubbi in merito alla puntuale attuazione delle previsioni sancite dal nuovo Regolamento: per garantire l'efficiente adempimento dei nuovi obblighi potrebbe nascere l'esigenza di indicare una figura dedicata, come un Responsabile della Protezione dei Dati con specifiche competenze legate al settore sanitario[270]. Entro il 26 marzo del

---

[265] Il Regolamento prevede che « Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, hanno il diritto di scaricare gratuitamente una copia elettronica almeno dei dati sanitari elettronici personali che rientrano nelle categorie prioritarie di cui all'articolo 14 relativi a tali persone fisiche, attraverso i servizi di accesso ai dati sanitari elettronici di cui all'articolo 4, nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15.»: articolo3, paragrafo 2, Regolamento.

[266] Articolo 11, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[267] Conformemente a quanto sancito dall'art. 6 del Regolamento UE n. 910 del 2014, art. 12 Regolamento.

[268] Articolo 13, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[269] Articolo 13, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[270] Cfr. con G. PEDRAZZI, *Il ruolo del Responsabile della protezione dei dati (dpo) nel settore sanitario, the role of data protection officer in the health sector*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 2019, 179.

2027 la Commissione stabilirà delle indicazioni relative alla qualità dei dati e alla completezza degli stessi[271].

Il Regolamento parla di categorie prioritarie di dati sanitari e stabilisce che in questo perimetro rientrano i profili sanitari sintetici dei pazienti, le prescrizioni elettroniche, dispensazioni elettroniche, esami diagnostici per immagini e relativi referti di immagini, risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti e lettere di dimissione[272].

La Commissione dovrà stabilire il formato di scambio delle cartelle cliniche elettroniche e gli Stati membri dovranno garantire che le categorie prioritarie di dati sanitari elettronici personali, di cui all'articolo 14, siano rilasciate compatibilmente alla scelta adottata dalla Commissione[273].

Al fine di garantire l'interoperabilità delle informazioni è previsto che in caso di richiesta elaborata dal paziente, il prestatore di assistenza sanitaria dovrà garantire la trasmissione delle informazioni appartenenti al singolo individuo.

Nel caso in cui l'interoperabilità coinvolga prestatori di assistenza sanitaria che si trovano in un altro Stato, la trasmissione dei dati dovrà avvenire nel formato europeo di scambio delle cartelle cliniche e mediante l'utilizzo dell'infrastruttura transfrontaliera prevista dal Regolamento stesso[274].

Gli Stati membri devono istituire servizi di delega che permettano ai pazienti di autorizzare l'accesso di altri soggetti ai propri dati clinici: tale concessione è fornita anche ai rappresentanti legali delle persone fisiche, in conformità al diritto nazionale[275].

Ogni individuo avrà una cartella clinica elettronica, che potrà essere integrata dal soggetto interessato e dai suoi rappresentanti, ma le

---

[271] Inoltre, il Regolamento prevede che i singoli Stati potranno stabilire delle categorie aggiuntive: Articolo 13, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[272] Articolo 14, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[273] Articolo 15, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[274] Articolo 7, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[275] Articolo 4, paragrafo 2, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

informazioni così inserite non saranno pienamente attendibili in quanto non registrate dal personale esperto, motivo per il quale all'interno della cartella clinica elettronica saranno distinguibili[276]. Dalla lettura della regolamentazione in oggetto, sorge un primo dubbio: il Regolamento conferisce all'individuo la possibilità di inserire informazioni cliniche, non pienamente attendibili in quanto non attribuibili all'inserimento effettuato da personale qualificato, senza stabilire un chiaro valore attribuibile. Tale interrogativo, di per sé rilevante, acquisisce una maggiore nota critica se contestualizzato in uno scenario di urgenza sanitaria, ove il personale medico avrà poco tempo a disposizione per effettuare una valutazione discrezionale e tempestiva, prima di poter procedere.

Inoltre, merita attenzione il fatto che è stata prevista la possibilità di limitare temporaneamente il diritto di accesso del paziente, o di un suo rappresentante, qualora ciò sia necessario per tutelare la persona fisica, al fine di preservare la sicurezza del paziente. La finalità è quella di garantire che l'utente venga a conoscenza di informazioni "sensibili" tramite un contatto diretto con il personale medico e non in autonomia con la presa visione della propria cartella clinica elettronica[277].

La scelta di consentire un ritardo nell'accesso ai propri dati sanitari potrebbe sollevare diversi problemi: centrale è l'autodeterminazione dell'individuo e la compromissione temporanea del controllo del paziente sui propri dati. In particolare, l'adozione di un sistema che consenta di ritardare l'accesso ad informazioni rilevanti, potrebbe generare la sfiducia del paziente, causata dalla possibile percezione di tale soluzione come una limitazione della libertà di gestione delle proprie informazioni cliniche.

Una previsione di tal tipo potrebbe dar vita ad un sistema che non sia in grado di rispettare le esigenze concrete del paziente: quest'ultimo potrebbe preferire l'assenza dell'intermediazione del medico nel venire a conoscenza

[276] Articolo 5, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[277] Articolo 3, paragrafo 1, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

di fatti clinici particolari. Una previsione troppo restrittiva potrebbe sfociare in un conflitto con la normativa sancita dal Regolamento (UE) 2016/679.
La scelta di differire alcune comunicazioni a momenti successivi, legati a un contatto diretto con il personale medico, potrebbe provocare un ingiustificato ritardo: anche se il Regolamento non indica in maniera chiara il confine da tracciare nella definizione dei casi, immaginando uno scenario concreto, potremmo simulare una situazione in cui l'applicazione della previsione fin qui analizzata, sia legata a casi relativi a una diagnosi di cancro o di malattia neurodegenerativa, ove la dilazione dei tempi di informazione potrebbe dar vita a ritardi rispetto alla scelta e all'attuazione di cure terapeutiche che richiedono tempestività.
Ma il Regolamento non stabilisce un corretto parametro in grado di definire un limitato spazio temporale all'interno del quale sia consentito posticipare l'informazione da trasmettere al paziente. Dunque, occorre domandarsi quali siano i limiti temporali da considerare accettabili, considerando che ogni paziente affronta una condizione clinica differente e maggiore attenzione andrebbe posta nel fornire informazioni a soggetti che riversano in particolari condizioni cliniche, si pensi ai disturbi psichiatrici, per i quali la limitazione temporale andrebbe applicata anche per informazioni cliniche meno preoccupanti. Pur comprendendo che situazioni diverse richiedono approcci e applicazioni normative differenti, ciò potrebbe tuttavia generare disparità di trattamento e lasciare alcune categorie meno tutelate rispetto ad altre, creando potenziali ingiustizie e carenze nel sistema di protezione dei diritti.
Uno dei principali problemi legati al nuovo Regolamento relativo allo Spazio europeo dei dati sanitari riguarda la scelta di adozione di "parametri" privi di contenuto che comportano conseguenze non accantonabili: sul punto, la normativa parla di «*informazioni che possono avere un impatto significativo sulla salute del paziente*»[278], senza definire ciò che si intende per impatto elevato. Il fatto che tale carenza non sia stata colmata mediante la previsione di elementi obiettivamente valutabili per determinare cosa

[278]Articolo 3, paragrafo 3, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

debba essere considerato come fortemente impattante sulla salute del paziente mette in dubbio l'uniformità della previsione all'interno di tutti gli Stati. Il fatto che venga rimandata la scelta ad ogni Stato potrebbe generare l'adozione di criteri di valutazione diversificati: in alcuni Paesi il paziente potrebbe avere accesso immediato ai propri dati, in altri invece potrebbe essere prevista la necessaria intermediazione del medico. Questo determinerà un probabile dirottamento della scelta di cura del paziente verso strutture site in Stati in cui vige un sistema sanitario maggiormente trasparente.

Le conseguenze legate alle differenti criticità della previsione analizzata potrebbero essere attenuate tramite la redazione di linee guida uniformi, a livello europeo, in grado di dirimere il più possibile le differenziazioni all'interno degli Stati membri. Altra importante soluzione, potrebbe riguardare la definizione di un limite massimo di differimento temporale, ad esempio 72 ore, per evitare ritardi ingiustificati nella comunicazione delle informazioni non inserite nella cartella clinica o creare dei sistemi di notifica tramite i quali si consiglia al paziente di contattare, nel minor tempo possibile, il medico o visualizzare l'informazione clinica di particolare rilievo nel proprio *database* sanitario.

Un'ultima osservazione. Una possibile soluzione potrebbe anche riguardare la subordinazione del differimento dell'inserimento di determinate informazioni a una scelta del paziente, mediante espresso consenso *ex ante*. In tal modo, l'utente potrà scegliere di venire autonomamente a conoscenza di eventuali informazioni particolarmente impattati sul proprio stato di salute, senza differire la comunicazione a un momento successivo caratterizzato da un incontro diretto con il personale medico, e viceversa.

7. Il diritto alla limitazione dell'accesso.

La regolamentazione dell'utilizzo primario dei dati sanitari lascia spazio ad una riflessione sul tipico schema di bilanciamento adottato dal legislatore europeo nei casi in cui è necessario individuare un equilibrio tra sacrificio e

tutela di diritti di eguale rilievo[279]. Parliamo del diritto alla riservatezza e del diritto alla salute del paziente. Occorre precisare che non esiste un modo univoco in grado di stabilire *ex ante* quale diritto prevale e quali sono le valutazioni da effettuare per stabilirlo: ogni situazione dovrà essere oggetto di attenta analisi.

L'uso primario dei dati sanitari dovrebbe promuovere la strumentalizzazione delle informazioni e il controllo proattivo ed effettivo da parte di ogni individuo sui propri dati sanitari, assicurando l'interoperabilità tra i sistemi sanitari nazionali. Obiettivo innovativo in quanto non previsto dal Regolamento UE 2016/679. O almeno questo è quello che *l'European Health Data Space* sembrerebbe voler garantire, considerando che vengono previste delle limitazioni volte a salvaguardare la riservatezza dei soggetti coinvolti. Sul punto, merita un'attenta analisi la previsione che riconosce alle persone fisiche il diritto di limitare, in maniera totale o parziale, l'accesso alle informazioni cliniche ai professionisti sanitari e ai prestatori di assistenza sanitaria[280].

Tale scelta potrebbe dar vita a diversi impatti negativi e in prima battuta appare opportuno focalizzarsi sull'importanza della continuità assistenziale: l'efficace gestione del quadro clinico di un individuo potrebbe essere compromessa in maniera significativa nel caso in cui un nuovo medico o specialista non riuscisse ad accedere a tutte le informazioni che riguardano la storia clinica del paziente. Immaginiamo il caso di un individuo affetto da malattia cronica, che sceglie di omettere alcuni dettagli rilevanti, conducendo il medico verso una soluzione non appropriata causata dall'assenza dell'esaustività delle informazioni cliniche visibili. Oltretutto, la mancata previsione di indicazioni effettive, relative a eventuali precedenti terapie, potrebbe dar vita a un concreto rischio di attuazione di scelte terapeutiche non adeguate.

[279] Per una breve riflessione sul tema v. G. ALPA*, Code is law: il bilanciamento dei valori e il ruolo del diritto*, in *Contratto e impresa*, 2021, 377 ss.
[280] Articolo 8, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

Inoltre, centralità va conferita alle situazioni di emergenza particolarmente rilevanti, caratterizzate da imponenti esigenze di celerità: supponiamo il caso di un grave trauma, un infarto o comunque una situazione clinica improvvisa e grave che richiede l'immediato intervento del personale addetto. Nel caso in cui i medici d'urgenza non riescano ad accedere tempestivamente a informazioni di fondamentale importanza come il gruppo sanguigno, allergie, precedenti infezioni, vaccini, risposte alle cure terapeutiche farmacologiche poste nel passato. o altre informazioni rilevanti, le scelte di cura potrebbero essere non adeguate e potrebbero dar vita a conseguenze irreversibili ma evitabili in caso di completa visione della cartella clinica.

Un ulteriore pericolo non trascurabile potrebbe riguardare il ritardo nell'individuazione della diagnosi e nella scelta delle cure da attuare. Una ricostruzione della storia clinica del paziente, tramite documenti cartacei e interviste, darà vita ad una inutile dilazione dei tempi necessari per giungere a una corretta diagnosi e, il ritardo della stessa, in alcuni casi, potrebbe favorire il peggioramento della patologia o essere addirittura fatale.

Altri due aspetti da non sottovalutare riguardo le spese sanitarie e l'efficacia dei programmi di prevenzione. Nel caso in cui vengano omesse delle informazioni relative a precedenti esami effettuati dal paziente, il personale medico potrebbe proporre la sottoposizione del medesimo ad accertamenti già effettuati nel breve periodo, dando vita alla possibile occlusione dei servizi erogati dalle strutture sanitarie a causa delle numerose richieste, alla ripetuta esposizione del paziente a radiazioni con annesse conseguenze per la salute e ulteriori criticità legate ai costi che le strutture sanitarie dovranno sostenere.

Il Regolamento prevede che le persone fisiche siano informate dei rischi legati alla scelta di limitare l'accesso ai propri dati e rimanda agli Stati membri l'effettiva regolamentazione e previsione di garanzia relative all'esercizio di tale limitazione[281].

[281] Articolo 8, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

Al fine di fronteggiare gli innumerevoli rischi legati ad un abuso della limitazione dell'accesso ai dati contenuti nelle cartelle cliniche, occorrerebbe dar vita a una corretta educazione dei soggetti interessati, al fine di radicare una concreta consapevolezza delle scelte adottate e creare dei sistemi automatizzati, all'interno dei quali venga stabilita una procedura da seguire per limitare l'accesso. Tale possibilità dovrebbe impostare una sorta di automatismo in grado di intervenire in tutti quei casi in cui il soggetto scelga di omettere la possibilità di rendere visibili alcune informazioni, ipoteticamente tramite l'utilizzo di una piattaforma in grado di interagire con il paziente, ad esempio anche tramite l'ausilio dell'AI, al fine di disincentivare un utilizzo inappropriato del diritto alla limitazione della consultazione.

Un'ulteriore soluzione potrebbe riguardare la previsione di una visualizzazione minima, garantita e obbligatoria, dei dati essenziali, al fine di rendere questi ultimi sempre disponibili, indipendentemente dalle scelte del soggetto coinvolto. Anche se tale possibilità potrebbe sfociare in una grave limitazione dell'autodeterminazione del paziente, correlata all'esercizio del diritto alla riservatezza: ma, in tale contesto, ha vita un bilanciamento che pone sotto i riflettori la riservatezza che si scontra con un avversario che merita maggiore attenzione, ovvero il diritto alla salute dell'interessato. Anche se quest'ultimo non si impone in maniera imprescindibile sugli altri diritti, capiamo bene che la giusta diligenza preme verso possibili soluzioni che limitano la scelta del riserbo.

Il Regolamento prevede che gli Stati europei stabiliranno le garanzie minime da dover attuare, scegliendo nuovamente di delegare la determinazione dell'effettività del contenuto normativo, con conseguente rischio di previsioni frammentate. In alcuni Stati potrebbero essere adottati strumenti o mezzi in grado di persuadere, in maniera maggiormente efficace, gli individui dal limitare l'accesso ai dati contenuti nelle cartelle cliniche, in altri meno. Elevando il rischio di compromissione della cooperazione fra gli Stati membri.

Inoltre, qualora uno Stato adotti modalità meno restrittive che favoriscano maggiormente la *privacy* dell'individuo, all'interno del più ampio contesto

del bilanciamento tra riservatezza e un'efficace presa in carico del paziente, e un altro Stato invece preveda soluzioni più restrittive, sarà necessario stabilire quale delle due impostazioni debba prevalere. Supponiamo che, in Italia, sia ammesso un regime maggiormente espansivo a favore del paziente, il quale può limitare l'accesso alle proprie informazioni cliniche, anche a costo di incidere potenzialmente sulla qualità dell'intervento medico. Al contrario, in Francia, il sistema potrebbe prevedere un approccio maggiormente restrittivo, basato su un accesso più ampio e meno condizionato alle informazioni sanitarie del paziente, favorevole all'efficacia clinica. In tale contesto, immaginiamo il caso concreto di un paziente italiano che venga sottoposto a cure mediche urgenti in Francia. Il fatto che abbia previamente esercitato il diritto alla limitazione del trattamento dei propri dati in Italia comporta che molte informazioni saranno oscurate. Tuttavia, tali informazioni, in base alla prassi francese, dovrebbero essere visibili al personale sanitario. Occorrerà dunque stabilire quale disciplina debba prevalere: se quella francese, con conseguente disconoscimento del diritto alla limitazione esercitato dal paziente italiano o se, in deroga alle regole interne francesi, si debba rispettare la volontà del paziente, garantendo l'accesso alle sole informazioni da lui rese disponibili.

La soluzione più adeguata sarebbe quella di prevedere criteri uniformi che stabiliscano quali dati devono essere limitati e in quali circostanze deve essere garantita la visibilità di alcune informazioni.

La giusta soluzione riguarda l'adozione di un modello uniforme, che non lasci ampi spazi discrezionali ai singoli Stati in merito alla determinazione di criteri diversificati che darebbero vita ad una maggiore o minore elasticità dell'esercizio del diritto alla limitazione dei dati, considerando che scelte differenti comprometterebbero l'efficace interoperabilità dei dati.

Sul punto, appare necessario uno sguardo critico alla scelta adottata dal legislatore europeo che avrebbe potuto dar vita ad una chiara e uniforme regolamentazione delle modalità di esercizio della limitazione dell'accesso ai dati sanitari.

8. Il diritto di esclusione riconosciuto alle persone fisiche e il problema del rilevamento dell'accesso ai dati.

Gli Stati membri possono riconoscere alle persone fisiche la possibilità di esclusione dall'accesso ai propri dati sanitari elettronici personali, con reversibilità di tale diritto.

La previsione di tale possibilità solleva numerosi interrogativi legati alle possibili ripercussioni sull'efficienza del sistema sanitario ma anche alla tutela dei diritti di pazienti e professionisti coinvolti nel processo di cura. La scelta di dar vita all'esclusione di dati potrebbe compromettere la qualità delle cure, in quanto genererebbe una discontinuità della collocazione delle informazioni cliniche, con differenti rischi legati alla possibilità che vengano scelte cure o trattamenti non adeguati.

Anche in questo caso, ulteriori rischi si presenterebbero in caso di emergenza, lì dove l'assenza di tempo non consentirebbe al personale medico coinvolto di raccogliere ulteriori informazioni in maniera alternativa.

Il Regolamento prevede che in caso di previsione del diritto di esclusione riguardo all'uso primario, gli Stati membri dovranno prevedere specifiche garanzie relative a tale meccanismo di esclusione.

In particolare, gli Stati possono stabilire che il personale sanitario può comunque accedere ai dati elettronici in questione, nel caso in cui il trattamento risulti essenziale per tutelare gli interessi vitali dell'interessato o di altra persona fisica[282]. Tale previsione, potrebbe dar vita a differenti interrogativi legati all'assenza di una chiara definizione di «interessi vitali». Appare necessario chiedersi se i casi di deroga siano circoscritti a situazioni emergenziali o se facciano ulteriormente riferimento a casi in cui vi è un

[282] «*Se uno Stato membro prevede il diritto di cui al paragrafo 1 del presente articolo, stabilisce le norme e le garanzie specifiche relative a tale meccanismo di esclusione. In particolare, gli Stati membri possono prevedere che un prestatore di assistenza sanitaria o un professionista sanitario possa accedere ai dati sanitari elettronici personali nei casi in cui il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica conformemente all'articolo 9, paragrafo 2, lettera c), del Regolamento (UE) 2016/679, anche se il paziente ha esercitato il diritto di esclusione riguardo all'uso primario.*»: Articolo 10 Regolamento, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

rischio medio-alto che si presentino conseguenze causate dalla trascuratezza di determinate informazioni.
Una possibile soluzione potrebbe dar vita alla creazione di criteri oggettivi che siano in grado di evitare scelte arbitrarie: il caso più importante riguarda le situazioni di pericolo caratterizzate da esigenze di celerità, come nel caso del paziente in fin di vita che si reca al pronto soccorso o nel caso in cui debbano essere somministrati farmaci che potrebbero scatenare reazioni allergiche. Tuttavia, occorre domandarsi in che modo viene stabilita *ex ante* l'effettiva possibilità che un farmaco possa o meno provocare reazioni allergiche.
Ancora si pensi ai casi in cui il soggetto non è in grado di esprimersi perché in stato di shock, confusione mentale o stato di incoscienza e infine, nei casi in cui la situazione clinica del paziente potrebbe dar vita a gravi conseguenze legate all'incolumità dei terzi: si pensi al caso di possibili malattie infettive.
Oltretutto, appare non univoca l'identificazione del soggetto o dei soggetti preposti alla valutazione della situazione clinica concreta del paziente. E dunque ci si chiede chi stabilirà quali sono i casi in cui potrà aver luogo una deroga che comprima il diritto di esclusione esercitato dal paziente.
L'attribuzione di una responsabilità di questo tipo al personale medico che si sta occupando del caso concreto conduce ad un ulteriore dubbio: la discrezionalità riconosciuta dovrebbe sfociare, o perlomeno tentare di sfociare, in soluzioni altamente obiettive, al fine di evitare che all'interno di una stessa struttura sanitaria o di uno stesso reparto, vengano adottate decisioni differenti basate sulla mancata obiettività del personale medico che si è occupato del caso concreto. Sarebbe preoccupante ritrovarsi in situazioni in cui ci sia una valutazione maggiormente stringente che comporti una compromissione dello stato di salute del paziente e altre, maggiormente permissive, che comprimano il diritto di esclusione esercitato dal paziente.
Al fine di evitare possibili abusi, potrebbero essere previsto un sistema di controlli *ex post*, attuato da un apposito comitato interno che dovrebbe occuparsi di una verifica periodica degli accessi, valutandone la legittimità e la conformità rispetto ai criteri stabiliti.

La decisione inerente alla scelta del soggetto che si occuperà della concessione di presa visione dei dati nonostante l'esercizio del diritto di esclusione è centrale, ma subordinata alla normativa adottata dai singoli Stati.

Una possibile soluzione potrebbe prevedere che in caso di emergenza, il medico predisposto all'attività di cura possa chiedere al paziente il consenso rispetto alla possibilità di superare la limitazione imposta. Ma, nel caso in cui il paziente non sia in grado di esprimersi potrebbe essere prospettata la seguente soluzione: il personale direttamente coinvolto potrebbe richiede l'autorizzazione di un apposito comitato o del direttore della struttura sanitaria.

Gli «interessi vitali» di cui all'art.9, paragrafo2, lettera c) del GDPR potrebbero essere tutelati attraverso l'intervento di soggetti differenti, in base alla natura e all'urgenza della situazione clinica. In caso di emergenza, il medico curante potrebbe essere chiamato ad intervenire tempestivamente e, per via della necessità di agire con immediatezza, non dovrebbe delegare tale scelta ad altri soggetti.

Nei casi in cui non vi è una situazione di urgenza imminente, la valutazione del caso potrebbe essere affidata al primario del reparto che potrà esprimersi e valutare se l'accesso sia giustificato o meno. Verifiche maggiormente rigorose potranno essere affidate al direttore sanitario della struttura, il quale dovrà garantire il rispetto delle normative e della proporzionalità dell'accesso ai dati.

Infine, in casi particolarmente complessi e delicati, ad esempio situazioni che coinvolgono malattie infettive a rischio per la collettività, potremmo immaginare che all'interno della struttura venga predisposto un comitato incaricato di esprimersi sull'ammissibilità dell'accesso ai dati oscurati, valutando gli aspetti etici, clinici e normativi connessi al caso di specie.

L'attribuzione di competenze differenziate in base al contesto[283], dovrebbe rendere il sistema di valutazione maggiormente garantito ed efficace. Una

[283] Con la previsione dell'intervento del medico curante in caso di emergenza, del direttore sanitario per un controllo sistematico e del comitato esperto in circostanze che richiedono una maggiore attenzione.

simile articolazione rappresenterebbe il giusto compromesso in grado di bilanciare gli interessi che entrano in tensione.

Forse la vera centralità andrebbe riconosciuta alla tracciabilità degli accessi attraverso appositi sistemi di controllo e alla previsione di controlli *ex post* mirati. Sembrerebbe utile la possibilità dell'utilizzo di un sistema automatizzato capace di stabilire, tramite l'ausilio di algoritmi, se il caso di specie richiede un superamento del diritto di esclusione esercitato dal paziente.

Un'ultima osservazione, al fine di evitare possibili abusi è necessario che gli Stati membri stabiliscano criteri chiari e condivisi che siano in grado di stabilire in maniera univoca cosa si intende per «interessi vitali».

Anche questa volta, la prima soluzione che viene proposta è quella che prevede la predisposizione di linee guida che contengano degli indici sintomatici che, di volta in volta, dovranno essere utilizzati per stabilire diversi livelli di gravità dello stato clinico del paziente, al fine di tentare di promuovere una valutazione obiettiva che prescinda dal personale che si esprimerà.

Un'ultima riflessione prevede un'analisi effettuata con un tono di rimprovero verso la scelta di delega adottata dal Regolamento: saranno gli Stati membri a stabilire norme e garanzie specifiche per il diritto di esclusione e ciò comporterà una forte disomogeneità nella gestione dei dati a livello europeo. Tale scelta darà vita all'adozione di sistemi disomogenei con annesse conseguenze.

Sembra indispensabile effettuare un'ulteriore riflessione sulla previsione del diritto di ottenere informazioni in merito all'accesso ai dati, anche tramite l'attivazione di notifiche che avranno il compito di garantire il monitoraggio degli accessi effettuati nei vari "archivi" contenenti dati sanitari elettronici[284]. Questa previsione dovrebbe aumentare il controllo, evitando, o almeno provando ad evitare, che si verifichino violazioni causate

[284] Articolo 9, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

da accessi non autorizzati[285]. La tracciabilità degli ingressi negli archivi digitali dovrà essere garantita tramite appositi sistemi in grado di rendere note le informazioni sul soggetto che ha avuto accesso ai dati elettronici, il tipo di dato oggetto della consultazione, la data e l'orario. Tuttavia, gli Stati membri potranno prevedere delle limitazioni: ad esempio nel caso in cui venga dimostrato che la divulgazione delle informazioni correlate al monitoraggio dell'accesso, potrebbe compromettere gli interessi vitali o i diritti del professionista sanitario, o influire negativamente sulle cure fornite alla persona fisica[286].

Anche in questo caso il Regolamento assume tratti assimilabili a quelli di una direttiva, rischiando che l'attuazione scelta dai singoli Stati dia vita a una disomogeneità normativa, con relative conseguenze. Potrebbero emergere differenziazioni significative che sfocerebbero in una disparità di trattamento dei diritti dei pazienti sul territorio europeo, con conseguenti difficoltà legate all'erogazione di cure transfrontaliere. Limitare il diritto dei pazienti di supervisione degli accessi ai propri dati potrebbe ridurre la loro fiducia nel sistema, in quanto tali eccezioni potrebbero essere percepite come un rischio di perdita di controllo effettivo sulle modalità di consultazione delle informazioni personali. Ciò potrebbe comportare anche una minore tutela della *privacy* dei soggetti coinvolti, i quali potrebbero vedersi negata, in modo quasi arbitrario, la possibilità di esercitare una supervisione delle consultazioni avvenute.

Un ulteriore critica va fatta sulla scelta del linguaggio adottato dal legislatore europeo che parla di «circostanze eccezionali» senza far riferimento ad una puntuale previsione. La scelta di far ricadere la possibilità di rettifica della limitazione della supervisione dell'accesso ai propri dati clinici in un perimetro tanto vasto potrebbe sfociare in un legittimo abuso dovuto all'incontrollata concessione di mancata

[285] Sul punto sembra pertinente un rinvio ai seguenti provvedimenti: Provvedimento del 21 aprile 2021, n. 155, (doc. *web* n. 9678507); Provvedimento del 22 febbraio 2024, n. 97, (doc. *web* n. 10001279).

[286] Articolo 9, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

visualizzazione degli accessi, giustificata da una pluralità di motivi generici e non catalogati.

Oltre a quanto appena detto, la mancata individuazione di un chiaro perimetro all'interno del quale definire quali sono le circostanze eccezionali che legittimano la mancata registrazione degli accessi, comporterebbe delle difficoltà, non secondarie, relative alla possibilità di contestazione da parte del paziente. Il Regolamento riconosce una sorta di discrezionalità abnorme.

Appare opportuno far riferimento al fatto che la previsione del monitoraggio degli accessi da parte del personale sanitario viene attuata al fine di limitare e punire gli abusi, che nel contesto sanitario sono stati numerosissimi. Sembra legittimo interrogarsi sul modo in cui un soggetto può tutelarsi da possibili abusi legati ad accessi impropri o non autorizzati se non potrà visualizzarne alcuni.

Tutto ciò potrebbe alimentare una generale sfiducia da parte dei pazienti, spingendoli a oscurare alcune informazioni presenti nella cartella clinica, nel timore che dati sensibili possano essere consultati senza la loro piena consapevolezza e controllo.

Possiamo sintetizzare il punto della situazione nel modo seguente: il Regolamento riconosce il diritto di oscurare determinate informazioni contenute nella cartella clinica. Tuttavia, tale possibilità può comportare gravi rischi, sia inerenti all'efficace interoperabilità dei dati sanitari, sia per la qualità delle cure, che potrebbero risultare compromesse qualora il paziente, nel tentativo di tutelare la sua *privacy*, ostacolasse l'accesso a informazioni rilevanti per il trattamento clinico.

A rafforzare tale criticità vi è la possibilità prevista dal Regolamento di consentire che "in circostanze eccezionali" il personale sanitario potrebbe accedere a tali informazioni senza che ciò lasci traccia nei registri di accesso, alimentando ulteriormente la sfiducia dei pazienti nel sistema.

Tali problematiche dovrebbero essere fronteggiate tramite una adeguata armonizzazione delle previsioni a livello europeo, che elimini il rischio di disomogeneità tra gli ordinamenti dei singoli Stati membri. Ciò sarebbe realizzabile tramite l'adozione di linee guida in grado di definire in modo

chiaro e preciso il perimetro applicativo delle «circostanze eccezionali» di cui all'art. 9, paragrafo 3, del Regolamento oggetto della nostra analisi.
Sarebbe inoltre indispensabile l'eventuale previsione di chiari sistemi di tutela per i pazienti, accompagnati da efficaci meccanismi sanzionatori. Questi ultimi dovrebbero essere in grado di stabilire conseguenze concrete in caso di accessi non tracciati, in circostanze in cui la visualizzazione dell'accesso da parte del paziente non avrebbe compromesso in alcun modo gli interessi vitali o i diritti del professionista sanitario o le cure assistenziali fornite al paziente interessato[287].

[287] Articolo 9, paragrafo 3, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

CAPITOLO IV

RICERCA SCIENTIFICA E USO SECONDARIO DEI DATI SANITARI

SOMMARIO: 1. L'uso secondario dei dati sanitari. – 2. Il ruolo degli Organismi responsabili dell'accesso ai dati sanitari. – 3. Il ruolo dei titolari del trattamento. – 4. Biobanche a scopo di ricerca medica e circolazione secondaria dei dati: *l'intuitus personae* e il trattamento dei dati personali.

1. L'uso secondario dei dati sanitari

Il Regolamento sulla creazione dello spazio europeo dei dati sanitari prova a istituire modalità di comune accesso ai dati sanitari elettronici per l'uso secondario all'interno di tutto il territorio europeo.

L'uso secondario dei dati sanitari dovrebbe generare notevoli benefici per la collettività. Per tale motivo è necessario che le informazioni fornite siano complete. Tuttavia, gli obiettivi perseguibili, richiedono l'applicazione di adeguate garanzie necessarie per fronteggiare possibili rischi legati al perseguimento dei benefici attesi[288]. Non a caso, l'uso secondario prevede l'utilizzo di dati anonimizzati[289].

«*L'uso secondario dei dati sanitari nello spazio europeo dei dati sanitari dovrebbe permettere ai soggetti pubblici, privati e senza scopo di lucro, così come ai singoli ricercatori, di avere accesso ai dati sanitari per la ricerca, l'innovazione, la definizione delle politiche, attività didattiche, la sicurezza dei pazienti, attività normative o la medicina personalizzata, in linea con le finalità stabilite nel presente Regolamento. L'accesso ai dati per l'uso secondario dovrebbe contribuire all'interesse generale della società. In particolare, l'uso secondario dei dati sanitari per finalità di*

[288] Considerando 53 Regolamento.
[289] Sul punto v. articolo 66 rubricato "Minimizzazione dei dati e limitazione della finalità".

ricerca e sviluppo dovrebbe contribuire a un beneficio per la società sotto forma di nuovi medicinali, dispositivi medici e prodotti e servizi sanitari a prezzi accessibili ed equi per tutti i cittadini dell'Unione, nonché rafforzarne l'accessibilità e la disponibilità in tutti gli Stati membri»[290].

In particolare, parlando di uso secondario occorre precisare che i titolari dei dati sanitari devono mettere a disposizione questa particolare categoria di informazioni provenienti da cartelle cliniche elettroniche, ma anche dati su fattori con un'incidenza sulla salute, dati relativi all'assistenza sanitaria, tra cui dati amministrativi e finanziari, dati sugli agenti patogeni che incidono sulla salute umana, dati genetici, epigenomici e genomici umani, altri dati molecolari umani, dati provenienti dalle applicazioni per il benessere, dati relativi ai professionisti sanitari coinvolti nel processo di cura di un paziente, dati provenienti da registri sanitari basati sulla popolazione, dati provenienti da differenti registri medici, dati provenienti da sperimentazioni cliniche[291], dati sanitari provenienti da dispositivi medici, dati provenienti da coorti di ricerca, questionari e indagini in materia di salute e dati provenienti da biobanche e banche dati associate[292]. Inoltre, il Regolamento riconosce agli Stati europei la possibilità di applicare misure maggiormente severe per rafforzare la tutela di dati genetici, epigenomici e genomici umani, altri dati molecolari umani, dati provenienti dalle applicazioni per il benessere e dati sanitari provenienti da biobanche banche dati associate[293]. Questa previsione spinge verso una prima riflessione: la scelta di conferire ai singoli Stati la possibilità di determinare la previsione di ulteriori misure e garanzie per tutelare determinate categorie di dati sanitari da trattare, porterà ad un panorama non uniforme. Sul punto

[290] Considerando 61 Regolamento

[291] In particolare, l'art. 51 del Regolamento stabilisce che rientrano «*dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni soggetti al Regolamento (UE) n. 536/2014, al Regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio (35), al Regolamento (UE) 2017/745 e al Regolamento (UE) 2017/746*».

[292] Articolo 51, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[293] «*Gli Stati membri notificano tali misure e garanzie alla Commissione e provvedono senza ritardo a darle notifica di ogni ulteriore modifica*.»: Articolo 51, paragrafo 4, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

occorre precisare che, seppur a differenza di altri casi, in tale occasione il Legislatore europeo ha scelto di predeterminare un margine di riferimento, stabilendo misure applicate "erga omnes" e prevedendo un ulteriore rafforzamento discrezionale. Tale scelta quasi certamente darà vita a possibili squilibri. In particolare, appare chiara la previsione di uno scenario in cui ci saranno Stati che applicheranno misure aggiuntive, meno favorevoli alla facile reperibilità e utilizzo dei dati per finalità di ricerca e altri in cui verranno applicate le sole misure già sancite a livello sovranazionale. Senza ombra di dubbio, verranno preferiti i dati provenienti da Nazioni che non hanno adottato misure aggiuntive.

Un'ulteriore facoltà riconosciuta agli Stati membri fa riferimento ad un margine di discrezionalità che consentirà agli stessi di stabilire categorie aggiuntive di dati elettronici[294].

Tale previsione dovrebbe essere analizzata sotto un duplice punto di vista: uno positivo e uno negativo. La scelta di consentire ai singoli Stati la possibilità di integrare l'elenco di dati sanitari ammessi per l'utilizzo secondario potrebbe dar vita ad una notevole espansione che con il tempo potrebbe fungere da esempio per gli altri Stati membri, favorendo l'implementazione di tecniche non ancora previste e la progressione dell'attività di ricerca. Inoltre, tale previsione sembrerebbe essere compatibile con le esigenze locali delle singole Nazioni, ove una sorta di personalizzazione evita di impedire che l'attività di ricerca venga limitata a quella categoria di dati predeterminati dal Regolamento, escludendo possibili risorse potenzialmente utili e reperibili all'interno di uno Stato.

Ma, uno scenario di questo tipo potrebbe dar vita ad una vasta frammentazione, con elevato rischio di compromissione della compatibilità di scambio dei dati in ogni Stato membro ed eventuale intensificazione delle attività burocratiche causato da ulteriori formalizzazioni ordinariamente non previste. Tutto questo potrebbe rallentare il processo di condivisione dei dati.

[294] Articolo 51, paragrafo 2, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

Andrebbero analizzati ulteriori rischi legati alla *privacy* e a un eventuale uso improprio dei dati non catalogati nell'art. 51 ed eventualmente aggiunti dai singoli Stati europei. In particolare, uno scenario frammentato potrebbe trasformarsi in un perimetro all'interno del quale lo squilibrio si riflette sulla tutela dei soggetti coinvolti: alcuni cittadini europei potrebbero trovarsi in una situazione di svantaggio causata da una maggiore esposizione a rischi di trattamento improprio, riferito a quelle categorie di dati che non vengono usati per finalità secondarie all'interno del resto del panorama europeo. Tale sproporzione potrebbe entrare in collisione con i principi sanciti dal Regolamento (UE) 2016/679, in particolare con il principio di minimizzazione dei dati[295]: dovrebbe essere sempre accertata la pertinenza dell'utilizzo degli ulteriori dati per le finalità di ricerca predeterminate.

Oltretutto, la catalogazione di informazioni aggiuntive riferite agli individui, potrebbe dar vita a una maggiore possibilità di reidentificazione del soggetto coinvolto, causato dalla raccolta di più elementi che nell'insieme potrebbero ricondurre alla riconoscibilità diretta del soggetto coinvolto.

Il Regolamento prevede un'altra importante possibilità di intervento: ogni Stato avrà la possibilità di stabilire norme per il trattamento e l'uso dei dati sanitari elettronici dando vita a rettifiche migliorative relative al loro trattamento, nonché eventuali annotazioni o arricchimenti, il tutto tramite un'apposita autorizzazione fornita dall'Organismo responsabile dell'accesso ai dati sanitari e in particolare dall'art. 68 del Regolamento stesso[296].

Centrale è la figura dell'Organismo responsabile dell'accesso ai dati sanitari che concede l'accesso ai dati elettronici a un utente nel momento in cui sussiste compatibilità fra il trattamento e le finalità elencate nella normativa sovranazionale oggetto della nostra analisi. In particolare, tra le differenti ipotesi catalogate dall'art. 53 rientrano l'interesse pubblico legato ad esigenze di sanità pubblica o della medicina del lavoro, attività d'istruzione

[295] Articolo 5, paragrafo 1, Regolamento (UE) 2016/679.
[296] Articolo 51, paragrafo 3, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

e formazione nel settore sanitario, attività di ricerca scientifica e miglioramento della prestazione di assistenza sanitaria[297].

La volontà del legislatore europeo di definire con precisione i limiti dell'uso lecito dei dati all'interno del più ampio ambito dell'utilizzo secondario emerge chiaramente dalla scelta di dedicare un articolo al tema. Precisamente, l'articolo 54 rubricato "Uso secondario vietato" elenca i casi in cui il trattamento non è considerato legittimo.

In particolare, il divieto si applica anche in presenza di autorizzazione rilasciata a norma dell'articolo 68 o sulla base di una richiesta dati approvata a norma dell'articolo 69.

Il legislatore pone particolare attenzione ai casi in cui i dati sanitari vengano trattati per l'adozione di decisioni pregiudizievoli a discapito di un singolo individuo o di un gruppo di persone, determinate da informazioni ottenute dall'analisi di tali dati. Si tratta, nello specifico, di decisioni capaci di produrre effetti giuridici, sociali o economici pregiudizievoli o incidere in modo analogo sui soggetti coinvolti. Tuttavia, la disposizione in questione, a meno che non funga da deterrente, non sembra in grado di poter

---

[297] «*Gli Organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell'utente è necessario per una delle finalità seguenti: a) pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici; b) definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e Organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati; c) statistiche quali definite all'articolo 3, punto 1), del Regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza; d) attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; e) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; f) miglioramento della prestazione di assistenza, ottimizzione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche.*»: Articolo 53, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

realmente disincentivare le condotte vietate ma prova semplicemente a mettere in atto una precisazione che opererà *ex post*, come rettifica a quanto già analizzato. Numerosi sono gli interrogativi che traggono origine dalla lettura della lettera a) dell'articolo 54: il fatto che il trattamento sia stato anticipatamente considerato lecito sulla base di una valutazione che ha consentito il rilascio dell'autorizzazione a norma dell'articolo 68 o l'approvazione della richiesta a norma dell'articolo 69, spinge a chiedersi in che modo verrà valutata la gravità delle finalità previste, in un momento differito e dunque probabilmente a seguito della commissione di azioni legate a finalità riprovevoli già messe in atto. Inoltre, sembra legittimo domandarsi cosa intenda dire il legislatore quando parla di effetti giuridici, sociali o economici e se esista una scala di valori di riferimento in grado di stabilire un limite alla rilevanza delle possibili conseguenze che potrebbero scaturire da un trattamento che persegue finalità pregiudizievoli, che sia in grado di definire ulteriori categorie di casi analoghi.

Nella scelta di definire il perimetro di liceità del trattamento, il Regolamento prosegue stabilendo che il trattamento è vietato nel caso in cui miri all'adozione di decisioni inerenti ad offerte di lavoro, determinazione di condizioni meno favorevoli nella fornitura di beni e servizi riguardanti un individuo o un gruppo o altre decisioni sfavorevoli che determinino una scelta discriminatoria basata sui dati sanitari ottenuti[298].

Da tale assunto trapela la forte rilevanza dell'incidenza della diffusione delle informazioni relative alla salute di un individuo: in particolare, occorre porre sotto i riflettori le conseguenze concrete che potrebbero derivare dall'uso improprio dei dati sanitari, legate alla possibilità che una persona affetta da una determinata patologia, o con un determinato passato clinico,

[298]Nello specifico il Regolamento stabilisce che il trattamento dei dati è vietato per i seguenti usi: «*adottare decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, per quanto riguarda offerte di lavoro, offrire condizioni meno favorevoli nella fornitura di beni o servizi, compresa l'esclusione di tali persone o gruppi dal beneficio di un contratto di assicurazione o di credito, la modifica dei loro contributi e premi assicurativi o le condizioni dei prestiti, o adottare altre decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, che risultino in una discriminazione nei loro confronti sulla base dei dati sanitari ottenuti.*»: Articolo 54, lettera b), Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

venga discriminata o penalizzata nel mondo del lavoro. Il rischio che informazioni sensibili vengano manovrate per influenzare decisioni a discapito dei singoli, come quelle occupazionali, rientra tra le forme più gravi di utilizzo pregiudizievole dei dati. Per evitare scenari di questo tipo, il legislatore europeo ha previsto espliciti divieti nell'ambito dell'uso secondario dei dati, all'interno del quale rientrano attività di natura pubblicitaria, attività finalizzate alla creazione di servizi o prodotti che siano in grado di danneggiare persone, sanità pubblica o società in generale o servizi e prodotti che siano in grado di danneggiare l'ordine pubblico o la moralità o causare un rischio per la salute umana. Infine, il Regolamento prevede che sono vietate le attività che entrano in contrasto con le disposizioni etiche sulla base di quanto sancito dal diritto nazionale.

Il riferimento a disposizioni etiche lascia un enorme interrogativo in merito alla chiara definizione di tale concetto che si diversifica all'interno di ogni Stato europeo. In particolare, la definizione di "etico" non solo si differenzia all'interno del singolo contesto nazionale ma per sua natura, è caratterizzato da confini difficilmente delineabili. Questo può dare origine a casi concreti in cui entrano in gioco interessi contrastanti da bilanciare: si pensi, ad esempio, al caso di terapie sperimentali, le quali potrebbero favorire un effettivo progresso medico, ma, allo stesso tempo, sollevare questioni di natura etica.

L'obiettivo del presente articolo è quello di definire in maniera chiara un perimetro entro cui limitare il trattamento connesso all'uso secondario dei dati, il quale dovrebbe avere come primaria finalità la promozione della ricerca scientifica, evitando ripercussioni sfavorevoli dovute all'elusione delle autorizzazioni concesse o all'impiego dei dati per il perseguimento di fini impropri.

Un'ultima osservazione sul tema. Determinare i casi in cui effettivamente l'utilizzo dei dati potrebbe fuoriuscire dalla area del lecito rappresenta una sfida difficile che pone l'esigenza di determinare l'individuazione di una figura, probabilmente compatibile con l'Organismo responsabile dell'accesso ai dati, alla quale spetterà la valutazione dei singoli casi, al fine di garantire ai soggetti coinvolti un'adeguata tutela. Quest'ultima potrebbe

essere garantita tramite l'elaborazione di un sistema di *audit* periodico, indispensabile per monitorare e garantire che l'utilizzo secondario non rientri nello schema del divieto definito dall'articolo 54 del Regolamento sullo spazio europeo dei dati sanitari.

2. Il ruolo degli Organismi responsabili dell'acceso ai dati sanitari.

Gli Organismi responsabili dell'accesso ai dati sanitari verranno istituiti e designati all'interno di ciascun Stato membro[299]. Ciascuno Stato informerà il pubblico dell'importanza del ruolo degli Organismi responsabili dell'accesso ai dati sanitari, i quali con cadenza bimestrale dovranno redigere una relazione sull'attività svolta che verrà resa pubblica tramite appositi siti web e presentata alla Commissione e al comitato EHDS negli ultimi sei mesi antecedenti alla chiusura del secondo anno di riferimento[300].

---

[299] In particolare, il Regolamento stabilisce che i compiti potranno essere ripartiti fra più Organismi all'interno dello stesso Stato membro, in tal caso solamente un organismo fungerà da coordinatore; Articolo 55, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[300] «*Tale relazione di attività segue una struttura concordata dal comitato EHDS a norma dell'articolo 94, paragrafo 2, lettera d), e contiene almeno le categorie di informazione seguenti: a) informazioni relative alle domande di accesso ai dati sanitari e alle richieste di dati sanitari presentate, quali i tipi di richiedenti di dati sanitari, il numero di autorizzazioni ai dati rilasciate o respinte, le categorie delle finalità dell'accesso e le categorie di dati sanitari elettronici a cui si è avuto accesso, nonché se del caso una sintesi dei risultati degli impieghi dei dati sanitari elettronici; b) informazioni sull'adempimento degli impegni normativi e contrattuali da parte degli utenti dei dati sanitari e dei titolari dei dati sanitari, nonché sul numero e sull'importo delle sanzioni amministrative pecuniarie imposte dagli Organismi responsabili dell'accesso ai dati sanitari; c) informazioni sugli audit effettuati sugli utenti dei dati sanitari per garantire la conformità del trattamento che questi effettuano in un ambiente di trattamento sicuro in conformità dell'articolo 73, paragrafo 1, lettera e); d) informazioni sugli audit interni e di terzi sulla conformità degli ambienti di trattamento sicuri alle norme, alle specifiche e alle prescrizioni stabilite, di cui all'articolo 73, paragrafo 3; e) informazioni sul trattamento delle richieste presentate da persone fisiche riguardo all'esercizio dei loro diritti alla protezione dei dati; f) una descrizione delle attività svolte dall'organismo responsabile dell'accesso ai dati sanitari in relazione al coinvolgimento e alla consultazione dei portatori di interessi pertinenti; g) le entrate derivanti da autorizzazioni ai dati e richieste di dati sanitari; h) il numero medio di giorni tra la domanda di accesso ai dati sanitari o la richiesta di dati sanitari e l'accesso ai dati; i) il numero di marchi di qualità dei dati rilasciati dai titolari dei dati sanitari, suddiviso per categoria di qualità; j) il numero di pubblicazioni di ricerca sottoposte a valutazione inter pares, documenti strategici e procedure di regolamentazione che utilizzano dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari; k) il numero di prodotti e servizi di sanità digitale, comprese le applicazioni di IA, sviluppati utilizzando dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari*» Articolo 59, paragrafo 1, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

Inoltre, gli Organismi responsabili dell'accesso si occuperanno della diffusione delle informazioni che stabiliscono le condizioni a cui i dati sanitari verranno messi a disposizione per l'uso secondario: la base giuridica che legittima l'accesso dell'utente, le misure adottate per garantire la tutela dei diritti delle persone fisiche, i diritti delle persone fisiche correlati all'uso secondario, i dati di contatto dell'organismo stesso, informazioni inerenti al soggetto che ha ottenuto l'accesso, nonché i risultati e gli esiti delle attività effettuate[301].

Le previsioni appena analizzate indicano la centralità di esigenze di trasparenza, correlata alla chiara volontà di garantire la partecipazione degli individui coinvolti.

La centralità di tale figura emerge dall'attenzione posta dal legislatore europeo rispetto all'elencazione delle attività attribuitegli: in prima battuta occorre focalizzarsi sul fatto che tali Organismi si occuperanno della decisione relativa alle domande di accesso pervenute da parte di persone fisiche o giuridiche[302], del rilascio delle autorizzazioni[303] e delle decisioni relative alle richieste elaborate [304]. Inoltre, cooperano tra di loro, a livello europeo e nazionale, al fine di armonizzare una normativa comune e definire le misure adeguate a garantire un ambiente di trattamento sicuro, fornendo una costante consulenza alla Commissione nell'individuazione delle migliori tecniche da adottare per l'uso secondario dei dati. Garantiranno la semplificazione delle modalità di accesso ai dati sanitari tramite la piattaforma HealthData@EU e saranno responsabili dei restanti obblighi, tra cui quelli di pubblicazione, per garantire la corretta applicazione del Regolamento nel contesto dell'uso secondario[305].

Tali Organismi svolgeranno un ruolo centrale nella valutazione dei criteri necessari per determinare il consenso o il diniego dell'accesso ai dati. In particolare, appare rilevante soffermarsi sulla valutazione della

[301]L'elenco completo è indicato dall'articolo 58, paragrafo 1, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.
[302] In particolare, l'articolo 67 disciplina le domande di accesso ai dati sanitari.
[303] Articolo 68, Regolamento (UE) 2025/327.
[304] Articolo 69, Regolamento (UE) 2025/327.
[305] Articolo 57, Regolamento (UE) 2025/327.

compatibilità tra le finalità che si intendono perseguire e i dati richiesti ove sarà determinante l'effettiva pertinenza degli stessi che dovranno essere necessari, proporzionati e adeguati con specifico riferimento al principio della minimizzazione del dato.

L'accertamento che precede il rilascio dell'autorizzazione prevede anche una valutazione dei rischi legati alla difesa nazionale, alla sicurezza e all'ordine pubblico e il rischio di compromissione della riservatezza dei contenuti delle banche dati governative.

La valutazione dei rischi, preliminare al rilascio del nulla osta che consente l'uso secondario dei dati sanitari, costituisce un dato centrale. Tale scelta sembrerebbe voler fronteggiare scenari critici, come l'utilizzo improprio di studi epidemiologici su larga scala. Inoltre, è necessario considerare il rischio di squilibri derivanti dalla diffusione non appropriata di dati sanitari, nonché alla circolazione di informazioni non attendibili, che potrebbero generare allarme sociale e compromettere l'ordine pubblico[306].

All'esito delle valutazioni effettuate, gli Organismi responsabili dell'accesso ai dati sanitari provvederanno al rilascio dell'autorizzazione[307]: concedendo o negando l'accesso ai dati sanitari, entro tre mesi dal ricevimento della domanda[308]. Il rilascio dell'autorizzazione comporterà la messa a

---

[306] Da queste brevi precisazioni si apre una grande riflessione che porterà nel prossimo capitolo all'analisi della *cybersicurezza* in quanto la protezione dei dati personali attualmente non interferisce solamente con l'esigenza di assicurare la *privacy* individuale ma ha un impatto diretto sulla sicurezza nazionale, la stabilità sociale e altri aspetti parimenti rilevanti.

[307] «*Qualora non siano soddisfatte le prescrizioni per il rilascio di un'autorizzazione ai dati, ma siano soddisfatte le prescrizioni perché sia fornita una risposta in forma statistica anonimizzata a norma dell'articolo 69, l'organismo responsabile dell'accesso ai dati sanitari può decidere di fornire tale risposta a condizione che ciò attenui i rischi e, se la finalità della domanda di accesso ai dati sanitari può essere in tal modo soddisfatta, a condizione che il richiedente di dati sanitari accetti di ricevere una risposta in forma statistica anonimizzata ai sensi dell'articolo 69*»: Articolo 68, paragrafo 3, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[308] Occorre far riferimento al fatto che il nuovo Regolamento prevede la possibilità di concessione di un termine quattro settimane entro cui il richiedente potrà integrare una domanda di accesso ai dati sanitari e, nel caso in cui una richiesta necessiti di particolare attenzione può essere prevista una proroga di tre mesi per una risposta ad una domanda di accesso ai dati sanitari; Articolo 68, paragrafo 4, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

disposizione dei dati a favore degli utenti, entro due mesi dal ricevimento degli stessi da parte dei rispettivi titolari[309].

Il rilascio dell'autorizzazione deve prevedere in maniera puntuale «*a) le categorie, la specifica e il formato dei dati sanitari elettronici a cui accedere contemplati dall'autorizzazione ai dati, comprese le relative fonti e, l'eventuale indicazione che l'accesso ai dati sanitari elettronici dovrà essere effettuato in forma pseudonimizzata nell'ambiente di trattamento sicuro; b) una descrizione dettagliata della finalità della messa a disposizione dei dati sanitari elettronici; c) qualora sia previsto un meccanismo di attuazione di un'eccezione e questo sia applicabile a norma dell'articolo 71, paragrafo 4, informazioni che indichino se è stata applicato e il motivo della relativa decisione; d) l'identità delle persone autorizzate, in particolare l'identità del ricercatore principale, con il diritto di accedere ai dati sanitari elettronici nell'ambiente di trattamento sicuro; e) durata dell'autorizzazione ai dati; f) informazioni sulle caratteristiche tecniche e sugli strumenti a disposizione dell'utente dei dati sanitari nell'ambiente di trattamento sicuro; g) tariffe a carico dell'utente dei dati sanitari; h) eventuali condizioni specifiche»*[310]. L'eventuale diniego presentato al richiedente deve essere motivato[311].

Il Regolamento, al fine di evitare un utilizzo non appropriato causato dall'assenza di vincoli temporali di concessione, stabilisce che la durata dell'autorizzazione deve essere commisurata al tempo necessario per il perseguimento della finalità richiesta, ma comunque non oltre i 10 anni. Con riconoscimento all'utente della possibilità di prorogare la durata accordata, sempre nel limite massimo di dieci anni, mediante la dimostrazione documentale di specifiche esigenze[312].

---

[309] Articolo 68, paragrafo 7, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[310] Articolo 68, paragrafo 10, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[311] Articolo 68, paragrafo 9, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[312] Il Regolamento stabilisce che i dati conservati nell'ambente sicuro per il trattamento siano cancellati nei sei mesi successivi alla scadenza dell'autorizzazione ma che su richiesta dell'utente, l'organismo responsabile potrà conservare la formula per la creazione della serie di dati richiesti; Articolo 68, paragrafo 12, Regolamento (UE) 2025/327 del

La previsione di una limitazione temporale è stata inserita al fine di imporre una sorta di restrizione all'innovazione, a vantaggio dei diritti dei cittadini. Tuttavia, tale previsione potrebbe dar vita a numerosi problemi e criticità: in particolare, numerosi progetti di ricerca richiedono una suddivisione del lavoro nel lungo periodo e la previsione del limite massimo di dieci anni potrebbe comportare una fatale interruzione con conseguente compromissione dell'attività svolta e dell'obiettivo che si intende perseguire. La previsione di possibili proroghe o rinnovi potrebbe comunque mettere a repentaglio il perseguimento di risultati ottimali di ricerca, con il possibile rischio di interruzione dei lavori e perdita di dati preziosi. Ciò potrebbe anche scoraggiare progetti di lungo termine che richiedono una quantità di dati storici, pensiamo a studi epidemiologici. Tuttavia, tale rischio potrebbe essere mitigato tramite la previsione di un'apposita autorizzazione, con durata più estesa, al fine di evitare una compromissione del raggiungimento del risultato atteso.

Oltretutto, il fatto che venga subordinata la possibilità di proroga «*sulla base di argomentazioni e documenti che giustifichino tale estensione*» non fornisce una precisa definizione di casi che legittimano l'estensione. Questo, come già analizzato in numerose altre previsioni del Regolamento, potrebbe comportare la creazione di divergenze all'interno degli Stati membri. Tali disallineamenti, potrebbero dar vita a squilibri in termini di ottimizzazione ed efficace raggiungimento degli obiettivi di ricerca a discapito di alcuni Stati, in riferimento a possibili valutazioni troppo discrezionali, non basate su elementi obiettivi predeterminati dal legislatore europeo.

Un primo grande passo sarebbe quello di inserire delle linee guida che definiscano criteri obiettivi in grado di valutare le esigenze specifiche che legittimano la concessione di una dilazione del termine di accesso originariamente accordato.

Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

3. Il ruolo dei titolari del trattamento

Una persona fisica o giuridica può presentare all'Organismo responsabile dell'accesso ai dati sanitari una domanda di accesso[313]. L'Organismo responsabile valuterà la conformità della domanda al fine di concedere l'accesso, tramite il rilascio di un'autorizzazione ai dati[314]. Per il perseguimento delle finalità di cui all'articolo 53[315], può essere presentata apposita richiesta che prevede una risposta in forma anonimizzata[316].

La richiesta di ottenimento dei dati per le finalità sancite dal Regolamento stesso, e precisamente dall'articolo 53, deve includere specifiche informazioni. In particolare, l'identità del richiedente, con annesso preciso riferimento alle attività e funzioni svolte dal punto di vista professionale, una descrizione che definisca l'utilizzo che si prevede fare, una descrizione

[313] Articolo 67, Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari.

[314] In particolare, gli artt. 67 e 68 del Regolamento disciplinano rispettivamente la domanda di accesso ai dati e l'autorizzazione ai dati.

[315] «*1. Gli Organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell'utente è necessario per una delle finalità seguenti: a) pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici; b) definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e Organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati; c) statistiche quali definite all'articolo 3, punto 1), del Regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza; d) attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; e) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; f) miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche*»: Articolo 53, paragrafo 1, Regolamento (UE) 2025/327.

[316] Articolo 69, paragrafo 1, Regolamento (UE) 2025/327.

dei dati sanitari elettronici richiesti e una definizione delle garanzie previste per impedire l'uso improprio delle informazioni[317].

La valutazione operata dall'Organismo responsabile dell'accesso ai dati sanitari dovrà avvenire entro tre mesi dal ricevimento della richiesta[318]. Il titolare dei dati sanitari comunica all'organismo responsabile dell'accesso la descrizione della serie di dati che detiene, conformemente all'articolo 77[319].

Tale breve premessa serve per introdurre una chiara particolarità: la ricezione di una domanda di accesso ai dati sanitari o una richiesta di dati sanitari elettronici conservati da un titolare di dati sanitari affidabile, prevede l'applicazione di un *iter* che differisce da quello ordinario.

In particolare, viene concessa la possibilità agli Stati membri di istituire una procedura che conferisce una sorta di qualifica legata all'affidabilità del soggetto coinvolto, basata su specifici requisiti che verranno valutati all'interno di ogni Stato, dall'Organismo responsabile dell'accesso ai dati[320].

Dunque, le domande di accesso e le richieste che riguardano dati di titolari affidabili, potranno essere trasmesse dall'Organismo responsabile dell'accesso ai dati al titolare di riferimento. Quest'ultimo valuterà la domanda tenendo conto delle finalità indicate, della proporzione fra i dati richiesti e le finalità perseguite e della conformità del trattamento con l'articolo 6, paragrafo 1, del Regolamento (UE) 2016/679[321]. La valutazione effettuata[322], con annessa proposta di decisione non vincolante, verrà indirizzata all'Organismo responsabile dell'accesso ai dati sanitari

---

[317] Inoltre l'articolo 69 prosegue sancendo che il richiedente dovrà fornire « *f) una descrizione delle modalità con cui il trattamento dei dati sanitari elettronici richiesti si conformerebbe all'articolo 6, paragrafo 1, del Regolamento (UE) 2016/679 o all'articolo 5, paragrafo 1, e all'articolo 10, paragrafo 2, del Regolamento (UE) 2018/1725; g) se il richiedente di dati sanitari intende avvalersi di un'eccezione a norma dell'articolo 71, paragrafo 4, la giustificazione richiesta a tale riguardo dal diritto nazionale ai sensi di tale articolo*».

[318] Articolo 69, Regolamento (UE) 2025/327.

[319] Articolo 60, Regolamento (UE) 2025/327.

[320] Il Regolamento prevede che sia necessario che «*i titolari di dati sanitari soddisfino le condizioni seguenti: a) sono in grado di fornire l'accesso ai dati sanitari tramite un ambiente di trattamento sicuro conforme all'articolo 73; b) dispongono delle competenze necessarie per valutare le domande di accesso ai dati sanitari e le richieste di dati sanitari; c) forniscono le garanzie necessarie per garantire il rispetto del presente Regolamento.*»: Articolo 72, Regolamento (UE) 2025/327.

[321] In particolare, la conformità dovrà tener conto delle previsioni sancite dall'articolo 68, paragrafo 1 e 2 del Regolamento (UE) 2025/327.

[322] Articolo 72, paragrafo 4, Regolamento (UE) 2025/327.

coinvolto. Entro due mesi quest'ultimo adotterà una decisione che potrà essere difforme rispetto alla proposta emessa dal titolare affidabile[323].

Anche in questo caso la decisione ultima spetterà all'Organismo responsabile dell'accesso ai dati sanitari che se opterà per il rilascio dell'autorizzazione o per l'approvazione della richiesta, attribuirà lo svolgimento degli ulteriori adempimenti al titolare di dati sanitari affidabile. In particolare, quest'ultimo fornirà l'accesso ai dati sanitari elettronici agli utenti in un ambiente di trattamento sicuro[324].

In sintesi, attraverso il conferimento agli Stati membri della possibilità di designare titolari affidabili viene prevista una modalità di autorizzazione semplificata, attuando un tentativo di alleggerimento del carico di responsabilità che il Regolamento affida agli Organismi responsabili dei dati sanitari[325].

La particolarità della previsione normativa che conferisce questo ruolo centrale ai titolari affidabili, sta nel fatto che vi è un semplice rinvio alla scelta degli Stati membri in merito alla possibilità di nomina di queste figure, senza un'attenta previsione dei requisiti necessari per definire, perlomeno in maniera sufficiente, le caratteristiche minime che un titolare dei dati dovrebbe avere per essere considerato affidabile.

Ancora una volta, appare opportuno rilevare come la previsione carente e lacunosa contenuta nel Regolamento attribuisca un ruolo centrale alle scelte che dovranno affrontare gli Stati, con il rischio che vengano adottate

---

[323] Articolo 72, paragrafo 5, Regolamento (UE) 2025/327.

[324] Il tutto avverrà conformemente a quanto previsto dall'articolo 57, lettera a), punto i) e lettera b), Regolamento (UE) 2025/327.

[325] «Gli *Stati membri dovrebbero essere autorizzati a designare titolari dei dati sanitari affidabili per i quali la procedura di rilascio dell'autorizzazione dei dati può essere eseguita in modo semplificato, al fine di alleviare l'onere amministrativo a carico degli Organismi responsabili dell'accesso ai dati sanitari nella gestione delle richieste di dati da essi trattati. I titolari dei dati sanitari affidabili dovrebbero essere autorizzati a valutare le domande di accesso ai dati sanitari presentate nell'ambito di questa procedura semplificata, sulla base delle loro competenze nell'affrontare il tipo di dati sanitari che stanno trattando, e di rilasciare una raccomandazione in merito a un'autorizzazione ai dati. L'organismo responsabile dell'accesso ai dati sanitari dovrebbe rimanere responsabile del rilascio dell'autorizzazione finale ai dati e non dovrebbe essere vincolato dalla raccomandazione fornita dal titolare dei dati sanitari affidabile. I soggetti di intermediazione dei dati sanitari non dovrebbero essere designati come titolari di dati sanitari affidabili*.» Considerando 76, Regolamento (UE) 2025/327.

soluzioni divergenti che potrebbero compromettere l'omogeneità della figura di tali titolari affidabili all'interno del territorio europeo.

4. Biobanche a scopo di ricerca medica e circolazione secondaria dei dati: *l'intuitus personae* e il trattamento dei dati personali.

La complessità della tutela afferente all'utilizzo secondario dei dati e alle biobanche[326], si evince dalla lettura di un'ordinanza che trae origine da una controversia creatasi a seguito di un provvedimento emanato dal Garante per la protezione dei dati personali, a discapito di una società del Regno Unito[327].

Il Garante, intervenuto su istanza delle pretese espresse dai donatori, si è pronunciato con l'intento di evitare un ingiustificato arbitrio nell'utilizzo dei dati contenuti nella biobanca, finalizzato alla "mercificazione" del genoma umano. La controversia si lega ad un interrogativo basato sulla necessità del rinnovo del consenso, per finalità prettamente garantiste. Sul punto, la Suprema Corte ha accolto le motivazioni contenute nel ricorso promosso dal Garante, basate sull'importanza dell'indissolubile legame tra l'*intuitus personae* e il trattamento dei dati personali, stabilendo la centralità del rinnovo del consenso nel caso di cessione di una biobanca e il necessario onere informativo a carico della società cessionaria[328].

La Corte di Cassazione si è espressa per la prima volta su questioni legate alla cessione di una banca dati genetica, applicando la vecchia disciplina del Codice della *privacy*, antecedente all'entrata in vigore del Regolamento Ue 2016/679 e alle conseguenti modifiche avvenute con il d.lgs n. 101 del 2018.

---

[326] Per una definizione di biobanche e approfondimento delle informazioni correlate v. *Linee guida per la certificazione delle biobanche*, 2006, 6.

[327] La società italiana SharDna S.p.A., nel 2000, diede vita ad una biobanca al fine di avviare uno studio sui campioni biologici umani, raccolti tramite donatori che volontariamente si erano sottoposti ad uno screening genetico, correlato allo svolgimento di visite mediche gratuite. Successivamente, con il fallimento della prima società e il conseguente acquisto del complesso aziendale da parte della T.L.S Plc., l'assente rinnovo del consenso da parte dei membri della comunità dell'Ogliastra coinvolti nella vicenda ha determinato l'intervento del Garante.

[328] Cass., 7 ottobre 2021, n. 27325, in *Diritto di famiglia e delle Persone*, 2022, con nota di M. CIANCIMINO, *Circolazione "secondaria" dei dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*; anche in *Nuova giur. civ. comm.*, 2022, con nota di D. CORTI, *Personalità (diritti della) - La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna;* anche in BioLaw *Journal*, 2022, con nota di S. FANNI, *Le biobanche di popolazione al vaglio della Suprema Corte di Cassazione: alcune note critiche sull'Ordinanza n. 27325 del 7 ottobre 2021.*

Attualmente, fattispecie di questo tipo si inseriscono in ipotesi di trattamento ulteriore da parte di terzi dei dati personali disciplinato dal "nuovo" art. 110 *bis* del d.lgs 30 giugno 2003, n. 196[329].

Dalla controversia appena descritta, e dalla conseguente posizione assunta dalla Corte di Cassazione, si evince che la circolazione dei dati sanitari rappresenta un'ampia area caratterizzata da numerosi profili, non ben definiti, che richiedono una diligente valutazione degli interessi coinvolti.

La ricerca rappresenta un contesto dinamico ove gli obiettivi iniziali potrebbero non essere ben delineati; da questo punto di vista un propedeutico intervento dell'interessato, attuerebbe un macchinoso dispendio di energie che intaccherebbe in maniera considerevole la speditezza nel lavoro svolto.

Già da tempo, il trattamento dei dati sanitari e la digitalizzazione si evolvono in un perimetro caratterizzato da un forte scontro fra esigenze contrapposte: il progresso richiede necessariamente la diffusione di informazioni con annessa trasformazione dei canali utilizzati e ciò comporta la conseguente esposizione a possibili rischi legati ad una incontrollata divulgazione dei dati.

L'inadeguata circolazione e l'errato utilizzo delle informazioni personali possono facilitare la profilazione del consumatore, la violazione della riservatezza e provocare molte altre conseguenze irreversibili per la qualità della vita dei soggetti coinvolti.

La "pressante" esigenza di individuare una disciplina che sia in grado di attuare un corretto bilanciamento degli interessi coinvolti, rappresenta il punto di partenza dei quesiti posti alla base della nostra ricerca: fino a che punto potrà spingersi il lecito sacrificio dell'identità del singolo?

Il ritratto della disciplina vigente prende forma come un vaso quasi privo di contenuto, in cui il consenso dell'interessato viene posto in secondo piano ed assume "fittiziamente" un ruolo centrale.

Appare evidente l'impossibilità di creare una puntuale disciplina che resti inamovibile rispetto alle esigenze dinamiche di ogni caso concreto.

---

[329] D. CORTI, *Personalità (diritti della) - La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna*, cit.

Focalizzando l'attenzione sulla ricerca, considerata come finalità principale dell'utilizzo dei campioni biologici, dal punto di vista giuridico occorre distinguere: il campione biologico inteso come una materia e il campione biologico inteso come fonte di informazione.

Nel tempo, l'attenzione è stata riservata alla sola considerazione del materiale biologico come informazione, lasciando credere, erroneamente, che la disciplina applicabile fosse esclusivamente ricavata da quella relativa al profilo informazionale. Così non è. La regolamentazione dell'utilizzo del materiale biologico deve tener conto di entrambi gli aspetti[330].

Particolare attenzione è rivolta al consenso del soggetto interessato, il quale rileva in due momenti distinti: l'estrazione del campione biologico e il successivo trattamento dei dati ricavati[331]. La questione centrale non risiede nell'individuazione di distinti modelli di consenso, bensì nella consapevolezza del soggetto di esprimersi rispetto a due differenti finalità[332]. Ciò si desume chiaramente dall'art. 7 del Regolamento Ue 2016/679 che stabilisce la necessità di una richiesta specifica di acquisizione del consenso, che deve essere distinta in un contesto in cui vengono coinvolte più questioni[333].

Pur parlando esplicitamente di consenso informato, occorre tener conto della reale accezione della consapevolezza del soggetto che ammette il trattamento delle informazioni estrapolate dal proprio materiale biologico. Appare difficile garantire una puntuale previsione dell'iter che verrà seguito nella fase di utilizzo dei dati genetici utilizzati e l'utilizzo di nuovi sistemi come AI fa emergere ulteriormente il problema legato al contenuto dell'informativa fornita al soggetto interessato. Non a caso, si parla di

---

330 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* in *Diritto di famiglia e delle Persone*, 2022, 1061 ss.

331 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1067 ss.

332 L'articolo 3 della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza) sancisce il principio del consenso informato nell'ambito della biologia e della medicina. La centralità del consenso del soggetto interessato trova inoltre fondamento in documenti di primaria importanza, quali il Codice di Norimberga del 1947 e la Dichiarazione di Helsinki del 1962. In questi testi si ribadisce che il consenso dei partecipanti a qualsiasi progetto di ricerca costituisce un elemento cardine per la tutela dei diritti umani nel contesto medico e scientifico: v. E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, cit., p. 110.

333 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1067 ss.

"consenso cieco" che conduce a una riflessione: acconsentire alla cessione del materiale biologico non equivale a fornire il consenso per il trattamento delle informazioni estrapolate dal campione stesso. Tuttavia, la cessione del materiale biologico pare essere equiparata ad una totale perdita del controllo sullo stesso: l'attività successiva al prelievo del materiale biologico, conduce a risultati che non possono essere completamente previsti *ex ante*[334].

In merito a questo punto, è importante considerare l'uso secondario delle informazioni per finalità compatibili con quelle originariamente stabilite. In tali circostanze, non è necessaria la riferibilità del consenso all'interessato, in quanto la compatibilità del fine successivo con quello originario, giustifica l'ulteriore trattamento[335].

L'importanza di tali precisazioni rileva dacché i campioni biologici consentono di ricavare informazioni in grado di far risalire alla fonte, ovvero al soggetto a cui appartengono[336], consentendo di estrapolarne altre legate alla storia famigliare del soggetto direttamente coinvolto [337]. I dati ricavati dal campione non riguardano esclusivamente l'individuo da cui provengono, ma possono estendersi a gruppi di persone che condividono il patrimonio genetico con il soggetto donatore[338].

"Qui sta l'ambiguità del dato genetico sotto il profilo della sua personalità: esso fotografa l'unicità dell'individuo e allo stesso tempo la sua collettività di appartenenza"[339].

Analizzando brevemente il contenuto del Regolamento (UE) 2016/679 emerge che il consenso del soggetto interessato deve essere espresso mediante un atto inequivocabile, tramite il quale si evince la chiara volontà di accettare il trattamento. In tale contesto, la manifestazione di volontà non dovrebbe derivare da una valutazione positiva di una mancata

---

334 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1085 ss.

335 V. art. 5, paragrafo1, lettera b) e art. 89, Regolamento UE 2016/679 e artt. 99, 107 e 110 *bis* d.lgs. 30 giugno 2003, n. 196, in riferimento all'uso secondario e al trattamento ulteriore dei dati.

336 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1068 ss.

337 E. STEFANINI, *Dati genetici e diritti fondamentali, Profili di diritto comparato ed europeo*, 2008, Milano, 3.

338 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1082 e ss.

339 V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1084.

espressione[340]. Sul punto, la centralità del consenso del diretto interessato rileva ma solleva degli interrogativi legati al potenziale coinvolgimento di informazioni legate a soggetti che non hanno espresso la propria volontà. In particolare, potremmo, in maniera poco risolutiva, tentare di collocare tale problema nello schema del considerando 33 del Regolamento (UE) 2016/679, seppur la lettura tradizionale dello stesso riguarda la mancata possibilità di completa previsione dell'attività di ricerca che verrà svolta, rispetto alla quale non sembra possibile anticipare chiaramente il perimetro del consenso prestato[341].

In realtà, già nella Dichiarazione Universale sul Genoma Umano e i Diritti Umani del 1997 si evince una valutazione non individuale, che ha posto sotto i riflettori l'importanza dei progressi raggiunti grazie all'utilizzo del genoma umano a livello collettivo[342]. Potremmo leggere tale indicazione come chiaro riferimento al fatto che lo studio del dato genetico mira al perseguimento di finalità che giovano all'intera collettività. Dunque, si può ragionevolmente sostenere tale conclusione: la centralità del consenso del singolo funge da base legittimante per l'utilizzo di quel dato che potrebbe portare all'estrapolazione di informazioni legate alla storia familiare del soggetto stesso, considerando che i risultati raggiunti comunque daranno vita a potenziali benefici a favore dell'intera collettività, soprattutto in riferimento ai soggetti geneticamente coinvolti dai benefici dell'attività di ricerca, ma esclusi dalla prestazione del consenso.

---

[340] Considerando 32, Regolamento (UE) 2016/679.

[341] «*Detto Considerando ha essenzialmente valore ricognitivo delle soluzioni emerse nella prassi per rispondere all'esigenza, particolarmente avvertita nella ricerca in ambito sanitario, di rendere ammissibile l'attività scientifica nonostante l'impossibilita`, quanto meno nelle prime fasi della ricerca (ad esempio, in sede di definizione del protocollo di uno studio clinico), di individuare in modo specifico gli scopi perseguiti e, dunque, di acquisire dalle persone da coinvolgere nella stessa un consenso pienamente informato.*»: così D. SBORLINI, *Il* broad consent *come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, *Contratto e impresa*, 2024, 226.

[342] «*a) Ognuno deve aver accesso ai progressi della biologia, della genetica e della medicina, concernenti il genoma umano, nel rispetto della propria dignità e dei propri diritti.*

b) La libertà della ricerca, necessaria al progresso della conoscenza deriva dalla libertà di pensiero. Le applicazioni della ricerca soprattutto quelle in biologia, genetica e medicina, concernenti il genoma umano, devono tendere ad alleviare la sofferenza ed a migliorare la salute dell'individuo e di tutta l'umanità.»: Articolo 12, *Dichiarazione universale sul genoma umano e i diritti umani,* 1997.

Occorre ricordare che fra i risultati più rilevanti raggiunti dalla ricerca genetica vi è la mappatura del genoma umano, completata nel 2003, che consente di analizzare e comprendere il patrimonio genetico di un essere umano. In tal modo è possibile identificare, mediante l'utilizzo di test genetici predittivi, presintomatici o diagnostici, eventuali mutazioni genetiche responsabili di patologie già presenti o suscettibili di insorgenza futura[343]. La particolarità del dato genetico sta nella sua natura permanente e inalterabile[344].

Il materiale biologico viene conservato all'interno di biobanche. Benché non esista una definizione univoca di queste ultime, possiamo definirle come strutture che si occupano della conservazione dei dati. Differenti sono le definizioni rese note per distinguerle da altri sistemi di archiviazione, tuttavia, un elemento caratterizzante è l'assenza dello scopo di lucro[345]. Non a caso, caratteristica principale delle informazioni genetiche è la gratuità già sancita nella Convenzione di Oviedo che stabilisce il cd. "Divieto di profitto" [346].

Il tema trattato necessita di una puntuale attenzione da parte del legislatore; dacché a livello nazionale non sussiste una vera normativa speciale che si occupi di biobanche, la sua disciplina può essere desunta dalla legislazione che ordinariamente si occupa della protezione dei dati anche in termini di trattamento dei campioni biologici.

Tuttavia, mediante l'Autorizzazione generale n. 8/2016[347] relativa al trattamento dei dati genetici e mediante l'Autorizzazione generale n.

---

343 Per una definizione di test genetici diagnostici, predittivi e presintomatici si veda E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, cit., 1.

344 L. VILLANI, *Biobanche e test rivelatori di informazioni genetiche: spunti di riflessione per un nuovo consenso informato*, in *Resp. Civ.*, 2010, 140.

345 Sul punto rileva una importante distinzione tra i casi in cui le bio-banche, note anche come bio-archivi, fungano unicamente da deposito dei campioni biologici e i casi in cui l'attività di stoccaggio venga affiancata da attività di elaborazione del dato. Ogni archivio racchiude differenti potenzialità collegate al diverso ruolo svolto e, in presenza di determinati elementi, si può parlare di Big Data. Per ulteriori approfondimenti sul punto, v. V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1075 ss.

346 Art. 21 *Convenzione per la protezione dei diritti dell'uomo e della dignità dell'essere umano rispetto alle applicazioni della biologia e della medicina* (Convenzione di Oviedo), 4 aprile 1997, in Gazzetta ufficiale del Consiglio d'Europa, n. 164, 1997.

347 Autorizzazione n.8/2016*, Autorizzazione generale al trattamento dei dati genetici*, 15 dicembre 2016, n. 530 (doc. *web* n. 5803688), efficace sino al 24 maggio 2018.

9/2016[348] relativa al trattamento dei dati personali per fini di ricerca, ha avuto luogo una parziale delineazione della materia.

Attualmente, nel panorama europeo i dati genetici e i dati sanitari rientrano nelle categorie particolari di dati il cui trattamento è disciplinato dall'art. 9 del Regolamento (UE) 2016/679[349].

Benché sia opinione diffusa che a livello europeo si voglia favorire la circolazione dei dati, la normativa è passata da uno schema di divieto generico e una tutela ispirata a quella del diritto assoluto, ad uno schema ove occorre bilanciare gli interessi coinvolti, favorendo la circolazione delle informazioni[350]. Vi è il rischio di compromissione della sicurezza legata ai diritti fondamentali degli individui[351].

Tale decisione solleva numerosi dubbi in quanto, come precedentemente visto, l'attività attuata dalle biobanche mira non solo alla conservazione dei campioni, ma anche allo sfruttamento delle informazioni legate a quel campione[352]. Le informazioni rappresentano il punto di partenza delle indagini poste alla base dell'attività di ricerca, ove il catalogo di dati estrapolati danno vita ad un vero e proprio *network*[353].

Nel tempo, sono stati sollevati numerosi interrogativi inerenti all'utilizzo dei dati genetici per finalità di ricerca, ma anche per scopi differenti legati all'ambito assicurativo, lavorativo o in attività legate al contrasto alla criminalità[354]. Infatti, l'interesse verso i dati contenuti nelle biobanche può essere manifestato da differenti soggetti, partendo dalla comunità

---

[348] Autorizzazione n. 9/2016, *Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica*, 15 dicembre 2016, n 531 (doc. *web* 5805552), efficace fino al 24 maggio 2018.

[349] Con l'entrata in vigore del Regolamento UE 2016/679 e del d.lgs. 101/2018, che ha modificato il Codice in materia di protezione dei dati personali, viene introdotto l'art. 2-septies, che stabilisce importanti garanzie per il trattamento dei dati biometrici, genetici e relativi alla salute, e rettificato l'art. 110, d.lgs. 30 giugno 2003, n. 196.

[350] V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1082.

[351] V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1072 ss.

[352] V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1075.

[353] A. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove Leggi Civili Commentate*, 2020, 175 ss.

[354] E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, cit., 3; sul punto, appare rilevante far riferimento all'adesione dell'Italia al Trattato di Prüm, avvenuta con l. 30 giugno 2009, n. 85, che ha dato vita alla creazione presso il Ministero dell'Interno della banca dati DNA.

scientifica[355], fino a soggetti economici privati. Nell'ultimo caso l'esigenza di tutelare la *privacy* dei soggetti coinvolti prevale, dacché si perfeziona un bilanciamento che non coinvolge finalità medico-scientifiche[356].

Le biobanche rappresentano una risorsa fondamentale per garantire la progressione della medicina: i dati genetici si distinguono dalle comuni informazioni personali per la loro natura immodificabile e immutabile, nonché per il loro carattere predittivo riguardo alle future condizioni di salute dell'individuo. Nel corso del tempo, si è diffusa una tendenza a favore della libertà di ricerca, consolidatasi principalmente durante il secolo scorso, quando il primato della tecnologia rappresentava ancora un aspetto remoto. Lo scenario nel quale si sviluppa il dibattito oggetto della nostra analisi si fonda su un modello pluralista, che rende difficile l'applicazione di una regola univoca in grado di sancire la prevalenza di un diritto o interesse su altri. Tuttavia, il primato della tutela della persona, sancito dalla Costituzione, ha già da tempo reso evidente l'impossibilità di garantire alla ricerca lo stesso grado di protezione riconosciuto ai diritti e agli interessi della persona. Nella costante lotta tra ricerca e libertà individuali trova una sorta di primato la tutela della dimensione umana, seppur in maniera non sempre chiara e condivisa[357]. O perlomeno questo appare a primo acchito: nel tempo si è assistito a una chiara erosione della prevalenza della tutela dei diritti del singolo.

Ponendo l'attenzione sulle finalità perseguite dalle biobanche, emerge che tale conflitto non si intreccia esclusivamente con esigenze che confluiscono all'interno della stessa dimensione umana: il bilanciamento coinvolge le sorti della collettività, e non del singolo individuo, che sono influenzate dall'andamento del progresso scientifico[358].

---

[355] V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso*, cit., 1061.
[356] E. STEFANINI, *Dati genetici e diritti fondamentali, Profili di diritto comparato ed europeo,* cit., 118.
[357] A. MUSUMECI, *Bioetica, Enc. Giur. Treccani*, V, Roma, 1998, 4.
[358] E. STEFANINI, *Dati genetici e diritti fondamentali, Profili di diritto comparato ed europeo,* cit., 108 ss.

Il paradosso di tale bilanciamento risiede nel fatto che la progressione scientifica è alimentata dall'informazione attinente al singolo individuo[359].
Lo sviluppo della ricerca può dar vita a significativi benefici, si pensi al caso della terapia genetica, ma comporta, al contempo, potenziali rischi. Pensiamo all'archiviazione di informazioni genetiche in grado di rilevare aspetti riservati legati all'identità dei soggetti coinvolti[360]. L'utilizzo di informazioni genetiche è strettamente collegato a possibili criticità, per tale motivo è indispensabile e imprescindibile la predisposizione di meccanismi che garantiscano la salvaguardia della dignità delle persone coinvolte[361].
In un contesto in cui gli sviluppi della scienza anticipano la regolamentazione del legislatore si è acceso un intenso dibattito sul tema della bioetica. Tale discussione ha generato, sia a livello internazionale che comunitario e nazionale, rilevanti interventi che hanno tentato di delineare un quadro giuridico in grado di bilanciare problematiche e vantaggi annessi alla progressione di tale settore ove significative opportunità per la salute umana si scontrano con possibili minacce per la tutela di interessi e diritti individuali. Il ritardo da parte dei legislatori nazionali va attribuito alla difficoltà di comprensione dei numerosi aspetti legati ai fenomeni bioetici che coinvolgono aspetti religiosi, etici e ideologici e che vanno calibrati al fine di individuare un corretto compromesso che giunga ad un risultato condivisibile. Gli aspetti appena citati, si combinano con ulteriori esigenze che riguardano l'autodeterminazione del soggetto interessato rispetto all'espressione del proprio consenso o, ancora, la *privacy* dei soggetti coinvolti e innumerevoli temi annessi[362].
L'attenzione si è progressivamente focalizzata sulla valutazione del campione biologico quale fonte di informazione, in quanto esso consente di

[359] Cfr. A. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, cit., 194 ss.
[360] Cfr. I. DE MIGUEL BERIAIN, *El uso de datos de salud para investigación biomédica a la luz de la propuesta de reglamento del Parlamento europeo y del Consejo sobre el espacio europeo de datos sanitarios,* in *Revista Jurídica de Castilla y León*, 2023.
[361] E. STEFANINI, *Dati genetici e diritti fondamentali, Profili di diritto comparato ed europeo*, cit., 8.
[362] E. STEFANINI, *Dati genetici e diritti fondamentali, Profili di diritto comparato ed europeo*, cit., 20 ss.

ottenere dati relativi alla salute, dati genetici[363] e dati biometrici[364], con conseguenze legate al tema della riservatezza[365].

Seppur con la legge 11 gennaio 2018, n. 3[366] abbiamo assistito ad un parziale passo in avanti, ancora oggi si evince una blanda concretezza della disciplina normativa e il Regolamento sullo spazio europeo dei dati sanitari non è stato utilizzato come strumento adatto per prevedere una più attenta disciplina sul tema dibattuto[367].

Questo sarebbe stato il contesto adatto per una più attenta definizione delle corrette modalità di utilizzo e regolamentazione; tuttavia, tale occasione è stata mancata, come dimostra il fatto che, effettuando per parole chiave all'interno del Regolamento, il termine «biobanche» appare solamente due

[363] Sono dati genetici «*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione»:* art. 4, n. 13), Regolamento (UE) 2016/679.

[364] Sono dati biometrici *«i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.»:* art. 4, n. 14), Regolamento (UE) 2016/679.

[365] «*La dimensione cosale è rimasta in secondo piano, con una scelta non priva di conseguenze. La minore visibilità della normativa in materia di campione inteso come materiale ha, infatti, ingenerato la convinzione secondo la quale il materiale biologico umano non sarebbe che il supporto materiale dei dati che esso fornisce o il loro contenitore.»:* così V. CAREDDA, *Campioni biologici e big data: l'evoluzione del consenso,* cit., 1064.

[366] A cui ha fatto seguito il d.lgs. 14 maggio 2019, n. 52, Attuazione della delega per il riassetto e la riforma della normativa in materia di sperimentazione clinica dei medicinali ad uso umano, ai sensi dell'articolo 1, commi 1 e 2, della legge 11 gennaio 2018, n. 3

[367] «*Non risulta allo stato sussistente una specifica ed organica disciplina delle biobanche di ricerca. Pertanto, premesso che è ormai accettato dalla comunità scientifica internazionale che l'utilizzo di organi, tessuti e cellule umane può dare un enorme contributo alla ricerca medica, su un argomento così complesso come quello dell'utilizzo di campioni biologici umani a tali fini, urge, in una prospettiva multidisciplinare ed inclusiva dei vari aspetti connessi, la predisposizione di una normativa che, per un verso, tuteli gli interessi dei concedenti e dei ricercatori, ponendo le condizioni atte a favorire il coinvolgimento dei primi nelle attività dei secondi, e che, per altro verso, disciplini in modo chiaro ed equilibrato tutte le problematiche legate alle varie attività delle biobanche di ricerca, tenendo sempre sullo sfondo il rispetto dei principi di uguaglianza, di autodeterminazione, di solidarietà e, soprattutto, di intangibilità e indisponibilità della persona umana. Occorre, quindi, una normativa specifica che regoli in maniera organica le varie fasi di trattamento del materiale biologico umano dal momento in cui viene prelevato dal paziente sino al momento del suo utilizzo per finalità legate alla ricerca*.»: così C. RICCI E P. RICCI, *Le biobanche di ricerca: questioni e disciplina research biobanks: questions and regulations*, *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 2018, 109 e 110.

volte: nel Considerando 92 e nell'articolo 51, che disciplina le categorie minime di dati sanitari elettronici per l'uso secondario.

CAPITOLO V

GOVERNANCE E SISTEMA SANZIONATORIO: PROFILI CRITICI.

SOMMARIO: 1. Equilibrio istituzionale del panorama europeo: riflessioni sulla *governance* nello Spazio europeo dei dati sanitari. 2. (segue) l'importante obiettivo di una *governance* armonizzata. 3. La frammentazione del sistema sanzionatorio delineato dallo *European Health Data Space*. 4. (segue) Possibili soluzioni per l'armonizzazione del sistema sanzionatorio.

1. Equilibrio istituzionale del panorama europeo: riflessioni sulla *governance* nello Spazio europeo dei dati sanitari.

Nel capitolo IV del presente lavoro è stato parzialmente approfondito il ruolo degli Organismi responsabili dell'accesso ai dati sanitari, figura predominante nel contesto europeo dedicato all'uso secondario dei dati sanitari[368] che nasce con l'obiettivo primario di soddisfare esigenze legate al pubblico interesse[369].

Va precisato che tali Organismi rivestono un ruolo cruciale anche nell'ambito del sistema sanzionatorio[370], in quanto incaricati di funzioni relative al monitoraggio e al controllo sull'uso secondario dei dati[371].

---

[368] Sul punto, v. anche S. N. NAVARRO, *Datos sanitarios electrónicos, El espacio europeo de datos sanitarios*, cit., 231 e ss.

[369] La *governance* adottata all'interno dello Spazio Europeo dei Dati Sanitari trae origine dal Regolamento (UE) 2022/868 relativo alla *governance* europea dei dati il cui articolo 7 prevede la designazione di uno o più Organismi competenti «*per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo delle categorie di dati*»: per un attento confronto v. Regolamento sulla *governance* dei dati (UE) 2022/868, 30 maggio 2022, in G.U.U.E., 3 giugno 2022, art. 7.

[370] Il presente capitolo è stato elaborato a partire dalla pubblicazione *"Il sistema sanzionatorio dell'European Health Data Space: tra armonizzazione e frammentazione normativa*", inerente al progetto di ricerca di Ateneo PRA 2023 – Università di Foggia "*Health Data: protection and free movement in the digital age*". In particolare, i paragrafi 3 e 4 si fondano sul contributo di Alessia Pia Mangiacotti (Dottoranda in Diritto e Sicurezza – Università di Foggia), il cui apporto ha rappresentato un riferimento significativo per l'approfondimento delle tematiche trattate.

[371] Articolo 57, paragrafo 1, lettera a), Regolamento (UE) 2025/327

Nel contesto di tali competenze, gli Organismi possono adottare misure appropriate qualora un utente o un titolare dei dati sanitari non rispetti le disposizioni previste dal Capo IV.

Nel perimetro relativo alla funzione sanzionatoria, in presenza di accertata non conformità che configuri una potenziale violazione del Regolamento 2016/679, è prevista l'immediata comunicazione all'Autorità di controllo competente, alla quale saranno trasmesse tutte le informazioni raccolte in precedenza dall'Organismo[372].

Questa precisazione apre una riflessione relativa agli interrogativi che emergono dal contesto in cui si inseriscono queste nuove figure istituzionali, nel quale sembra necessario definire con maggiore precisione il confine tra le competenze. Potrebbe infatti verificarsi una sovrapposizione di funzioni tra gli Organismi preposti alla gestione dei dati sanitari e l'Autorità garante per la protezione dei dati personali[373].

A tal proposito, è fondamentale chiarire che le figure embrionali preposte alla supervisione e attuazione dell'uso secondario dei dati sanitari devono operare evitando interferenze o duplicazioni di competenze, in particolare in riferimento a provvedimenti già adottati da altre Autorità. L'operato delle figure chiamate a vigilare e a intervenire in caso di violazioni deve

---

[372] Articolo 63, Regolamento (UE) 2025/327

[373] L'applicazione del Regolamento (UE) 2016/679 è di competenze delle Autorità designate che si occupano di protezione dei dati personali. In Italia l'Autorità di riferimento è il Garante per la protezione dei dati personali il Garante per la protezione dei dati personali, istituita dalla cosiddetta legge 31 dicembre 1996, n. 675, poi disciplinata dal Codice in materia di protezione dei dati personali (D.lg. 30 giugno 2003 n. 196), successivamente modificato dal Decreto legislativo 10 agosto 2018, n. 101.

Sul punto, v. Articolo 51, Regolamento (UE) 2016/679: *«1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»). 2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII. 3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63. 4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica*.»

necessariamente essere coordinato, assicurando il rispetto del quadro normativo nazionale e sovranazionale[374].

In particolare, la normativa europea riconosce agli individui e ai soggetti collettivi la facoltà di presentare un reclamo in caso di compromissione o lesione di diritti o interessi reputati rilevanti[375] e la gestione del reclamo sarà deferita all'Autorità di controllo competente, in conformità con il Regolamento generale sulla protezione dei dati[376]. Sarà questo il contesto in cui l'Organismo responsabile dell'accesso ai dati sanitari coinvolto dovrà tempestivamente trasferire le informazioni in suo possesso all'Autorità di controllo, agevolando la valutazione del reclamo e collaborando per la realizzazione di una tutela completa a vantaggio dei diritti degli interessati[377].

Gli Organismi, deputati alla gestione delle richieste di accesso ai dati per l'uso secondario, all'autorizzazione dell'accesso, alla predisposizione dei dati necessari e al monitoraggio del loro utilizzo, non devono interferire con le Autorità incaricate per la protezione dei dati[378] che continueranno ad agire per assicurare il rispetto del Regolamento generale sulla protezione

---

374 Sul punto rileva la previsione sancita dall'articolo 63, paragrafo 2, del Regolamento di nuova adozione, il quale stabilisce che nella fase di monitoraggio e controllo, gli Organismi coinvolti effettueranno puntuali comunicazioni all'Autorità per la protezione dei dati, qualora l'accertamento della non conformità riguardi una possibile violazione del Regolamento (UE) 2016/679, fornendo tutte le informazioni utili: Articolo 63, paragrafo 2, Regolamento (UE) 2025/327.

375 Articolo 81, paragrafo 1, Regolamento (UE) 2025/327.

376 L'articolo 71, rubricato *"Diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali per l'uso secondario"*, disciplina il diritto delle persone fisiche di escludere, senza necessaria motivazione, il trattamento dei propri dati sanitari elettronici per l'uso secondario: Articolo 71, Regolamento (UE) 2025/327.

377 In seguito a un adeguata attività istruttoria, l'Organismo competente dovrà informare il soggetto interessato sullo stato del reclamo entro un termine ragionevole: Articolo 81, paragrafo 2, Regolamento (UE) 2025/327; Al fine di rendere maggiormente agevole la proposizione di reclami, ciascun Organismo sarà chiamato ad adottare misure di supporto adeguate, anche attraverso la predisposizione di appositi moduli e procedure semplificate per la proposizione dei reclami: v., Articolo 81, paragrafo 3, Regolamento (UE) 2025/327.

378 Il Regolamento sulla protezione dei dati personali stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, con l'obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali: Articolo 1, Regolamento (UE) 2016/679. Per un approfondimento contestualizzato al tema oggetto di analisi, v. F. MATTEI, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie* in *Le nuove frontiere della medicina, Assetti istituzionali e gestione dei dati*, cit., 125 e ss.

dei dati[379], restando le uniche responsabili della sua corretta applicazione[380].

Ulteriore interrogativo, con fondamenta simili, può essere condotto in riferimento al ruolo delle Autorità di sanità digitale[381], protagoniste della *governance* relativa all'uso primario dei dati sanitari e responsabili della corretta applicazione delle disposizioni normative contenute nel Capo II. Nello specifico, la violazione dei diritti connessi all'utilizzo primario dei dati sanitari può essere contestata dalle persone interessate mediante la presentazione di un reclamo alle Autorità di sanità digitale[382], con particolare attenzione alla natura e all'ambito della condotta lesiva. Se il reclamo riguarderà l'accesso ai propri dati sanitari elettronici personali[383], l'inserimento di informazioni nella cartella clinica elettronica[384], la rettifica

[379] Il Regolamento sulla protezione dei dati personali stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, con l'obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali: Articolo 1, Regolamento (UE) 2016/679.

[380] Si rinvia alle definizioni contenute nel Regolamento (UE) 2016/679. In particolare, si richiama l'attenzione sulla definizione di «violazione dei dati personali» intesa come «*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*»: Articolo 4, paragrafo 12, Regolamento (UE) 2016/679.

[381] «*Ciascuno Stato membro designa una o più autorità di sanità digitale responsabili dell'attuazione e dell'applicazione del presente capo a livello nazionale. Gli Stati membri informano la Commissione in merito all'identità delle autorità di sanità digitale entro il 26 marzo 2027. Qualora uno Stato membro designi più autorità di sanità digitale o l'autorità di sanità digitale sia composta da più organizzazioni, lo Stato membro interessato comunica alla Commissione una descrizione della distribuzione dei compiti tra le diverse autorità o organizzazioni. Qualora uno Stato membro designi più autorità di sanità digitale, ne designa una che funga da coordinatore. La Commissione mette tali informazioni a disposizione del pubblico.*»: Articolo 19, paragrafo 1, Regolamento (UE) 2025/327.

[382] Articolo 21, paragrafo 1, Regolamento (UE) 2025/327.

[383] Articolo 3, paragrafo 3, Regolamento (UE) 2025/327; La disciplina del diritto di accesso è contenuta nell'art. 15 del Reg. (UE) 2016/679, rubricato "*Diritto di accesso dell'interessato*".
Inoltre, per un approfondimento relativo alla privacy e all'accesso civico in relazione alle strutture sanitarie pubbliche, v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità, Teoria e pratica del diritto*, cit., 101 e ss.

[384] Articolo 5, Regolamento (UE) 2025/327.

dei dati[385], il diritto alla portabilità[386], la limitazione dell'accesso[387], la tracciabilità[388]e il diritto di esclusione riguardo all'uso primario[389], l'Autorità di sanità digitale trasmetterà il reclamo all'Autorità per la protezione dei dati personali, fornendole tutte le informazioni necessarie[390]. Dunque, le previsioni normative presenti nello Spazio europeo dei dati sanitari tracciano un confine tra l'operato degli Organismi responsabili dell'accesso ai dati sanitari, le Autorità di sanità digitale e le Autorità per la protezione dei dati personali, provando a stabilire un discrimine relativo ai contesti di intervento delle diverse istituzioni. Inoltre, il regolamento prevede che le Autorità protagoniste del GDPR saranno chiamate a svolgere un ruolo primario di monitoraggio a garanzia dell'applicazione degli stessi diritti per i quali è sancito il loro intervento relativamente alla proposizione di reclami da parte dei soggetti coinvolti[391], cooperando per concretizzare una corretta applicazione del regolamento sullo EHDS nell'ambito delle rispettive competenze[392] e continuando ad intervenire attivamente per preservare la protezione dei dati personali[393].

---

[385] Articolo 6, Regolamento (UE) 2025/327, conformemente all'articolo 16 del Regolamento (UE) 2016/679 il quale sancisce che: «*L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.*»

[386] Articolo 7, Regolamento (UE) 2025/327; La disciplina del diritto alla portabilità dei dati è contenuta nell'articolo 20 del Regolamento (UE) 2016/679.

[387] Il Regolamento prevede che le persone fisiche siano informate dei rischi legati alla scelta di limitare l'accesso ai propri dati e rimanda agli Stati membri l'effettiva regolamentazione e previsione di garanzie relative all'esercizio di tale limitazione: Articolo 8, Regolamento (UE) 2025/327.

[388] «*Gli Stati membri possono prevedere limitazioni al diritto di cui al paragrafo 1 in circostanze eccezionali, qualora vi siano indicazioni concrete che la divulgazione metterebbe a rischio gli interessi vitali o i diritti del professionista sanitario o le cure assistenziali fornite alla persona fisica*.»: Articolo 9, Regolamento (UE) 2025/327.

[389] Articolo 9, Regolamento (UE) 2025/327.

[390] Articolo 21, paragrafo 2, Regolamento (UE) 2025/327.

[391] «*L'autorità o le autorità di controllo responsabili di monitorare e assicurare l'applicazione del regolamento (UE) 2016/679 sono altresì competenti di monitorare e assicurare l'applicazione dell'articolo 3 e degli articoli da 5 a 10 del presente regolamento. Le pertinenti disposizioni del regolamento (UE) 2016/679 si applicano mutatis mutandis. Le autorità di controllo hanno il potere di infliggere sanzioni amministrative pecuniarie fino all'importo di cui all'articolo83, paragrafo 5, del regolamento (UE) 2016/679*»: Articolo 22, paragrafo 1, Regolamento (UE) 2025/327.

[392] Articolo 22, paragrafo 2, Regolamento (UE) 2025/327.

[393] Per un approfondimento relativo al ruolo Garante Privacy, relativo al trattamento di dati sulla salute, v. G. AMARÙ, A. FAVA, M. FOSSI, F. MAINARDI, *La privacy del dato sanitario,*

Alla luce di tali riflessioni, appare chiara la soluzione relativa al quesito posto: le diverse Autorità opereranno in ambiti distinti con una netta suddivisione del perimetro di intervento. In particolare, le Autorità per la protezione dei dati personali conservano la competenza esclusiva relativa alle violazioni sul Regolamento generale sulla protezione dei dati, mentre le figure emergenti nel panorama europeo interverranno in caso di violazioni espressamente previste dallo stesso regolamento, rispettivamente riferite all'uso primario dei dati per le Autorità di sanità digitali e all'uso secondario per gli Organismi responsabili dell'accesso ai dati[394].

Dunque, i diversi protagonisti del panorama sanzionatorio europeo relativo allo spazio sanitario di recente costruzione, pur operando in settori contigui, svolgeranno ruoli complementari, non sovrapponibili, evitando l'alterazione dell'equilibrio istituzionale.

Ad oggi, questo sembra emergere da un'analisi teorica della normativa vigente che sul piano pratico potrebbe sorprendere con eventuali violazioni delle aree di azione costruite.

2. (segue) l'importante obiettivo di una *governance* armonizzata.

Il lavoro sinergico non rappresenta esclusivamente un obiettivo all'interno della singola nazione, ma dovrà essere perseguito anche a livello unionale; per tale motivo ogni Organismo, impegnandosi al fine di assicurare l'adozione di condotte coerenti, collaborerà con la Commissione e con le medesime figure degli altri Stati.

L'attività svolta[395] dagli Organismi sarà contenuta in una relazione che verrà redatta bimestralmente e che sarà pubblicata in appositi siti *web* e

Manuale per operatori e professionisti che trattano dati relativi alla salute e per chi vuole saperne di più, cit., 91 e ss.

394 Considerando 65, Regolamento (UE) 2025/327.

395 «*Ogni due anni ciascun organismo responsabile dell'accesso ai dati sanitari pubblica una relazione di attività e la rende pubblicamente disponibile sul suo sito web. Se uno Stato membro designa più di un organismo responsabile dell'accesso ai dati sanitari, l'organismo di coordinamento di cui all'articolo 55, paragrafo 1, è responsabile della relazione di attività e richiede le informazioni necessarie agli altri organismi responsabili dell'accesso ai dati sanitari. Tale relazione di attività segue una struttura concordata dal comitato EHDS a norma dell'articolo 94, paragrafo 2, lettera d), e contiene almeno le categorie di informazione seguenti:*

presentata alla Commissione e al Comitato dello spazio europeo dei dati sanitari entro sei mesi dalla fine del secondo anno del periodo di riferimento[396].

Nella fase di "preparazione", gli Stati membri hanno evidenziato la necessità di implementare una piattaforma comune, utile per la condivisione delle eccellenze operative, l'esposizione delle problematiche e per il rafforzamento della collaborazione, anche finalizzata alla creazione e gestione dello sviluppo degli Organismi. Per soddisfare questa esigenza, hanno scelto di creare una Comunità di Pratica *Health Data Access Body* (HDAB)[397], nota come HDABs-CoP, composta dalle Autorità competenti e

a) informazioni relative alle domande di accesso ai dati sanitari e alle richieste di dati sanitari presentate, quali i tipi di
richiedenti di dati sanitari, il numero di autorizzazioni ai dati rilasciate o respinte, le categorie delle finalità dell'accesso
e le categorie di dati sanitari elettronici a cui si è avuto accesso, nonché se del caso una sintesi dei risultati degli impieghi
dei dati sanitari elettronici;
b) informazioni sull'adempimento degli impegni normativi e contrattuali da parte degli utenti dei dati sanitari e dei titolari dei dati sanitari, nonché sul numero e sull'importo delle sanzioni amministrative pecuniarie imposte dagli organismi responsabili dell'accesso ai dati sanitari;
c) informazioni sugli audit effettuati sugli utenti dei dati sanitari per garantire la conformità del trattamento che questi
effettuano in un ambiente di trattamento sicuro in conformità dell'articolo 73, paragrafo 1, lettera e);
d) informazioni sugli audit interni e di terzi sulla conformità degli ambienti di trattamento sicuri alle norme, alle specifiche e alle prescrizioni stabilite, di cui all'articolo 73, paragrafo 3;
e) informazioni sul trattamento delle richieste presentate da persone fisiche riguardo all'esercizio dei loro diritti alla protezione dei dati;
f) una descrizione delle attività svolte dall'organismo responsabile dell'accesso ai dati sanitari in relazione al coinvolgimento e alla consultazione dei portatori di interessi pertinenti;
g) le entrate derivanti da autorizzazioni ai dati e richieste di dati sanitari;
h) il numero medio di giorni tra la domanda di accesso ai dati sanitari o la richiesta di dati sanitari e l'accesso ai dati;
i) il numero di marchi di qualità dei dati rilasciati dai titolari dei dati sanitari, suddiviso per categoria di qualità;
j) il numero di pubblicazioni di ricerca sottoposte a valutazione inter pares*, documenti strategici e procedure di regolamentazione che utilizzano dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari;*
k) il numero di prodotti e servizi di sanità digitale, comprese le applicazioni di IA, sviluppati utilizzando dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari»: Articolo 59, paragrafo 1, Regolamento (UE), 2025/327.

[396] Articolo 59, paragrafo 2, Regolamento (UE), 2025/327.

[397] Per un ulteriore approfondimento v. *Health Data Access Bodies – Community of Practice* in *European Commission*.

dagli enti affiliati agli Stati europei e ai paesi SEE[398], destinata a supportare l'evoluzione dell'assetto istituzionale all'interno dello Spazio europeo dei dati sanitari[399].

La decisione di valorizzare i benefici prevedibili attraverso un approccio sinergico rappresenta l'esito delle consultazioni svoltesi in fase di predisposizione delle domande di sovvenzione per l'istituzione degli Organismi. In tale sede, gli Stati membri hanno manifestato con chiarezza l'intenzione di agevolare la creazione e il consolidamento degli Organismi, promuovendo l'adozione di modelli operativi standardizzati.

In questo scenario, assume particolare importanza il ruolo degli Stati membri e, in modo specifico, delle Autorità nazionali competenti in materia di protezione dei dati, le quali contribuiranno, in maniera determinante, all'attuazione di un'interpretazione coordinata delle disposizioni. Tale contributo è essenziale per semplificare le procedure di richiesta, ridurre al minimo i tempi di valutazione e limitare le revisioni dei protocolli di studio relativi alle domande presentate[400]. Tale approccio include anche la progettazione e l'erogazione di programmi di formazione, la fornitura di risorse e la facilitazione di discussioni guidate da esperti, con l'obiettivo di

[398] Lo Spazio economico europeo (SEE) è stato istituito nel 1994 allo scopo di estendere le disposizioni applicate dall'Unione europea al proprio mercato interno ai paesi dell'Associazione europea di libero scambio (EFTA), per ulteriori approfondimenti sul punto, v. A. RAZAUSKAS, *Lo Spazio economico europeo (SEE), la Svizzera e il Nord, Note tematiche sull'Unione europea* in *Note tematiche sull'Unione europea*, 2025.

[399] In particolare la missione della Comunità di Pratica degli Organismi responsabili dell'accesso ai dati sanitari riguarda la condivisione di conoscenze fra le autorità coinvolte nella definizione effettiva degli Organismi responsabili dell'accesso ai dati, al fine di sostenere l'istituzione degli stessi, rafforzarne la cooperazione, creare una piattaforma per coordinare le informazioni e le strategie da attuare, condividere informazioni di natura tecnica e conoscenze, ottimizzare l'operato, promuovere l'armonizzazione e l'interoperabilità, al fine di creare solide strategie di diffusione dei risultati. Per ulteriori approfondimenti, v. *Health Data Access Bodies – Community of Practice, European Commission.*

[400] Appare interessante sottolineare che dal questionario HDAB in materia di conformità legale e normativa, inerente alla sfida prevista per l'implementazione degli organismi nazionali, è emerso che: il 5% degli intervistati non prevede alcuna sfida, il 5% prevede una sfida lieve, il 35% prevede una sfida moderata e il 55% prevede una sfida significativa: sul punto, v. WP7, Appendice 5 - Questionario HDAB e D9, *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, 27 febbraio 2025, 37 e ss.

dotare le Autorità competenti degli strumenti e delle conoscenze necessarie per operare con la giusta consapevolezza[401].

Il 25 gennaio 2024 si è tenuto l'incontro inaugurale della Comunità di Pratica delle Autorità competenti dello Spazio europeo dei dati sanitari, promosso per avviare le attività della Comunità stessa e per adottare il *Working Arrangements Document*[402] ed eleggere relatori e presidenti degli organi direttivi.

In questa prima fase, gli Organismi responsabili dell'accesso ai dati sanitari di alcuni Stati (Danimarca, Norvegia, Finlandia e Francia) hanno condiviso la propria esperienza relativa all'istituzione di tali figure[403].

Durante la seconda riunione dell'Assemblea generale della Comunità di Pratica delle Autorità competenti, del 25 giugno 2024, sono state fornite informazioni su progetti di particolare rilievo, tra cui *Second Joint Action Towards the European Health Data Space* (TEHDAS2)[404], fondamentale per favorire l'allineamento degli sforzi nazionali agli obiettivi europei,

---

401 *EHDS Community of Practice for Secondary Use*, *Working Arrangements, CoP drafting Task Force*, 22 gennaio 2024.

402 «*The WAD, prepared by a task force, sets out the CoP's mission and objectives, organization, procedures, roles, and responsibilities. It also identifies relevant stakeholders and outlines a roadmap of meetings and workplan for 2024. The WAD proposes the creation of six subgroups including the aim, objectives, results expected from each subgroup as well as the interdependencies between them. • Subgroup 1 Data Access Application systems (DAAM) • Subgroup 2 Health Datasets Metadata Catalogue (HDsC) and Data Quality and Utility (DQU) • Subgroup 3 Secure Processing Environments (SPEs) • Subgroup 4 Cross-border Gateways • Subgroup 5 Deployment and Operations • Subgroup 6 Stakeholder's Fora The WAD also includes a proposal for a set of collaborative tools (toolbox) to support the CoP to accomplish its goals. The WAD was adopted by consensus, and the chairs and rapporteurs for the General Assembly and Steering Board were elected. It was noted that this is the first version of the WAD which reflects the current needs of the CoP. A revision is welcome in one year, as the WAD acts as a "living" document which reflects the requirements at the time of production. »:* European Health Data Space, *Kick-off meeting Competent Authorities – Community of Practice in secondary use of health data Meeting Summary,* 25 gennaio 2024.

403 European Health Data Space, *Kick-off meeting Competent Authorities – Community of Practice in secondary use of health data Meeting Summary,* cit.

404 Tale programma mira allo sviluppo di Linee guida concrete e alla definizione di tecniche per facilitare l'utilizzo dei dati sanitari in diversi Paesi, nonché al sostegno per l'attuazione armonizzata della legislazione relativa allo Spazio Europeo dei Dati Sanitari: sul punto, v. I. A. KESSISSOGLOU, S. M. COSGROVE, L. A. ABBOUD, P. BOGAERT, M. PEOLSSON, N. CALLEJA, *Are EU member states ready for the European Health Data Space? Lessons learnt on the secondary use of health data from the TEHDAS Joint Action* in *European Journal of Public Health*, 2024, 1102 e ss.

assicurando allo stesso tempo coerenza e supporto tra le diverse iniziative[405].

La fase iniziale di attuazione richiede un dialogo continuo con la *governance* dello *European Health Data Space,* a conferma della centralità di un coordinamento multilivello. In tale prospettiva, il Comitato dello Spazio europeo dei dati sanitari è stato istituito con l'obiettivo di favorire la cooperazione e lo scambio informativo tra gli Stati membri e la Commissione Europea, assumendo un ruolo strategico nella gestione della comunicazione e nell'orientamento delle decisioni.

Il Comitato è composto da due rappresentanti per ciascuno Stato membro: uno incaricato dell'uso primario dei dati sanitari e l'altro dedicato all'uso secondario, a garanzia di una visione integrata e bilanciata delle diverse finalità di trattamento[406].

Il Comitato ha il compito di coadiuvare le decisioni sull'uso dei dati sanitari elettronici, anche invitando esperti, Autorità e organizzazioni pertinenti esterne; può creare sottogruppi specifici per affrontare tematiche dettagliate, mirando ad una efficace e ottimizzata operatività. La sua azione è finalizzata al perseguimento di interessi di natura collettiva[407].

Il Comitato opera in stretta collaborazione con altri Organismi, come il Comitato europeo per la Protezione dei Dati (EDPB)[408] e l'Agenzia dell'Unione europea per la *cybersicurezza* (ENISA), garantendo coerenza

---

[405] Già nel febbraio del 2021 è stato avviato un primo progetto congiunto europeo dedicato alla costruzione dello Spazio Europeo dei Dati Sanitari, terminato a luglio del 2023, con l'obiettivo di supportare gli Stati membri dell'Unione Europea e la Commissione europea nella fase di sviluppo di principi per l'uso secondario transfrontaliero dei dati sanitari. Per ulteriori approfondimenti, visitare il sito web ufficiale: *Joint Action Towards the European Health Data Space – TEHDAS1*

[406] «*L'articolo 92 istituisce un meccanismo di coordinamento centrale tra gli Stati membri e la Commissione europea. La creazione del Comitato EHDS garantisce che le decisioni in materia di gestione e utilizzo dei dati sanitari elettronici siano condivise e basate su un processo partecipativo. Il sistema a doppia rappresentazione per Stato membro (uso primario e uso secondario) è un'innovazione importante, poiché consente di considerare le esigenze sia dell'assistenza sanitaria diretta che della ricerca e innovazione.»:* M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari, Reg. UE 11 febbraio 2025, n. 327 (EHDS),* 2025, 130 e ss.; Articolo 92, paragrafo 1, Regolamento (UE) 2025/327; sul punto, v. anche Considerando 95.

[407] Articolo 92, paragrafi 5 e 6, Regolamento (UE) 2025/327.

[408] Il Comitato europeo per la protezione dei dati garantisce la coerente applicazione nel territorio europeo del Regolamento generale sulla protezione dei dati personali, Regolamento (UE) 2016/679. Per un ulteriore approfondimento sul programma di lavoro del Comitato, v. *EDPB Work Programme 2024–2025*, 8 ottobre 2024.

delle conclusioni avanzate per l'utilizzo dei dati nel settore della ricerca e dell'innovazione e assicurando il raggiungimento di obiettivi coerenti con i più recenti sviluppi tecnologici[409]. Tale attività è volta a garantire una coerente applicazione del regolamento, attraverso l'elaborazione di *best practices*[410] e la facilitazione del dialogo con i portatori di interessi coinvolti, inclusi pazienti, professionisti sanitari, ricercatori e responsabili politici[411].
In sintesi, il Comitato dello Spazio europeo dei dati sanitari svolge un ruolo di supporto fondamentale per gli Stati membri, favorendo il coordinamento e l'attuazione del regolamento attraverso la promozione della cooperazione e dello scambio informativo tra tutti gli attori coinvolti. Tale assetto organizzativo è orientato alla costruzione di un sistema armonizzato, in cui l'azione congiunta degli Stati e della Commissione garantisca una gestione dei dati coerente con gli standard di sicurezza informatica e di tutela della *privacy*[412].
In questo quadro, il coordinamento tra le istituzioni coinvolte rappresenta un elemento chiave per l'efficace implementazione del regolamento recentemente adottato. Una *governance* integrata e armonizzata deve costituire un obiettivo prioritario sin dalle prime fasi di attuazione, in particolare nel processo di individuazione degli Organismi responsabili dell'accesso ai dati sanitari in ciascuno Stato membro.
Il perseguimento degli obiettivi delineati dal regolamento è funzionalmente collegato al rafforzamento della *governance* istituzionale e alla predisposizione di strumenti operativi a supporto della sua attuazione. In

[409] Articolo 92, paragrafo 8, Regolamento (UE) 2025/327.
[410] Per un approfondimento delle best practices di gestione dei dati sanitari in altri paesi, v. M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari, Reg. UE 11 febbraio 2025, n. 327 (EHDS),* 2025,165 ss.
[411] Articolo 94, paragrafo 2, Regolamento (UE) 2025/327; inoltre, il Comitato per lo Spazio europeo dei dati sanitari svolge un ruolo specifico in relazione all'uso primario dei dati sanitari fornendo assistenza agli Stati, per assicurare a questi ultimi il coordinamento con le pratiche adottate dalle autorità di sanità digitale, redigendo contributi volti a promuovere lo scambio delle migliori pratiche relative all'uso primario dei dati, facilitando la cooperazione tra le autorità di sanità digitale, condividendo informazioni volte ad ottimizzare la gestione del rischio legato ad eventuali incidenti che potrebbero riguardare la violazione di dati contenuti nelle cartelle cliniche e semplificando la consultazione dei portatori di interessi coinvolti: sul punto, v. articolo 94, paragrafo 1, Regolamento (UE) 2025/327.
[412] M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, cit., 130 e ss.

tale contesto si collocano le numerose iniziative già avviate dagli Stati membri, nonché gli orientamenti attesi dalla Commissione, che dovranno essere emanati entro il 26 marzo 2032[413].

3. La frammentazione del sistema sanzionatorio delineato dallo European Health Data Space.

Il sistema sanzionatorio previsto dal regolamento sullo *European Health Data Space* solleva numerosi interrogativi giuridici, soprattutto a causa delle ampie zone di discrezionalità lasciate agli Stati membri. La scelta del legislatore europeo di non adottare un impianto sanzionatorio chiaro e vincolante ha originato un quadro frammentato, con potenziali ricadute sull'efficacia e sull'uniformità dell'applicazione delle norme.

Per approfondire i punti critici del sistema sanzionatorio è necessario analizzarne il contenuto: l'articolo 63 del Regolamento disciplina le violazioni distinguendo sotto il profilo soggettivo le condotte che riguardano i titolari dei dati sanitari da quelle attribuibili agli utenti. In caso di violazione, saranno gli Organismi responsabili dell'accesso ai dati sanitari a informare tempestivamente l'interessato, concedendogli quattro settimane per presentare osservazioni e, qualora la violazione rientri nell'ambito del GDPR, notificare la questione alle Autorità competenti[414].

Per quanto riguarda gli utenti dei dati sanitari, le sanzioni possono prevedere la revoca dell'autorizzazione all'uso dei dati, l'interruzione del trattamento dei dati senza ritardo e l'esclusione dell'utente dall'accesso ai dati per uso secondario fino a cinque anni, in conformità al diritto nazionale[415].

Per i titolari, invece, qualora ostacolino l'accesso ai dati o non rispettino i termini stabiliti, è prevista l'irrogazione di penalità di mora giornaliere, proporzionate e trasparenti. In caso di reiterate violazioni, possono inoltre

[413] Articolo 63, Regolamento (UE) 2025/327.
[414] Articolo 63, paragrafo 2, Regolamento (UE) 2025/327.
[415] Articolo 63, paragrafo 3, Regolamento (UE) 2025/327.

essere esclusi dalla possibilità di richiedere accesso ai dati per un periodo massimo di cinque anni; durante tale periodo, se previsto, restano comunque tenuti a garantirne la disponibilità[416].

Si tratta di misure fortemente incisive, potenzialmente idonee a generare effetti rilevanti e a porre interrogativi circa la compatibilità con il principio di proporzionalità sancito dal diritto dell'Unione[417].

Un sistema sanzionatorio basato su un modello non completo accentua il rischio di disomogeneità applicativa tra gli Stati membri, che potrebbe essere attenuato mediante l'introduzione di meccanismi di coordinamento volti a favorire un confronto costante tra le Autorità nazionali competenti. In tale prospettiva, il ruolo della Commissione risulta determinante nel promuovere l'armonizzazione delle prassi sanzionatorie.

Le misure adottate devono essere comunicate senza ritardo agli interessati, corredate da una motivazione e da un termine entro cui conformarsi[418]. Esse devono poi essere condivise con gli altri Organismi tramite uno strumento informatico dedicato e possono essere pubblicate sui relativi siti *web*.[419].

Infatti, il Regolamento prevede che la Commissione europea, mediante atti di esecuzione, definisca l'architettura di uno strumento, quale componente dell'infrastruttura DatiSanitari@UE, destinato a gestire in modo trasparente penalità di mora, revoche ed esclusioni[420].

Rimane tuttavia incerta la natura giuridica della notifica effettuata: non è chiaro se essa debba avere valore meramente informativo o se produca effetti vincolanti. Sarebbe pertanto auspicabile un chiarimento volto a stabilire se tale notifica produca effetti giuridici o abbia solo una funzione gestionale.

Il regolamento contempla anche sanzioni amministrative pecuniarie che devono essere effettive, proporzionate e dissuasive; quindi, tali da produrre un impatto concreto, commisurate alla gravità della violazione e idonee a scoraggiare future condotte illecite.

---

[416] Articolo 63, paragrafo 4, Regolamento (UE) 2025/327.
[417] Articolo 5, paragrafo 4, Trattato sull'Unione europea (TUE), GU C 202 del 7.6.2016
[418] Articolo 63, paragrafo 5, Regolamento (UE) 2025/327.
[419] Articolo 63, paragrafo 6, Regolamento (UE) 2025/327.
[420] Articolo 63, paragrafo 7, Regolamento (UE) 2025/327.

L'importo sarà determinato a seconda che si tratti di violazioni meno gravi[421] o più gravi, come la reidentificazione delle persone o l'uso improprio dei dati ottenuti tramite autorizzazione[422]: fino a 10 milioni di euro o al 2% del fatturato annuo per le violazioni meno gravi, e fino a 20 milioni di euro o al 4% per quelle più gravi. L'articolo 64, poi, stabilisce che tali sanzioni potranno essere applicate in aggiunta o in alternativa alle misure correttive previste dall'articolo 63[423].

In questo contesto, gli Organismi responsabili dell'accesso ai dati sanitari sono chiamati a valutare le violazioni considerando una pluralità di fattori, tra cui: *« la natura, la gravità e la durata della violazione; se le sanzioni o le sanzioni amministrative pecuniarie siano state già irrogate da altre autorità competenti per la stessa violazione; il carattere doloso o colposo della violazione; le misure adottate dal titolare dei dati sanitari o dall'utente dei dati sanitari per attenuare il danno causato; il grado di responsabilità dell'utente dei dati sanitari, tenendo conto delle misure tecniche e organizzative da esso messe in atto[424]; eventuali precedenti violazioni pertinenti commesse dal titolare dei dati sanitari o dall'utente dei dati sanitari; il grado di cooperazione del titolare dei dati sanitari o dell'utente dei dati sanitari con l'organismo responsabile dell'accesso ai dati sanitari al fine di porre rimedio alla violazione e attenuarne i possibili*

---

[421] «In *conformità del paragrafo 2 del presente articolo, le violazioni degli obblighi del titolare dei dati sanitari o dell'utente dei dati sanitari a norma dell'articolo 60 e dell'articolo 61, paragrafi 1, 5 e 6, sono soggette a sanzioni amministrative pecuniarie fino a 10 000 000 EUR o, per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*»: Articolo 64, paragrafo 4, Regolamento (UE) 2025/327.

[422] *«5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli utenti dei dati sanitari che trattano i dati sanitari elettronici ottenuti mediante un'autorizzazione ai dati rilasciata a norma dell'articolo 68 per le finalità di cui all'articolo 54; b) gli utenti dei dati sanitari che estraggono dati sanitari elettronici personali da ambienti di trattamento sicuri; c) la reidentificazione o il tentativo di reidentificazione di persone fisiche cui si riferiscono i dati sanitari elettronici ottenuti dall'utente di dati sanitari sulla base di un'autorizzazione ai dati o di una richiesta di dati sanitari a norma dell'articolo 61, paragrafo 3; d) la non conformità alle misure di esecuzione adottate dall'organismo responsabile dell'accesso ai dati sanitari a norma dell'articolo 63, paragrafi 3 e 4.*»: Articolo 64, paragrafo 5, Regolamento (UE) 2025/327.

[423] Articolo 63, paragrafo 3, Regolamento (UE) 2025/327.

[424] Articolo 67, paragrafo 2, lettera g); Articolo 67, paragrafo 4, Regolamento (UE) 2025/327.

effetti negativi; la maniera in cui l'organismo responsabile dell'accesso ai dati sanitari ha preso conoscenza della violazione, in particolare se e in che misura l'utente dei dati sanitari gli ha notificato la violazione; il rispetto delle misure di esecuzione[425] *e che siano stati precedentemente disposte nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto; eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, tramite la violazione*[426]*.».*

L'iter valutativo richiede dunque un'analisi ampia e approfondita che consideri il numero dei soggetti coinvolti, la quantità di dati trattati illecitamente, la durata del trattamento non conforme, la natura episodica o continuativa dell'evento e l'impatto sui diritti degli interessati. Una valutazione uniforme della gravità delle violazioni, basata su casi specifici come l'errata applicazione di tecniche di protezione, accessi non autorizzati o utilizzi difformi dei dati, è fondamentale per evitare una frammentazione normativa che comprometta l'equità sanzionatoria tra Stati membri. Tuttavia, l'assenza di parametri oggettivi e tassativi genera incertezza applicativa.

L'articolo 64 prevede anche che, in presenza di più violazioni commesse in relazione alla stessa richiesta o autorizzazione, la sanzione complessiva non possa superare quella prevista per la violazione più grave[427] , indicando importi limite distinti per violazioni meno gravi e più gravi[428].

Inoltre, se un ordinamento nazionale non prevede sanzioni pecuniarie, esso deve comunque garantire misure equivalenti in termini di efficacia e dissuasione. Le disposizioni nazionali dovranno essere comunicate alla Commissione entro il 26 marzo 2029[429]. Tale impostazione implica che imprese ed enti sanitari operanti in più Stati membri in cui non è previsto un regime sanzionatorio pecuniario, si troveranno a fronteggiare regimi

[425] Articolo 63, paragrafi 3 e 4 Regolamento (UE) 2025/327.
[426] Articolo 64, paragrafo 2, Regolamento (UE) 2025/327.
[427] Articolo 64, paragrafo 3, Regolamento (UE) 2025/327.
[428] Articolo 64, paragrafo 5, Regolamento (UE) 2025/327.
[429] Articolo 64, paragrafo 8, Regolamento (UE) 2025/327.

sanzionatori differenti, con ricadute sulla compliance e sulla gestione del rischio, beneficiando o subendo livelli di tutela diseguali.

L'articolo 64 consente inoltre agli Stati membri di determinare se e in quale misura le sanzioni pecuniarie possano essere applicate ad autorità e agli organismi pubblici nazionali, senza tuttavia escludere i poteri correttivi riconosciuti agli Organismi responsabili dell'accesso ai dati sanitari[430]. Questi ultimi avranno un ruolo rilevante, potendo operare con un ampio margine di discrezionalità grazie alla possibilità di applicare sanzioni in aggiunta o in sostituzione delle misure previste dall'articolo 63, paragrafi 3 e 4. In assenza di criteri interpretativi uniformi, ciò potrebbe dar luogo a una cumulabilità delle sanzioni variabile da Stato a Stato[431].

La facoltà concessa agli Stati di determinare come applicare le sanzioni alle autorità pubbliche e la possibilità per gli Organismi responsabili di modulare le misure correttive rischiano di alimentare una marcata disomogeneità applicativa. La stessa violazione, in mancanza di parametri chiari, potrebbe essere sanzionata in modo diverso a seconda del Paese. E misure incisive come la revoca dell'autorizzazione o l'esclusione fino a cinque anni, pur potenzialmente efficaci, possono risultare arbitrarie in assenza di criteri oggettivi.

Sarebbe pertanto opportuno introdurre linee guida che individuino casi tassativi – ad esempio violazioni intenzionali o particolarmente gravi, come la profilazione illecita – al fine di agevolare l'operato degli Organismi responsabili e garantire un'applicazione più coerente e prevedibile del regolamento nello spazio europeo. L'attuale impostazione, che prevede criteri valutativi prevalentemente indicativi, genera infatti un'elevata incertezza applicativa che potrebbe essere colmata da interventi mirati della Commissione, finalizzati a costruire un sistema sanzionatorio non identico ma almeno coerente tra gli Stati membri.

---

[430] Articolo 64, paragrafo 6, Regolamento (UE) 2025/327.

[431] «*Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di esecuzione di cui all'articolo 63, paragrafi 3 e 4, o in luogo di tali misure*.»: Articolo 64, paragrafo 2, regolamento (UE) 2025/327.

Ad oggi non emerge un meccanismo di coordinamento effettivo e solo una cornice interpretativa uniforme potrebbe garantire un'applicazione armonizzata; obiettivo che appare ancora distante.
All'interno di questo quadro caratterizzato da una struttura normativa esile, costituisce un elemento positivo la previsione di una scadenza, fissata al 26 marzo 2027, per la comunicazione alla Commissione delle norme nazionali adottate: ogni Stato membro deve definire le proprie regole sulle sanzioni da applicare quando qualcuno viola il regolamento. Queste sanzioni riguardano in particolare le violazioni che non sono già coperte dalle misure previste dagli articoli 63 e 64. Tale previsione, tuttavia, risulta insufficiente se non accompagnata da strumenti di controllo e intervento: il regolamento, pur richiedendo la trasmissione delle normative nazionali, non stabilisce modalità di verifica né procedure da seguire in caso di ritardi o incoerenze, confermando un paradosso normativo che potrebbe sfociare in una forma di autosabotaggio[432].

4. (segue) possibili soluzioni per l'armonizzazione del sistema sanzionatorio.

Anche nell'ambito del sistema sanzionatorio emerge la necessità di individuare un compromesso, spesso definito in questo lavoro come "equilibrio", ove si scontrano l'esigenza di uniformità sanzionatoria a livello sovranazionale e il rispetto dell'autonomia normativa all'interno dei singoli Stati.
Il margine di autodeterminazione che il regolamento riconosce agli Stati si manifesta nella possibilità di introdurre ulteriori sanzioni per le violazioni non espressamente previste dal regolamento, confermando così una certa flessibilità normativa. Tuttavia, pur nel rispetto del principio di sussidiarietà, tale facoltà comporta il rischio di una forte frammentazione regolatoria che potrebbe compromettere l'obiettivo di armonizzazione sovranazionale, con il risultato di trattare violazioni di pari gravità in modo disomogeneo tra gli ordinamenti, come già evidenziato in altre sezioni di

[432] Articolo 99, Regolamento (UE) 2025/327.

questo elaborato. L'ampia discrezionalità concessa agli Stati prevale sul tentativo di definire radicati principi comuni di regolamentazione.

Da questa riflessione finale emerge che i regolamenti europei, concepiti come strumenti di armonizzazione normativa, non sempre riescono a realizzare pienamente tale obiettivo: l'apparato sanzionatorio dell'*European Health Data Space* ne è una conferma.

Questo approccio critico dovrebbe, però, considerare anche un'altra prospettiva: intervenire sul sistema sanzionatorio di uno Stato significa addentrarsi in ambiti radicati della sovranità nazionale, caratterizzati da una tradizione punitiva eterogenea. La frammentarietà del sistema sanzionatorio delineato dallo *European Health Data Spac*e è dunque comprensibile, se non inevitabile. Forzare un'uniformità assoluta negli Stati appare, in questo contesto, non solo difficile, ma utopico.

Pur riconoscendo le criticità, è possibile affermare che la costruzione di una convergenza progressiva potrebbe, nel tempo, rappresentare la soluzione più adatta al contesto di riferimento, sostenibile nel lungo periodo.

Alla luce di quanto esposto, una possibile soluzione potrebbe consistere nel rafforzamento delle figure europee di riferimento, come lo stesso Comitato EHDS, cui potrebbe essere attribuito un ruolo più incisivo nel coordinamento interpretativo e operativo. Inoltre, i richiami presenti nel Regolamento sullo Spazio Europeo dei Dati Sanitari al GDPR, in particolare per quanto riguarda l'intervento dell'Autorità garante per la protezione dei dati personali, suggerisce la possibilità di ricorrere, almeno in via transitoria, alle linee guida dell'EDPB in materia sanzionatoria. Tale riferimento potrebbe fungere da strumento di supporto interpretativo, un palliativo, in attesa di un intervento strutturato[433].

Le criticità evidenziate sembrano inoltre convergere verso una soluzione che attribuisce centralità alle linee guida della Commissione europea, in

[433] Sul punto, v. *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 - WP253*. entrate in vigore nel 2018 ed alle L*inee guida 4/2022 sul calcolo dell'ammontare delle sanzioni amministrative ai sensi del GDPR*, adottate a maggio 2023. Entrambe mirano a garantire un'applicazione uniforme, proporzionata ed effettiva delle sanzioni amministrative previste dal GDPR.

particolare di quelle espressamente previste in materia di misure di esecuzione[434].

In tale contesto, sarebbe auspicabile che la Commissione adottasse sin da subito strumenti di *soft law* o orientamenti provvisori, al fine di garantire coerenza applicativa a supporto del ruolo sanzionatorio attribuito agli Organismi coinvolti.

Non a caso, «la ragione del ricorso al *soft law* è spesso proprio la creazione di una disciplina flessibile, in grado di adattarsi alla rapida evoluzione tipica di alcuni settori»[435]. Il ricorso alle Linee guida apre una riflessione sulla loro forza vincolante[436]: sembra condivisibile ammettere che esse «si inseriscono nel quadro più ampio degli strumenti *non-binding* a supporto dell'applicazione uniforme del diritto europeo».

Oltre che a livello europeo[437], anche a livello nazionale, sono diffusi strumenti di *soft law* privi di efficacia vincolante, ma utili a orientare l'applicazione e l'interpretazione delle norme[438].

---

434 Articolo 63, paragrafo 8, Regolamento (UE) 2025/327.Tuttavia, occorre sottolineare che poiché tali linee guida saranno pubblicate solo nel 2032, le misure correttive entreranno in vigore prima della loro adozione, creando un vuoto interpretativo. Occorre dunque chiarire quale disciplina si applichi nell'intervallo temporale e se le linee guida avranno natura vincolante o meramente interpretativa.

435 M. CHIARELLI*, Il soft law e le linee guida nella pandemia, Corti supreme e salute*, 2020, 620 e 621.

436 Antecedentemente alla pandemia da Covid 19, la vincolatività delle linee guida era discussa soprattutto nel diritto amministrativo, con particolare riferimento agli appalti pubblici. Ma con il Decreto-legge n. 33 del 2020 hanno assunto una valenza normativa più ampia: il mancato rispetto delle stesse comporta sanzioni. Per alcuni, questa linea evolutiva dimostra che le stesse linee guida stanno assumendo carattere vincolante assimilabile a quello delle norme regolamentari di attuazione con diretta incidenza sui destinatari. M. CHIARELLI*, Il soft law e le linee guida nella pandemia, Corti supreme e salute*, 2020, 622 ss.

437 In riferimento all'AI Act che prevede una categorizzazione dei "rischi sistemici", intesi come i rischi che possono avere effetti trasversali e ampi sulla società e sull'economia a causa della versatilità e della diffusione delle tecnologie sono state emanate apposite linee guida: Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA), Bruxelles, 29.7.2025 C (2025), 5052 final. Sul punto, v. I. SPEZIALE, *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate, Contratto e impresa,* 2025, 346.

438 «Un esempio emblematico è rappresentato dalle linee guida adottate in ambito medico, quali le raccomandazioni delle società scientifiche, che, sebbene non abbiano valore normativo, sono richiamate dalla giurisprudenza – anche alla luce della l. 8 marzo 2017, n. 24 (c.d. Legge Gelli Bianco) – come parametro per la valutazione della diligenza professionale.»: I. SPEZIALE, *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate, Contratto e impresa,* 2025, 345.

Pertanto, «le Linee guida, collocandosi nell'ambito della *soft law*, non producono effetti giuridici vincolanti, ma contribuiscono a garantire un'applicazione coerente e orientativa, cioè per l'appunto "guidata" del diritto dell'Unione, specie in ambiti tecnici o complessi»[439]. In questa prospettiva, la fiducia non può che essere riposta nell'immediata azione della Commissione europea e nella diligenza degli Stati membri nell'assicurare un'applicazione quanto più possibile uniforme.

[439] I. SPEZIALE, *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate, Contratto e impresa,* cit., 343 e 344.

Conclusioni

L'analisi condotta pone in evidenza le rilevanti carenze strutturali del quadro normativo vigente, tali da prevedere significative difficoltà applicative e un'inevitabile eterogeneità delle prassi all'interno dello *European Health Data Space*. Tali criticità impattano negativamente sulla certezza del diritto e sulla definizione della sua essenza intesa come contenuto normativo di chiara comprensione e applicazione.

Alla luce di tali risultanze, l'impiego di strumenti di *soft law* si configura come una soluzione idonea a colmare le lacune interpretative individuate, tramite l'utilizzo di orientamenti applicativi uniformi che non incidono sul dato normativo primario ma lo supportano, facilitandone l'applicazione.

Tuttavia, l'effettività di tale approccio richiede una responsabilizzazione piena e consapevole di tutti i soggetti partecipi del sistema, da perseguire anche attraverso piani di formazione chiari e sistematici, volti a garantire un'adeguata conoscenza degli obblighi imposti e di un apparato sanzionatorio capace di esercitare un effetto realmente dissuasivo rispetto alla violazione delle prescrizioni.

BIBLIOGRAFIA

- ALPA G., *Code is law: il bilanciamento dei valori e il ruolo del diritto*, in *Contratto e impresa*, 2021;
- AMARÙ G., FAVA A., FOSSI M., MAINARDI F., *La privacy del dato sanitario, Manuale per operatori e professionisti che trattano dati relativi alla salute e per chi vuole saperne di più*, Milano, 2024;
- AYAZ M., PASHA M. F., ALZAHRANI M. Y., BUDIARTO R., STIAWAN D., *The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities,* in *JMIR Medical Informatics*, 2021;
- BERNES A., *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove Leggi Civili Commentate*, 2020;
- CAPILLI G., *Diritto sanitario privato*, Pisa, 2022;
- CAREDDA V., *Campioni biologici e big data: l'evoluzione del consenso,* in *Diritto di famiglia e delle Persone*, 2022;
- CARLUCCIO P., FINOCCHI GHERSI R., *Il caso Ilva: tutela dell'ambiente, bilanciamento tra diritti fondamentali e riserva di giurisdizione*, in *Giornale di diritto amministrativo*, 2013;
- CARRO G., MASATO S., PARLA M. D., *La privacy nella sanità*, Milano, 2018;
- CHIARELLI M., *Il soft law e le linee guida nella pandemia, Corti supreme e salute*, 2020;

- CIANCIMINO M., *Circolazione "secondaria" dei dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in *Diritto di famiglia e delle Persone*, 2022;
- CIANCIMINO M., *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, *I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, in *Quaderni della Rassegna di diritto civile* (a cura di) P. PERLINGIERI, Napoli, 2020
- CIMBALI F., *La Governance della sanità digitale*, 2023, Milano;
- CINQUE A., *Privacy, big-data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute, Nuova Giurisprudenza Civile Commentata,* 2021;
- CORSO S., *Il fascicolo sanitario 2.0 Spunti per una lettura critica*, in *Nuove leggi civili commentate*, 2024;
- CORTI D., *Personalità (diritti della) - La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna*, in *Nuova giur. civ. comm.*, 2022;
- COVINO F., *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in *federalismi.it*, 2021
- D'ONOFRIO P., *Il diritto alla salute tra tradizione costituzionale e innovazione tecnologica*, 2022, Milano;
- DE MIGUEL BERIAIN I., *El uso de datos de salud para investigación biomédica a la luz de la propuesta de reglamento del Parlamento europeo y del Consejo sobre el espacio europeo de datos sanitarios,* in *Revista Jurídica de Castilla y León*, 2023;

- DE SIMONE F., DI MAJO L., RUSSO M., *Le transizioni digitali*, in *Rivista di Diritto dei Media*, 2025.
- FALLETTA P., *Lezioni di diritto pubblico del digitale*, CEDAM, 2024, in *One legale*;
- FANNI S., *Le biobanche di popolazione al vaglio della Suprema Corte di Cassazione: alcune note critiche sull'Ordinanza n. 27325 del 7 ottobre 2021,* in BioLaw *Journal*, 2022;
- FARINA M., *Il cloud computing in ambito sanitario tra security e privacy*, in *Informatica Giuridica*, (a cura di) G. ZICCARDI E P. PIERRI, Milano, 2019.
- FERONI G. C., *Le nuove frontiere della telemedicina. Assetti istituzionali e gestione dei dati*, Mulino, 2024;
- FERONI G. C., *Sanità digitale e assetti istituzionali. Una lettura costituzionalistica*, in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, G. C. FERONI, (a cura di) Bologna, 2022;
- GAMBINO A. M., MAGGIO E., OCCORSIO V., *La riforma del fascicolo sanitario elettronico*, in *Diritto mercato tecnologia*, 2020;
- GAZZARATA R., ALMEIDA J., LINDSKOLD L., CANGIOLI G., GAETA E., FICO G., CHRONAKI C. E., *HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: Scoping review, in International Journal of Medical Informatics*, 2024;

- GHIGLIA A., *La pandemia tra rischi e opportunità,* in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, G. C. FERONI, (a cura di) Bologna, 2022;
- GIARDINA C.C., *Il Data breach in ambito sanitario: l'importanza di una corretta policy per evitare sanzioni da parte del Garante della Privacy,* in *Azienditalia*, 2021;
- GOOSSEN W., LANGFORD L. H., *Exchanging care records using HL7 V3 care provision messages, J Am Med Inform Assoc*, 2014;
- GORASSINI A., *Lo spazio digitale come oggetto di un diritto reale?*, in *Rivista di diritto dei media*, 2, 2018;
- GUARDA P., BINCOLETTO G., *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023;
- HUSSAIN M. A., LANGER S. G., KOHLI M., *Learning HL7 FHIR Using the HAPI FHIR Server and Its Use in Medical Imaging with the SIIM Dataset, Journal of Digital Imaging*, 2018;
- IASELLI M., *Le nuove regole per l'uso primario e secondario dei dati sanitari, Reg. UE 11 febbraio 2025, n. 327 (EHDS),* 2025;
- LEHNE M., SASS J., ESSENWANGER A., LEHNE M., SCHEPERS J. e THUN S., *Why digital medicine depends on interoperability*, in *Digit Med*, 2019;
- LOFARO G., *Dati sanitari e e-Health europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *mediaLaws*, 2022;
- MACRÌ I., *Digitalizzazione, innovazione e sicurezza nella P.A.,* Milano, 2022, in *One legale*;

- MAGGIOLINI M., *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari*, in *Rivista scientifica trimestrale di diritto amministrativo, 2025;*
- MATTEI F., *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie*, in *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, G. C. FERONI (a cura di), Bologna, 2022;
- MELCHIONNA S., *Sanità digitale e innovazione*, in *Privacy e diritto dei dati sanitari*, L. BOLOGNINI, S. ZIPPONI (a cura di), Milano, 2024;
- MORACE PINELLI A., *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in *Nuov. Giur. civ. comm.*, 2025;
- MORELLI A., *I diritti e la rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet,* in *Federalismi.it*, 2015;
- MULLINS C. D., DRUMMOND M. F., *Data Privacy and Health: How Do We Achieve the Right Balance?*, in *Value Heal*th, 2023;
- MUSUMECI A., *Bioetica, Enc. Giur. Treccani*, V, Roma, 1998;
- N. DUEÑAS, P. A. TIFFIN, G. M. FINN, *Understanding gateway to medicine programmes,* in *Clean Teach,* 2021;
- NAVARRO S. N., *Datos sanitarios electrónicos, El espacio europeo de datos sanitarios*, Madrid, 2023;
- PEDRAZZI G., *Il ruolo del Responsabile della protezione dei dati (dpo) nel settore sanitario, the role of data protection officer in the health sector*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario*), 2019;

- PICA N., *Una lettura giuspubblicistica del dibattito civilistico sulla patrimonializzazione dei dati personali,* in *Rivista di diritto amministrativo*, 2021;
- PROSIA L., *Privacy o salute pubblica? Un apparente dilemma*, D. MORANA. S. MABELLINI (a cura di), *L'emergenza pandemica e l'impatto sul diritto pubblico: innovazione e prospettive future*, Cedam, 2022;
- RAMPULLA F. C., RICCIARDI G. C., VENTURI A., *Digitalizzazione delle amministrazioni e accesso ai dati e ai documenti informatici sanitari,* in *Federalismi.it*, 2024;
- RAPISARDA I.*, Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?,* in *Europa e Diritto Privato*, 2021;
- RAZAUSKAS A., *Lo Spazio economico europeo (SEE), la Svizzera e il Nord, Note tematiche sull'Unione europea* in *Note tematiche sull'Unione europea*, 2025;
- RENNA M., *Sicurezza e gestione del rischio nel trattamento dei dati personali, Responsabilità Civile e Previdenza,* 2020;
- RICCI C., RICCI P., *Le biobanche di ricerca: questioni e disciplina research biobanks: questions and regulations*, *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 2018;
- ROSANÒ A., *Tra Neuromanti e pecore elettriche: Metaverso e tutela dei dati personali e della privacy*, *in Rivista di Diritto dei Media*, 2025

- SBORLINI D., *Il* broad consent *come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, *Contratto e impresa*, 2024;
- SCORZA G., *Disposizioni generali,* in *comm. GDPR e normativa privacy*, G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), Milano, 2018;
- SIMONCINI A., LONGO E., *Articolo 32 Costituzione*, R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, I, 2006;
- SPEZIALE I., *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate, Contratto e impresa,* 2025;
- STANZIONE M. G., *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, *Europa e Diritto Privato*, 2016;
- STEFANINI E., *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, 2008, Milano;
- TRINCIA F., *La tutela del diritto alla salute secondo la direttiva 2011/23/UE,* in *Lavoro Diritti Europa,* 2, 2018;
- VILLANI L., *Biobanche e test rivelatori di informazioni genetiche: spunti di riflessione per un nuovo consenso informato*, in *Resp. Civ.*, 2010;
- ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista,* in *Rivista di diritto dei media*, 2, 2018.

INDICE DELLA GIURISPRUDENZA

SITOGRAFIA

Definizione e caratteristiche dello standard HL7 (Health Level 7), in *Informatica e Ingegneria Online*, LAVECCHIA V., (https://vitolavecchia.altervista.org/lo-standard-hl7-health-level-7/);

Electronic cross-border health services, (https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en);

Fascicolo sanitario elettronico (FSE), 2024, Garante per la protezione dei dati personali, (https://www.garanteprivacy.it/temi/fse);

Health Data Access Bodies – Community of Practice in *European Commission*. (Health Data Access Bodies – Community of Practice - Public Health);

Middleware regionali con FSE 2.0 (https://github.com/ministero-salute/it-fse-support/tree/main/doc/middleware-regionale);

Monitoraggio Fascicolo sanitario elettronico effettuato dall'Agenzia per l'Italia Digitale, (https://www.fascicolosanitario.gov.it/monitoraggio);

MyHealth@EU Monitoring Framework (KPIs), number of Countries with Operational NCPeH, (https://experience.arcgis.com/experience/77f459be23e545b48f46a79cfaf19423/page/1_1/);

Realm Italiano, *Specifiche, Guide e White Paper di HL7 Italia*, (Realm Italiano – HL7 Italia);

Regolamento sullo Spazio Europeo dei Dati Sanitari (https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_it);

Specifiche di integrazione ai servizi *gateway* (https://github.com/ministero-salute/it-fse-support/tree/main/doc/integrazione-gateway#1-introduzione).

ALTRI DOCUMENTI CONSULTATI

EHDS Community of Practice for Secondary Use, *Working Arrangements, CoP drafting Task Force*, 22 gennaio 2024;

European Health Data Space, *Kick-off meeting Competent Authorities – Community of Practice in secondary use of health data Meeting Summary,* 25 gennaio 2024;

Joint Action Towards the European Health Data Space – TEHDAS1;

EDPB Work Programme 2024–2025, 8 ottobre 2024;

Deliverable D4.1 Recommendations for establishing Health Data Access Bodies, 27 febbraio 2025.