Politecnico di Milano

Dipartimento di Architettura e Studi Urbani

MASTER UNIVERSITARIO DI II LIVELLO

"DATA PROTECTION OFFICER E TRANSIZIONE DIGITALE (DPOTD)"

A.A. 2024-2025

L'Ecosistema dei Dati Sanitari: analisi di governance, interoperabilità e tutela dei diritti nel contesto digitale europeo

Relatore

Prof. Avv. Giovanni Battista Gallus

Tesi Master

Dott.ssa Paola Cattide

A mio figlio

A te che mi hai accompagnato in questo percorso

ancor prima di venire al mondo

SOMMARIO

PREMESSA

Negli ultimi decenni, il progresso tecnologico ha inciso profondamente sulla società contemporanea, modificando le modalità di comunicazione, l'organizzazione del lavoro e, in maniera significativa, l'approccio alla salute. La digitalizzazione ha investito con forza il settore sanitario, accelerando il cambiamento in particolare a seguito della crisi pandemica da COVID-19, che ha evidenziato l'urgenza di soluzioni digitali a supporto della resilienza e dell'efficienza dei sistemi sanitari.

In questo scenario, la sanità digitale ha assunto un ruolo centrale anche nelle politiche pubbliche italiane ed europee. Il Piano Nazionale di Ripresa e Resilienza (PNRR) ha riconosciuto nella digitalizzazione della sanità uno dei suoi obiettivi strategici, con interventi mirati alla diffusione della telemedicina e all'innovazione infrastrutturale del Servizio Sanitario Nazionale, nell'ambito della Missione 6 dedicata alla salute.

La trasformazione digitale ha accresciuto in modo esponenziale il valore strategico dei dati sanitari, che oggi rappresentano un asset fondamentale per migliorare la qualità dell'assistenza, promuovere la ricerca scientifica e sostenere decisioni di politica sanitaria.

Allo stesso tempo, questi dati, per loro natura altamente sensibili, richiedono forme rafforzate di tutela, in grado di garantire che il trattamento avvenga nel pieno rispetto dei diritti fondamentali della persona.

Il processo di valorizzazione dei dati sanitari si inserisce in un più ampio disegno europeo volto alla creazione di un mercato unico dei dati, considerato una leva essenziale per lo sviluppo economico, sociale e tecnologico. Le istituzioni dell'Unione Europea hanno avviato una serie di iniziative legislative orientate a promuovere il riutilizzo sicuro e responsabile delle informazioni, incentivando la creazione di prodotti e servizi innovativi.

L'emergere di nuovi settori legati all'elaborazione massiva di dati ha reso evidente la necessità di regole chiare, di strumenti tecnici adeguati e di una governance dei dati trasparente e interoperabile.

Tuttavia, se da un lato l'utilizzo consapevole dei dati può portare benefici tangibili in termini di salute pubblica, dall'altro solleva problematiche rilevanti in materia di protezione dei dati personali, soprattutto in assenza di meccanismi di controllo efficaci.

In questo contesto, l'istituzione dello Spazio Europeo dei Dati Sanitari (EHDS) rappresenta un progetto di ampia portata, destinato a ridisegnare la gestione e la condivisione

dei dati sanitari a livello europeo. L'obiettivo è duplice: da un lato migliorare l'accesso e la qualità delle cure attraverso l'uso secondario dei dati, dall'altro garantire che tale utilizzo avvenga nel pieno rispetto della privacy e della sicurezza.

La presente tesi si propone di analizzare le opportunità, le implicazioni e le sfide legate all'adozione dell'EHDS, con particolare attenzione al quadro normativo europeo, agli strumenti di interoperabilità, alla sicurezza dei trattamenti e al ruolo cruciale del Data Protection Officer (DPO), figura centrale nella costruzione di una governance dei dati sanitari conforme al Regolamento (UE) 2016/679 (GDPR).

Il lavoro si articola in quattro capitoli:

- Capitolo I: analizza il contesto europeo delle politiche e strategie sui dati sanitari, soffermandosi sulla Strategia europea dei dati e sul nuovo Regolamento EHDS;
- Capitolo II: esamina il quadro giuridico della protezione dei dati sanitari, con attenzione al rapporto tra GDPR, diritto alla salute e normativa sulla sicurezza informatica (Direttiva NIS 2);
- Capitolo III: descrive l'ecosistema italiano dei dati sanitari, analizzando i principali attori, i flussi informativi e lo sviluppo del Fascicolo Sanitario Elettronico (FSE);
- Capitolo IV: approfondisce le dinamiche di governance e gli strumenti di compliance, con un focus sul ruolo del DPO, sul sistema di gestione della privacy (SGP), sui codici di condotta, le certificazioni e gli audit.

Nel complesso, la digitalizzazione della sanità costituisce un'opportunità strategica per migliorare l'efficacia delle cure e rafforzare l'equità del sistema, ma la sua piena realizzazione richiede una gestione responsabile dei dati, una governance lungimirante e un sistema normativo coerente. Il rispetto della dignità umana, come stabilito dall'articolo 32 della Costituzione italiana, deve restare il principio guida nella progettazione e nell'implementazione della sanità digitale, affinché l'innovazione tecnologica non si traduca in nuove forme di esclusione, ma in un progresso realmente inclusivo e sostenibile.

In qualità di impiegata amministrativa presso la SC Affari Generali e Legali della ASL 3 di Nuoro, quotidianamente mi confronto con le sfide operative della protezione dei dati sanitari in un contesto locale. Questa esperienza professionale ha fornito uno sguardo privilegiato e concreto sulle criticità, sulle *best practice* e sull'applicazione delle normative europee e nazionali nella realtà quotidiana di un'azienda sanitaria territoriale.

CAPITOLO I

Politiche e strategie per i dati sanitari nell'Unione europea

I.1. La Strategia europea dei dati (COM (2020) 66) e i «Common European Data Spaces»

L'Unione Europea ha intrapreso, negli ultimi due decenni, un cammino articolato e progressivo verso la definizione di un ecosistema digitale in cui i dati sono riconosciuti e valorizzati come una risorsa strategica fondamentale. Questo percorso non è stato lineare, ma piuttosto un'evoluzione graduale, caratterizzata da una crescente consapevolezza del potenziale economico e sociale dei dati e dalla necessità di un quadro normativo che ne bilanciasse la libera circolazione con la tutela dei diritti fondamentali.

Le prime mosse significative dell'UE si sono concentrate sull'informazione del settore pubblico (Public Sector Information - PSI). La Direttiva 2003/98/CE[1] ha rappresentato il primo tentativo organico di armonizzare le condizioni per il riutilizzo dei documenti detenuti dalle pubbliche amministrazioni negli Stati membri.

L'idea era che tali informazioni potessero generare valore aggiunto se rese disponibili per nuovi utilizzi da parte di imprese e cittadini, stimolando la creazione di servizi informativi innovativi. Tuttavia, questa prima direttiva presentava un approccio ancora cauto, lasciando ampia discrezionalità agli Stati membri e non imponendo formati specifici o la gratuità generalizzata.

La consapevolezza del potenziale non pienamente sfruttato ha portato a una prima revisione con la Direttiva 2013/37/UE[2], che ha esteso l'ambito di applicazione della normativa includendo, ad esempio, i dati detenuti da musei, biblioteche e archivi, e ha introdotto il principio secondo cui le tariffe per il riutilizzo non dovrebbero, di norma, superare i costi marginali di riproduzione e diffusione. Nonostante questi progressi, la frammentazione persisteva e il pieno potenziale economico dei dati pubblici rimaneva in gran parte inespresso.

Un cambiamento di paradigma più incisivo si è concretizzato con la Direttiva (UE) 2019/1024[3], nota come "Direttiva Open Data". Questa normativa ha segnato un punto di svolta, recependo pienamente i principi dell'Open Data e spingendo per una maggiore

[1]Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.

[2] Direttiva 2013/37/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.

[3]Direttiva 2013/37/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.

apertura e accessibilità. Tra le innovazioni più rilevanti, la Direttiva ha introdotto l'obbligo di rendere disponibili i dati in formati aperti, leggibili meccanicamente e tramite Interfacce di Programmazione delle Applicazioni (API), facilitandone così l'integrazione automatizzata in nuovi prodotti e servizi.

Di particolare rilievo è stata l'introduzione del concetto di "dati dinamici" e, soprattutto, dei "dati ad alto valore" (*High-Value Datasets - HVDs*), ovvero categorie specifiche di dati (come quelli geospaziali, statistici, meteorologici, relativi alle imprese) il cui riutilizzo è associato a benefici particolarmente significativi per la società e l'economia. Per questi HVDs, la Direttiva ha previsto la disponibilità gratuita (salvo eccezioni molto limitate) e condizioni di riutilizzo minime[4].

Questa Direttiva ha agito come un catalizzatore, non solo promuovendo la trasparenza e la partecipazione civica, ma anche stimolando l'innovazione e la crescita nel nascente mercato dei dati. Ha creato, di fatto, il presupposto culturale e normativo per una visione più ambiziosa.

Parallelamente a queste iniziative, l'Unione Europea ha continuato a sviluppare un quadro normativo che favorisse la disponibilità e il riutilizzo di diverse tipologie di dati. In particolare, la Direttiva 2007/2/CE[5] (Direttiva c.d. INSPIRE), entrata in vigore a maggio 2007, ha rappresentato un passo fondamentale per la creazione di un'infrastruttura per l'informazione spaziale nella Comunità Europea.

La Direttiva INSPIRE assume un ruolo strategico nel promuovere un modello comune di gestione dei dati spaziali, in grado di supportare efficacemente i processi decisionali in materia ambientale e territoriale.

Alla base della direttiva si collocano alcuni principi fondamentali. Si afferma, innanzitutto, che i dati devono essere raccolti una sola volta e gestiti nel punto in cui ciò risulta più efficiente, riducendo la duplicazione degli sforzi e razionalizzando le risorse. L'interoperabilità rappresenta un ulteriore cardine: le informazioni devono poter essere combinate e utilizzate congiuntamente, anche se provenienti da fonti diverse, in modo da assicurare continuità e coerenza semantica. Al tempo stesso, si pone l'accento sull'importanza della condivisione delle informazioni tra tutti i livelli di governo, dal locale all'europeo, al fine di rendere le politiche più coordinate ed efficaci. La direttiva insiste inoltre sulla necessità che l'informazione geografica sia disponibile in quantità adeguata, facilmente reperibile e

[4] Agenzia per l'Italia Digitale (AgID), Guida operativa sulle serie di dati di elevato valore. Documento di orientamento per l'attuazione del Regolamento di esecuzione (UE) 2023/138 e delle Linee Guida per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico

[5] Direttiva 2007/2/CE del Parlamento europeo e dal Consiglio, del 14 marzo 2007, che istituisce l'infrastruttura per l'informazione territoriale nell'Unione europea (Inspire)

accessibile in condizioni che ne incentivino l'utilizzo. È essenziale, infine, che l'utente sia in grado di identificare con facilità quali dati siano disponibili, comprenderne la rilevanza per i propri scopi e conoscere le condizioni d'uso.

A livello tecnico, l'infrastruttura si fonda su diversi componenti tra loro integrati. I metadati, innanzitutto, descrivono dataset e servizi associati, facilitandone la ricerca e la comprensione. La dimensione dell'interoperabilità si concretizza attraverso specifiche comuni che riguardano la struttura dei dati, la codifica degli oggetti territoriali, i loro attributi essenziali, le relazioni spaziali e temporali tra entità e la tracciabilità degli aggiornamenti. A ciò si affiancano i servizi di rete, che permettono operazioni come la consultazione online, lo scaricamento, la trasformazione dei dati secondo specifici formati standardizzati e l'esplorazione dei metadati attraverso strumenti di ricerca dedicati. Particolare rilevanza è attribuita alla possibilità di condividere e riutilizzare i dati tra le autorità pubbliche per l'esercizio di funzioni che abbiano impatto sull'ambiente, contribuendo a una governance multilivello più efficiente e trasparente. Il tutto è sostenuto da misure di coordinamento che garantiscono l'effettiva cooperazione tra i diversi attori coinvolti – produttori, fornitori di servizi, utilizzatori e organismi istituzionali – attraverso meccanismi strutturati di governance e monitoraggio.

In Italia, la direttiva è stata recepita con il decreto legislativo 27 gennaio 2010, n. 32[6], che ha dato vita all'Infrastruttura nazionale per l'informazione territoriale e il monitoraggio ambientale, riconosciuta come nodo italiano della più ampia rete europea. L'autorità responsabile per l'attuazione della normativa è il Ministero dell'Ambiente e della Sicurezza Energetica, presso il quale è stato istituito il punto di contatto nazionale, con funzioni di coordinamento e raccordo con la Commissione europea e gli altri Stati membri. Nell'ambito dell'implementazione italiana riveste un ruolo centrale il Geoportale Nazionale, previsto dall'articolo 8 del decreto. Esso rappresenta il principale punto di accesso ai servizi previsti dalla direttiva per il territorio nazionale, fornendo strumenti per la consultazione e l'interazione con i dati territoriali e ambientali disponibili, nonché l'interfaccia verso i cataloghi informativi delle autorità pubbliche e la rete SINAnet, la quale integra i sistemi informativi ambientali delle principali istituzioni nazionali. Il Geoportale, dunque, svolge una funzione abilitante per la fruizione trasparente e integrata dei dati territoriali in Italia, contribuendo a garantire l'allineamento dell'infrastruttura nazionale ai requisiti comunitari.

[6] D.lgs. 27 gennaio 2010, n. 32 di "*Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunita' europea (INSPIRE)"*

Successivamente, il Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, ha affrontato la questione della libera circolazione dei dati non personali nell'Unione europea. Il Regolamento FFD riguarda soltanto i dati non personali, ossia quei dati diversi dai dati personali definiti dall'art. 4 punto 1[7] del Regolamento UE n. 2016/679. Si applica, nello specifico, a dati non personali gestiti come servizio o per uso interno da parte di soggetti stabiliti nell'UE, rafforzando la certezza del quadro giuridico per le imprese e favorendo un mercato dei dati più fluido e competitivo.

Questo regolamento è stato fondamentale per superare le barriere normative che ostacolavano la mobilità dei dati non personali (come dati di processo, industriali o generati da macchine) tra gli Stati membri. Infatti, l'obiettivo era quello di garantire che i dati non personali potessero essere archiviati ed elaborati in qualsiasi parte dell'UE, senza restrizioni ingiustificate basate sulla loro localizzazione geografica. Questo ha favorito lo sviluppo di servizi *cloud* e l'economia dei dati, riconoscendo il valore economico e sociale di queste informazioni e completando il quadro normativo sui dati personali fornito dal GDPR.

Un altro elemento previsto dal regolamento è l'istituzione di un meccanismo di cooperazione tra autorità nazionali e Commissione, volto a garantire l'effettività del divieto di localizzazione e a consentire l'accesso ai dati per scopi ispettivi o regolatori. È stato introdotto anche il diritto alla portabilità dei dati, con l'incentivo a sviluppare codici di condotta autonomi al fine di prevedere formati aperti, trasparenza contrattuale, informazione minima chiara e sistemi di certificazione per facilitare il cambio del fornitore.

Il rapporto tra il Regolamento 2018/1807 e il GDPR è stato oggetto di linee guida specifiche nel 2019[8]:

Nel suo insieme, l'azione normativa dell'UE su INSPIRE e sul Regolamento 2018/1807 rappresentano basi giuridiche e operative già consolidate, che ne anticipano alcune logiche fondative dell'ecosistema dei dati europeo. Questi strumenti, infatti, operano in sinergia: INSPIRE assicura la qualità e l'interoperabilità tecnica dei dati ambientali, mentre il Regolamento 2018/1807 garantisce la libertà e l'efficienza nella circolazione delle stesse risorse digitali, rendendo possibile l'innovazione, la sfida competitiva e l'integrazione transnazionale nel pieno rispetto dei diritti e dei valori europei.

[7] "*qualsiasi informazione riguardante una persona fisica identificata o identificabile, il c.d. interessato*"

[8] COM(2019) 250 final, Comunicazione della Commissione al Parlamento Europeo e al Consiglio "*Empty, guidance on the Regulation on a framework for the free flow of non-personal data in the European Union"*

È in questo contesto di crescente maturità che nel mese di febbraio 2020 la Commissione Europea ha presentato la Comunicazione "Una Strategia europea per i dati"[9].

Questo documento è il frutto di una visione trasversale che ha posto le basi per la creazione di un vero e proprio mercato unico dei dati nell'UE.

La Strategia ha riconosciuto i dati come elemento chiave per affrontare le grandi sfide sociali, in particolar modo la salute e il cambiamento climatico.

Al centro della stessa vi è l'ambizione di creare "Spazi Comuni Europei di Dati" (*Common European Data Spaces*) in settori strategici, tra cui la sanità, l'industria, l'energia, l'agricoltura, la finanza, la mobilità, il Green Deal e le competenze.

Questi spazi vengono concepiti come l'unione di ecosistemi interoperabili, in cui i dati possano fluire in modo sicuro e affidabile, nel rispetto dei valori europei di riservatezza e sicurezza.

La Strategia ha posto l'accento sulla necessità di un quadro di *governance* chiaro, di investimenti in infrastrutture e tecnologie e sullo sviluppo di competenze digitali, al fine di posizionare l'Europa come leader globale nell'economia dei dati.

Uno degli assunti centrali su cui si fonda l'impianto strategico è la centralità dell'individuo.

In linea con il dettato dell'art. 8 della Carta dei diritti fondamentali dell'UE[10] e con il Regolamento Generale sulla Protezione dei Dati (GDPR), la strategia pone esplicitamente "*al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europee*"[11]. Ciò implica che ogni innovazione, ogni forma di riutilizzo o scambio di dati personali deve avvenire nel pieno rispetto della dignità umana, della privacy e dell'autonomia individuale. L'ambizione europea è quella di costruire un "mercato unico dei dati" che sia fondato sulla fiducia, condizione essenziale affinché i cittadini decidano di condividere i propri dati in un contesto percepito come sicuro e controllabile[12].

L'affidabilità del sistema normativo europeo in materia di dati è quindi non solo un vincolo etico, ma anche una condizione abilitante per lo sviluppo tecnologico. I cittadini

---

[9] Risoluzione del Parlamento europeo del 25 marzo 2021 su una strategia europea per i dati (2020/2217(INI))

[10] *"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".*

[11] COM(2020) 66 final. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. *Una strategia europea per i dati.*

[12] PAVEL V., *Rethinking data and rebalancing digital power. Report training data,* in Ada Lovelace Institute. https://www.adalovelaceinstitute.org/report/rethinking-data/

daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati.

In questa prospettiva, il GDPR non è visto come un ostacolo all'innovazione, bensì come un *framework* di garanzia capace di generare valore attraverso la trasparenza, la responsabilizzazione e la tracciabilità.

Un secondo asse fondamentale della strategia riguarda il ruolo dei dati come "carburante" per l'intelligenza artificiale. I sistemi di IA, in particolare quelli basati sull'apprendimento automatico (*machine learning),* necessitano di grandi quantità di dati per essere addestrati, testati e ottimizzati. Inoltre, occorre evidenziare come il modello europeo di *governance* dei dati e dell'intelligenza artificiale si distingua per il suo approccio basato sul rischio e sulla responsabilità etica.

Come evidenziato dalla Commissione Europea[13], il valore dei dati risiede non solo nella loro disponibilità quantitativa, ma anche nella loro qualità, accessibilità e interoperabilità. In tal senso, i dati costituiscono la materia prima dell'economia digitale e assumono una funzione abilitante in ogni settore, dalla sanità all'energia, dalla mobilità all'agricoltura.

La sfida, tuttavia, non si esaurisce nella disponibilità del dato, ma si estende alla sua capacità di garantire un accesso equo, controllato e trasparente da parte di attori pubblici e privati.

Pertanto, la Strategia europea per i dati propone un modello di sovranità digitale inclusiva, in cui il valore dei dati non è solo economico, ma anche sociale, culturale ed etico.

Da ciò si evince come la Strategia del 2020 abbia gettato le fondamenta per un intenso periodo di attività legislativa, volto a tradurre la visione in norme concrete.

I principali pilastri di questo nuovo contesto normativo sono:

- il Regolamento sulla Governance dei Dati (Data Governance Act - DGA), (UE) 2022/868[14]: entrato in vigore il 24 settembre 2023, con la piena applicabilità ha fatto da impalcatura al funzionamento dello Spazio comune europeo dei dati, già prefigurato nella Comunicazione della Commissione UE del 19 febbraio 2020 e richiamato nel considerando 2 del DGA[15]. È il primo atto legislativo chiave derivante dalla Strategia. Il suo scopo

[13] Cfr. COM(2020) 66 final. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. *Una strategia europea per i dati*

[14] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)

[15] CATALETTA A., *Data Governance Act ora applicativo: così cambia l'economia digitale*, in Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/la-data-economy-alla-prova-del-data-governance-act-lo-scenario/

principale è accrescere la fiducia nella condivisione dei dati e facilitare la disponibilità di più dati per il riutilizzo. Ha introdotto meccanismi per il riutilizzo di determinate categorie di dati del settore pubblico che non possono essere resi disponibili come open data. Di fondamentale importanza è la creazione di un regime per i fornitori di servizi di intermediazione dei dati, che agiscono come terze parti neutrali e affidabili per facilitare la condivisione dei dati tra detentori e utenti. Inoltre, il DGA promuove il "*data altruism*"[16], incoraggiando la donazione volontaria di dati per finalità di interesse generale, inclusa la ricerca scientifica e il miglioramento della sanità pubblica, attraverso un meccanismo di registrazione dei dati e un modulo di consenso europeo.

Il Regolamento sui Dati (Data Act), (UE) 2023/2854[17] si concentra sulla giustizia e sull'equità nell'economia dei dati, in particolare per quanto riguarda i dati generati dall'Internet of Things (IoT). Il Data Act stabilisce norme per l'utilizzazione dei dati generati dai prodotti connessi e a quali condizioni. Gli utenti di dispositivi connessi (siano essi individui o aziende) avranno il diritto di accedere ai dati che generano e di condividerli con terze parti di loro scelta. Inoltre, mira a prevenire clausole contrattuali abusive imposte dalle grandi aziende alle PMI, a consentire agli enti pubblici di accedere ai dati del settore privato in situazioni di eccezionale necessità (come le emergenze sanitarie), e a facilitare il passaggio tra fornitori di servizi *cloud*, promuovendo l'interoperabilità. Per il settore sanitario, ciò implica una maggiore trasparenza e controllo sui dati generati da dispositivi medici connessi e app per il benessere.

Parallelamente alle norme citate precedentemente, la Commissione ha iniziato a proporre regolamenti specifici per i singoli Spazi Comuni Europei di Dati.

Il Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS), (UE) 2025/327[18], è il primo e più emblematico di questi. È stato concepito dalla Commissione europea come un ecosistema digitale dedicato al settore sanitario, fondato su regole, standard tecnici,

[16] Pone le basi per garantire che cittadini e imprese, nel momento in cui decidono volontariamente di mettere a disposizione i propri dati per scopi collettivi, possano farlo affidandosi a enti ritenuti affidabili e coerenti con i valori e i principi fondamentali dell'Unione Europea. Le realtà che rendono disponibili dati rilevanti con finalità di interesse generale potranno ottenere la qualifica di "organizzazioni riconosciute per l'altruismo dei dati" all'interno dell'Unione. Tali enti dovranno operare senza fini di lucro, assicurare elevati livelli di trasparenza e offrire tutele concrete a favore delle persone fisiche e giuridiche che condividono i propri dati. Saranno inoltre tenuti al rispetto di un quadro normativo specifico, che comprenderà obblighi informativi, requisiti tecnici e di sicurezza, modalità di comunicazione strutturate e linee guida sull'interoperabilità. Questo insieme di regole verrà definito dalla Commissione Europea in stretta collaborazione con le organizzazioni per l'altruismo dei dati e con altri stakeholder di rilievo.

[17] Unione Europea, *Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 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 (regolamento sui dati).*

[18] Unione Europea**,** *Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847*

pratiche condivise, infrastrutture comuni e un quadro di governance armonizzato a livello dell'Unione[19]. L'obiettivo è quello di creare un ambiente sicuro, interoperabile e affidabile per la gestione e la condivisione dei dati sanitari, nel pieno rispetto dei diritti fondamentali dei cittadini europei.

Esso mira a creare un ecosistema specifico, facilitando l'accesso dei cittadini ai propri dati sanitari a livello transfrontaliero (uso primario) e promuovendo l'uso secondario di dati sanitari anonimizzati o pseudonimizzati per ricerca, innovazione e policy making. L'EHDS si basa sui principi e sui meccanismi stabiliti dal GDPR, dal DGA e dal Data Act, adattandoli alle specificità e alla sensibilità dei dati sanitari.

Da ciò si evince come il percorso dell'UE sia stato caratterizzato da una progressiva estensione dell'ambito di applicazione e da un approfondimento degli strumenti normativi: dalla semplice promozione del riutilizzo dell'informazione del settore pubblico si è passati a una visione strategica per un mercato unico dei dati, supportata da un pacchetto legislativo robusto che mira a bilanciare l'innovazione e la crescita economica con la protezione dei diritti fondamentali e la promozione di un'economia dei dati equa, trasparente e basata sulla fiducia.

L'EHDS si configura come un elemento chiave per la costruzione di un'Unione europea della salute più forte e resiliente[20]. A tal fine, il Regolamento stabilisce regole comuni, standard, infrastrutture e un quadro di governance per facilitare l'accesso ai dati sanitari elettronici. Tuttavia, la piena realizzazione dell'EHDS richiederà un avanzamento significativo nel processo di digitalizzazione dei sistemi sanitari nazionali, nonché il raggiungimento di un'elevata interoperabilità tra gli Stati membri.

I.2. Il Regolamento (UE) 2025/327 sull'European Health Data Space (EHDS): obiettivi, principi e ambiti di applicazione

Il 5 marzo 2025 è stata una data significativa per il panorama sanitario europeo, segnata dalla pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea del Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS). Questo regolamento si inserisce in un

[19] Consiglio Dell'Unione Europea, *Spazio europeo dei dati sanitari: il Consiglio adotta un nuovo regolamento che migliora l'accesso transfrontaliero ai dati sanitari dell'UE*, Comunicato stampa del 14 gennaio 2025, https://www.consilium.europa.eu/it/press/press-releases/2025/01/21/european-health-data-space-council-adopts-new-regulation-improving-cross-border-access-to-eu-health-data/

[20] LICHERI G., *EHDS ed EDS: al via la rivoluzione dei dati sanitari in Europa e in Italia,* I-Com.it, http/www.i-com.it/2025/03/14/ehds-ed-eds-al-via-la-rivoluzione-dei-dati-sanitari-in-europa-e-in-italia/, 14 marzo 2025.

contesto più ampio, quello della Strategia europea per i dati promossa dalla Commissione Europea a partire dal febbraio 2020. L'obiettivo di tale Strategia è la creazione di un mercato unico dei dati, realizzato attraverso la costituzione di spazi comuni europei di dati in settori strategici e di fondamentale importanza per la società. Tra questi settori, la sanità assume un ruolo preminente, accanto ad altri quali la pubblica amministrazione, l'agricoltura, l'industria manifatturiera, l'energia, la mobilità e la finanza. L'obiettivo primario è l'eliminazione delle barriere che attualmente ostacolano la condivisione e lo scambio di dati sanitari tra i diversi Stati europei[21].

Il regolamento sull'EHDS trova il suo fondamento giuridico negli articoli 16 e 114 del Trattato sul Funzionamento dell'UE (TFUE)[22]. Coerentemente con quanto stabilito dall'articolo 168 TFUE, che definisce le competenze dell'UE in materia di sanità pubblica, il regolamento persegue la creazione di un quadro giuridico chiaro ed efficiente per il riutilizzo dei dati sanitari personali. Tale riutilizzo è inteso per una varietà di finalità, che spaziano dalla ricerca e l'innovazione alla definizione delle politiche e alle attività normative, fino ad altre finalità specificate nel Considerando 53 del regolamento stesso [23].

L'uso primario dei dati riguarda l'impiego delle informazioni sanitarie al fine di fornire cure appropriate, sicure e tempestive al paziente, anche in ambito transfrontaliero. Ciò implica che i cittadini dell'Unione Europea possano accedere ai propri dati clinici e condividerli con professionisti sanitari in altri Stati membri, garantendo la continuità assistenziale anche al di fuori del proprio Paese di residenza[24]. L'obiettivo è quello di agevolare l'erogazione dell'assistenza sanitaria in ambito transfrontaliero, facilitando la mobilità dei pazienti tra gli Stati membri e promuovendo l'accesso equo e tempestivo alle prestazioni sanitarie nei diversi sistemi nazionali.

---

[21] MAGGIOLINI M., *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitar*i, Rivista scientifica trimestrale di diritto amministrativo (Classe A), Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico".

[22] Versione consolidata Del Trattato Sull'unione Europea e del Trattato sul funzionamento dell'Unione Europea (2012/C 326/01),

[23] "*I dati sanitari elettronici usati per uso secondario possono apportare grandi benefici per la società. È opportuno incoraggiare l'utilizzo di dati e prove reali, tra cui le informazioni sui risultati comunicati dai pazienti, per scopi normativi e strategici basati su dati probanti, nonché per la ricerca, la valutazione delle tecnologie sanitarie e gli obiettivi clinici. I dati e le prove reali sono in grado di integrare i dati sanitari attualmente resi disponibili. Per conseguire tale obiettivo, è importante che le serie di dati messe a disposizione per l'uso secondario a norma del presente regolamento siano quanto più complete possibile. Il presente regolamento fornisce le garanzie necessarie per attenuare determinati rischi connessi al conseguimento di tali benefici. L'uso secondario di dati sanitari elettronici si basa su dati pseudonimizzati o anonimizzati, al fine di impedire l'identificazione degli interessati*", Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

[24] COM(2022) 197 final, Commissione Europea, Proposta di Regolamento sull' Health Data Space, art. 3.

Questo uso è finalizzato alla presa in carico individuale del paziente, ed è regolato da principi di necessità, proporzionalità e sicurezza nell'accesso ai dati, soprattutto in relazione al rispetto del GDPR.

L'uso secondario, invece, riguarda l'impiego dei dati sanitari raccolti in ambito assistenziale per finalità diverse dalla cura diretta, quali la ricerca scientifica, l'elaborazione di politiche pubbliche, l'innovazione tecnologica, la farmacovigilanza e l'analisi epidemiologica. Tali utilizzi sono regolati da un sistema di accesso controllato e sono resi disponibili solo per progetti ritenuti di interesse pubblico o conformi a criteri scientifici ed etici rigorosi[25].

Il legislatore europeo fa rientrare le finalità di ricerca scientifica tra quelle di interesse pubblico per le quali, ai sensi del considerando 50 del GDPR, pur permanendo il diritto di obiezione, il consenso non è più necessario quale condizione legittimante[26].

Un ambito particolarmente rilevante di applicazione dell'uso secondario è rappresentato dall'impiego dei dati per l'addestramento, il test e la validazione di algoritmi di intelligenza artificiale nel settore sanitario. L'uso dei dati per training di sistemi AI è espressamente contemplato tra le finalità ammesse[27], purché non siano utilizzati per sviluppare prodotti o servizi che possano arrecare danno alle persone o essere impiegati per scopi discriminatori o commerciali non autorizzati. È inoltre richiesto che i dati vengano trattati in ambienti sicuri, siano pseudonimizzati o anonimizzati, e che l'accesso sia concesso solo a soggetti accreditati, previa valutazione del progetto e dei suoi impatti etico-giuridici.

Tale utilizzo è anche strettamente connesso con le disposizioni del Regolamento sull'intelligenza artificiale che classifica i sistemi di AI destinati a fini sanitari come ad alto rischio, imponendo obblighi rigorosi in termini di qualità dei dati, trasparenza, sorveglianza post-marketing e tracciabilità[28].

Il Regolamento EHDS prevede il diritto dei pazienti di opporsi al trattamento dei propri dati sanitari elettronici per uso secondario (diritto di *opt-out*). Tuttavia, consente comunque l'accesso a questi dati per scopi di interesse pubblico, sviluppo di politiche sanitarie, nonché per finalità statistiche e di ricerca condotte nel pubblico interesse.

---

[25] Commissione Europea, EHDS Impact Assessment, SWD(2022) 101 final, p. 22

[26] Il GDPR riconosce che, in determinati contesti, come quello della ricerca medica o biomedica, la tutela dell'interesse collettivo può giustificare il trattamento dei dati personali anche senza il previo consenso dell'interessato, purché siano rispettati rigorosi criteri di sicurezza, anonimizzazione (ove possibile) e proporzionalità. Questo principio consente di agevolare l'attività scientifica e promuovere l'innovazione nel rispetto dei diritti fondamentali, bilanciando le esigenze del progresso con la protezione dei dati personali.

[27] L'art. Articolo 53, Finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario prevede l'utilizzo per "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"

[28] Regolamento (UE) 2024/1084 sull'intelligenza artificiale (AI Act), art. 6 e Allegato III, punto 5.

Inoltre, prevede l'istituzione in ogni Stato membro di organismi responsabili dell'accesso ai dati sanitari (Health Data Access Body – HDAB)[29]. Questi enti del settore pubblico, esistenti o di nuova costituzione, consentiranno un accesso prevedibile e semplificato ai dati sanitari elettronici e garantiranno un elevato livello di trasparenza, responsabilizzazione e sicurezza nel trattamento di tali dati per gli usi secondari legittimati dall'art. 53.

Gli HDAB, in presenza dei requisiti prescritti dagli articoli 68, 69 e 73 del regolamento, forniscono ai soggetti richiedenti (data user) l'accesso ai dati sanitari per usi secondari, in forma anonima o pseudonimizzata (considerando 72).

Il regolamento EHDS istituisce un meccanismo unico (regole, requisiti e infrastrutture comuni) per accedere ai dati sanitari elettronici personali e non personali per l'uso secondario.

Tra le infrastrutture dedicate occorre ricordare MyHealth@EU[30] per l'uso primario e HealthData@EU per l'uso secondario[31].

Il Parlamento europeo, con gli emendamenti approvati il 13 dicembre 2023, ha ulteriormente rafforzato il testo, introducendo importanti garanzie a tutela della privacy e del consenso informato[32].

Gli Stati membri, con riferimento al trattamento dei dati personali per uso secondario, potranno interpretare diversamente il diritto di obiezione del soggetto interessato (il paziente) riguardo alle categorie di dati e alle finalità di uso secondario cui essi possono essere destinati[33].

Il legislatore europeo si è dunque espresso con una *lex specialis* per disciplinare il riutilizzo dei dati sanitari elettronici (personali e non), che prevarrà sulle norme generali nazionali.

---

[29] Commissione Europea, Health Data Access Bodies – Community of Practice

[30] *"L'infrastruttura di servizi digitali per l'assistenza sanitaria online (eHealth) garantisce la continuità delle cure mediche ai cittadini europei che viaggiano all'interno dell'UE. Ciò offre ai paesi dell'UE la possibilità di scambiarsi dati sanitari in modo sicuro, efficiente e interoperabile. I cittadini possono facilmente riconoscere la disponibilità dei servizi con il marchio "MyHealth@EU".*

[31] GORGONI G, *EHDS, "verso l'unione sanitaria europea: cos'è, le cautele, i vantaggi per i cittadini"*, in Agenda Digitale, https://www.agendadigitale.eu/sanita/ehds-verso-lunione-sanitaria-europea-cose-le-cautele-i-vantaggi-per-i-cittadini/

[32] Parlamento Europeo, Risoluzione del Parlamento europeo del 22 novembre 2023 sui progetti del Parlamento europeo intesi a modificare i trattati (2022/2051(INL)

[33] ARCURI M.A., *EHDS ed EDS: la tutela della salute migliora attraverso la digitalizzazione della sanità e la ricerca scientifica. L'uso secondario dei dati sanitari personali. Il Regolamento (UE) 2025/327 e l'Ecosistema nazionale di dati sanitari*, Agenda Digitale, https://www.altalex.com/documents/news/2025/05/05/ehds-eds-tutela-salute-migliora-attraverso-digitalizzazione-sanita-ricerca-scientifica, 05 maggio 2025

Al fine di consentire una transizione ordinata e un'adeguata preparazione da parte degli attori coinvolti, l'applicazione del presente regolamento è strutturata in fasi progressive, secondo la seguente articolazione temporale:

- dal 26 marzo 2027 entreranno in vigore le disposizioni relative all'accesso primario e all'infrastruttura di base, con l'obbligo per gli Stati membri di attivare i servizi di accesso digitali, come portali online o app per i pazienti, la designazione delle autorità sanitarie digitali nazionali e degli organismi di accesso ai dati (HDAB);
- dal 26 marzo 2029 troveranno applicazione le disposizioni relative alle categorie prioritarie di dati sanitari elettronici di cui all'articolo 14, paragrafo 1, lettere a), b) e c), e i sistemi di cartelle cliniche elettroniche: profili sanitari sintetici dei pazienti, prescrizioni elettroniche e dispensazioni elettroniche;
- dal 26 marzo 2031 entreranno in vigore le disposizioni relative a categorie di dati più "sensibili" o complesse, quali esami diagnostici per immagini (radiografie, TAC, ecc.), risultati degli esami medici (analisi del sangue, ecc.) e lettere di dimissione.

In definitiva, l'istituzione dell'EHDS rappresenta un punto di svolta nel panorama della sanità digitale europea, delineando un modello in cui il paziente assume un ruolo centrale e proattivo. Attraverso la garanzia di un accesso facilitato, di una tutela rigorosa e di un controllo effettivo sui propri dati sanitari elettronici, promuove l'autodeterminazione informativa, consentendo al singolo cittadino di esercitare una piena facoltà decisionale in merito alla circolazione e all'utilizzo delle informazioni che lo riguardano.

CAPITOLO II

Il quadro giuridico di protezione e sicurezza dei dati sanitari

II.1. Il GDPR quale *Lex generalis*

Il Regolamento generale per la protezione dei dati personali 679/2016 (*General Data Protection Regulation* o GDPR) è la principale normativa europea in materia di protezione dei dati personali, entrato in vigore a maggio 2018. Può essere considerato il risultato di un lungo percorso di riflessione e consolidamento normativo sviluppatosi in Europa nel corso degli ultimi due decenni.

Il GDPR persegue un obiettivo: armonizzare le leggi in materia di riservatezza in tutta Europa, assicurando protezione dei dati di tutti i cittadini, dando a tutte le organizzazioni gli strumenti necessari per assicurare la riservatezza di tali dati.

Più che proporre un cambiamento radicale, si configura come uno strumento che mira a riordinare e attualizzare l'impianto normativo precedente alla luce delle nuove sfide poste dalla società digitale.

In tale ottica, alcune delle sue disposizioni non introducono principi radicalmente nuovi, ma rielaborano concetti già presenti nella normativa antecedente, rendendoli più coerenti, accessibili e adatti al mutato contesto tecnologico e giuridico.

È composto da 99 articoli divisi in 11 Capi.

Attribuisce diritti a tutti gli individui, a prescindere dalla loro nazionalità o dalla loro residenza, ponendo obblighi in capo ad aziende, autorità o enti pubblici.

Il Regolamento nasce per la tutela del diritto alla protezione dei dati personali inteso come diritto fondamentale delle persone fisiche. In quest'ottica il principio cardine del regolamento è costituito dall'autodeterminazione informativa, una condizione necessaria per il libero sviluppo della personalità del cittadino e anche un elemento essenziale di una società democratica.

Il Regolamento definisce il dato personale come qualsiasi elemento informativo riferibile a una persona fisica identificata o identificabile. Rientrano in questa categoria non solo il nome o un numero identificativo, ma anche dati relativi alla localizzazione, identificativi online, oppure elementi inerenti alle caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali di un individuo (art. 4 par. 1, n. 1).

Tale definizione, sebbene formalizzata nel GDPR, non costituisce una novità assoluta: essa riprende in modo quasi letterale quanto già previsto dalla Direttiva 95/46/CE

all'art. 2, mostrando così un intento di continuità normativa piuttosto che di innovazione[34].

Occorre tuttavia distinguere tra le nozioni di "dato" e di "informazione", spesso erroneamente sovrapposte. Mentre il dato personale rappresenta un elemento grezzo, cioè la materia prima, l'informazione costituisce il risultato di una sua elaborazione, organizzazione o interpretazione. Si può dunque affermare che il dato è il contenitore dal quale si può estrarre un'informazione, ma non le coincide integralmente[35].

L'evoluzione della società digitale ha determinato un ampliamento esponenziale delle categorie di dati suscettibili di trattamento, introducendo nuove forme di tracciabilità e profilazione. Di conseguenza, il legislatore europeo ha inteso rafforzare le garanzie offerte agli individui, ponendo particolare attenzione alla ampiezza della nozione di "dato personale", resa evidente anche dalla scelta lessicale di includere "qualsiasi informazione", espressione che sottolinea la volontà di offrire una tutela ad ampio spettro[36].

Tra le numerose definizioni introdotte dal Regolamento (UE) 2016/679, all'articolo 4 troviamo la specificazione di tre tipologie di dati che rientrano nella più ampia categoria di dati personali: i dati genetici, i dati biometrici e i dati relativi alla salute.

I dati genetici sono definiti come quei dati personali che contengono informazioni sulle caratteristiche ereditarie o acquisite di un individuo, ottenute in particolare attraverso l'analisi di campioni biologici, e che offrono elementi univoci per comprendere aspetti della fisiologia o dello stato di salute della persona interessata. I dati biometrici, invece, comprendono tutte le informazioni personali derivanti da trattamenti tecnici specifici — come l'analisi dell'immagine facciale o delle impronte digitali — che consentono l'identificazione certa della persona. Infine, i dati relativi alla salute comprendono informazioni personali che riguardano la condizione fisica o mentale di un individuo, incluse quelle derivanti dalla fruizione di servizi sanitari.

Queste categorie, pur essendo formalmente distinte, presentano una notevole sovrapposizione, essendo tutte strettamente legate alla dimensione corporea e sanitaria dell'individuo. Tuttavia, a differenza della generica nozione di "dato personale", molto ampia e comprensiva, queste tipologie rappresentano dei sottogruppi particolari, per i quali il Regolamento prevede tutele rafforzate in virtù della loro sensibilità intrinseca[37].

---

[34] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, art. 2, lett. a).
[35] RODOTÀ S., *Tecnologie e diritti*, Bologna, Il Mulino, 1995, pp. 75-78.
[36] PIZZETTI F., *Privacy e il nuovo diritto europeo dei dati personali*, Giappichelli, 2016, pp. 21-23.
[37] MANTELERO A., *Il nuovo Regolamento europeo sulla protezione dei dati personali*, Giappichelli, 2017.

Nel quadro normativo precedente, ossia sotto la Direttiva 95/46/CE e il Codice Privacy italiano, le categorie erano tre: dati personali, dati sensibili e dati giudiziari. I dati genetici e sanitari rientravano all'interno dei dati sensibili, che godevano di un regime di protezione più rigoroso. Con l'introduzione del GDPR, il legislatore ha preferito un approccio unificato, accorpando tutte le tipologie sotto l'unica etichetta di "dati personali", pur mantenendo distinzioni funzionali attraverso l'espressione "categorie particolari di dati personali".

L'articolo 4 del Regolamento definisce anche il concetto di trattamento, che rappresenta il cuore operativo della disciplina. Esso viene descritto come qualsiasi operazione effettuata sui dati personali, sia essa eseguita con strumenti automatizzati o manuali. Le operazioni elencate spaziano dalla raccolta, registrazione, organizzazione, conservazione, fino alla cancellazione o distruzione. Ne deriva che anche un'unica attività tra quelle menzionate, se applicata a dati riferibili a una persona fisica, è sufficiente per configurare un "trattamento" ai sensi del GDPR.

Non è dunque necessario che vi sia un sistema informatico o una banca dati formalmente costituita: anche un singolo foglio cartaceo contenente dati personali, se sottoposto ad una delle operazioni indicate, rientra nella disciplina di tutela. Il focus della norma non è infatti sulla riservatezza in senso stretto, ma piuttosto sul controllo e sull'utilizzo delle informazioni personali, indipendentemente dal supporto utilizzato per il trattamento.

Nel passare all'analisi dei soggetti coinvolti nel trattamento dei dati personali, si nota subito un'assenza rilevante: il Regolamento (UE) 2016/679, pur fornendo un elenco dettagliato di definizioni, non include esplicitamente quella di "interessato".

Tuttavia, questa figura fondamentale può essere dedotta dalla definizione di "dato personale" contenuta nell'art. 4, par. 1 del GDPR.

L'interessato è, innanzitutto, una persona fisica, mai una persona giuridica, identificata o identificabile attraverso uno o più elementi specifici, che possono includere dati anagrafici (come il nome), informazioni geografiche (ubicazione), oppure identificativi più moderni e sensibili come quelli biometrici o genetici.

Tali elementi sono ampiamente commentati nel considerando n. 30[38] del Regolamento, dove si riconosce che l'identificazione può avvenire anche per via indiretta, attraverso la combinazione di dati diversi.

[38] "*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con*

È importante sottolineare che la qualifica di interessato si estingue con la morte della persona, ma il Regolamento lascia ai singoli Stati membri la facoltà di adottare normative interne relative al trattamento dei dati delle persone decedute. Discorso analogo riguarda i nascituri, il cui trattamento può anch'esso essere oggetto di regolamentazione nazionale.

Dal punto di vista giuridico, l'interessato rappresenta il soggetto passivo del trattamento, ossia colui i cui dati sono oggetto delle operazioni regolate dal GDPR.

Tuttavia, il suo ruolo non è affatto passivo in senso stretto: egli è anche portatore di diritti soggettivi e può attivamente determinare la liceità del trattamento mediante il rilascio del consenso, che rappresenta uno dei principali fondamenti di legittimità previsti dall'art. 6 del Regolamento.

In questo modo, l'interessato assume una posizione centrale all'interno del sistema della protezione dei dati personali, diventando il perno attorno al quale ruotano le garanzie, i diritti e i meccanismi di controllo sul trattamento delle informazioni che lo riguardano.

Il GDPR distingue, invece, gli altri soggetti in funzione del ruolo che svolgono nel trattamento dei dati: "Titolare" del trattamento, "Responsabile" del trattamento, "Autorizzato" al trattamento, "Responsabile" della protezione dei dati.

Il "Titolare" del trattamento è la persona fisica o giuridica che decide finalità e mezzi del trattamento. Il "Responsabile" del trattamento è la persona fisica o giuridica che tratta i dati per conto del titolare. La nomina a Responsabile deve essere fatta tramite contratto o altro atto giuridico, che definisca quali dati vengono trattati, per quanto tempo e con quali finalità. L' "Autorizzato" al trattamento è colui che ha accesso ai dati e può trattarli solo se ha ricevuto specifiche istruzioni da parte del titolare o del responsabile del trattamento e sostituisce la figura dell'incaricato prevista nella legislazione precedente.

Il Responsabile della protezione dati (DPO) è una figura chiave per garantire la conformità alle normative sulla protezione dei dati personali. La sua nomina, sebbene obbligatoria in alcuni casi, è spesso vantaggiosa per le organizzazioni di tutti i tipi, in quanto contribuisce a migliorare la gestione dei dati personali, ridurre il rischio di sanzioni e aumentare la fiducia degli interessati.

Il Regolamento (UE) 2016/679, in continuità con quanto già previsto dalla Direttiva 95/46/CE, dedica attenzione anche alla definizione della figura del "terzo". Secondo quanto stabilito dall'art. 4, par. 10 del GDPR, non sono considerati terzi: l'interessato, il

*identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarl*e".

titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile. Da questa definizione si deduce che il terzo è qualsiasi soggetto estraneo al perimetro dei soggetti legittimati a trattare dati personali. In altre parole, si tratta di una figura che non intrattiene alcuna relazione diretta o funzionale con il trattamento stesso, né è coinvolta nelle attività che vi fanno capo.

Occorre, poi, distinguere il terzo dalla figura del "destinatario", con cui potrebbe sembrare condividere alcune caratteristiche. Tuttavia, mentre il destinatario è colui al quale vengono effettivamente comunicati i dati, in virtù di un rapporto giuridico con il titolare o il responsabile, il terzo non riceve alcuna comunicazione né partecipa, anche indirettamente, al trattamento.

Un ulteriore soggetto da menzionare è il "rappresentante", definito all'art. 4, par. 17 del Regolamento. Si tratta di una persona fisica o giuridica stabilita all'interno dell'Unione Europea, che viene formalmente designata dal titolare o dal responsabile del trattamento, conformemente all'art. 27 GDPR. Il rappresentante agisce per conto del titolare o del responsabile e svolge i compiti ad essi attribuiti dal Regolamento, assumendo un ruolo di interfaccia con le autorità di controllo e con gli interessati quando i titolari non sono stabiliti nell'Unione.

Il Capo II del Regolamento (UE) 2016/679, comprendente gli articoli da 5 a 11, è interamente dedicato alla definizione dei principi generali che regolano il trattamento dei dati personali.

L'articolo 5 del Regolamento, intitolato "Principi applicabili al trattamento dei dati personali", individua sei principi cardine che ogni trattamento deve rispettare. Essi rappresentano il nucleo etico e giuridico della disciplina sulla protezione dei dati e possono essere così sintetizzati:

- liceità, correttezza e trasparenza: il trattamento deve essere svolto nel rispetto della legalità, in modo equo nei confronti dell'interessato e con la massima trasparenza;
- limitazione della finalità: i dati devono essere raccolti per scopi specifici, espliciti e legittimi, e non devono essere successivamente utilizzati per finalità incompatibili. Tuttavia, è ammesso un trattamento ulteriore per finalità di archiviazione nel pubblico interesse, ricerca scientifica o storica e per fini statistici, purché siano adottate misure adeguate a tutelare i diritti dell'interessato;

- minimizzazione dei dati: i dati trattati devono essere pertinenti, adeguati e limitati a quanto necessario rispetto agli scopi per cui sono raccolti. Questo principio invita alla riduzione del dato all'essenziale, in un'ottica di contenimento del rischio e di rispetto della proporzionalità;
- esattezza: i dati personali devono essere accurati e, se necessario, aggiornati. È compito del titolare adottare misure ragionevoli per correggere o eliminare tempestivamente eventuali inesattezze. Ciò tutela l'interessato da decisioni o trattamenti basati su informazioni errate;
- limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati solo per il tempo strettamente necessario al raggiungimento delle finalità previste. È prevista la possibilità di una conservazione più prolungata a fini di archiviazione, ricerca o statistica, sempre nel rispetto delle misure di garanzia richieste dal Regolamento;
- integrità e riservatezza: il trattamento deve avvenire in modo da assicurare la sicurezza dei dati, evitando accessi non autorizzati, perdite accidentali, distruzioni o danni. Il Regolamento impone l'adozione di misure tecniche e organizzative appropriate, come la pseudonimizzazione, la crittografia o sistemi di controllo degli accessi.

A questi principi si affianca il principio di responsabilizzazione (*accountability*), espresso al paragrafo 2 dell'articolo 5. Esso stabilisce che il titolare del trattamento non solo è tenuto a garantire il rispetto dei principi sopra elencati, ma deve anche essere in grado di dimostrarlo concretamente. Ciò implica una gestione documentale accurata, una valutazione preventiva dei rischi e l'adozione di politiche interne coerenti con i requisiti normativi.

Il Capo III del Regolamento (UE) 2016/679, che si estende dagli articoli 12 a 23, disciplina in modo dettagliato i diritti riconosciuti all'interessato nel contesto del trattamento dei dati personali. Alcuni di questi diritti derivano dalla normativa previgente, ma con un livello di precisione e garanzia rafforzato; altri, invece, rappresentano novità introdotte dal GDPR, in linea con l'evoluzione tecnologica e con la crescente importanza del controllo dei dati nella società digitale. L'interessato, cioè la persona fisica cui si riferiscono i dati personali, non è più un soggetto meramente passivo, bensì un protagonista attivo del trattamento, titolare di un ampio ventaglio di facoltà giuridiche finalizzate a garantire

trasparenza, accesso, rettifica e limitazione del trattamento dei propri dati. Queste prerogative non necessitano di particolari formalità per essere esercitate, riflettendo un principio di effettività e accessibilità del diritto.

Come evidenziato in dottrina, il controllo sulle proprie informazioni personali costituisce uno strumento fondamentale attraverso cui l'individuo costruisce e protegge la propria identità. In tale ottica, i diritti dell'interessato si configurano come manifestazioni concrete del principio di autodeterminazione informativa, ovvero della possibilità per ciascun individuo di decidere come, quando e in che misura le proprie informazioni possano essere utilizzate da terzi, anche in assenza di violazioni manifeste[39].

L'articolo 12 ribadisce e amplia il diritto all'informazione, che impone al titolare del trattamento precisi doveri informativi nei confronti dell'interessato, al fine di garantirne una piena consapevolezza. Tra le principali previsioni si segnalano:

- l'obbligo di fornire le informazioni relative al trattamento in modo chiaro, conciso, trasparente e facilmente comprensibile, utilizzando un linguaggio semplice e accessibile anche ai non esperti;
- la necessità che tali informazioni siano trasmesse per iscritto o tramite strumenti elettronici; l'uso della forma orale è ammesso solo su richiesta dell'interessato e previo accertamento della sua identità;
- in caso di diniego di una richiesta, il titolare deve motivare la decisione entro un mese, informando altresì l'interessato circa la possibilità di proporre reclamo all'autorità di controllo o ricorso giurisdizionale;
- se le richieste sono considerate manifestamente infondate o eccessive, il titolare può rifiutarsi di procedere o imporre un contributo spese, ma in tal caso ha l'onere di dimostrare l'abusività della richiesta.

Gli articoli 13 e 14 specificano quali informazioni devono essere fornite rispettivamente: quando i dati personali sono raccolti direttamente presso l'interessato (art. 13); quando invece i dati non sono stati ottenuti direttamente presso lo stesso (art. 14).

Con l'articolo 15 viene consacrato il diritto dell'interessato di ottenere conferma dal titolare circa l'esistenza di un trattamento relativo ai propri dati personali. Qualora tale trattamento sia in corso, l'interessato ha diritto a:

- accedere ai dati oggetto di trattamento;
- ricevere una serie di informazioni aggiuntive, indicate puntualmente nel paragrafo 1 dell'articolo, tra cui le finalità del trattamento, le categorie di dati, i destinatari,

[39] RODOTÀ S., "*Intervista su privacy e libertà*", a cura di Paolo Conti, 2005.

i criteri di conservazione, e l'esistenza di diritti ulteriori come rettifica o cancellazione.

L'articolo 16 introduce espressamente il diritto alla rettifica, che consente all'interessato di chiedere la correzione di dati inesatti o l'integrazione di dati incompleti che lo riguardano, senza ingiustificato ritardo. Rispetto alla disciplina pregressa, questo diritto viene reso autonomo e operativo, assumendo una valenza fondamentale per la tutela dell'esattezza e affidabilità del dato.

Tra le innovazioni più significative introdotte dal Regolamento (UE) 2016/679, un ruolo di primo piano è occupato dall'articolo 17, che sancisce il diritto alla cancellazione dei dati personali, noto anche con l'espressione "diritto all'oblio".

Questa disposizione rappresenta un punto di svolta nell'evoluzione del diritto alla protezione dei dati, poiché riconosce all'interessato la facoltà di ottenere dal titolare del trattamento la cancellazione dei propri dati personali, a determinate condizioni. Tale diritto può essere esercitato senza ingiustificato ritardo, e risponde all'esigenza di garantire all'individuo la possibilità di far "scomparire" tracce digitali che non siano più necessarie, pertinenti o conformi alla liceità del trattamento.

L'articolo 17 prevede che il titolare debba procedere alla cancellazione dei dati personali nei casi in cui:

- i dati non siano più necessari rispetto alle finalità per le quali erano stati raccolti o trattati;
- l'interessato revochi il consenso su cui si fondava il trattamento, e non sussista altro fondamento giuridico;
- l'interessato si opponga al trattamento ai sensi dell'articolo 21 e non prevalgano motivi legittimi per procedere al trattamento;
- i dati siano stati trattati illecitamente;
- i dati debbano essere cancellati per adempiere a un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;
- i dati siano stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori, in conformità all'art. 8 del Regolamento.

Accanto a queste ipotesi, l'articolo 17 stabilisce anche i limiti e le eccezioni al diritto all'oblio. In particolare, la cancellazione può non essere imposta nei casi in cui il trattamento sia necessario, ad esempio, per:

- esercitare il diritto alla libertà di espressione e di informazione;
- adempiere a un obbligo legale o svolgere un compito di interesse pubblico;

- motivi di interesse pubblico nel settore sanitario;
- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto all'oblio, già delineato nella giurisprudenza della Corte di Giustizia dell'Unione Europea (in particolare con la sentenza *Google Spain*, C-131/12)[40], trova dunque nel GDPR un riconoscimento normativo esplicito, e riflette l'esigenza, sempre più avvertita nell'era digitale, di garantire un controllo pieno e attivo sulla propria identità digitale.

L'articolo 18 stabilisce i casi specifici in cui l'interessato può esercitare il diritto alla limitazione del trattamento dei propri dati personali. Questo diritto consente all'interessato di richiedere al titolare che il trattamento dei suoi dati venga temporaneamente sospeso, pur rimanendo i dati stessi conservati. Ciò implica che il titolare del trattamento, una volta ricevuta la richiesta dell'interessato, debba identificare e segregare i dati in questione, affinché non possano essere oggetto di ulteriori operazioni, salvo che non ricorrano eccezioni espressamente previste dalla legge.

Questo diritto è strettamente collegato a quanto disciplinato anche nell'articolo 19 del GDPR, che impone al titolare di informare i destinatari ai quali i dati sono stati comunicati, circa l'eventuale limitazione, rettifica o cancellazione.

Il Considerando 67[41] del Regolamento approfondisce le modalità pratiche di applicazione della limitazione, offrendo esempi di come i dati possano essere limitati.

Una delle innovazioni più rilevanti è senza dubbio il cosiddetto diritto alla portabilità dei dati, previsto dall'articolo 20. Questo diritto rappresenta un significativo passo avanti nel riconoscimento e nella tutela dell'autonomia dell'interessato rispetto alle informazioni personali che lo riguardano.

In termini semplici, il diritto alla portabilità consente all'individuo di ottenere, dal titolare del trattamento, i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivi automatici.

---

[40] La sentenza Google Spain (C-131/12), pronunciata dalla Corte di Giustizia dell'Unione Europea l'8 maggio 2014, è una decisione storica in materia di protezione dei dati personali e ha posto le basi per il cosiddetto "diritto all'oblio".

[41] *"Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato".*

Il principio della portabilità riflette una concezione della persona come soggetto attivo nella sfera digitale, titolare di diritti che si estendono alla possibilità di disporre dei propri dati in modo libero e consapevole[42].

A questa visione si collega, in modo complementare, quanto previsto dal Data Act, che rappresenta una novità significativa nella regolazione europea dei dati. Infatti, il regolamento estende il concetto di portabilità anche ai dati non personali, come quelli generati automaticamente da dispositivi intelligenti, da macchinari industriali o da sistemi connessi *all'Internet of Things*.

Il Regolamento introduce, inoltre, diritti di accesso e riutilizzo dei dati generati dall'utilizzatore, anche se non si tratta di dati personali in senso stretto, favorendo così una distribuzione più equa del valore dei dati tra produttori, fornitori di servizi e utenti[43].

L'elemento di continuità tra il GDPR e il Data Act è dato dall'enfasi posta sulla centralità dell'utente nella circolazione e nel controllo dei dati, siano essi personali o non personali, delineando un modello europeo di governance dei dati fondato su trasparenza, accesso e interoperabilità, che mira a riequilibrare i rapporti tra grandi piattaforme e soggetti individuali, promuovendo un'economia digitale più inclusiva e competitiva[44].

In definitiva, la portabilità assume nel diritto europeo una funzione strategica: essa non solo tutela l'individuo come soggetto di diritti, ma funge anche da leva per l'innovazione e la concorrenza, incentivando la mobilità dei dati e l'emergere di nuovi operatori digitali.

L'articolo 22, paragrafo 1, del Regolamento UE 2016/679 sancisce un principio fondamentale, ovvero il diritto dell'interessato a non essere sottoposto a decisioni basate esclusivamente su un trattamento automatizzato, inclusa la profilazione, che possano avere effetti giuridici vincolanti o incidere significativamente sulla sua persona. Questa norma mira a tutelare l'individuo da processi decisionali automatizzati che potrebbero influenzare in modo rilevante la sua vita, senza che vi sia un intervento umano di verifica o possibilità di contestazione.

Il paragrafo 2, tuttavia, prevede alcune eccezioni a questa regola generale, specificando in quali casi il divieto di decisione automatizzata non si applica. A complemento, i paragrafi 3 e 4 chiariscono rispettivamente quando è necessario un intervento umano nel

---

[42] RODOTÀ S., *Il diritto di avere diritti*. Roma-Bari: Laterza, 2015

[43] BASSAN F., *Dati non personali e regolazione europea: Il Data Act tra accesso e competitività*. in Diritto dell'economia digitale, n. 2. 2023

[44] Viola G*, Governare i dati in Europa. Dal GDPR al Data Act: nuove sfide normative*. Milano: Giuffrè Francis Lefebvre. 2024

processo decisionale e quali categorie di diritti possono essere escluse in particolari circostanze.

Tale disciplina si intreccia profondamente con quanto stabilito dal recente AI Act[45], adottato dall'Unione Europea nel 2024, che istituisce un quadro giuridico orizzontale per l'impiego dei sistemi di intelligenza artificiale. L'AI Act classifica i sistemi di IA secondo livelli di rischio, imponendo requisiti rigorosi per i sistemi ad "alto rischio", tra cui rientrano anche quelli impiegati nei settori dell'occupazione, dell'istruzione, del credito e dei servizi pubblici[27]. In questi ambiti, la presenza di decisioni automatizzate con impatto diretto sulle persone richiama direttamente le garanzie previste dall'art. 22 GDPR. Non a caso, il regolamento sull'IA richiede, tra le altre cose, trasparenza, supervisione umana e auditabilità dei sistemi impiegati: principi che trovano un riscontro normativo proprio nella logica dell'art. 22, che non vieta tout court l'automazione decisionale, ma ne condiziona l'ammissibilità al rispetto di precise garanzie procedurali.

La relazione tra GDPR e AI Act è da intendersi in termini di complementarietà funzionale: mentre il primo garantisce una tutela centrata sui diritti individuali e sul controllo dei dati personali, il secondo previene i rischi sistemici associati all'utilizzo di IA in contesti ad alto impatto, configurandosi come uno strumento di regolazione ex ante[46].

In questo senso, l'art. 22 del GDPR non è solo un baluardo contro gli abusi della profilazione automatizzata, ma diventa anche un punto di raccordo tra la protezione dei dati personali e la governance responsabile dell'intelligenza artificiale, come delineata dal nuovo regolamento europeo.

Nell'ambito dello stesso Capo III, la Sezione 4 introduce anche l'articolo 21, dedicato al diritto di opposizione. Questo diritto attribuisce all'interessato la facoltà di opporsi al trattamento dei propri dati personali per motivi legati alla sua situazione particolare. Tale opposizione è applicabile quando il trattamento si fonda su specifiche basi giuridiche, come l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri, oppure il perseguimento di un legittimo interesse del titolare del trattamento o di terzi. In queste situazioni, a fronte dell'opposizione dell'interessato, il titolare deve cessare il trattamento a meno che non dimostri l'esistenza di motivi legittimi e prevalenti che giustifichino la prosecuzione, o che il trattamento sia necessario per l'accertamento o la difesa di un diritto in sede giudiziaria.

[45] Parlamento Europeo e Consiglio dell'UE. Regolamento sull'intelligenza artificiale (AI Act), artt. 5–6

[46] SARTOR G., *Etica e diritto dell'intelligenza artificiale. Dal GDPR all'AI Act.* Bologna: Il Mulino.2023

Infine, il Capo III si conclude con l'articolo 23, che contempla la possibilità di limitare, tramite norme legislative, l'esercizio dei diritti dell'interessato finora descritti. Tale limitazione è ammessa solo se rispetta l'essenza dei diritti e delle libertà fondamentali e rappresenta una misura necessaria e proporzionata in una società democratica per tutelare interessi rilevanti come la sicurezza nazionale, la difesa, la sicurezza pubblica, nonché per la prevenzione e il perseguimento dei reati, tra le altre situazioni tassativamente elencate.

Il Capo IV del Regolamento GDPR è dedicato alle figure del titolare del trattamento e del responsabile del trattamento, sottolineando come, accanto al rafforzamento dei diritti dell'interessato, crescano in modo significativo anche gli obblighi e le responsabilità di chi gestisce i dati personali. Le definizioni di queste due figure si trovano rispettivamente negli articoli 24 e 28.

L'articolo 24 introduce il principio di responsabilità (accountability), secondo cui il titolare del trattamento deve adottare misure tecniche e organizzative adeguate per garantire e dimostrare la conformità al Regolamento, tenendo conto della natura, del contesto e dei rischi del trattamento. Tali misure devono essere regolarmente aggiornate e, se opportuno, accompagnate da politiche interne specifiche sulla protezione dei dati. L'adesione a codici di condotta o a meccanismi di certificazione può rappresentare una prova del rispetto di questi obblighi.

L'articolo 28 disciplina invece il ruolo del responsabile del trattamento, che agisce per conto del titolare e deve garantire adeguate garanzie tecniche e organizzative per la tutela dei dati personali. Il responsabile non può delegare a terzi senza autorizzazione del titolare, e ogni trattamento affidato deve essere regolato da un contratto o atto giuridico che definisca chiaramente i compiti, le responsabilità e le caratteristiche del trattamento.

Il principio di accountability rappresenta una novità rispetto alla precedente Direttiva 95/46/CE e costituisce oggi un approccio pratico alla privacy: consente alle organizzazioni di misurare e dimostrare la propria responsabilità nella gestione dei dati. Questo principio trova particolare applicazione nel campo della sicurezza informatica, dove garantisce la tracciabilità e il controllo delle azioni degli utenti all'interno dei sistemi, grazie a sistemi di autenticazione e audit.

In sintesi, il Capo IV rafforza il quadro normativo imponendo ai titolari e responsabili del trattamento un ruolo attivo e consapevole nella protezione dei dati, con strumenti concreti per garantire trasparenza e responsabilità.

Gli articoli successivi del Regolamento dettagliano una serie di obblighi specifici che titolare e responsabile del trattamento devono rispettare. Tra questi spiccano: l'obbligo di

sicurezza, l'obbligo di effettuare valutazioni d'impatto sulla protezione dei dati (Data Protection Impact Assessment), la notifica tempestiva di eventuali violazioni di dati personali alle autorità competenti, la tenuta di registri aggiornati sulle attività di trattamento, l'adesione a codici di condotta o meccanismi di certificazione, nonché la nomina di un Responsabile della Protezione dei Dati (Data Protection Officer).

In particolare, il Regolamento introduce due principi fondamentali per la gestione responsabile dei dati, espressi all'articolo 25: la "*privacy by design*" e la "*privacy by default*".

Questi concetti impongono al titolare del trattamento di integrare la protezione dei dati personali fin dalle fasi iniziali della progettazione di sistemi e processi (privacy by design), e di garantire che, in modo predefinito, vengano adottate le impostazioni più rigorose in termini di riservatezza e sicurezza (privacy by default).

Tali principi rappresentano un'importante evoluzione normativa, che sposta l'attenzione dalla mera conformità a un approccio proattivo e preventivo nella tutela della privacy.

Dal Capo V in poi, il Regolamento 2016/679 si fa ancora più concreto e incisivo nel delineare le modalità con cui deve avvenire la protezione dei dati personali, focalizzandosi su temi di grande rilievo nella realtà attuale, dove le informazioni viaggiano con estrema facilità oltre i confini nazionali e dove la tecnologia spinge costantemente verso nuove frontiere.

Uno degli aspetti più rilevanti è senza dubbio il trasferimento dei dati verso paesi terzi o organizzazioni internazionali. Il Regolamento stabilisce che tali trasferimenti possono avvenire solo se viene garantito un livello di protezione adeguato, analogo a quello previsto dalla normativa europea. Questa norma non è semplicemente un vincolo burocratico, ma rappresenta una tutela essenziale per gli interessati, impedendo che i dati personali finiscano in Paesi dove la tutela della privacy è carente o inesistente[47]. In tal senso, il Regolamento promuove una vera e propria "esportazione" del modello europeo di protezione, imponendo ai titolari e responsabili del trattamento di adottare misure stringenti per assicurare la riservatezza e l'integrità dei dati anche oltre i confini dell'UE[48]. Quando

[47] Art. 44-50 Regolamento UE 2016/679: si evidenzia come il trasferimento di dati all'estero costituisca un tema cruciale nella protezione internazionale della privacy (Kuner, C. "Transborder Data Flows and Data Privacy Law," Oxford University Press, 2013).

[48] Si tratta di una vera e propria "esportazione" dei principi GDPR, che ha un impatto anche nelle strategie aziendali globali (Schrems II, Corte di Giustizia UE, C-311/18).

non è possibile riconoscere l'adeguatezza di un Paese terzo, il Regolamento prevede l'adozione di strumenti giuridici come clausole contrattuali standard o norme vincolanti d'impresa, che vincolano i soggetti coinvolti a rispettare rigorosamente i diritti degli interessati.

Proseguendo, nel Capo VI emerge il ruolo fondamentale delle Autorità di controllo nazionali, che sono i veri pilastri del sistema di protezione. Queste Autorità non si limitano a un ruolo passivo o meramente consultivo, ma dispongono di ampi poteri ispettivi, sanzionatori e decisionali. La loro indipendenza è garantita da disposizioni che ne impediscono l'influenza da parte di soggetti politici o economici, assicurando così che la protezione dei dati sia sempre perseguita con imparzialità e rigore. In un contesto europeo così ampio, la collaborazione e il coordinamento tra queste Autorità, disciplinati nel Capo VII, sono determinanti per evitare discrepanze e per assicurare un'applicazione uniforme del Regolamento in tutti gli Stati membri, proteggendo l'interessato in modo omogeneo e coerente, qualunque sia il paese in cui si trovi.

Il GDPR non si limita a dettare regole astratte, ma prevede strumenti concreti di tutela giuridica nel Capo VIII. Gli interessati, infatti, hanno diritto a ricorrere alle Autorità di controllo, ma anche ai Tribunali nazionali, con la possibilità di azioni rapide e semplificate. Questo aspetto è particolarmente importante, perché riconosce un potere effettivo al singolo cittadino, rendendo la protezione dei dati non solo un diritto formale ma un diritto sostanziale e concretamente esercitabile. Inoltre, le sanzioni previste dal Regolamento sono significative e dissuasive: si parla di multe che possono raggiungere fino al 4% del fatturato annuo globale dell'impresa o 20 milioni di euro, a seconda di quale valore sia superiore.

Questo sistema sanzionatorio sottolinea con forza come la privacy non possa essere trascurata o relegata a un ruolo marginale, ma debba essere centrale nell'organizzazione aziendale e istituzionale.

Non da ultimo, il GDPR si dimostra anche un testo dinamico, capace di adattarsi al cambiamento tecnologico e normativo. Attraverso gli atti delegati e di esecuzione, l'Unione Europea può aggiornare le norme in modo rapido e coordinato, garantendo che la regolamentazione resti al passo con le innovazioni digitali, senza perdere di vista i principi fondamentali di tutela.

In sintesi, il Regolamento configura un sistema robusto, articolato e coerente, in cui la protezione dei dati personali è assicurata da regole chiare, da autorità forti, da strumenti di tutela efficaci e da un meccanismo sanzionatorio rigoroso.

L'obiettivo è duplice: da un lato rafforzare i diritti degli interessati, garantendo loro un controllo reale e consapevole sui propri dati; dall'altro, responsabilizzare chi tratta dati, affinché la privacy non sia mai un optional ma un valore da rispettare in ogni fase del trattamento.

Questa impostazione rappresenta un vero e proprio cambio di paradigma nella cultura della protezione dei dati, ponendo la persona al centro di un sistema giuridico che tutela la sua dignità e libertà nell'era digitale.

II.2. Protezione della privacy e diritto alla salute: un equilibrio normativo delicato

La crescente digitalizzazione del settore sanitario ha aperto nuove prospettive per la gestione dei dati relativi alla salute, offrendo strumenti efficaci per migliorare la diagnosi, la cura e la ricerca medica.

Tuttavia, questo progresso si accompagna a sfide significative riguardo alla protezione della privacy e alla sicurezza dei dati personali, elementi essenziali per tutelare i diritti fondamentali degli individui.

In questo contesto, il Regolamento (UE) 2016/679 (GDPR) e il Codice Privacy aggiornato dal D.lgs. 101/2018 hanno introdotto un quadro normativo rigoroso e articolato, che impone obblighi stringenti a chi tratta dati sanitari e al contempo garantisce diritti robusti agli interessati.

Per questi dati, le tutele sono ulteriormente rafforzate e le condizioni per il trattamento sono molto più restrittive, proprio perché il rischio di lesione della dignità e dei diritti della persona è particolarmente elevato. Questo aspetto riflette un'idea di protezione della privacy non solo come tutela formale, ma come salvaguardia della persona nella sua interezza.

Infatti, il trattamento dei dati personali necessita particolari attenzioni per il rispetto dei diritti fondamentali dei soggetti interessati, al fine di evitare pregiudizi e lesione della tutela della persona, in particolare in ambito sanitario, dove il Diritto alla Privacy si incontra con diritti costituzionali di pari importanza, quali la salute pubblica o il diritto alla salute.

La definizione di dati sanitari, nonché la delimitazione del loro ambito applicativo ha dato luogo a contrasti interpretativi. A tal proposito, infatti, prima dell'entrata in vigore

del Regolamento una parte della dottrina ha sottolineato come manchi effettivamente una definizione di dato sanitario, riconducendo tale scelta alla finalità di «lasciare una libertà al singolo operatore pratico di individuare di volta in volta quale informazione possa essere idonea a fornire indicazioni sullo stato di salute di un soggetto... guardando probabilmente più che al contenuto delle informazioni, alle finalità cui essa è destinata[49]».

Altra parte della dottrina, invece, si interroga se debbano intendersi alla stregua dei dati sanitari solo quelli che rivelano una malattia o anche le informazioni dalle quali emerge che un problema di salute possa comunque sussistere[50].

Il Consiglio d'Europa ha considerato i dati inerenti alla salute «tutti i dati a carattere personale relativi alla salute di una persona. Si riferisce egualmente ai dati aventi un collegamento stretto e manifesto con la salute così come i dati genetici[51]», dando quindi una lettura piuttosto restrittiva.

L'entrata in vigore del Regolamento UE 679/2016 ha elevato al rango di definizione la categoria dei dati sanitari. Infatti, l'art. 4 par. 1, n. 15 del Regolamento definisce i «dati relativi alla salute» come «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». L'art. 9 del Regolamento pone un divieto al trattamento dei dati relativi alla salute: «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». Tuttavia, tale divieto non è assoluto in quanto, in presenza di una serie di condizioni di legittimità, espressamente elencate nel testo normativo, la preclusione non opera.

Le condizioni di legittimità riguardano determinate condizioni, tra cui il consenso esplicito dell'interessato, la necessità per un interesse pubblico rilevante, o la necessità per la tutela della salute o degli interessi vitali dell'interessato. Appare chiaro come il legislatore europeo lasci agli Stati membri margine di intervento, introducendo norme che i legislatori nazionali recepiscono in conformità alle proprie tradizioni giuridiche, consentendo loro

[49] CAGGIA F., *Il trattamento dei dati dei dati sanitari sulla salute, con particolare riferimento all'ambito sanitario,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, p. 407-410.
[50] FINOCCHIARO G., *Privacy e protezione dei dati*, p. 62-63.
[51] Si rinviene traccia dell'applicazione nazionale di tale disposizione negli artt. 22 e 23 della Legge.

di introdurre ulteriori condizioni per il trattamento dei dati genetici, biometrici o relativi alla salute[52].

La violazione della privacy e della sicurezza dei dati può assumere diverse forme e manifestarsi attraverso modalità eterogenee, che includono, ad esempio, accessi non autorizzati, trattamenti illeciti, perdita di integrità o disponibilità delle informazioni, nonché usi impropri rispetto alle finalità dichiarate.

Il paziente interessato dal trattamento oggi è esposto a numerosi rischi rispetto al passato in un'ottica di digitalizzazione ed esposizione quotidiana dei dati personali a queste fonti di rischio informatico. A tale scopo, si è reso necessario intervenire per intensificare il controllo e la tracciabilità di tali informazioni, in modo da prevenire e minimizzare gli eventuali danni conseguenti alla violazione della privacy, in particolare nell'ambito sanitario.

L'uso sistematico di dati clinici da parte di dispositivi elettromedicali sia nella prospettiva clinica che a fini di ricerca necessita una regolamentazione più chiara e precisa sulle modalità di trattamento e sulle misure di sicurezza per i dati sanitari.

Il professionista sanitario non deve richiedere il consenso dell'interessato per i trattamenti necessari alla erogazione delle prestazioni sanitarie richieste dal paziente, sia se operi in qualità di libero professionista, sia se operi all'interno di una struttura sanitaria, pubblica o privata. Il consenso esplicito dell'interessato diventa obbligatorio quando i dati sanitari vengono trattati per finalità diverse dalla cura o dall'assistenza medica diretta. In questi casi, infatti, il trattamento va oltre le necessità sanitarie primarie e richiede un'autorizzazione specifica da parte dell'interessato.

Situazioni in cui è necessario raccogliere il consenso preventivo del paziente per i trattamenti di dati sanitari possono essere connessi all'utilizzo di dispositivi o applicazioni mediche, preordinati alla fidelizzazione della clientela effettuati da strutture sanitarie per finalità promozionali o commerciali (es. promozioni su programmi di screening), ovvero effettuati da professionisti sanitari attraverso il Fascicolo sanitario elettronico, ad esclusione del trattamento per finalità di cura Per l'inserimento e la consultazione dei dati, in quanto considerato necessario per motivi di interesse pubblico rilevante e per la tutela della salute dell'interessato, come previsto dall'art. 9 par. 2 lett. h) del GDPR e dalla normativa nazionale.

[52] Secondo il quarto paragrafo dell'art. 9 del Regolamento: «*Gli Stati membri possono mantenere o introdurre nuove condizioni, comprese limitazioni con riguardo al trattamento dei dati genetici, dati biometrici o dati relativi alla salute*».

Tuttavia, l'interessato ha il diritto di oscurare singoli documenti presenti nel FSE, e può limitare l'accesso ai propri dati.

A tal proposito il GDPR richiede che gli operatori sanitari forniscano agli interessati un'informativa chiara e completa sul trattamento dei loro dati personali. Questa informativa deve includere: le finalità del trattamento dei dati, la base giuridica che lo rende legittimo, i diritti dell'interessato, come il diritto di accesso, rettifica, cancellazione, e portabilità dei dati, la durata della conservazione dei dati sanitari e i criteri utilizzati per stabilirla.

Il Regolamento impone ai Titolari del trattamento di mantenere un Registro delle Attività di Trattamento, strumento fondamentale per documentare e dimostrare la conformità alle normative in materia di protezione dei dati personali. Questo registro deve contenere tutte le informazioni principali relative alle operazioni di trattamento effettuate.

I professionisti e le strutture sanitarie devono garantire che i pazienti siano sempre consapevoli di come i loro dati vengono gestiti, rispettando i loro diritti e fornendo tutte le informazioni necessarie in modo chiaro e trasparente.

La protezione dei dati sanitari è oggi più che mai una questione centrale, che tocca non solo la sfera giuridica ma anche quella personale e quotidiana di ciascuno di noi.

Il GDPR ha portato un importante passo avanti, definendo con chiarezza chi può trattare i dati, in quali casi e con quali garanzie. Soprattutto, ha posto al centro la persona, riconoscendo a ogni cittadino il diritto di sapere, controllare e decidere come vengono usate le informazioni sulla propria salute.

In un mondo sempre più digitalizzato, dove le informazioni circolano con grande velocità, è fondamentale che i dati sensibili, come quelli sanitari, siano gestiti con estrema attenzione. Le strutture sanitarie e i professionisti hanno oggi una grande responsabilità: proteggere non solo la salute, ma anche la riservatezza e la dignità delle persone.

Applicare il GDPR in ambito sanitario non è semplice. Da un lato, il settore deve fare i conti con un contesto tecnologico in rapida evoluzione e con la necessità di accesso e condivisione dei dati per migliorare le prestazioni cliniche e promuovere la ricerca. Dall'altro, deve garantire il rispetto rigoroso dei diritti degli interessati, come il diritto all'informazione, all'accesso, alla portabilità e alla cancellazione dei dati.

Il Garante, in risposta a molteplici richieste di chiarimento da parte di operatori sanitari e istituzioni, il 7 marzo 2019 ha emanato il provvedimento n. 55[53], un documento chiave che offre indicazioni pratiche sull'applicazione del GDPR in ambito sanitario. Tale

[53] Garante della Privacy, "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*" Doc-Web 9091942.

provvedimento ha una duplice funzione: da un lato, aumentare la consapevolezza dei rischi e delle responsabilità connesse al trattamento dei dati sanitari; dall'altro, promuovere il rispetto delle norme e l'adozione di misure efficaci per tutelare i diritti degli interessati.

Tra le misure più significative richieste dal Regolamento figurano la valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA), e la notifica tempestiva di eventuali violazioni di dati personali.

Il Garante, nel suo provvedimento, ha sottolineato l'importanza di bilanciare questi aspetti, ribadendo che il trattamento deve essere sempre proporzionato, necessario e rispettoso dei principi di minimizzazione e limitazione delle finalità[7].

Il processo di implementazione del GDPR in sanità è ancora in evoluzione.

Il Garante è impegnato costantemente nella definizione di ulteriori provvedimenti e regole deontologiche specifiche, che dovranno garantire uniformità e chiarezza nel rispetto delle norme. Questo lavoro rappresenta un passo fondamentale per accompagnare i titolari e responsabili del trattamento in un percorso di compliance che coniughi tutela della privacy e progresso sanitario.

Tuttavia, va rilevato, che il Garante per la protezione dei dati personali non ha ancora adottato i provvedimenti generali previsti dall'art. 2-septies del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, come modificato dal d.lgs. 10 agosto 2018, n. 101), nonostante il lungo tempo trascorso dalla sua entrata in vigore.

Tale disposizione, introdotta per conformare la disciplina nazionale al Regolamento (UE) 2016/679 (GDPR), demanda all'Autorità garante il compito di individuare, con provvedimenti di garanzia, "*misure appropriate e specifiche a tutela dei diritti fondamentali e delle libertà dell'interessato" nei trattamenti di dati genetici, biometrici e relativi alla salute*"[54]. La mancata emanazione di tali atti ha determinato una situazione di incertezza giuridica, specialmente nei settori sanitario e di ricerca scientifica, dove l'assenza di linee guida vincolanti rende più complessa l'applicazione uniforme dei principi di minimizzazione, proporzionalità e sicurezza del trattamento.

[54] Art. 2-septies, comma 1, d.lgs. 196/2003, secondo cui "*il trattamento dei dati genetici, biometrici o relativi alla salute è consentito [...] nel rispetto delle misure di garanzia individuate dal Garante per la protezione dei dati personali con provvedimenti di carattere generale*".

La dottrina ha più volte sottolineato come l'inattività dell'Autorità in questa specifica materia rischi di compromettere l'effettività delle garanzie previste dal GDPR, che attribuisce agli Stati membri un margine di manovra proprio in relazione al trattamento di categorie particolari di dati[55].

Nel contesto della ASL di Nuoro, come in tutte le aziende sanitarie pubbliche, la tutela della privacy dei pazienti rappresenta una componente essenziale della qualità assistenziale e della conformità normativa.

Tuttavia, l'implementazione concreta delle disposizioni del Regolamento (UE) 2016/679 (GDPR) può presentare criticità operative, che emergono soprattutto nei reparti ospedalieri, negli ambulatori periferici e nei flussi informativi digitali.

Negli ultimi anni, l'ASL 3 di Nuoro ha avviato un percorso di adeguamento progressivo alla normativa europea in materia di protezione dei dati personali.

Nel processo di adeguamento in atto, l'azienda ha formalmente nominato un Data Protection Officer (DPO), in conformità all'art. 37 del GDPR, con il compito di vigilare sull'osservanza della normativa, fungere da punto di contatto con l'Autorità Garante e fornire consulenza interna.

Il DPO coadiuvato dal personale della S.C. Affari Generali e Legali, ha avviato una serie di attività ispettive e di auditing nei reparti ospedalieri e nei servizi territoriali, volte a:

- verificare la corretta correttezza e gestione delle informative ai pazienti;
- mappare i flussi di trattamento dei dati sanitari;
- valutare i rischi legati a eventuali accessi impropri o non autorizzati;
- promuovere l'adozione di misure organizzative e tecniche adeguate, come previsto dall'art. 32 del GDPR.

Parallelamente, l'azienda ha iniziato a organizzare sessioni di formazione periodica rivolte al personale sanitario, amministrativo e tecnico, per favorire una maggiore consapevolezza dei principi di liceità, minimizzazione e sicurezza nel trattamento dei dati personali.

In particolare, l'azienda ha aderito al progetto Medicina Digitale Sardegna (MEDS)[56], promosso dall'Azienda Regionale della Salute (ARES) Sardegna, che si configura come un'iniziativa strategica per il potenziamento del sistema sanitario regional, allineandosi agli

[55] FINOCCHIARO G., *Privacy e protezione dei dati personali. Commentario al GDPR e al Codice della privacy*, Bologna, Zanichelli, 2019, p. 512 ss.; MANTELERO A., *Dati personali e decisioni automatizzate: la protezione dei diritti nell'era dell'algoritmo*, in Rivista critica del diritto privato, 2018, n. 3, p. 347.

[56] ARES Sardegna, *MEDS. Un progetto di ARES Sardegna per una sanità più innovativa.* https://www.ares-sardegna.it/meds-un-progetto-di-ares-sardegna-per-una-sanita-piu-innovativa/

obiettivi della Missione 6, Componente 2 del Piano Nazionale di Ripresa e Resilienza (PNRR) al fine di rafforzare le competenze digitali nel settore sanitario.

Infatti, l'obiettivo primario del progetto è l'incremento delle competenze per un bacino di 29.000 professionisti del Servizio Sanitario Regionale (SSR) in un anno, includendo personale medico, infermieristico, amministrativo, tecnico dei sistemi informativi e altre professioni sanitarie.

Il percorso formativo, articolato in sessioni a distanza e in presenza arricchite da materiali asincroni per garantire flessibilità, è progettato per fornire conoscenze avanzate su aree tematiche fondamentali quali la gestione sicura dell'identità digitale, l'interoperabilità degli strumenti come il Fascicolo Sanitario Elettronico (FSE) e i Sistemi Informativi Sanitari (SIS), la dematerializzazione dei processi inclusa la firma digitale, e la sicurezza informatica in conformità al GDPR.

L'impatto atteso è quello di rendere i professionisti sanitari attori protagonisti della trasformazione digitale, ottimizzando il lavoro quotidiano, migliorando l'efficienza e la qualità delle cure e contribuendo attivamente alla modernizzazione complessiva del sistema sanitario sardo.

Nonostante persistano alcune criticità di natura operativa, è tuttavia evidente l'impegno crescente che la ASL 3 sta profondendo per rafforzare la cultura della privacy e promuovere una compliance sistemica.

In questa prospettiva, appare fondamentale proseguire in questo percorso e promuovere all'interno dell'azienda, una cultura della protezione dei dati personali pienamente consapevole, dove la delicatezza delle informazioni trattate richiede un livello particolarmente elevato di garanzie e responsabilità.

Infatti, il rispetto dei diritti del paziente, inteso non solo come soggetto "curato" ma anche come titolare del proprio patrimonio informativo, costituisce la base per un sistema sanitario che sia al contempo moderno, tecnologicamente avanzato, ma anche sicuro e profondamente umano.

L'importanza di questa cultura è confermata da numerosi interventi dell'Autorità Garante, che ha più volte sanzionato strutture sanitarie pubbliche e private per gravi violazioni dei principi di sicurezza, riservatezza e *accountability*, specie nei casi di accessi impropri ai dati dei pazienti

Tra i provvedimenti più recenti:

- provvedimento n. 10002324, 10002533, 10002287 del 21 marzo 2024. Attacco ransomware ai sistemi sanitari della Regione Lazio: il Garante ha irrogato sanzioni

per un totale di € 401.000 a LAZIOcrea, Regione Lazio e ASL Roma 3, in seguito ai gravissimi malfunzionamenti verificatisi nella gestione prenotazioni e referti, nonché all'esposizione di dati sanitari di milioni di assistiti;

- provvedimento n. 10001279 del 22 febbraio 2024. Accessi impropri al dossier sanitario elettronico dell'Alto Adige (ASDAA): multa da € 75.000 per l'assenza di controlli atti a prevenire accessi da parte di personale non coinvolto, con evidenze di consultazioni non autorizzate;
- provvedimento n. 9941232 del 28 settembre 2023. Attacco ransomware alla ASL Napoli 3 Sud: sanzione di € 30.000 per violazione dei principi di "privacy by design" e accountability, con compromissione di dati di circa 842.000 pazienti.

Questi provvedimenti evidenziano la gravità delle carenze nelle infrastrutture e nei controlli interni alle aziende sanitarie, che favoriscono *data breach*, accessi impropri e scarsa protezione dei dati sanitari. Inoltre, si evince l'esigenza di integrare le misure tecniche con un rigoroso investimento formativo, come sottolineato dal Garante stesso in diverse occasioni, per alimentare una cultura della privacy effettiva e diffusa.

In linea con quanto evidenziato, il perseguimento di una cultura della privacy non è solo un obbligo normativo, ma il presupposto per la costruzione di un sistema sanitario moderno e sicuro.

II.3. La Direttiva NIS 2 e il suo recepimento in Italia: verso un nuovo paradigma europeo di cybersecurity

La Direttiva NIS 2 (Direttiva UE 2022/2555[57]), approvata dal Consiglio dell'Unione Europea il 28 novembre 2022, rappresenta un passo significativo verso il rafforzamento della sicurezza informatica all'interno dell'Unione.

Questo intervento normativo riflette l'impegno dell'UE nel promuovere una cultura della sicurezza digitale, rafforzando al contempo la cooperazione tra autorità pubbliche e soggetti privati e mira a colmare le lacune emerse nell'attuazione della prima Direttiva NIS del 2016, introducendo un approccio più sistemico, armonizzato e resiliente alla gestione del rischio informatico.

[57] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

Uno degli elementi innovativi della NIS 2 risiede nella ridefinizione dell'ambito di applicazione. Essa amplia infatti il numero e la tipologia dei soggetti obbligati, includendo anche attori di medio-grandi dimensioni attivi in settori considerati critici per il funzionamento degli Stati membri e dell'intera Unione, quali l'energia, i trasporti, la sanità, i servizi finanziari, le infrastrutture digitali, le amministrazioni pubbliche, l'approvvigionamento idrico, i fornitori di servizi ICT e le industrie manifatturiere di rilevanza strategica.

Essa mira a migliorare la protezione delle reti e dei sistemi informativi, ponendo particolare attenzione alla resilienza delle infrastrutture critiche e alla capacità collettiva di rispondere in maniera coordinata ed efficace alle crescenti minacce cibernetiche[58].

Inoltre, intende eliminare divergenze nell'attuazione della normativa tra gli Stati membri, promuovendo un quadro normativo più uniforme e coordinato[59].

Un elemento centrale della Direttiva è l'introduzione di una classificazione dei soggetti in due categorie: "essenziali" e "importanti":

- gli Enti Essenziali[60], essendo soggetti a un livello di rischio più elevato per la collettività, sono sottoposti a controlli più stringenti e a una supervisione proattiva da parte delle autorità competenti;
- gli Enti Importanti[61], sebbene anch'essi sottoposti a obblighi di sicurezza, sono invece monitorati principalmente attraverso un approccio reattivo, con controlli ex post e valutazioni basate su incidenti o segnalazioni.

---

[58] MINISTERO DELLA SALUTE, Autorità di Settore NIS e Settori di competenza

[59] DI GIACOMO L., *La Direttiva europea NIS2 per punti essenziali,* in Diritto.it. https://www.diritto.it/la-direttiva-europea-nis2-per-punti-essenziali/

[60] In particolare, un soggetto è ritenuto essenziale se opera in un settore considerato ad alta criticità (vedasi l'allegato I della Direttiva) e soddisfa una o più delle seguenti condizioni, tali da farlo considerare una grande impresa: occupa almeno 250 persone; ha un fatturato annuo superiore a 50 milioni di euro; ha un totale di bilancio (ossia il totale dell'attivo patrimoniale) annuo superiore a 43 milioni di euro.
Sono altresì considerati essenziali, a prescindere dal superamento delle anzidette soglie: i prestatori di servizi fiduciari qualificati, i gestori di registri dei nomi di dominio di primo livello e i prestatori di servizi DNS; i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese; qualsiasi altro soggetto di cui al citato allegato I o II che lo Stato identifica come soggetto essenziale in conformità con la Direttiva. Nel dettaglio, l'Italia considera soggetti essenziali, indipendentemente dalle loro dimensioni, gli organi costituzionali e di rilievo costituzionale, la Presidenza del Consiglio dei ministri e i ministeri, le agenzie fiscali e le autorità amministrative indipendenti; le «infrastrutture critiche» ai sensi della cosiddetta direttiva CER, ossia la direttiva UE 2557/2022. Si tratta di quelle infrastrutture che sono essenziali per il funzionamento del tessuto sociale ed economico: ne sono esempi le infrastrutture energetiche, sanitarie, bancarie, delle comunicazioni, bancarie, della sicurezza alimentare e di trasporto.

[61] Un soggetto è invece ritenuto importante se, alternativamente: opera in un settore considerato ad alta criticità ai sensi del citato allegato I e ha tra i 50 e i 249 dipendenti o un fatturato annuo tra 10.000.000,01 e 50 milioni di euro o un totale di bilancio tra 10.000.000,01 e 43 milioni di euro (dunque, si deve trattare di una media impresa, cioè un soggetto che supera i massimali per essere considerato una piccola impresa, ma non soddisfa le condizioni tali da farlo considerare una grande impresa); opera negli altri settori critici di cui all'allegato II della Direttiva ed è considerato una grande impresa oppure una media impresa in base alle condizioni enunciate nel precedente punto (cioè, l'avere almeno 50 dipendenti, un fatturato annuo superiore a 10 milioni di euro oppure un totale di bilancio annuo superiore a 10 milioni di euro).

Tale distinzione consente di modulare le misure di sicurezza e gli obblighi di vigilanza in base al ruolo strategico ricoperto dai diversi operatori all'interno dei settori vitali per il funzionamento della società e dell'economia.

La NIS 2 non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa, del contrasto, dell'accertamento e del perseguimento dei reati.

In particolare, i soggetti considerati essenziali sono sottoposti a un sistema di vigilanza più rigoroso, che prevede controlli preventivi (ex ante) e monitoraggi costanti da parte delle autorità competenti. A questi soggetti è richiesto di adottare misure di sicurezza informatica particolarmente avanzate, di segnalare con tempestività eventuali incidenti e di assicurare l'affidabilità e la continuità operativa delle infrastrutture critiche.

Al contrario, i soggetti classificati come importanti, pur essendo tenuti a rispettare obblighi analoghi, sono inseriti in un contesto di vigilanza meno stringente.

In questi casi, i controlli sono prevalentemente successivi (ex post) e le autorità intervengono principalmente in presenza di violazioni manifeste o a seguito di segnalazioni di inadempienze[62].

Ogni organizzazione, sia essa pubblica o privata, di medie o grandi dimensioni, è tenuta a condurre una valutazione preliminare interna al fine di verificare il proprio eventuale rientro nell'ambito di applicazione della Direttiva NIS 2[63]. Tale processo di autovalutazione rappresenta il primo passaggio necessario per accertare se l'ente possa essere qualificato come soggetto essenziale o soggetto importante, in conformità ai criteri stabiliti dal quadro normativo vigente.

Qualora emerga l'inclusione tra i soggetti destinatari della normativa, l'organizzazione è obbligata a procedere con la registrazione sulla piattaforma digitale messa a disposizione dall'Agenzia per la Cybersicurezza Nazionale (ACN). A seguito dell'invio delle informazioni richieste, sarà l'ACN a esaminare i dati trasmessi e a formalizzare, mediante notifica, il riconoscimento dello status di soggetto NIS.

A partire dal 2026, tutte le entità così classificate saranno soggette a obblighi cogenti, tra cui la segnalazione tempestiva degli incidenti informatici al *Computer Security Incident Response Team* (CSIRT) nazionale e la piena conformità alle misure di sicurezza informatica previste dalla Direttiva NIS 2 e dal relativo decreto di recepimento (D.lgs. 138/24).

---

[62] MAGAGNA F., *Soggetti «essenziali» e «importanti» secondo la NIS 2: differenze e implicazioni, in Lex* Tech Hub,https://www.dataprotectionforum.eu/post/soggetti-essenziali-e-importanti-secondo-la-nis-2-differenze-e-implicazioni.

[63] Data Log, Direttiva NIS2: nuove regole per la cybersecurity, in https://www.datalog.it/nis-2-regole-cybersecurity.

A tal proposito, la normativa prevede un iter rigoroso per la segnalazione degli incidenti. La normativa prevede un iter rigoroso per la segnalazione degli incidenti.

Infatti, le organizzazioni soggette alla Direttiva NIS 2 devono notificare al CSIRT Italia[64] (*Computer Security Incident Response* Team nell'ambito dell'Agenzia per la cybersicurezza nazionale) ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi.

In conformità con gli obblighi introdotti dalla Direttiva NIS 2, le organizzazioni classificate come soggetti NIS sono tenute a seguire una procedura strutturata di notifica degli incidenti informatici, articolata in più fasi temporali.

- Entro 24 ore dalla rilevazione dell'incidente, deve essere inviata una pre-notifica al CSIRT nazionale, contenente informazioni preliminari circa la possibile origine dolosa dell'evento e l'eventuale presenza di impatti transfrontalieri.
- Entro 72 ore, l'organizzazione è obbligata a trasmettere una notifica completa, contenente un'analisi iniziale dell'accaduto. Tale comunicazione deve includere dettagli relativi alla natura dell'incidente, ai sistemi compromessi e alle prime misure di contenimento adottate.
- In caso di richiesta da parte delle autorità competenti, può essere richiesta una relazione intermedia che descriva l'evoluzione della situazione, le azioni correttive in corso e le strategie previste per la risoluzione definitiva.
- Entro 30 giorni dall'evento, è infine necessario inoltrare un report finale. Questo documento deve fornire una ricostruzione completa delle cause dell'incidente, indicare gli interventi attuati per prevenirne la reiterazione, e valutare l'impatto, sia a livello nazionale che internazionale.

Per assicurare la piena conformità al quadro regolamentare, le organizzazioni devono promuovere una cultura della sicurezza informatica, fondata su programmi di formazione permanente destinati a tutto il personale. La sensibilizzazione e la preparazione degli operatori aziendali sono elementi essenziali per garantire la tempestiva identificazione e gestione delle minacce cibernetiche.

A tale scopo, può rendersi necessario investire in tecnologie evolute, potenziare il capitale umano mediante l'inserimento di profili professionali specializzati e mantenere

[64] l CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale. I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4. Essi includono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT; il servizio di monitoraggio delle potenziali vulnerabilità sugli asset esposti.

un costante aggiornamento dei sistemi informativi. Inoltre, è fondamentale adottare un approccio dinamico nella gestione delle politiche di sicurezza: ciò implica la revisione periodica delle procedure interne, l'aggiornamento dei piani di risposta agli incidenti e il monitoraggio continuo della conformità rispetto ai requisiti della Direttiva.

II.3.1. La Direttiva NIS 2: la guida operativa dell'ACN

L'Italia ha recepito la Direttiva NIS 2 attraverso il Decreto Legislativo 4 settembre 2024, n. 138[65], adottando un insieme di misure mirate a garantire un elevato livello di sicurezza cibernetica su scala nazionale.

Il percorso di implementazione, tuttavia, non si è fermato al recepimento legislativo. Dando attuazione a quanto previsto dal decreto stesso (in particolare agli articoli 31, 40 e 42), l'Agenzia per la Cybersicurezza Nazionale (ACN) è intervenuta con un atto successivo per tradurre la norma in pratica.

Si tratta della Determinazione del Direttore Generale del 14 aprile 2025, con la quale sono state delineate le prime direttive operative e le specifiche tecniche per guidare gli attori coinvolti nell'adempimento delle nuove prescrizioni cogenti.

Tale provvedimento definisce le modalità e le tempistiche per l'attuazione degli obblighi in materia di cybersicurezza, stabilisce criteri basati sul principio di proporzionalità, ponderando il profilo di rischio, la dimensione strutturale dei soggetti interessati e la potenziale magnitudo degli eventi avversi, anche sotto il profilo dell'impatto economico e sociale.

L'individuazione delle specifiche tecniche è stata il risultato di un iter consultivo strutturato, che ha visto il coinvolgimento del Tavolo per l'attuazione della disciplina NIS e dei tavoli settoriali costituiti con le Autorità di settore e le principali rappresentanze di categoria.

La Determinazione si compone di dieci articoli e quattro allegati, attraverso i quali l'ACN ha definito le specifiche basali del nuovo assetto normativo.

Gli Allegati 1 e 2 contengono le misure di sicurezza cibernetica, differenziate in base alla qualificazione del soggetto come "importante" o "essenziale".

[65] Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148

Gli Allegati 3 e 4 individuano, con la medesima distinzione soggettiva, gli eventi incidentali rilevanti che innescano obblighi di segnalazione.

Le tempistiche di adeguamento sono stabilite negli articoli 3 e 4: le misure di sicurezza devono essere adottate entro diciotto mesi, mentre l'obbligo di notifica degli incidenti diviene operativo dopo nove mesi dalla comunicazione di iscrizione nell'elenco dei soggetti NIS.

Il provvedimento introduce altresì regimi speciali e transitori per soggetti già regolati da normative precedenti, quali i PSNC-NIS[66], gli Operatori di Servizi Essenziali (OSE) e gli operatori di telecomunicazioni. Una specifica attenzione è riservata ai gestori dei nomi di dominio di primo livello e ai fornitori di servizi di registrazione, tenuti ad adeguarsi, entro diciotto mesi, ai requisiti di sicurezza dell'articolo 29 del decreto NIS.

Gli articoli 6 e 7 delineano un regime transitorio per OSE e operatori telco: i primi devono mantenere le misure già adottate ai sensi del D.lgs. 18 maggio 2018, n. 65[67], limitatamente ai sistemi informativi e di rete OSE; i secondi devono conformarsi alle misure vigenti ai sensi del decreto ministeriale 12 dicembre 2018 per i sistemi telco. Entrambe le categorie, nell'adempimento dell'obbligo di notifica, applicano le definizioni di incidente significativo previste negli allegati 3 e 4, in base alla propria classificazione. Per gli operatori telco, l'Allegato 4 specifica soglie tecniche basate sulla combinazione tra durata dell'evento e percentuale di utenza colpita, per una qualificazione oggettiva degli eventi segnalabili.

L'Allegato 1 elenca le misure di sicurezza informatica di base per i soggetti "importanti", strutturate in sei domini funzionali: governo, identificazione, protezione, rilevamento, risposta e ripristino. Queste misure disciplinano il ciclo organizzativo e tecnico della sicurezza informatica, dalla definizione del contesto e delle politiche alla gestione degli incidenti e delle crisi. Viene conferito peculiare rilievo alla formalizzazione e approvazione delle policy da parte degli organi di amministrazione, alla centralità del piano di gestione del rischio informatico, alla tracciabilità delle responsabilità e all'integrazione delle valutazioni di rischio con i processi di approvvigionamento e sviluppo. Le misure

[66] Il D.L. n. 105/2019, convertito con modificazioni dalla legge n. 133/2019, istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) con l'obiettivo di tutelare la sicurezza, dello Stato e garantire un elevato livello di sicurezza cibernetica delle reti, dei sistemi informativi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato. Il PSNC è da intendersi come una Legge di sicurezza nazionale, che mira a rinforzare il livello di sicurezza nel settore digitale.

[67] D.lgs. 18 maggio 2018, n. 65 "Attuazione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"

prevedono cicli di revisione periodica e aggiornamento continuo, in linea con l'evoluzione tecnologica, e richiamano l'obbligo di formazione continua per il personale e i vertici aziendali, come stabilito dall'art. 24 del D.lgs. 138/2024.

L'Allegato 2, destinato ai soggetti "essenziali", pur richiamando la medesima architettura funzionale, presenta un elevato grado di formalizzazione e specificità operativa, coerentemente con la rilevanza sistemica dei servizi erogati. Si evidenzia una maggiore articolazione interna delle singole misure, con dettagli prescrittivi su modalità organizzative, tempistiche di revisione e soggetti competenti. L'Allegato 2 introduce inoltre prescrizioni supplementari non presenti nell'Allegato 1, tra cui: formazione mirata per il personale specialistico; integrazione della sicurezza informatica nelle pratiche di gestione delle risorse umane (incluse clausole post-contrattuali di riservatezza); obbligo di valutazione documentata del rischio delle forniture in fase di progettazione; mantenimento di registri periodici; introduzione di piani strutturati di adeguamento e verifica dell'efficacia delle misure, da sottoporre agli organi apicali. In entrambi gli allegati, le misure rivestono natura prescrittiva e impongono obblighi di rendicontazione continua, richiedendo la conservazione sistematica della documentazione probatoria, l'adozione di evidenze dimostrative e la predisposizione di meccanismi atti a comprovare l'efficace implementazione e l'aggiornamento periodico delle misure, in osservanza dei principi di *accountability* e tracciabilità.

Gli Allegati 3 e 4 definiscono i criteri minimi per la qualificazione degli incidenti rilevanti che innescano gli obblighi di notifica. Entrambi gli allegati individuano tre categorie comuni di incidente:

- IS-1: Esfiltrazione di dati digitali, con violazione della riservatezza esterna.
- IS-2: Alterazione dell'integrità dei dati, con ripercussioni esterne.
- IS-3: Inadempienza rispetto ai livelli di servizio attesi, determinata sulla base di parametri predefiniti.

Per i soli soggetti "essenziali", si aggiunge una quarta fattispecie: IS-4: accesso non autorizzato o abuso di privilegi a dati digitali del soggetto NIS, accertato sulla base di parametri quali-quantitativi specifici. Questa estensione riflette l'accresciuta esposizione al rischio sistemico dei soggetti essenziali e l'esigenza di un rafforzamento del presidio contro tentativi di accesso illecito o l'uso improprio delle prerogative interne, includendo specificamente il fenomeno dell'abuso interno da parte di soggetti legittimamente autorizzati ma operanti in violazione delle policy di sicurezza.

II.3.2. I soggetti interessati

Come anticipato in precedenza, la prima innovazione riguarda il novero di soggetti interessati dalla Direttiva che appare ampliato rispetto alla precedente normativa.

La NIS 2 distingue tra operatori di "servizi essenziali" e di "servizi importanti". Nella prima categoria vi rientrano, a differenza della precedente normativa, anche le Pubbliche Amministrazioni, che si affiancano ad operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali, delle acque.

Tra i "servizi importanti", invece, si annoverano operatori di servizi postali e di corriere, di gestione dei rifiuti, del settore chimico, del settore agroalimentare e così via.

Secondo quanto disposto dall'art. 2 della NIS 2, questa si applica, in generale, ai soggetti pubblici o privati operanti in uno dei settori sopra menzionati, che sono considerati medie imprese ai sensi dell'art. 2, par. 1 dell'allegato alla Raccomandazione 2003/361/CE (meno di 250 persone; fatturato annuo non superiore ai 50 milioni di euro; bilancio annuo non superiore a 43 milioni di euro) o che superano i massimali previsti dallo stesso articolo. Vengono dunque escluse dall'ambito di applicazione della Direttiva, con qualche eccezione in concreto residuale, solamente le piccole imprese e le microimprese.

È bene sottolineare che, in ogni caso, come disposto dal considerando n. 13, gli Stati Membri dovranno adoperarsi per garantire che i soggetti esclusi dall'ambito di applicazione della NIS 2 raggiungano un livello elevato di cibersicurezza. Questo anche in ottica di rafforzamento della sicurezza informatica della *supply chain.*

Il legislatore europeo, consapevole dell'impossibilità di emanare una normativa contente obblighi puntuali, aggiornati e condivisi da tutti i settori sopra riportati, ha deciso di introdurre il concetto di Accountability anche in ambito di cybersecurity. L'approccio è quello di responsabilizzare i soggetti interessati, che dovranno essere in grado di rendicontare il loro operato.

Così, ai sensi dell'art. 21 della NIS 2, viene sancito che gli Stati membri provvedano affinché i soggetti essenziali e importanti adottino misure tecniche, operative ed organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi.

Nella valutazione di adeguatezza delle misure individuate, occorre tenere in debita considerazione:

- l'esposizione del soggetto ai rischi;
- la grandezza del soggetto;
- la probabilità che si verifichino incidenti e la loro gravità;
- l'impatto sociale ed economico dell'incidente.

Il medesimo art. 21 individua poi le misure minime da adottare. Tra queste, per sottolineare l'attenzione posta sulla *supply chain*, con particolare attenzione sula valutazione della sicurezza della citazione di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori (art. 21 par. 2 lett d).

La direttiva NIS 2, ai sensi dell'art. 34, prevede sanzioni molto alte in caso di violazione di una o più previsioni sancite agli articoli 21 o 23 da parte di un operatore di Servizi essenziali (fino a 10 milioni di euro o al 2% del totale del fatturato mondiale annuo per l'esercizio precedente) o di servizi importanti (fino a 7 milioni di euro o all'1,4% del fatturato mondiale annuo per l'esercizio precedente).

Gli operatori di servizi essenziali o importanti sono gravati da obblighi di segnalazione. Dovranno infatti notificare al CSIRT o, se opportuno, alla propria autorità competente, senza indebito ritardo e non oltre 72 ore dalla venuta a conoscenza tutti quegli incidenti in grado di causare una grave perturbazione del servizio oppure se l'incidente può avere conseguenze (o ha già avuto conseguenze) su altre persone fisiche o giuridiche causando perdite considerevoli. Il tutto secondo quanto stabilito all'art. 23.

Inoltre, pur non trovando qui spazio per un'analisi approfondita, vale la pena ricordare che la Direttiva NIS 2 prevede obblighi di vigilanza ed esecuzione in capo agli Stati membri e norme in materia di condivisione delle informazioni sulla cibersicurezza tra le varie Autorità europee.

La Direttiva NIS 2 è solo uno dei passi del Legislatore europeo, che punta a vincere la partita della sovranità digitale. Il GDPR, il Cybersecurity ACT, il Cyber Resilience Act, la Direttiva CER e il Regolamento DORA[68], sono solo alcuni degli atti che possono intersecarsi con la normativa qui in analisi.

Infatti, si percepisce il tentativo delle istituzioni europee di creare un comparto di norme che dialoghi tra loro e tuteli tutti i principali aspetti della società dell'informazione.

[68] Il Digital Operational Resilience Act, o DORA, è un regolamento dell'Unione Europea (UE) che stabilisce un framework vincolante e completo relativo alla gestione del rischio delle tecnologie di informazione e comunicazione (ICT) per il settore finanziario dell'UE. Il regolamento DORA stabilisce gli standard tecnici che le entità finanziarie e i loro fornitori critici di servizi tecnologici di terze parti devono implementare nei propri sistemi ICT.

A proposito, si pensi, ad esempio, ai numerosi riferimenti ad ENISA (il cui mandato è stato reso permanente proprio dal Cybersecurity Act).[69]

In definitiva, la Direttiva NIS 2 e il relativo recepimento in Italia segnano un passaggio fondamentale verso un modello di cybersecurity più maturo, coordinato e integrato, capace di affrontare le sfide poste da un panorama di minacce in continua evoluzione. L'adozione di un approccio più inclusivo e strutturato rappresenta non solo un adeguamento normativo, ma anche un'opportunità per rafforzare la resilienza digitale dell'intero sistema-Paese.

II.3.3. La Direttiva NIS 2 e gli impatti sulla sanità

Negli ultimi anni, la crescente esposizione della Sanità alle minacce informatiche ha reso evidente l'urgenza di rafforzare i meccanismi di protezione e risposta a livello europeo. In questo contesto nasce la Direttiva NIS 2, pensata per garantire una gestione sicura, armonizzata e conforme degli scambi digitali – soprattutto quando coinvolgono dati sensibili e transfrontalieri. La sua finalità principale è assicurare la continuità operativa dei servizi digitali anche in caso di incidenti informatici, attraverso una cooperazione strutturata e reattiva tra tutti gli Stati membri dell'UE.

Questa nuova direttiva rappresenta un'evoluzione significativa rispetto alla prima Direttiva NIS (UE 2016/1148), che pure aveva posto le basi per una strategia comune in materia di sicurezza informatica. Tuttavia, l'esperienza pratica ha mostrato limiti importanti: ogni Stato membro ha interpretato e applicato la norma in modo diverso, generando disomogeneità sia nei requisiti normativi sia nei meccanismi di controllo.

Queste discrepanze hanno comportato complessità operative e oneri aggiuntivi per le organizzazioni attive in più Paesi, mettendo a rischio l'efficacia complessiva del sistema. Inoltre, un'applicazione diseguale delle misure di sicurezza rischiava di lasciare alcuni Paesi e, di conseguenza l'intero sistema europeo, più esposti agli attacchi informatici. Con la NIS 2 si punta a colmare queste lacune, rafforzando la resilienza cibernetica in modo più uniforme e coordinato su scala continentale[70].

[69] DHOOR SINGH D., *Cibersicurezza, la Direttiva NIS 2*, in Altalex, https://www.altalex.com/documents/news/2023/01/24/cibersicurezza-direttiva-nis-2.

[70] Direttiva NIS 2: l'impatto sulla Sanità, in Healthe360, ttps://www.healthtech360.it/law-security/nis-2-sanita/

Il settore sanitario si confronta con una duplice criticità: da un lato, la centralità dei dati clinici per l'erogazione delle cure, dall'altro, il ritardo tecnologico accumulato da molte strutture ospedaliere. Gran parte degli ospedali si avvale ancora di sistemi *legacy* eterogenei, spesso sviluppati in maniera indipendente e con livelli insufficienti di sicurezza e resilienza.

Questa frammentazione rende gli enti sanitari particolarmente vulnerabili: i criminali informatici sono consapevoli di poter compromettere facilmente i sistemi e bloccarne le attività, facendo leva sull'urgenza di ripristinare l'accesso a informazioni critiche per ottenere il pagamento di riscatti.

Le informazioni trattate dai sistemi sanitari sono tra le più delicate in assoluto.

Secondo il Rapporto Clusit 2025[71], solo in Italia il 100% degli incidenti informatici registrati nel 2024 nel settore sanitario ha avuto impatti gravi (62%) o hechaddirittura gravissimi (38%). Un dato allarmante, che conferma quanto siano elevati i rischi legati alla vulnerabilità dei sistemi ospedalieri, non solo in termini di furto di dati, ma anche di interruzione dei servizi e compromissione della sicurezza dei pazienti.

In questo scenario, la NIS 2 non è semplicemente una normativa da attuare, ma una strategia di trasformazione che coinvolge governance, tecnologie e cultura della sicurezza.

Le vulnerabilità appena descritte si traducono in una varietà di minacce concrete che le strutture sanitarie devono affrontare costantemente.

Le principali tipologie di rischio includono:

- ransomware: l'attacco più frequente e devastante. I dati vengono cifrati e le attività sanitarie paralizzate fino al pagamento di un riscatto;
- violazioni dei dati: furti di informazioni sensibili, come referti, esami diagnostici, numeri di previdenza sociale e informazioni di contatto dei pazienti;
- accessi non autorizzati: spesso legati a credenziali rubate o insufficientemente protette;
- dispositivi medici connessi: l'aumento dei dispositivi medici IoT introduce una significativa vulnerabilità, con il rischio di attacchi cibernetici capaci di compromettere la sicurezza e la salute dei pazienti.

Un altro punto critico riguarda la supply chain sanitaria. Le strutture si affidano sempre più a fornitori esterni per servizi IT, diagnostica, telemedicina, gestione dei dati. Tuttavia, questi fornitori non sempre dispongono di adeguate misure di sicurezza e diventano un punto di ingresso vulnerabile per gli attacchi.

[71] Il Rapporto gli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2024, confrontandoli con i dati raccolti negli anni precedenti, anche attraverso l'utilizzo delle segnalazioni della Polizia Postale e per la Sicurezza Cibernetica, in Clusit 25, https://clusit.it/rapporto-clusit/.

L'accesso ai sistemi tramite credenziali fornite ai partner esterni, se non protetto da sistemi come l'autenticazione a più fattori, può facilitare l'infiltrazione.

Le disposizioni contenute nella direttiva riguardano infatti tutti gli attori coinvolti nell'erogazione di servizi sanitari digitali. Ciò include non solo le strutture ospedaliere pubbliche e private, ma anche le aziende sanitarie territoriali, i laboratori, i fornitori di servizi digitali in ambito salute (come i gestori del Fascicolo Sanitario Elettronico), e persino le imprese private che trattano dati sanitari su incarico della pubblica amministrazione.

L'adozione della Direttiva NIS 2 in ambito sanitario richiede non solo aggiornamenti tecnologici, ma anche una nuova cultura organizzativa in cui la sicurezza informatica rivesta un ruolo cruciale nella strategia operativa delle strutture sanitarie. Ciò comporta impatti significativi, in quanto la direttiva impone, in primis, un approccio strategico nella gestione della sicurezza informatica, coinvolgendo l'organo di gestione nel processo di approvazione delle modalità di implementazione delle misure di gestione dei rischi e nella supervisione di suddette misure[72].

La NIS 2, infatti, impone una serie di misure tecniche e organizzative, che non si limitano alla prevenzione degli attacchi, ma coinvolgono l'intera governance della sicurezza informatica. Tra le più rilevanti si annoverano:

- l'adozione di un sistema di gestione dei rischi informatici, comprensivo di politiche per la sicurezza dei dati e dei sistemi;
- il rafforzamento della cybersecurity nella catena di fornitura, imponendo alle strutture sanitarie di vigilare anche sui propri partner e fornitori;
- l'obbligo di notifica tempestiva degli incidenti significativi entro 24 ore, al fine di garantire una risposta coordinata a livello nazionale;
- l'introduzione di responsabilità specifiche in capo ai vertici aziendali, che dovranno dimostrare la conformità alle disposizioni attraverso audit e documentazione adeguata.

È importante sottolineare che l'inosservanza di tali obblighi potrà comportare sanzioni amministrative consistenti, nonché l'adozione di misure correttive da parte delle autorità competenti.

Uno degli ambiti in cui l'applicazione della NIS 2 è particolarmente rilevante è quello del Fascicolo Sanitario Elettronico (FSE 2.0).

---

[72] BACCHIERI S, *Direttiva NIS 2: requisiti e impatti per il settore sanitario*, in Cyber security 360, https://www.cybersecurity360.it/legal/direttiva-nis-2-requisiti-e-impatti-per-il-settore-sanitario/

La nuova versione del FSE, destinata a diventare il principale strumento di interoperabilità dei dati sanitari a livello nazionale, richiede garanzie robuste in termini di riservatezza, integrità e disponibilità delle informazioni.

In questo senso, la NIS 2 si integra profondamente con altri strumenti normativi europei, come il Regolamento (UE) 2016/679 (GDPR), e con le strategie nazionali per la trasformazione digitale della sanità. Essa impone una visione olistica della sicurezza, in cui la tecnologia, l'organizzazione e la cultura del rischio devono cooperare per garantire la protezione di uno dei beni più preziosi: la salute dei cittadini.

Nel settore sanitario, la NIS 2 richiede l'implementazione di misure di sicurezza informatica avanzate per la tutela di infrastrutture IT e dati sensibili. Tra gli obblighi chiave spiccano il significativo miglioramento della cybersecurity, attraverso l'adozione di tecnologie come la crittografia robusta, l'autenticazione a più fattori e firewall di ultima generazione.

Le aziende sanitarie devono inoltre sviluppare piani di gestione del rischio che includano una dettagliata valutazione delle minacce e protocolli efficaci per mitigarne gli impatti.

La sorveglianza costante dei sistemi è essenziale per rilevare tempestivamente eventuali anomalie, così come la predisposizione di procedure di risposta rapida agli incidenti, con l'obbligo di notificare alle autorità competenti eventuali violazioni entro 24 ore.

Infine, la NIS 2 pone un'enfasi cruciale sulla formazione continua del personale, riconoscendo il ruolo fondamentale della consapevolezza umana nella difesa contro gli attacchi cibernetici.

Un'efficace cybersecurity in sanità non è solo un'esigenza tecnica, ma un pilastro per costruire un sistema sanitario sostenibile. La sicurezza informatica permette di evitare interruzioni nei servizi, protegge i dati sensibili, favorisce l'interoperabilità tra sistemi e riduce i costi derivanti da incidenti e contenziosi.

Questo percorso è più efficace e gestibile laddove è assicurata una governance solida della cybersecurity e dell'IT, garantendo la separazione di ruoli (*segregation of duties*), ottenibile con un approccio programmatico, strutturato e integrato, fondato sulla gestione del rischio.

Infatti, solo attraverso la definizione di un corretto assetto organizzativo, in termini di ruoli e responsabilità, efficienti processi di sicurezza e una corretta gestione della catena di approvvigionamento, sarà possibile, insieme all'adozione di soluzioni tecnologiche, ridurre il rischio di rimanere vittime di incidenti informatici.

Il cambiamento di tipo strategico-organizzativo deve essere accompagnato da un cambiamento culturale verso una maggiore consapevolezza della sicurezza informatica tra tutti i dipendenti, non solo per quelli IT.

A seguito dell'entrata in vigore della Direttiva (UE) 2022/2555 NIS 2, le strutture sanitarie come la ASL 3 di Nuoro sono state riconosciute come "Entità essenziali" secondo i criteri della normativa, dovendo conformarsi a una serie di stringenti obblighi relativi alla sicurezza delle reti e dei sistemi informativi. Tra gli adempimenti posti in essere dall'Azienda ci sono la registrazione presso il portale dedicato dell'Agenzia per la Cybersecurity Nazionale (ACN) e la designazione di un referente per la cybersecurity, che cura i rapporti con l'ACN e garantisce l'inserimento nella banca dati nazionale.

Il percorso di adeguamento alla direttiva NIS2 è attualmente in fase di attuazione. La ASL di Nuoro ha avviato un processo di verifica dei requisiti minimi di sicurezza, con particolare attenzione alla mappatura delle infrastrutture critiche, alla valutazione del rischio e alla definizione di misure tecniche e organizzative atte a garantire la continuità operativa e la resilienza digitale.

Pur trattandosi di un percorso ancora in evoluzione, si evidenzia un concreto impegno da parte dell'Azienda nel rafforzare la protezione dei dati e dei servizi essenziali, in piena coerenza con gli standard introdotti a livello europeo. Il completamento delle attività di monitoraggio, auditing interno e aggiornamento continuo delle policy rappresenta un presupposto fondamentale per il raggiungimento di una compliance strutturata e sostenibile nel tempo.

CAPITOLO III

Ecosistema dei dati sanitari: attori, flussi informativi e interoperabilità

III.1. Il Fascicolo Sanitario Elettronico: evoluzione, contenuti e implicazioni normative

Il Fascicolo Sanitario Elettronico (FSE) è la raccolta digitale di dati e documenti clinici relativi a un paziente, generati da eventi presenti e trascorsi, riguardanti l'assistenza sanitaria ricevuta. È uno strumento che permette di avere una visione completa e cronologica della storia sanitaria di una persona, facilitando la condivisione delle informazioni tra i professionisti sanitari coinvolti nella sua cura.

Il percorso che ha portato allo sviluppo e all'implementazione del Fascicolo Sanitario Elettronico (FSE) è frutto di un'evoluzione normativa e tecnologica progressiva, mirata a superare i limiti della documentazione cartacea e a favorire la condivisione delle informazioni sanitarie.

L'esigenza da cui prese avvio la creazione del FSE era un bisogno avvertito dagli operatori sanitari sia dagli utenti del sistema sanitario, non solo a livello nazionale, italiano e straniero, ma anche internazionale[73].

Le prime visioni di un fascicolo sanitario informatizzato emergono già nei primi anni 2000, spinte dalla crescente consapevolezza del potenziale delle tecnologie dell'informazione e della comunicazione (ICT) in ambito sanitario.

L'obiettivo primario era la dematerializzazione dei referti e delle cartelle cliniche, al fine di ottimizzare i processi amministrativi e clinici e raccogliere ogni informazione attinente alla salute di un paziente e condividerla fra più soggetti per via elettronica.

Il FSE costituiva «una nuova forma di comunicazione e gestione dei dati del paziente, che permette di far confluire in un unico documento informatizzato tutti i dati sanitari di quest'ultimo, in modo da facilitare l'accesso e l'utilizzo degli stessi da parte dei terzi autorizzati al momento del bisogno[74].

---

[73] GUARDA, I dati sanitari e le Comunicazioni della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, COM/2004/0356, *Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, 30 aprile 2004, e COM/2005/0229, i2010 – *Una società dell'informazione per la crescita e l'impiego*, entrambe consultabili in www.eur-lex.europa.eu. V. anche VICARELLI e BRONZINI, *La sanità digitale: dimensioni di analisi e prospettive di ricerca,* in Politiche sociali, 2018, fasc. 2, 147 ss., spec. 150.

[74] COMANDÉ, NOCCO, PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinar*e, in Riv. it. med. leg., 2012, 105 s.

Era uno strumento pensato per la persona e subordinato alla volontà della stessa[75].

Nelle linee guida del 16 luglio 2009, veniva qualificato dal Garante per la protezione dei dati personali come «condivisione informatica, da parte di distinti organismi o 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 in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica[76].

Con il Decreto Legge del 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221 venne istituito il Fascicolo Sanitario Elettronico.

Il decreto all' art.12, comma 1, definiva il FSE come «l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito».

Il FSE venne utilizzato dalle Regioni e dalle Province autonome con finalità di prevenzione, diagnosi, cura e riabilitazione, lo studio e la ricerca scientifica in campo medico, biomedico ed epidemiologico; la programmazione sanitaria, la verifica delle qualità delle cure e la valutazione dell'assistenza, garantendo inoltre l'interoperabilità dello strumento su tutto il territorio nazionale.

Il DPCM 29 settembre 2015, n. 178[77], di approvazione del regolamento di attuazione del FSE, stabiliva che ciascuna Regione e Provincia autonoma doveva "istituire il Fascicolo Sanitario Elettronico (FSE) attraverso una infrastruttura tecnologica capace di interoperare con le altre soluzioni regionali di FSE, esponendo opportuni servizi che consentono la realizzazione di una serie di processi interregionali". Quindi, il Decreto stabiliva cosa era il FSE e quali erano contenuti minimi:

- dati identificativi e amministrativi dell'assistito;
- referti;
- verbali pronto soccorso;
- lettere di dimissione;

---

[75] FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit 305: «*Molte sarebbero state le scelte possibili nel delineare l'architettura giuridica del fascicolo sanitario elettronico, come pure del dossier sanitario: lo si sarebbe potuto incentrare sul medico, garantendo la completezza delle informazioni, o sulla struttura sanitaria, conferendo maggiore rilevanza agli aspetti amministrativi. Si è scelto, invece, di incentrarlo sull'individuo e di garantire l'autodeterminazione del medesimo. Il fascicolo sanitario elettronico, in questa concezione, è dell'individuo e questi ne gestisce le informazioni. Può decidere, quindi, non solo se costituirlo o meno, ma anche quali eventi sanitari rendere visibili, quali oscurare e quali deoscurare. Il principio di autodeterminazione prevale quindi su altre diverse esigenze, quali appunto quella già citata della completezza delle informazioni contenute nel fascicolo».*

[76] Garante della Privacy, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*" del 16 luglio 2009.

[77] DPR 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico.

- profilo sanitario sintetico;
- dossier farmaceutico.

Nell'ambito della Strategia per la crescita digitale 2014-2020, presentata dall'Agenzia per l'Italia Digitale a marzo 2015, è stato sviluppato il Patto per la Sanità digitale, con l'obiettivo di definire la azioni di intervento per promuovere la trasformazione digitale[78].

Al fine di rendere interoperabile il FSE è intervenuta, attraverso un apposito stanziamento, la legge di bilancio 2017 (art. 1, co. 382, L. 232/2016) disponendo, mediante l'infrastruttura del Sistema Tessera Sanitaria, l'identificazione dell'assistito registrato all'Anagrafe Nazionale degli Assistiti (ANA), oltre ad una serie di servizi idonei ad interrogare il Sistema.

Con il Decreto Legge n. 34 del 2020[79] sono state apportate diverse novità rilevanti:

la prima riguardava la modifica dell'art. 12 del D.lgs. 179/2012, abrogando il paragrafo 3 bis, con la conseguente l'eliminazione del consenso all'alimentazione del FSE decretando

di fatto l'apertura di un FSE per ogni cittadino; la seconda consentiva l'ampliamento della base dati, con la conseguente apertura a tutti i documenti digitali sanitari e socio-sanitari, riferiti alle prestazioni sia a carico del Sistema Sanitario Nazionale che fuori del SSN[80].

Quindi, fino al 2020 ogni Regione si era dotata di un proprio sistema per la gestione del Fascicolo sanitario elettronico, di cui alcune in regime di sussidiarietà, fino ad arrivare al PNRR che, anche attraverso il coinvolgimento dell'Agenzia nazionale per i servizi sanitari regionali (Agenas), ha previsto il potenziamento dei sistemi informativi e degli strumenti digitali sanitari nell'ambito dei finanziamenti della Missione 6-Salute.

Come evidenziato nelle Linee guida per l'attuazione del FSE, adottate con Decreto del Ministero della salute del 20 maggio 2022[81] (32), il FSE era concepito in modo basilare e la sua attuazione e diffusione erano parziali. Risultava un'alimentazione non uniforme

---

[78] Camera dei Deputati, *Il nuovo fascicolo sanitario elettronico*, in https://temi.camera.it/leg19/post/il-nuovo-fascicolo-sanitario

[79] Decreto Legge n. 34/2020, *Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19 (c.d. "Rilancio")*

[80] I continui interventi del legislatore, susseguitisi in arco di tempo particolarmente ristretto, evidenziano la delicatezza e la problematicità del tema. La cospicua attività dell'Autorità garante, non solo di monitoraggio, sanzionatoria e consultiva, ne conferma la complessità. Si considerino, ad esempio, il provvedimento del Garante per la protezione dei dati personali del 26 luglio 2017, n. 341, "*Parere su uno schema di decreto del MEF di concerto con il Ministero della salute, concernente le modalità tecniche e i servizi telematici resi disponibili all'infrastruttura nazionale per l'interoperabilità dei FSE*", e il provvedimento del Garante per la protezione dei dati personali del 27 settembre 2018, n. 456, "*Parere su uno schema di decreto in tema di interoperabilità del Fascicolo Sanitario Elettronico (FSE) - 27 settembre 2018*".

[81] D.M. 20 maggio 2022, *Adozione delle Linee guida per l'attuazione del Fasciolo sanitario elettronico*

nelle varie Regioni. Infatti, il FSE non veniva alimentato allo stesso modo da parte di tutte le strutture sanitarie. Questo comportava l'incapacità di rispondere ai bisogni dei pazienti[82].

In seguito, il percorso normativo ha condotto al Decreto del Ministero della Salute del 7 settembre 2023, che ha introdotto il concetto di Fascicolo Sanitario Elettronico 2.0.

Come avremo modo di vedere nel paragrafo successivo, il FSE 2.0 ha consolidato il ruolo del FSE come strumento per rendere disponibili i dati sanitari personali per garantire le migliori cure, contenendo la storia clinica dei pazienti ed essendo accessibile al paziente stesso e ai medici.

Questo aggiornamento ha rafforzato le funzionalità del FSE, migliorando l'interoperabilità tra i sistemi regionali e nazionali e definendo standard più stringenti per la qualità e la sicurezza dei dati.

III.1.1. Il Fascicolo Sanitario Elettronico 2.0

Come evidenziato nel paragrafo precedente, l'evoluzione normativa del Fascicolo Sanitario Elettronico ha trovato un punto di svolta con il Decreto del Ministro della Salute del 7 settembre 2023, pubblicato nella Gazzetta Ufficiale n. 249 del 24 ottobre 2023, noto come Decreto FSE 2.0.

Il FSE 2.0 è frutto di una lunga interlocuzione istituzionale tra diversi organi e del Garante privacy, anche a seguito dei citati pareri: n. 294 del 22 agosto 2022 non favorevole sullo schema di Decreto del Ministero della salute, parallelo al provvedimento n. 295 del 2022, sullo schema di decreto relativo all'EDS e n. 256 dell'8 giugno 2023, che ha espresso il parere positivo in relazione allo schema di decreto sul FSE[83].

Il delineato FSE 2.0 è un sistema centrale per l'ammodernamento tecnologico dei servizi sanitari e, nell'ordinamento italiano, una delle maggiori sfide per la regolamentazione del trattamento dei dati relativi alla salute con il conseguente bilanciamento di interessi[84].

Nel quadro del Piano Nazionale di Ripresa e Resilienza (PNRR), il progetto del FSE ha assunto un nuovo volto, dando vita al cosiddetto FSE 2.0. Il PNRR ha rappresentato

[82] CORSO S., *Il Fascicolo Sanitario Elettronico 2.0. Spunti per una lettura critica*, NLCC 2/2024

[83] POSTERARO, *Parere del Garante privacy sullo schema di decreto sul Fascicolo Sanitario Elettronico (FSE)*, in www.federalismi.it, Osservatorio di diritto sanitario, ottobre 2023.

[84] CORSO S., *Il Fascicolo Sanitario Elettronico 2.0. Spunti per una lettura critica*, NLCC 2/2024

e rappresenta una straordinaria occasione di trasformazione e progressione digitale per il Servizio Sanitario Nazionale (SSN[85]).

Questa nuova versione non è solo un aggiornamento tecnico, ma un cambio di paradigma. L'obiettivo era creare una piattaforma nazionale interoperabile, in grado di garantire: uniformità nell'accesso e nei servizi su tutto il territorio; interoperabilità tra i sistemi regionali e le strutture sanitarie pubbliche e private; strumenti intelligenti per l'analisi dei dati clinici a fini di ricerca, epidemiologia e governance sanitaria.

Questo Decreto ha ridefinito i contenuti del FSE, delineato le responsabilità dei soggetti coinvolti nella sua implementazione e stabilito le misure di sicurezza per il trattamento dei dati personali, introducendo rilevanti innovazioni sotto il profilo tecnologico, organizzativo e giuridico.

Nel FSE 2.0, consultabile sia dai pazienti sia dagli operatori, è possibile avere una visione di sintesi dello stato di salute, sia consultare tutta la storia clinica del paziente.

L'ambito di applicazione è ampio, rivolto a tutti i cittadini iscritti al SSN.

Di seguito una descrizione sommaria dei principali articoli.

Fin dalle prime disposizioni (Art. 1), il decreto sottolinea la funzione centrale del FSE 2.0 nel contesto del SSN. Non si tratta più solo di un archivio digitale della documentazione sanitaria, ma di una piattaforma strategica per:

- promuovere la continuità assistenziale, grazie alla condivisione tempestiva delle informazioni tra professionisti sanitari;

- migliorare l'efficienza dei servizi e la personalizzazione delle cure;

- fornire dati strutturati per il monitoraggio e la programmazione sanitaria, anche in ottica predittiva e di sanità pubblica.

All'articolo 2, individua i contenuti del FSE, i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità di accesso.

Uno degli aspetti più innovativi è disciplinato dall'Articolo 3, che prevede l'alimentazione automatica e standardizzata del FSE con tutti i dati e documenti generati nell'ambito del SSN o da professionisti accreditati. Questo passaggio segna la fine della logica opt-in, tipica del primo FSE, e introduce un modello per cui l'alimentazione è obbligatoria e continua, a prescindere dal consenso esplicito.

[85] ANDREA ROTOLO, FRANCESCO LONGO, CLAUDIO CACCIA, *Una visione sistemica per i silos digitali del PNRR*, Mecosan – Issn 1121-6921, Issne 2384-8804, 2024, 130 Doi.

Tale innovazione mira a superare la frammentarietà e l'incompletezza dei fascicoli, garantendo una base informativa completa e aggiornata, indispensabile per cure efficaci e sicure.

Tuttavia, la riorganizzazione non è comunque definitiva, in quanto il comma 3 dello stesso rinvia a successivi decreti, ex art. 12, comma 7, D.L. n. 179/2012, per regolare i contenuti degli ulteriori dati e documenti.

L'Articolo 4 specifica in modo puntuale le tipologie di documenti che devono essere presenti nel FSE, includendo: referti, lettere di dimissione, verbali di pronto soccorso, prescrizioni, piani terapeutici, vaccinazioni, dati provenienti dalla medicina generale e pediatria di libera scelta, informazioni amministrative, come esenzioni o scelta del medico.

Una novità rilevante è l'apertura all'inserimento di dati auto-generati dal cittadino, attraverso dispositivi digitali, che potranno integrare il fascicolo con informazioni utili alla personalizzazione delle cure.

Il rapporto tra il cittadino e il proprio fascicolo è disciplinato dall'Articolo 5, che definisce il FSE come uno strumento di *empowerment* del paziente. I diritti riconosciuti includono:

- l'accesso integrale e gratuito ai propri dati;
- il download dei documenti e possibilità di condividerli;
- integrazione di note personali;
- oscuramento selettivo di singoli documenti (anche per il medico curante);
- revoca del consenso alla visione per scopi diversi dalla cura.

Questo approccio rispecchia il principio europeo del *data ownership*[86], per cui il paziente è al centro del sistema informativo e mantiene il controllo sul trattamento dei propri dati.

Il dossier farmaceutico è stato invece espunto dal testo del decreto e non trova più diretta disciplina all'interno del nuovo impianto normativo del FSE 2.0[87]. La sua regolamentazione è rinviata a un successivo decreto attuativo, previsto dal comma 15-quater dell'articolo 12 del Decreto Legge n. 179 del 2012.

[86] Il concetto di data ownership nel FSE 2.0 è in linea con il Regolamento Generale sulla Protezione dei Dati, che stabilisce i diritti degli individui riguardo al trattamento dei propri dati personali. In particolare, il GDPR garantisce: il diritto di accesso ai propri dati personali, Il diritto di rettifica dei dati inesatti., alla cancellazione, alla limitazione del trattamento e alla portabilità dei dati.

[87] CORSO S., *Il Fascicolo Sanitario Elettronico 2.0. Spunti per una lettura critica*, NLCC 2/2024

In tale contesto, il dossier farmaceutico sarà configurato come un servizio erogato tramite l'Ecosistema dei Dati Sanitari (EDS), a conferma della tendenza verso una maggiore modularità e personalizzazione dei servizi digitali in ambito sanitario.

Secondo l'Articolo 6, l'accesso al FSE da parte degli operatori è strettamente subordinato all'esistenza di una relazione di cura attiva. Ogni consultazione è tracciata, e il cittadino può visualizzare chi ha avuto accesso al fascicolo e in quale data. Questo meccanismo garantisce sia il rispetto della riservatezza e della finalità clinica che la responsabilità degli operatori nel trattamento dei dati, prevenendo gli accessi impropri.

L'Articolo 8 affronta il delicato tema del trattamento dei dati, armonizzando la normativa italiana con il Regolamento (UE) 2016/679 (GDPR). Il trattamento dei dati all'interno del FSE è considerato lecito anche senza consenso, se finalizzato alla cura, alla sanità pubblica o alla ricerca scientifica (in forma pseudonimizzata). Viene così valorizzato l'interesse collettivo alla salute, senza rinunciare alle garanzie individuali, quali la sicurezza, la minimizzazione dei dati, il diritto di accesso e di rettifica.

All'art. 9, fra i diritti dell'assistito, si riconferma il diritto all'oscuramento. Il suo esercizio comporta che i documenti scelti dall'assistito stesso non siano più visibili nel FSE, compreso lo stesso oscuramento (c.d. oscuramento dell'oscuramento). L'oscuramento potrà essere revocato. Un aspetto centrale della disciplina del Fascicolo Sanitario Elettronico 2.0 riguarda la gestione dei documenti oscurati dal cittadino. È importante sottolineare che tali documenti, anche se oscurati, non vengono eliminati dal sistema: restano comunque archiviati all'interno del FSE. Il decreto, infatti, non prevede alcuna facoltà per l'utente di cancellare o rimuovere dati o documenti una volta che questi siano stati inseriti nel fascicolo, indipendentemente dalla loro natura o dal livello di sensibilità delle informazioni contenute.

Tra le novità più rilevanti introdotte dal Decreto del 7 settembre 2023 vi è l'articolo 12, comma 3, che rappresenta un significativo passo avanti rispetto alla versione precedente del sistema. In questa disposizione, si sancisce esplicitamente la responsabilità dei soggetti coinvolti nell'alimentazione del FSE — come medici, strutture sanitarie pubbliche e private — in caso di mancato, errato o tardivo caricamento dei dati sanitari.

Questa previsione recepisce direttamente le osservazioni espresse dal Garante per la protezione dei dati personali nel provvedimento n. 294 del 2022.

Il periodo di conservazione è stabilito dall'Articolo 10, il quale prevede che i dati e i documenti sanitari inseriti nel FSE devono essere conservati per un periodo di 10 anni a partire dalla data di inserimento. Tale periodo può essere esteso nel caso in cui sussistano

specifiche esigenze legate alla tutela della salute dell'assistito o per finalità di ricerca scientifica, nel rispetto delle normative vigenti in materia di protezione dei dati personali.

La disposizione mira a garantire un equilibrio tra la necessità di conservare le informazioni sanitarie per un adeguato periodo, al fine di assicurare la continuità delle cure e supportare attività di ricerca e pianificazione sanitaria, e la tutela dei diritti dell'assistito in materia di privacy e protezione dei dati personali.

Fondamentale è il principio di interoperabilità[88]: ogni FSE regionale deve essere integrato nella Piattaforma Nazionale e seguire standard comuni, al fine di garantire la continuità assistenziale anche in mobilità.

L'Articolo 12 stabilisce quali sono i soggetti che concorrono alla alimentazione del FSE. Relativamente alla consultazione di tali dati e documenti, per la finalità di cura, fermo restando il rispetto dei diritti dell'assistito di cui all'Art. 9, potrà accedere il personale

sanitario autorizzato.

Sul punto, l'Art. 15 ne riporta un cospicuo elenco, consultabile nel suddetto decreto.

L'art. 16 prevede il diritto per l'assistito di accedere integralmente al proprio FSE, consultare i dati e i documenti presenti, e gestire le autorizzazioni relative alla visibilità delle informazioni, attraverso strumenti digitali per facilitare l'accesso.

L'art. 17 stabilisce che l'accesso al FSE da parte di soggetti terzi, diversi dai professionisti sanitari e dall'assistito, è consentito solo nei casi previsti dalla legge, come per finalità di ricerca scientifica o sanità pubblica, e comunque nel rispetto delle normative sulla protezione dei dati personali.

Gli articoli dal 18 al 27 del Decreto del 7 settembre 2023 completano il quadro normativo del Fascicolo Sanitario Elettronico 2.0, affrontando aspetti cruciali legati alla governance, alla sicurezza e all'interoperabilità del sistema.

Si parte con il riconoscimento del ruolo centrale del Ministero della Salute, che assume la titolarità del trattamento dei dati contenuti nel FSE quando questi sono utilizzati per finalità di profilassi internazionale. In un mondo sempre più interconnesso, dove le emergenze sanitarie possono rapidamente oltrepassare i confini nazionali, è fondamentale che il Ministero possa accedere e trattare dati come vaccinazioni, esiti di test diagnostici e certificazioni sanitarie, per garantire la sicurezza collettiva anche in ambito internazionale.

[88] Uno degli elementi cardine del Fascicolo Sanitario Elettronico 2.0 è rappresentato dal principio di interoperabilità, inteso come la capacità dei diversi sistemi informativi sanitari — regionali, nazionali e anche europei — di comunicare tra loro, scambiando e comprendendo dati in maniera coerente, sicura e strutturata. In linea con le iniziative dell'Unione Europea per l'European Health Data Space (EHDS), permetterà ai cittadini europei di accedere ai propri dati sanitari anche quando si trovano in un altro Stato membro, facilitando la mobilità sanitaria.

Il decreto prevede inoltre che, in situazioni di emergenza, gli operatori sanitari possano accedere al FSE anche in assenza di una relazione di cura attiva. Questa previsione, contenuta nell'articolo 20, è pensata per tutelare la salute del paziente in contesti critici, dove la tempestività delle informazioni può fare la differenza tra un intervento efficace e un rischio evitabile.

Per garantire trasparenza e responsabilità, ogni operazione effettuata sul FSE viene registrata: chi accede, quando e per quale motivo. A rafforzare ulteriormente la fiducia dei cittadini, è previsto un servizio di notifica che li informa in tempo reale su eventuali consultazioni o modifiche del proprio fascicolo.

Il FSE non si limita a raccogliere dati clinici, ma integra anche informazioni amministrative fondamentali, come il codice fiscale, le esenzioni e la scelta del medico. Questo consente una visione completa e coerente del percorso assistenziale del cittadino. Anche chi non ha un medico di riferimento, come i cittadini temporaneamente presenti sul territorio nazionale, viene incluso nel sistema grazie a un indice nazionale che ne garantisce la tracciabilità e l'accesso ai servizi.

La sicurezza dei dati è un pilastro imprescindibile del nuovo impianto normativo. Il decreto impone misure tecniche e organizzative rigorose: dalla cifratura dei dati all'autenticazione forte, fino al controllo degli accessi. Tutto è pensato per proteggere la riservatezza e l'integrità delle informazioni, in piena conformità con il GDPR.

Un altro elemento chiave è l'interoperabilità. Ogni sistema regionale deve dialogare con la Piattaforma Nazionale, seguendo standard comuni. Questo garantisce che il cittadino possa ricevere cure coerenti e coordinate, ovunque si trovi sul territorio nazionale.

Infine, l'articolo 27 disciplina la fase di transizione dal vecchio al nuovo sistema. Vengono stabiliti tempi e modalità per l'adeguamento dei sistemi informativi regionali e delle strutture sanitarie, assicurando che il passaggio al FSE 2.0 avvenga in modo ordinato, senza interruzioni nei servizi e con il massimo rispetto dei diritti degli assistiti.

Da ciò si evince la portata del nuovo Fascicolo Sanitario Elettronico 2.0, il quale segna un'evoluzione normativa e culturale tale da trasformarlo da strumento passivo di archiviazione a piattaforma attiva di cura, governance e innovazione.

Gli articoli descritti forniscono un'ossatura solida e ambiziosa, ma pongono anche sfide significative in termini di attuazione, uniformità territoriale, alfabetizzazione digitale e sostenibilità.

Il successo del FSE 2.0 dipenderà dalla capacità del sistema sanitario di riorganizzarsi in chiave digitale, nel rispetto dei diritti e dei bisogni dei cittadini.

Le sfide future riguarderanno principalmente il consolidamento dell'interoperabilità, l'affinamento delle misure di sicurezza e la promozione di una cultura della protezione dei dati che bilanci l'innovazione con la tutela dei diritti fondamentali. La piena realizzazione del potenziale dell'EDS e la sua armonizzazione con l'EHDS richiederanno un impegno costante e una collaborazione sinergica tra tutti gli attori coinvolti, per garantire che i dati sanitari siano una risorsa preziosa per la salute collettiva, gestita con la massima responsabilità e rispetto per l'individuo.

III.1.2. Indicatori sull'utilizzo del FSE

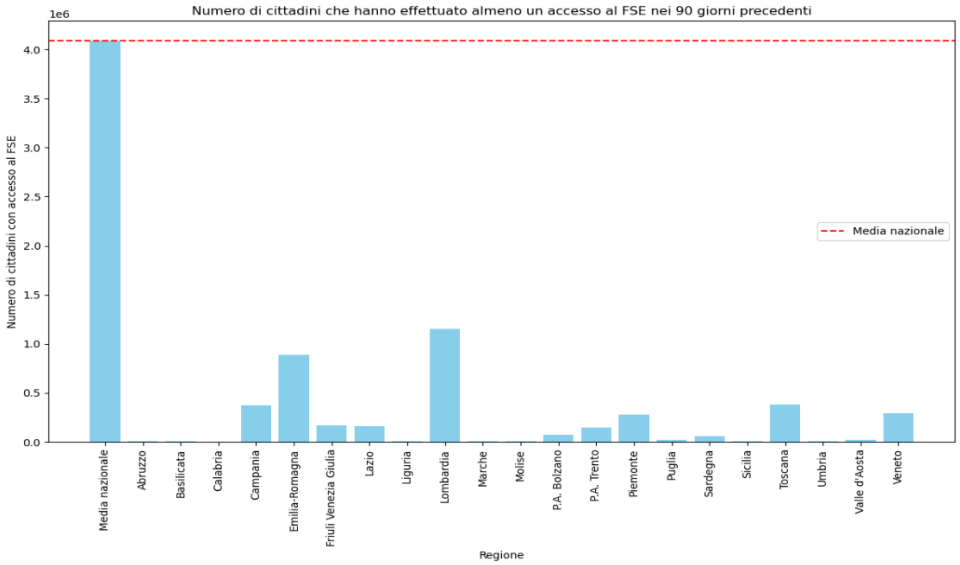
L'analisi dell'utilizzo del Fascicolo Sanitario Elettronico (FSE) rappresenta un elemento cruciale per valutare l'efficacia delle politiche di digitalizzazione della sanità in Italia. Il presente documento riporta i risultati di un'analisi condotta dal Ministero della Salute e dal Dipartimento per la Trasformazione Digitale, con dati aggiornati al 30 novembre 2024. L'elaborazione e la visualizzazione dei dati sono state supportate da un sistema di intelligenza artificiale sviluppato da Microsoft, al fine di facilitare la comprensione e l'interpretazione delle informazioni relative all'adozione dell'FSE.

L'analisi si concentra su due dimensioni principali: l'accesso al FSE da parte dei cittadini e l'utilizzo dello strumento da parte dei professionisti sanitari, in particolare Medici di Medicina Generale (MMG) e medici specialisti[89].

Secondo i dati disponibili, l'utilizzo del FSE da parte dei cittadini italiani è ancora limitato. In media, solo il 18% dei cittadini ha effettuato l'accesso al proprio fascicolo elettronico nel trimestre compreso tra giugno e agosto 2024.

L'indicatore evidenzia il numero di cittadini assistiti per Regione e Provincia autonoma che hanno effettuato almeno un accesso nei 90 giorni precedenti alla data di rilevazione rispetto al totale degli assistiti per i quali è stato messo a disposizione sul fascicolo almeno un documento nello stesso periodo.

[89]Ministero della Salute e Dipartimento per La Trasformazione Digitale, I dati di utilizzo del Fascicolo Sanitario Elettronico da parte di cittadini, medici e aziende sanitarie, https://monitopen.fse.salute.gov.it/usage#companies.

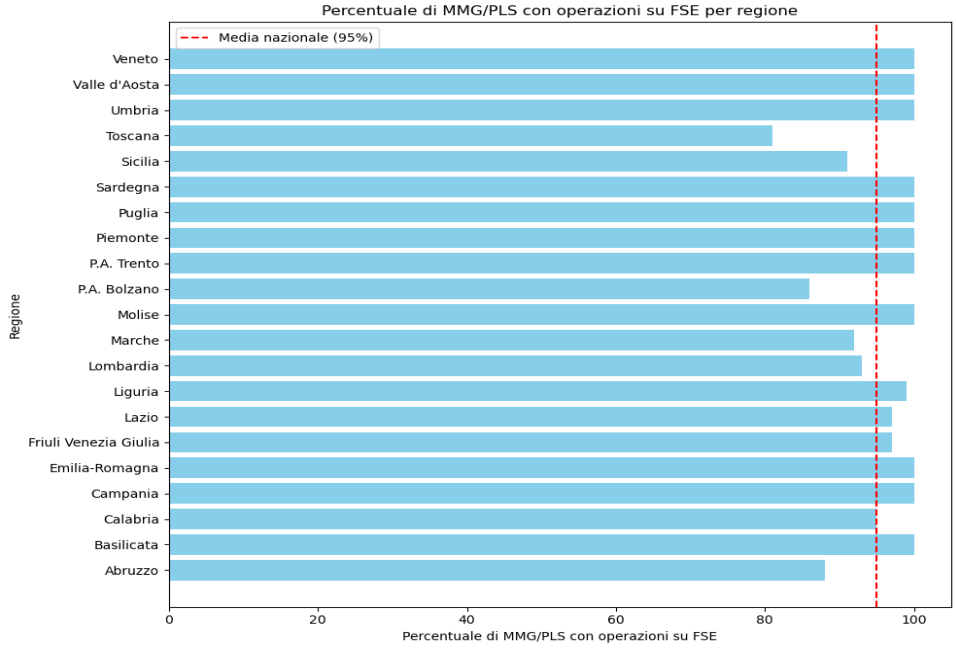


Dal grafico si evince che Lombardia è la regione con il numero assoluto più alto di accessi (oltre 1,15 milioni), seguita da Emilia-Romagna e Campania.

Alcune regioni, pur avendo una percentuale alta (es. P.A. Trento con il 51%), mostrano numeri assoluti più contenuti a causa della popolazione inferiore.

Regioni come Sicilia, Calabria e Abruzzo registrano sia percentuali che numeri assoluti molto bassi, indicando una doppia criticità: bassa penetrazione e basso coinvolgimento.

Per quanto riguarda l'utilizzo da parte dei MMG si evidenzia un'elevata partecipazione con un tasso di utilizzo del 95%.



L'utilizzo del fascicolo sanitario da parte delle aziende sanitarie è misurato attraverso il conteggio dei medici specialisti, dipendenti da aziende sanitarie pubbliche, abilitati al Fascicolo Sanitario Elettronico.

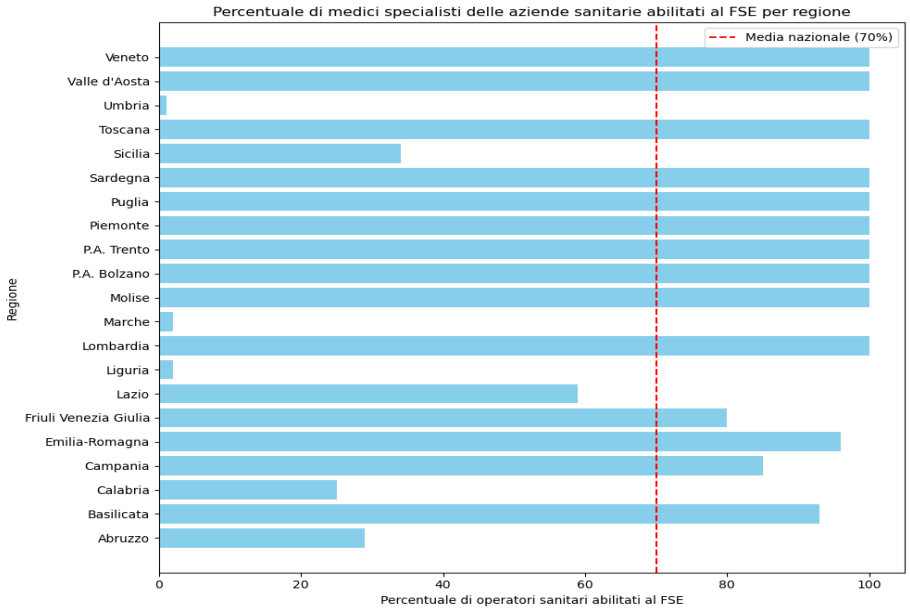
L'abilitazione dei medici specialisti alla consultazione del Fascicolo Sanitario Elettronico (FSE) rappresenta un indicatore fondamentale per valutare il grado di integrazione digitale all'interno delle aziende sanitarie pubbliche italiane. Questo parametro misura la percentuale di specialisti che, formalmente, hanno accesso alla piattaforma FSE e possono quindi consultare i documenti clinici dei pazienti, contribuendo a una presa in carico più informata e coordinata.

A livello nazionale, la media di abilitazione si attesta al 70%, ma l'analisi regionale rivela una forte disomogeneità.

Le Regioni e Province autonome virtuose sono ben 11 e raggiungono il 100% di abilitazione, segno di un'infrastruttura digitale ben consolidata e di una governance efficace: Lombardia, Molise, P.A. Bolzano, P.A. Trento, Piemonte, Puglia, Sardegna, Toscana, Valle d'Aosta e Veneto.

Le Regioni in difficoltà sono Umbria (1%), Liguria (2%) e Marche (2%), le quali mostrano livelli di abilitazione estremamente bassi, che potrebbero riflettere criticità organizzative, ritardi nell'implementazione o mancanza di formazione del personale.

Inoltre, si notano situazioni intermedie come il Lazio (59%) e Sicilia (34%), pur avendo un numero elevato di specialisti, si collocano sotto la media nazionale, suggerendo margini di miglioramento significativi.



I dati presentati delineano un quadro eterogeneo dell'adozione del FSE in Italia.

Sebbene si osservi un'elevata partecipazione dei Medici di Medicina Generale, l'accesso da parte dei cittadini rimane limitato e l'abilitazione dei medici specialisti mostra forti disomogeneità regionali.

Questi risultati evidenziano la necessità di interventi mirati a livello nazionale per promuovere un utilizzo più ampio ed equo del FSE.

Tali interventi dovrebbero concentrarsi sia sull'incentivazione dell'accesso da parte dei cittadini, attraverso campagne di informazione e semplificazione delle procedure, sia sul superamento delle criticità organizzative e formative che ostacolano l'abilitazione e l'utilizzo efficace del FSE da parte dei medici specialisti. Solo attraverso un'azione coordinata e sinergica sarà possibile sfruttare appieno il potenziale del FSE per una sanità digitale realmente integrata e orientata al paziente.

III.2. La costruzione dell'Ecosistema dei Dati Sanitari in Italia: il ruolo del Garante per la protezione dei dati personali nel bilanciamento tra innovazione digitale e diritti fondamentali

Parallelamente al Regolamento europeo sull'EHDS, l'Italia ha lavorato all'elaborazione di un Decreto legislativo per disciplinare l'Ecosistema Dati Sanitari (EDS), strumento essenziale per l'organizzazione, l'interoperabilità e la valorizzazione dei dati sanitari nel nostro Paese.

Il percorso che ha portato alla definizione del decreto sull'Ecosistema dei Dati Sanitari è stato tutt'altro che lineare.

Un primo passo significativo verso la realizzazione di tale ecosistema è stato compiuto con l'introduzione dell'art. 12, comma 15-quater del D.L. 179/2012, convertito con modificazioni dalla L. 221/2012 e successivamente integrato. Questa norma ha rappresentato una svolta nell'architettura istituzionale e tecnica della sanità digitale italiana, delineando con chiarezza le responsabilità dei diversi attori pubblici coinvolti e i requisiti tecnologici a cui l'EDS avrebbe dovuto conformarsi.

Il Ministero della Salute, in collaborazione con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, è in-

caricato della progettazione e implementazione dell'Ecosistema. Tale governance è pensata per garantire omogeneità a livello nazionale, adeguatezza delle infrastrutture tecnologiche e soprattutto sicurezza cibernetica, attraverso un raccordo con l'Agenzia per la cybersicurezza nazionale.

L'EDS si configura come una piattaforma federata e interoperabile, alimentata dai dati trasmessi dalle strutture sanitarie e socio-sanitarie pubbliche e private accreditate, dagli enti del Servizio Sanitario Nazionale e dai flussi gestiti attraverso il Sistema Tessera Sanitaria. Questo lo qualifica come nodo cruciale nella gestione e valorizzazione dei dati sanitari su scala nazionale, ma anche come punto di raccordo con le strategie europee per la circolazione secondaria dei dati per finalità di ricerca, sanità pubblica e policy making.

Particolare attenzione è stata dedicata, all'interno dello stesso comma, alla qualità e coerenza semantica dei dati. A tale scopo, l'AGENAS è chiamata a rendere disponibili alle strutture sanitarie strumenti informatici standardizzati per la validazione formale e semantica dei documenti, la loro trasformazione in formati interoperabili, e il loro invio corretto sia all'EDS nazionale che al Fascicolo Sanitario Elettronico (FSE) regionale. In tal modo, il legislatore ha cercato di superare la frammentazione informativa tra Regioni, promuovendo l'armonizzazione dei dati a livello nazionale.

Un ulteriore elemento qualificante è rappresentato dalle disposizioni relative alla tutela dei dati personali particolarmente sensibili. Il legislatore prevede esplicitamente che i dati relativi a condizioni sanitarie meritevoli di particolare protezione (ad esempio, sieropositività, IVG, violenza sessuale, tossicodipendenza, parto in anonimato) siano accessibili esclusivamente all'assistito. Solo con il consenso esplicito, informato e specifico dell'interessato, tali dati possono essere resi visibili a terzi, inclusi i professionisti sanitari. È inoltre garantito all'assistito il diritto all'oscuramento, esercitabile in fase di erogazione della prestazione o successivamente, anche attraverso funzionalità online. Questo diritto, che può essere revocato in ogni momento, è strutturato in modo da impedire che la semplice oscurata possa rivelare indirettamente l'esistenza di informazioni sensibili, assicurando così un elevato livello di protezione.

L'art. 12, comma 15-quater si pone quindi come dispositivo normativo centrale nel processo di digitalizzazione della sanità, esprimendo l'intento del legislatore di conciliare innovazione tecnologica, efficienza amministrativa e garanzie sostanziali di tutela dei diritti fondamentali. In esso si riflette una visione della sanità digitale che va oltre la mera informatizzazione dei servizi, e che ambisce invece alla costruzione di un'infrastruttura

pubblica orientata alla fiducia, alla responsabilità e alla partecipazione consapevole dei cittadini.

Tra le tappe più significative c'è sicuramente il ruolo svolto dal Garante per la protezione dei dati personali, che non si è limitato a esprimere un parere tecnico, ma ha assunto un vero e proprio ruolo di garante sostanziale dell'equilibrio tra innovazione e diritti.

Prima dell'adozione definitiva, infatti, lo schema di Decreto è stato sottoposto dal Ministero della Salute al parere obbligatorio del Garante per la protezione dei dati personali, come previsto dall'art. 36, commi 4 e 5 del GDPR[90].

Nella nota di trasmissione, il Ministero ha evidenziato che lo schema di Decreto e quello sul Fascicolo sanitario elettronico (FSE), peraltro trasmesso nella stessa data, si inserivano nel percorso per la riforma delle disposizioni attuative del FSE alla luce dello specifico investimento del Piano Nazionale di Ripresa e Resilienza.

Il parere, espresso dal Garante il 22 agosto 2022 (Doc-Web 9802752)[91], è stato nettamente negativo. L'Autorità ha sollevato osservazioni molto critiche non solo sul merito del testo ma anche sul metodo seguito per costruirlo.

In primis, il Garante ha sottolineato l'impossibilità di valutare seriamente il sistema basato proprio sul Fascicolo Sanitario Elettronico (FSE), senza definire con precisione proprio il funzionamento e le regole del FSE stesso.

Infatti, in sostanza, se lo scopo dell'EDS era l'utilizzo di dati provenienti dal Fascicolo, senza aver prima completato la riforma del FSE, né aver dato seguito alle numerose raccomandazioni che l'Autorità aveva già espresso negli anni sul tema.

Pertanto, l'impostazione normativa rischiava di essere fragile e scollegata dalla realtà operativa, in quanto costruita su un sistema non ancora ben definito.

Peraltro, il testo presentato risultava incompleto anche nei contenuti: molte delle decisioni venivano rimandate ad atti successivi ancora da emanare.

Tra i principali motivi della bocciatura si evidenziano:

- La carente tutela dei diritti degli interessati: il testo non prevedeva meccanismi sufficienti per garantire che i cittadini fossero consapevoli e pienamente informati

[90] "4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento. 5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica".

[91] Garante della Privacy, 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) del 22 agosto 2022.

sull'utilizzo dei loro dati. Mancava una disciplina chiara in merito al consenso e alla possibilità di opporsi all'uso secondario dei dati (come ricerca, pianificazione, policy making);

- l'assenza di trasparenza e controllabilità: non erano previste misure adeguate volte ad informare gli utenti sul trattamento dei dati, sulle finalità specifiche e sui soggetti autorizzati all'accesso. Il rischio era quello di un sistema poco rispettoso dell'autodeterminazione informativa;
- l'insufficienza delle garanzie per l'uso secondario dei dati: l'uso dei dati per finalità diverse da quelle di cura (uso secondario) avrebbe potuto avvenire anche in assenza del consenso espresso dell'interessato, con una presunzione di legittimità che il Garante ha ritenuto inaccettabile, soprattutto in relazione alla delicatezza dei dati sanitari;
- la debolezza nelle misure di sicurezza e governance: il Decreto non specificava in modo chiaro i livelli minimi di sicurezza e le modalità operative per proteggere i dati durante i processi di accesso, trattamento e condivisione, né definiva chiaramente i soggetti responsabili di tali attività.

Alla luce di queste considerazioni, il Garante ha ritenuto impossibile esprimere un parere completo e fondato, rimandando ogni valutazione a un momento successivo, ovvero, all'approvazione del Fascicolo Sanitario Elettronico adeguato agli standard di protezione dei dati indicati dall'Autorità nel parere espresso (Doc-Web 9802729)[92].

Questi rilievi sono stati considerati tanto gravi da indurre il Garante a non autorizzare il proseguimento dell'iter normativo, invitando il Governo a rivedere profondamente l'impianto del Decreto.

Successivamente, il Ministero della Salute ha avviato un dialogo tecnico-istituzionale con il Garante e gli altri attori coinvolti, al fine di superare le criticità emerse.

Il testo è stato quindi rielaborato completamente, introducendo numerose modifiche sostanziali sia sul piano dei principi che su quello operativo.

[92] Garante della Privacy, 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) del 22 agosto 2022.

Nel secondo parere, adottato con provvedimento n. 605 del 26 settembre 2024 (Doc-Web 10062302)[93], l'Autorità ha potuto esprimere valutazione positiva, in virtù di diversi elementi migliorativi.

Il parere dell'Autorità delinea la fisionomia dell'Ecosistema dei dati sanitari, il quale assume forme e caratteristiche diverse rispetto a quello originario.

Nella nuova versione, infatti, l'EDS ha subito un processo evolutivo passando da "più grande banca dati sulla salute" a infrastruttura abilitante l'erogazione di servizi per finalità di cura, prevenzione e di profilassi internazionale, nonché di governo e ricerca scientifica.

Le modifiche introdotte nel testo definitivo del Decreto hanno interessato principalmente tre aspetti fondamentali:

- una prima, importante revisione riguarda la delimitazione della fonte dei dati sanitari che alimentano l'EDS, riconducendo l'origine dei dati esclusivamente al Fascicolo Sanitario Elettronico (FSE);
- la seconda riguarda la funzione e le modalità di utilizzo dei dati raccolti: non sono più trattati indiscriminatamente, ma vengono elaborati esclusivamente per fornire servizi mirati, su richiesta, a soggetti ben identificati;
- il terzo aspetto riguarda la governance del sistema: nel nuovo Decreto, il Ministero della Salute assume il ruolo di titolare del trattamento dei dati trattati all'interno dell'EDS, mentre la gestione tecnica e operativa è affidata ad Agenas, che opera in qualità di responsabile del trattamento. Questa struttura contribuisce a rafforzare la trasparenza e la tracciabilità delle responsabilità lungo l'intera filiera del trattamento dei dati sanitari.

Il secondo parere, frutto del dialogo costruttivo tra istituzioni, ha aperto la strada all'approvazione del Decreto.

Il testo riformulato è apparso più equilibrato, più vicino ai principi del GDPR e più attento alla fiducia dei cittadini.

Da ciò si evince che la protezione dei dati non è un ostacolo all'innovazione, ma una condizione per renderla possibile in modo etico, trasparente e duraturo. E in questo processo, il contributo del Garante si è rivelato fondamentale.

[93] Garante della Privacy, Parere sullo schema di decreto del Ministero della salute sull'Ecosistema Dati Sanitari (EDS), ai sensi dell'art. 12, comma 15-quater, del decreto-legge 18 ottobre 2012, n. 179 del 26 settembre 2024.

III.3. Il nuovo quadro normativo per la sanità digitale

Il presente paragrafo si propone di analizzare il recente Decreto del Ministero della Salute del 31 dicembre 2024, che istituisce l'Ecosistema dei Dati Sanitari (EDS) pubblicato nella Gazzetta Ufficiale del 5 marzo 2025 con decreto ministeriale del 31 dicembre 2024. Questo Decreto rappresenta un tassello fondamentale per lo sviluppo della sanità digitale italiana ed europea, aprendo nuove prospettive nella valorizzazione delle informazioni e per la trasformazione digitale dei servizi sanitari.

L'EDS, in attuazione di quanto previsto nella Missione 6 del PNRR, ha lo scopo di coordinare l'informatizzazione e l'erogazione di servizi sanitari omogenei su tutto il territorio nazionale, offrendo un accesso tempestivo a dati sanitari, aggiornati in tempo reale, contenuti nei Fascicoli Sanitari Elettronici (FSE).

Il sistema sarà pienamente operativo entro il 31 marzo 2026 e permetterà di centralizzare e ottimizzare la gestione dei dati sanitari nel rispetto degli obiettivi previsti dal PNRR.

In linea con gli obiettivi di digitalizzazione, l'EDS persegue due finalità principali:

- la sicurezza e tutela dei dati personali: l'EDS è stato sviluppato nel rispetto delle normative europee, con sistemi avanzati di crittografia e tracciabilità, come riconosciuto dal Garante per la protezione dei dati personali (provvedimento n. 10062302 del 26 settembre 2024);
- il sostegno alla ricerca: l'art. 17[94] dell'EDS introduce un'apertura significativa per l'accesso ai dati a fini di ricerca. Consente di utilizzare i dati per finalità di prevenzione, profilassi internazionale, governo, studio e ricerca, e in situazioni di emergenza.

L'Ecosistema dei dati sanitari, inoltre, permette di assicurare, su richiesta, servizi avanzati di ricerca, consultazione, estrazione e analisi dei dati.

L'EDS facilita l'accesso strutturato alle informazioni per i professionisti sanitari coinvolti nella cura del paziente, anche al di fuori del SSN, previo consenso dell'assistito.

[94] Art. 17: "*Accesso ai servizi dell'EDS per la finalità di studio e ricerca scientifica. La finalità di governo di cui all'art. 1, lettera jj), del presente decreto, è perseguita esclusivamente attraverso l'EDS che rende disponibili al personale dei competenti uffici del Ministero della salute, di Agenas e delle regioni e province autonome competenti in materia di governo, un insieme di servizi omogenei sul territorio nazionale, descritti nell'allegato A e pertinenti alla finalità di governo, cui gli stessi accedono, nel rispetto dei principi di minimizzazione, necessità e pertinenza, secondo i livelli diversificati di accesso ivi indicati.)[…]*"

Uno degli elementi di maggior rilievo è l'introduzione del dossier farmaceutico, che mira a migliorare la qualità e la sicurezza nella dispensazione dei medicinali.

L'operatività dell'EDS consiste nella centralizzazione e standardizzazione dei dati: raccoglie e integra dati provenienti da diverse fonti, tra cui ospedali, cliniche, medici di base, farmacie e servizi sociosanitari, centralizzandoli in un unico ecosistema digitale. Questo garantisce un'interoperabilità ottimale tra i vari sistemi informatici sanitari e permette una gestione coerente delle informazioni, riducendo il rischio di frammentazione dei dati.

L'EDS facilita la condivisione sicura dei dati sanitari su scala nazionale, promuovendo una maggiore continuità assistenziale. Oltre all'uso clinico, il sistema è progettato per supportare anche la ricerca scientifica, il monitoraggio epidemiologico e le strategie di prevenzione sanitaria, attraverso l'uso di dati aggregati e anonimizzati.

Per garantire la sicurezza, l'EDS utilizza unità di archiviazione separate per gestire i dati in chiaro, pseudonimizzati e anonimizzati, limitando l'accesso ai soli profili autorizzati.

Il nuovo Decreto sull'Ecosistema Dati Sanitari (EDS) si compone di **26 articoli** e tre allegati tecnici:

- Allegato A: descrive i contenuti, i servizi e le tipologie di dati trattati dall'EDS;
- Allegato B: definisce le misure di sicurezza da adottare;
- Allegato C: illustra l'architettura e i moduli funzionali dell'EDS.

Gli articoli 1 e 2 contengono rispettivamente le definizioni e l'ambito di applicazione.

L'istituzione dell'EDS è funzionale al Sistema FSE, poiché risponde alle finalità di cui all'art. 12, comma 15-quater, il quale richiama l'art. 12, comma 2, del medesimo decreto.

L'Articolo 3 stabilisce che l'EDS contiene i dati conferiti al sistema FSE dalle strutture sanitarie e socio-sanitarie, validati ed estratti dalle soluzioni tecnologiche, nonché quelli resi disponibili tramite il Sistema tessera sanitaria:

È previsto che i dati oggetto di oscuramento ai sensi degli articoli 6[95] e 9[96] del decreto del 7 settembre 2023 non alimentino l'EDS. Ciò significa che le informazioni sanitarie

---

[96] *"[…] Il diritto di oscuramento può essere esercitato al momento dell'erogazione della prestazione, prima dell'alimentazione del FSE, direttamente nei confronti del soggetto che la 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 realizzazione di altri documenti, quali il Profilo sanitario sintetico di cui all'art. 4, rispetto ai quali può autonomamente esercitare il medesimo diritto. 4. Il diritto di oscuramento può essere esercitato anche tramite una apposita funzionalità online resa disponibile nel FSE e, in*

particolarmente sensibili, il cui accesso è limitato, non saranno incluse nell'EDS, a ulteriore garanzia della riservatezza dei pazienti.

L'EDS è, pertanto, alimentato dai seguenti dati:

- dati del FSE – dati identificativi e amministrativi dell'assistito (esenzioni per reddito e patologia, contatti, delegati); referti, verbali pronto soccorso; lettere di dimissione; profilo sanitario sintetico; prescrizioni specialistiche e farmaceutiche; cartelle cliniche; erogazione farmaci a carico SSN e non a carico SSN; vaccinazioni; erogazione di prestazioni di assistenza specialistica; taccuino personale dell'assistito di cui all'art. 5; dati delle tessere per i portatori di impianto; lettera di invito per screening.
- dati resi disponibili tramite il Sistema tessera sanitaria,

Questi dati possono essere elaborati dall'EDS mediante la ricerca, consultazione, estrazione e analisi dei dati, nonché per la realizzazione del Dossier Farmaceutico.

Quest'ultimo (che è una novità) è costituito da (Allegato A):

- dati anagrafici dell'assistito, Informazioni sulle esenzioni del paziente, dettagli sulle prescrizioni farmaceutiche (data della prescrizione, medico prescrittore, numero di ricetta elettronica (NRE), farmaci prescritti (nome, codice, dosaggio e posologia);
- dati sulle erogazioni dei farmaci (confezioni dispensate, data di erogazione, struttura o farmacia erogatrice) piani terapeutici;
- informazioni sulle somministrazioni dei farmaci (periodo di somministrazione, patologia trattata, via e sito di somministrazione, dosi somministrate)

L'Articolo 4 descrive la soluzione architetturale, basata su un sistema di unità di archiviazione distinte e indipendenti, volte a garantire la completa separazione dei dati in base alla tipologia e al relativo livello di rischio. Questa scelta tecnica è fondamentale per minimizzare i rischi di *data breach* e accessi non autorizzati, in linea con i principi di "*privacy by design*" e "*security by design*". L'architettura del sistema prevede, infatti, la gestione dei dati in unità di archiviazione separate, dedicate alla gestione dei dati in chiaro associati a ciascuna Regione e Provincia autonoma, ai sistemi di assistenza sanitaria ai naviganti (SASN), ai dati pseudonimizzati e ai dati anonimi.

L'Articolo 5 introduce il dossier farmaceutico, un servizio reso disponibile dall'EDS per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali

e l'aderenza alla terapia. L'EDS estrae i dati relativi a prescrizioni farmaceutiche ed erogazioni di farmaci dai documenti del FSE e dai dati resi disponibili dal Sistema Tessera Sanitaria (TS) e dall'Anagrafe Nazionale degli Assistiti (ANA).

Il dossier farmaceutico rappresenta uno strumento utile per migliorare la gestione della terapia farmacologica, ridurre gli errori di prescrizione e favorire la comunicazione tra i professionisti sanitari.

In nessun caso l'accesso al dossier farmaceutico potrà consentire, da parte di soggetti diversi dall'assistito, la consultazione di documenti oscurati ai sensi dell'art. 9 del decreto FSE 2.0.

Gli Articoli 6, 7 e 8 disciplinano le modalità di alimentazione dell'EDS: l'informativa all'assistito e il consenso al trattamento dei dati. L'Articolo 6 stabilisce che le regioni e le province autonome sono titolari dei trattamenti di estrazione dei dati e di trasmissione degli stessi all'EDS, attraverso soluzioni tecnologiche, garantendo la riconducibilità del dato estratto al documento medesimo; l'Articolo 7, in attuazione degli articoli 13 e 14 del Regolamento UE n. 2016/679 (GDPR), prevede che il Ministero della salute, le Regioni e le Province Autonome forniscano all'assistito un'idonea informativa sui trattamenti dei dati effettuati attraverso l'EDS. Al fine di garantire un'informazione omogenea ed uniforme sul territorio nazionale, il Ministero della Salute, in collaborazione con le Regioni e le Province Autonome, integra il modello di informativa relativa al FSE con i trattamenti dei dati effettuati attraverso l'EDS; l'Articolo 8 disciplina il consenso dell'assistito all'elaborazione dei dati dell'EDS per le finalità di cura, prevenzione e profilassi internazionale. Il consenso deve essere libero, specifico, informato, inequivocabile ed esplicito. Per i minori e i soggetti incapaci, il consenso è espresso dai rispettivi rappresentanti legali. La revoca del consenso comporta la disabilitazione dell'accesso ai servizi dell'EDS per le specifiche finalità per le quali è stato revocato.

Gli Articoli dal 13 al 17 regolamentano l'accesso ai servizi dell'EDS per le diverse finalità del trattamento, definendo i soggetti autorizzati e i limiti di tale accesso: accesso per finalità di cura, prevenzione, profilassi internazionale, studio e per finalità di governo.

Il decreto si chiude con una serie di disposizioni relative alle misure di sicurezza, stabilendo che sono assicurati:

"a*) il rispetto delle disposizioni di cui all'art. 51 del CAD*[97] *in materia di sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, nonché delle linee guida rese disponibili da AGID e ACN in materia di sviluppo e gestione dei sistemi informativi;*

b) idonei sistemi di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento;

c) procedure per la verifica periodica dei profili di autorizzazione assegnati agli incaricati;

d) protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati;

e) la cifratura o la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;

f) tracciabilità degli accessi e delle operazioni effettuate;

g) sistemi di audit log per il controllo degli accessi e per il rilevamento di eventuali anomalie;

h) procedure di pseudonimizzazione;

i) idonee misure tecniche e organizzative per la protezione dei dati registrati rispetto a potenziali rischi di accesso abusivo, furto o smarrimento, parziali o integrali, dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi".

Inoltre, viene previsto un servizio di notifica per avvertire gli assistiti delle operazioni tramite un'applicazione per dispositivi mobili, o attraverso l'invio di un messaggio alla casella di posta elettronica registrata dall'assistito. L'assistito può, in ogni momento, disattivare e riattivare il servizio di notifica che viene attivato in automatico, accedendo all'apposita funzionalità presente nel portale FSE istituito presso ogni Regione o in quello nazionale.

Il Decreto del Ministero della Salute del 31 dicembre 2024 istituisce un quadro normativo complesso e articolato per la gestione dei dati sanitari in ambiente digitale. L'EDS rappresenta uno strumento potenzialmente molto utile per migliorare l'efficienza del sistema sanitario, la qualità delle cure e la promozione della ricerca scientifica. Tuttavia, la sua corretta attuazione richiede un'attenzione costante alla tutela dei diritti dei pazienti, in particolare il diritto alla protezione dei dati personali. Sarà fondamentale monitorare l'implementazione del Decreto e valutare la necessità di eventuali aggiustamenti o integrazioni future.

1. [97] Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.
2. "*I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta*".

CAPITOLO IV

Governance, compliance e ruolo del DPO in sanità

IV.1. Principi di *good data governance* (*accountability*, *data minimisation*, *privacy-by-design*)

Il Regolamento Generale sulla Protezione dei Dati Personali (GDPR) pone le basi per una *good data governance*[98] attraverso una serie di principi fondamentali che le organizzazioni devono adottare.

La *governance* si configura come una disciplina strategica e operativa di fondamentale importanza per le organizzazioni contemporanee, in quanto assicura una gestione responsabile, sicura ed etica delle informazioni, in particolare dei dati personali.

L'adozione di detti principi non è soltanto una questione di conformità normativa, ma rappresenta una vera e propria cultura organizzativa volta a tutelare i diritti degli individui e a ottimizzare l'utilizzo dei dati come asset strategico.

Tra i principi cardine che sorreggono una buona governance dei dati vi sono l'*accountability*, la *data minimisation* e *la privacy-by-design*, ciascuno dei quali riveste un ruolo specifico e integrato nella gestione complessiva dei dati.

Il termine *accountability* ha origine nel contesto anglosassone, dove è ampiamente utilizzato in settori come la finanza, la revisione contabile e altri ambiti professionali specializzati. Non è semplice fornire una definizione univoca di cosa implichi concretamente questo concetto, soprattutto perché assume sfumature differenti a seconda del settore di applicazione.

Nelle lingue europee continentali, e in particolare nell'ambito giuridico italiano, il termine non ha un'esatta corrispondenza. Questa difficoltà deriva soprattutto dalle diversità tra i sistemi giuridici. Dal punto di vista linguistico, *accountability* è una parola composta: il verbo *to account* può essere tradotto come "rendere conto", mentre il suffisso *-ability* indica la capacità o l'attitudine a compiere un'azione[99].

La traduzione italiana più ricorrente è "responsabilizzazione", ma anche questa risulta generica e non priva di ambiguità interpretative. Alcuni propongono "rendicontabilità" come alternativa, ma anche in questo caso il termine può prestarsi a differenti letture, spesso legate al contesto contabile più che giuridico o organizzativo.

---

[98] WEBER, OTTO E ÖSTERLE (2009) la definiscono come "*la specificazione dei diritti decisionali e di un quadro di responsabilità per incoraggiare comportamenti desiderabili nella valutazione, creazione, archiviazione, utilizzo, conservazione e cancellazione delle informazioni*" 2009. One size does not fit all — a contingency approach to data governance. Journal of Data and Information Quality, 1(1), 1-27).

[99] ATERNO S., *Principio di accountability nel Gdpr, significato e applicazione,* in Agenda Digitale, https://www.agendadigitale.eu/sicurezza/principio-di-accountability-nel-gdpr-significato-e-applicazione/

Per comprendere appieno il concetto di *accountability* è necessario contestualizzarlo, poiché non si limita a un semplice obbligo giuridico, ma implica una vera e propria cultura della responsabilità, della trasparenza e della capacità di dimostrare, in maniera attiva e documentata, la conformità alle norme.

Il concetto di responsabilizzazione, si presenta come un principio flessibile e adattabile, il cui significato può variare in base al contesto specifico. Questa natura poliedrica rende talvolta complessa la sua applicazione pratica per chi si occupa del trattamento dei dati personali.

Questa complessità può rappresentare una sfida per i soggetti che trattano dati personali, ma allo stesso tempo costituisce una tutela fondamentale per l'interessato, riconosciuto come la parte più vulnerabile nella relazione tra titolare e soggetto dei dati. Per tradurre efficacemente questo principio in pratica, l'approccio europeo alla protezione dei dati si basa su una gestione attenta e proporzionata del rischio (*risk-based approach*)[100].

Questo approccio *risk-based* si realizza tramite diversi strumenti e processi, che contribuiscono a definire la filosofia della protezione dei dati nell'Unione Europea. Tra questi vi sono il principio di minimizzazione del trattamento, la progettazione e configurazione dei sistemi secondo le tecniche di privacy by design e by default, la tenuta dei registri delle attività di trattamento, la conduzione di valutazioni d'impatto e consultazioni preventive, la figura del responsabile della protezione dei dati (data protection officer), nonché l'adozione di codici di condotta e certificazioni[101]. Questi elementi, combinati tra loro, fungono da meccanismi di prevenzione, mirati a garantire la tutela dei dati personali sin dalle prime fasi che precedono l'effettivo trattamento.

Peranto, si evince dalle intenzioni del legislatore europeo, che questo concetto racchiude l'insieme di azioni dinamiche volte a comprovare l'adozione di tutte le misure richieste dal GDPR da parte di chiunque tratti dati, in primis il titolare e il responsabile. L'obiettivo è che tali soggetti siano sempre in grado di attestare la conformità delle operazioni di trattamento e la validità delle misure implementate, a prescindere dall'effettiva occorrenza di una perdita di dati.

Il Garante italiano stesso sottolinea che "*il Regolamento pone l'accento sulla responsabilizzazione di titolari e responsabili, ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25, in*

---

[100] GIANNONE G.*, Risk-based approach e trattamento dei dati personali. La nuova disciplina europea della privacy*, S. Sica, V. D'Antonio, G.M. Riccio (a cura di), Padova, Cedam, 2016.

[101] CALIFANO L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali.*

particolare, e l'intero Capo IV del Regolamento). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento". Peraltro, nella sua "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali"[102] si impegna ad assistere i titolari nel passaggio da una visione burocratica di semplice adempimento normativo a una prospettiva operativa orientata alla protezione concreta dei dati.

In sostanza, si comprende come non sia sufficiente implementare misure di sicurezza che inizialmente rispondano alle esigenze, è invece fondamentale una verifica continua della loro perdurante idoneità nel tempo. Qualora tali misure dovessero rivelarsi obsolete, il titolare ha l'obbligo di aggiornarle per ristabilirne l'adeguatezza.

Questo implica, in primo luogo, l'adozione di un sistema di gestione della privacy che preveda la definizione chiara di ruoli e responsabilità, come la nomina di un Data Protection Officer (DPO), con il compito di monitorare e garantire la compliance interna[103].

Inoltre, il principio di *accountability* richiede la documentazione sistematica di tutte le attività di trattamento dei dati, l'implementazione di politiche interne, e l'effettuazione di audit e verifiche periodiche per valutare l'efficacia delle misure adottate.

Questo approccio responsabile e proattivo, infatti, permette all'organizzazione di rispondere prontamente a eventuali richieste di autorità o di interessati, e di correggere tempestivamente eventuali criticità, promuovendo una cultura della trasparenza e della responsabilità diffusa.

Parallelamente, il principio della minimizzazione enunciato dall' 5 del Regolamento Europeo 679/2016, rappresenta una delle strategie più efficaci per ridurre il rischio di violazioni della privacy e di esposizione indebita delle informazioni. L'art. enuncia, nello specifico la lettera c) testualmente riporta: *"1. I dati personali sono: … c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati)".*

Dall'interpretazione della norma si evince che il trattamento dei dati deve essere limitato esclusivamente a quelli necessari, pertinenti e adeguati rispetto agli scopi specifici per cui sono raccolti. La minimizzazione dei dati non riguarda soltanto la fase di raccolta,

---

[102] Garante della Privacy, Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

[103] Il concetto di *accountability* è sancito dall'articolo 5(2) del GDPR, che obbliga i titolari del trattamento a dimostrare la conformità ai principi fondamentali del trattamento dati. Per un approfondimento si veda: Regulation (EU) 2016/679, Official Journal of the European Union, 2016; e la guida del WP29 (Working Party 29) sulla responsabilità (WP260).

ma anche la conservazione e l'utilizzo, prevedendo che i dati non siano mantenuti per un periodo superiore a quanto necessario e che vengano periodicamente rivisti e, se non più necessari, eliminati o anonimizzati[104]. Questo principio consente di evitare accumuli di dati superflui, che rappresenterebbero un inutile onere gestionale e un potenziale vettore di rischi. Inoltre, la data *minimisation* facilita il rispetto dei diritti degli interessati, quali il diritto alla cancellazione e alla limitazione del trattamento, rafforzando così la fiducia degli utenti nell'organizzazione.

Il terzo principio, la *privacy by design*, incarna un paradigma innovativo e proattivo che invita le organizzazioni ad integrare la protezione dei dati fin dalla fase di progettazione e sviluppo di sistemi, prodotti e processi. Contrariamente a un approccio reattivo, che interviene dopo che un sistema è stato realizzato, la privacy-by-design richiede che la tutela della riservatezza e della sicurezza dei dati sia un requisito strutturale e imprescindibile fin dalle prime fasi, mediante l'analisi preventiva dei rischi e l'adozione di misure tecniche e organizzative adeguate[105].

Tra queste misure si annoverano l'uso della crittografia, la pseudonimizzazione, l'implementazione di controlli di accesso rigorosi, e la configurazione di impostazioni predefinite orientate alla privacy (privacy-by-default). L'obiettivo è quello di minimizzare l'impatto sui diritti degli interessati, garantendo che la privacy sia garantita senza compromessi e senza richiedere interventi successivi. Questo approccio è riconosciuto come best practice dalle normative europee e internazionali e rappresenta un fattore chiave per costruire sistemi affidabili e rispettosi della dignità individuale.

In conclusione, l'applicazione integrata dei principi di *accountability*, data *minimisation* e *privacy by design* costituisce il fondamento di una governance dei dati efficace e sostenibile. Tali principi non solo permettono alle organizzazioni di conformarsi alle normative, ma favoriscono anche la creazione di un ambiente di fiducia reciproca con gli utenti e la valorizzazione del dato come risorsa strategica. Investire in una buona governance dei dati significa, quindi, adottare un approccio sistemico e lungimirante, capace di rispondere alle sfide normative e tecnologiche contemporanee e di promuovere uno sviluppo etico e responsabile della digitalizzazione.

---

[104] Il principio di minimizzazione dei dati è descritto all'articolo 5(1)(c) del GDPR e rappresenta una misura essenziale per la protezione della privacy. Sul tema si consulti anche Cavoukian, A. (2010). "Privacy by Design: The 7 Foundational Principles". Information and Privacy Commissioner of Ontario.

[105] La privacy-by-design, introdotta da Ann Cavoukian nel 2009, è definita dall'articolo 25 del GDPR come "*data protection by design and by default*". La sua applicazione pratica è illustrata in numerose linee guida europee e internazionali, ad esempio il documento dell'EDPB (European Data Protection Board) sulla protezione dei dati fin dalla progettazione.

IV.2. Il Data Protection Officer (DPO) nel settore sanitario

L'introduzione della figura del Data Protection Officer (DPO) con il Regolamento Europeo sulla protezione dei dati personali (GDPR – Reg. UE 2016/679) ha rappresentato una svolta significativa nel garantire la gestione trasparente e sicura delle informazioni personali, specialmente nei contesti ad alta intensità di dati sensibili, come quello sanitario. Il regolamento stabilisce dettagliatamente non solo i casi in cui la nomina di un DPO è obbligatoria (art. 37), ma anche le funzioni che questa figura è chiamata a svolgere (art. 39), e la sua posizione di autonomia e indipendenza all'interno delle organizzazioni.

Nel settore della sanità, la designazione di un DPO è quasi sempre necessaria per due ragioni fondamentali. Da un lato, molte strutture sanitarie sono enti pubblici o accreditati, e rientrano quindi nei soggetti obbligati alla nomina in base alla natura giuridica dell'organizzazione. Dall'altro lato, anche quando si tratta di soggetti privati, il trattamento sistematico e su larga scala di categorie particolari di dati, in primis quelli relativi alla salute, fa scattare l'obbligo secondo quanto previsto dall'art. 37, par. 1, lett. c) del Regolamento (UE) 2016/679. Tale obbligo può estendersi anche alle aziende che offrono servizi alle strutture sanitarie, qualora siano coinvolte nel trattamento regolare e continuativo di dati sanitari.

Tuttavia, esistono anche eccezioni: operatori sanitari individuali, farmacie e piccole realtà non effettuanti trattamenti su vasta scala possono essere esentati, come suggerito dal considerando 91[106], che lascia intendere che l'obbligatorietà sia proporzionata all'impatto e all'estensione del trattamento effettuato.

Una volta nominato il DPO, deve essere inviata all'autorità Garante Privacy formale comunicazione dell'avvenuta nomina[107].

Nel contesto sanitario, il DPO è chiamato a ricoprire un ruolo tanto tecnico quanto strategico. Infatti, non si limita a garantire l'osservanza della normativa, ma funge da guida e supporto costante nella definizione di processi che proteggano davvero i diritti degli interessati.

---

[106] "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*".

[107] Una volta che l'organizzazione decide, per volontà o per obbligo di nominare il Data Protection Officer dovrà pensare all'invio di apposita comunicazione all'Autorità Garante (art. 37, par. 7, GDPR). Presso l'Autorità, difatti, è presente un registro dei nominativi di tutti i DPO presenti sul territorio italiano.

Può essere nominata una figura interna o esterna all'azienda, l'importante è che presenti i requisiti necessari, sia dal punto di vista della formazione personale sia dal punto di vista dell'imparzialità e dell'indipendenza nello svolgimento del suo ruolo.

Le competenze sono fondamentali, infatti, oltre a possedere conoscenze giuridiche solide, è necessaria una buona comprensione del contesto tecnologico e delle dinamiche clinico-organizzative.

Nel settore sanitario, la complessità del trattamento dei dati e la delicatezza delle informazioni trattate rendono la presenza del DPO particolarmente rilevante: cartelle cliniche, diagnosi, terapie, referti, dati genetici e biometrici costituiscono elementi fondamentali per l'erogazione delle cure, ma al contempo rappresentano dati ad alta esposizione al rischio di violazione.

In questo scenario, la figura del Responsabile della Protezione dei Dati assume un ruolo strategico, non solo per garantire il rispetto della normativa, ma anche per favorire una cultura organizzativa orientata alla tutela della persona, al corretto trattamento dei dati e alla prevenzione di rischi giuridici e reputazionali.

L'introduzione del Regolamento (UE) 2016/679 ha segnato un passaggio epocale, ridefinendo non solo le regole per il trattamento dei dati personali, ma anche le responsabilità delle strutture sanitarie e dei professionisti che vi operano.

L'art. 39 del GDPR, stabilisce i compiti del DPO, che nella pratica quotidiana delle strutture sanitarie, si declinano in attività concrete[108]:

a) monitoraggio e vigilanza: il DPO è il garante della corretta applicazione delle norme in materia di protezione dei dati. Supervisiona procedure, controlla che il personale segua protocolli adeguati, verifica che le banche dati siano aggiornate e sicure.
b) consulenza nei trattamenti più delicati: quando una struttura decide di avviare un nuovo progetto, ad esempio un sistema di telemedicina o un'applicazione per la gestione dei referti, il DPO entra in gioco per valutare i rischi legati al trattamento dei dati. In alcuni casi, deve redigere o supervisionare una Valutazione d'Impatto (DPIA), uno strumento previsto proprio per anticipare criticità e prevenire danni.
c) formazione e cultura della privacy: il DPO ha anche un ruolo formativo, difatti deve aiutare tutto il personale sanitario, tecnico e amministrativo a comprendere l'importanza della privacy e ad applicare correttamente le regole. In un contesto

[108] *DPO nel mondo sanitario*, in Mondo Privacy, https://mondoprivacy.it/blog/dpo/il-dpo-nel-mondo-sanitario/

complesso come quello sanitario, dove i dati vengono trattati da decine di figure diverse, la formazione continua è essenziale.

d) collaborazione alla sicurezza dei sistemi: il DPO deve saper valutare l'efficacia delle misure di sicurezza adottate. Partecipa alla scelta dei sistemi, verifica le politiche di accesso alle cartelle cliniche, monitora la tracciabilità degli accessi e contribuisce a prevenire intrusioni o perdite di dati.

Il Regolamento chiarisce che il DPO deve godere di autonomia e indipendenza: non può essere influenzato, né ricevere ordini che condizionino il suo giudizio. Inoltre, non deve ricoprire incarichi che possano generare conflitti di interesse.

Allo stesso tempo, il DPO ha bisogno di interagire costantemente con la Direzione aziendale, con il personale, con i tecnici e con gli utenti, per costruire un sistema che funzioni davvero e che sia rispettoso dei diritti di tutti.

È fondamentale che il DPO venga coinvolto tempestivamente in tutte le decisioni che ineriscono la protezione dei dati personali.

Uno degli aspetti centrali dell'attività del DPO in sanità è il controllo dei flussi informativi: i dati dei pazienti transitano attraverso molteplici attori e piattaforme, generando potenziali criticità in termini di sicurezza e integrità. Il DPO è tenuto, quindi, a monitorare i percorsi di trasmissione dei dati – ad esempio nella refertazione o nella gestione di prestazioni ambulatoriali – e a suggerire misure di sicurezza adeguate, anche in relazione ai canali di comunicazione.

Analogamente, deve vigilare affinché gli accessi ai dati siano profilati in base alle mansioni e ai ruoli: il personale amministrativo, ad esempio, non dovrebbe mai poter consultare dati clinici se non strettamente necessari.

Anche la gestione delle cartelle cliniche deve avvenire nel rispetto dei principi di accuratezza, pertinenza e conservazione sicura, con un controllo sulla completezza dei dati e sulla tracciabilità delle modifiche.

In un'epoca in cui la digitalizzazione della sanità avanza rapidamente, tra fascicoli elettronici, applicazioni mediche, intelligenza artificiale e telemedicina, la sua funzione diventa ancora più centrale.

La corretta alimentazione del FSE è un ulteriore ambito di intervento del DPO[109]. Questo strumento digitale, destinato a raccogliere in modo strutturato tutte le informazioni sanitarie del cittadino, comporta sfide importanti sotto il profilo della protezione dei

[109]DE PRETIS G., *Dpo in Sanità, un ruolo essenziale: come sceglierlo*, in Agenda Digitale, https://www.agendadigitale.eu/sanita/sanita-il-ruolo-essenziale-del-dpo-come-sceglierlo/

dati. Il DPO deve assicurarsi che solo i soggetti autorizzati abbiano accesso al caricamento e alla consultazione dei dati, verificando la corretta implementazione delle misure di sicurezza previste, nonché il rispetto delle regole di trasparenza e informazione nei confronti degli utenti.

Garantire che l'innovazione non metta a rischio la privacy è una sfida complessa, che solo un professionista formato può affrontare con successo.

La sua azione contribuisce non solo a prevenire sanzioni o contenziosi, ma a costruire un clima di fiducia tra struttura e paziente, dove ciascuno si sente al sicuro, anche dal punto di vista della propria identità digitale.

Uno dei principali limiti che rischia di ridurre l'efficacia della funzione del DPO è la mera considerazione dello stesso come adempimento formale rispetto alle prescrizioni di cui all'art. 37 del GDPR. Difatti, il DPO viene coinvolto soltanto in fase di emergenza, quando, per esempio, si verifica una violazione dei dati.

La complessità del sistema sanitario richiede una visione sistemica che deve andare oltre l'applicazione delle norme.

Per superare le criticità emergenti nella gestione dei dati sanitari, soprattutto alla luce dell'accelerazione impressa dalla digitalizzazione, una soluzione che si prospetta particolarmente idonea è la costituzione di una rete nazionale dei Responsabili della Protezione dei Dati (DPO) della sanità pubblica. Una rete che consenta una gestione coordinata, coerente e uniforme dei dati personali custoditi dai singoli enti sanitari, garantendo così un'applicazione omogenea delle norme e una tutela efficace dei diritti degli interessati su tutto il territorio nazionale.

In questo contesto, l'esperienza della Sardegna si pone come esempio virtuoso e replicabile.

Infatti, il contesto sanitario sardo si distingue nel panorama nazionale per l'adozione di un modello organizzativo innovativo in materia di protezione dei dati personali, con particolare riferimento alla digitalizzazione dei servizi sanitari. In Sardegna, infatti, l'Azienda Regionale della Salute (ARES) ha promosso un approccio finalizzato a gestire in modo sinergico ed efficace le complesse dinamiche connesse all'impiego delle nuove tecnologie sanitarie e alla conseguente elaborazione di dati personali.

A tale scopo, è stato istituito un Gruppo di Lavoro Permanente, composto dai Responsabili della Protezione dei Dati (DPO) delle otto Aziende Sanitarie Locali presenti

sul territorio regionale, nonché dei principali poli ospedalieri e universitari – tra cui l'ARNAS G. Brotzu, le Aziende Ospedaliere Universitarie di Cagliari e Sassari – e dell'AREUS (l'Azienda Regionale dell'Emergenza Urgenza della Sardegna).

Questo organismo si configura come una soluzione strategica e condivisa per affrontare, in maniera coordinata, le criticità e le difformità che possono emergere nella gestione dei dati all'interno delle singole strutture sanitarie. Il modello si basa su una governance integrata e partecipativa, finalizzata alla progettazione e all'implementazione di prassi comuni, all'elaborazione di procedure standardizzate e al monitoraggio continuo delle attività legate al trattamento dei dati sanitari.

L'obiettivo primario è quello di assicurare un'applicazione uniforme delle normative in materia di privacy e protezione dei dati personali su tutto il territorio regionale, offrendo ai cittadini un livello omogeneo di tutela, indipendentemente dalla struttura sanitaria presso cui si rivolgono. In questo modo, il sistema sanitario regionale non solo rafforza la propria conformità normativa, ma promuove anche una cultura della protezione dei dati più solida, trasparente e orientata alla centralità del paziente.

In conclusione, l'esperienza della Sardegna rappresenta un esempio virtuoso e replicabile di come la collaborazione tra i DPO possa trasformarsi in uno strumento concreto per migliorare l'efficienza amministrativa, la sicurezza informativa e la qualità complessiva dei servizi sanitari, nel pieno rispetto dei diritti fondamentali degli interessati[110].

Un ulteriore elemento cruciale riguarda la necessità di integrare in modo strutturale la funzione del DPO con le altre aree strategiche aziendali, in particolare con *l'Information Technology,* la cybersecurity e la gestione dei processi, soprattutto in relazione alla governance degli affidamenti a terzi, come sottolineato anche dal Considerando 74[111].

Solo una collaborazione sinergica e continuativa tra i diversi attori interni può garantire una gestione efficace e sicura del patrimonio informativo aziendale, in un contesto sanitario sempre più complesso e interconnesso.

---

[110] ARES SARDEGNA, Sanità Digitale e protezione dei dati: insediato il Gruppo di Lavoro, https://www.aressardegna.it/sanita-digitale-e-protezione-dei-dati-insediato-il-gruppo-di-lavoro/

[111] "*È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.*
In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

Nella mia esperienza lavorativa alla ASL 3 di Nuoro, il DPO rappresenta un punto di riferimento non solo per la compliance normativa, ma c'è un confronto costante, soprattutto per risolvere questioni più o meno complesse, dubbi interpretativi, per la formazione continua del personale e il monitoraggio delle procedure interne.

In definitiva, il DPO non rappresenta solo una figura di garanzia normativa, ma assume un ruolo strategico, culturale e organizzativo. Perché questo ruolo possa esprimere appieno il suo potenziale, è fondamentale investire risorse, formazione e fiducia, riconoscendo al DPO una funzione chiave nel costruire una sanità moderna, sicura, digitale ma sempre centrata sulla persona.

IV.3. Il sistema di gestione privacy (SGP)

La salvaguardia dei diritti e delle libertà degli individui in relazione al trattamento dei loro dati personali richiede l'implementazione di misure tecniche e organizzative adeguate, volte a garantire il pieno rispetto delle norme previste dal regolamento.

Per poter dimostrare la propria conformità a tali disposizioni, il titolare del trattamento deve mettere in atto politiche interne efficaci e adottare accorgimenti specifici che prevedono la protezione dei dati sin dalla fase di progettazione.

Nel contesto attuale, dove il trattamento dei dati personali è diventato parte integrante dei processi digitali e organizzativi, disporre di un Sistema di Gestione della Privacy (SGP) rappresenta una scelta strategica fondamentale.

Non si tratta soltanto di adempiere agli obblighi imposti dal Regolamento Europeo sulla protezione dei dati (GDPR), ma di costruire una cultura della responsabilità e del rispetto verso le informazioni delle persone.

Un SGP è, in sostanza, un insieme coordinato di attività, procedure e misure, pensato per garantire che ogni fase del trattamento dei dati sia gestita con attenzione, trasparenza e coerenza. Non si limita a documentare ciò che viene fatto, ma offre una struttura per prevenire i rischi, affrontare le criticità e migliorare nel tempo la protezione delle informazioni.

Ogni passaggio è orientato a far sì che la tutela dei dati non sia solo un adempimento formale, ma un principio realmente integrato nella gestione quotidiana dell'ente o dell'azienda.

Alla base del SGP c'è un approccio proattivo, in cui l'azienda non aspetta di reagire agli incidenti, ma si prepara e si organizza per evitarli, attraverso audit interni, procedure documentate, policy chiare e aggiornate.

Questo sistema prevede vari strumenti operativi: dalla mappatura dei trattamenti alla tenuta aggiornata del registro delle attività, dalla definizione delle responsabilità interne alla formazione del personale, fino alla valutazione d'impatto sulla privacy (DPIA) per i trattamenti più delicati.

Sebbene il GDPR specifichi con precisione "cosa" sia necessario fare per salvaguardare i diritti e le libertà fondamentali degli individui, non fornisce indicazioni dettagliate su "come" tali prescrizioni debbano essere concretamente implementate all'interno delle organizzazioni.

Un SGP ben costruito permette di prevenire rischi, rafforzare la sicurezza informatica, rispondere tempestivamente a eventuali incidenti, e soprattutto, di trattare i dati in modo etico e responsabile

In definitiva, la realizzazione di un Sistema di Gestione della Privacy rappresenta un investimento strategico: contribuisce a rendere la protezione dei dati parte integrante della governance aziendale e non un mero obbligo normativo. La protezione dei dati è un diritto che deve tradursi in pratica, non solo in teoria[112].

Come osservano Pizzetti[113] e Rodotà[114], la protezione dei dati non deve essere vissuta come un ostacolo, ma come un'opportunità per accrescere la qualità dell'organizzazione aziendale e rafforzare la fiducia degli utenti.

IV.3.1. Il registro delle attività di trattamento

Uno tra i principali adempimenti consiste nella predisposizione del Registro dei trattamenti di cui all'art. 30 del GDPR. Si tratta di un documento formale, in formato cartaceo o digitale, che rappresenta la sintesi organizzata delle attività di trattamento condotte all'interno dell'organizzazione, sulla base di una preventiva attività di ricognizione e mappatura dei trattamenti.

Mappare significa creare una relazione tra i dati trattati ed altri aspetti dell'organizzazione che li tratta, come:

---

[112] BUTTARELLI, G., *Privacy 2030. Una nuova visione per l'Europa.* 2019
[113] PIZZETTI, F., *Privacy e il diritto europeo alla protezione dei dati personali.* Giappichelli
[114] RODOTÀ, S., *Tecnologie e diritti*. Laterza

- i processi aziendali che usano i dati personali,
- le persone autorizzate a trattare i dati personali,
- le operazioni di trattamento compiute sui dati (es. acquisizione, consultazione, modifica, cancellazione, ecc.),
- le risorse (asset) utilizzate per trattare i dati (es. infrastrutture fisiche, hardware, software, pc client, stampanti, ecc.).

La mappatura dei dati personali è un processo che può avvenire mediante:

- interviste esplorative con i referenti delle varie funzioni aziendali coinvolte nel trattamento dei dati;
- il coinvolgimento di figure strategiche quali il DPO, il responsabile IT, il responsabile HR e altri ruoli funzionali;
- l'analisi documentale (procedure interne, contratti, informative, checklist, ecc.);
- la successiva validazione della bozza di registro, da condividere con la direzione per apportare correzioni o integrazioni.

Ogniqualvolta che si verifica un cambiamento la mappa dei dati personali deve essere aggiornata in modo corrispondente. Soltanto in questo modo la mappa potrà fornire indicazioni utili sempre aggiornate[115].

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del RGPD) e in quello del responsabile (art. 30, par. 2 del RGPD): «*Con riferimento ai contenuti si rappresenta quanto segue: (a) nel campo "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del RGPD; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2del RGPD; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del RGPD; (b) nel campo*

[115] D'ALESSI F., *Il ruolo del Registro delle Attività di Trattamento nelle aziende, in* Mondo Privacy, https://mondoprivacy.it/blog/accountability/registro-delle-attivita-di-trattamento/

"descrizione delle categorie di interessati e delle categorie di dati personali" andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.); (c) nel campo "categorie di destinatari a cui i dati sono stati o saranno comunicati" andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali; (d) nel campo "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.); (e) nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso"); (f) nel campo "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.)»[116].

[116] Garante della Privacy, Registro delle attività di trattamento, https://www.garanteprivacy.it/registro-delle-attivita-di-trattamento

Inoltre, ove richiesto, il registro deve essere sempre messo a disposizione dell'autorità di controllo.

Lungi dal rappresentare un onere documentale, il Registro delle attività di trattamento si configura come uno strumento operativo a supporto della governance della privacy.

In ASL, la tenuta e l'aggiornamento del registro dei trattamenti è una delle attività operative più rilevanti. La complessità di questa attività deriva da diversi fattori. In primo luogo, la molteplicità degli attori coinvolti, quali le direzioni sanitarie, servizi informatici, uffici amministrativi, operatori dei front-office, rende necessario un lavoro costante di coordinamento e comunicazione. Ogni area organizzativa gestisce flussi informativi specifici che devono essere compresi nel dettaglio per poter essere correttamente censiti. Inoltre, la distinzione tra ruoli di Titolare, Contitolare e Responsabile del trattamento non è sempre immediata, specialmente nei casi in cui si ricorre a piattaforme condivise, gestite da fornitori esterni o dalla Regione Sardegna.

Un'altra criticità è rappresentata dalla continua evoluzione dei sistemi informativi e delle procedure interne, che comporta la necessità di aggiornare il registro in modo tempestivo e accurato. Tuttavia, la rilevazione di nuove attività o di modifiche a trattamenti esistenti non sempre viene comunicata con la necessaria tempestività all' ufficio privacy, causando potenziali disallineamenti documentali e di responsabilità.

La raccolta delle informazioni necessarie per compilare il registro si scontra, inoltre, con una generale difficoltà culturale nel riconoscere il valore e la funzione di questo strumento. Non di rado, gli operatori vedono la compilazione delle schede di trattamento come un mero adempimento formale, piuttosto che come un'opportunità per migliorare trasparenza, responsabilizzazione e consapevolezza interna.

Per affrontare queste difficoltà, risulta fondamentale implementare momenti di formazione dedicata, strumenti di raccolta standardizzati, e una governance interna che preveda referenti privacy distribuiti nelle diverse strutture. Solo in questo modo è possibile costruire un registro realmente utile, aggiornato e conforme ai requisiti dell'art. 30 del GDPR, capace di supportare audit interni, valutazioni d'impatto, e risposte efficaci alle richieste dell'Autorità Garante.

Questa attività, soprattutto nella prima stesura, è stata particolarmente complessa, soprattutto nell'organizzazione e nel confronto con le unità operative per l'individuazione dei trattamenti sanitari.

In conclusione, un registro ben progettato e aggiornato testimonia l'adozione di una vera cultura della protezione dei dati. Esso costituisce un indicatore di maturità organizzativa e di adesione concreta ai principi del GDPR, nonché uno strumento chiave per rafforzare la fiducia degli stakeholder e prevenire responsabilità legali.

IV.3.2. La valutazione di impatto (DPIA)

La valutazione d'impatto sulla protezione dei dati (nota anche come DPIA – *Data Protection Impact Assessment*) rappresenta una delle innovazioni più significative introdotte dal GDPR.

La DPIA consiste in un'analisi preventiva e approfondita che il titolare del trattamento deve condurre ogni volta che intenda avviare un trattamento di dati potenzialmente rischioso per i diritti e le libertà delle persone coinvolte.

Questo vale soprattutto quando si utilizzano nuove tecnologie, quando vengono trattati dati sensibili o si opera in contesti complessi.

L'obiettivo principale è quello di accertare, prima dell'avvio del trattamento, se vi siano potenziali rischi per i diritti e la riservatezza degli interessati e, in tal caso, individuare soluzioni efficaci per prevenirli o mitigarli attraverso l'adozione di misure tecniche e organizzative appropriate.

In sostanza, si tratta di un esercizio di responsabilità che serve a mettere a fuoco i rischi reali e a valutare se il trattamento sia sostenibile, non solo dal punto di vista normativo, ma anche in termini di rispetto delle persone. Nel caso in cui l'analisi dovesse rivelare criticità non risolvibili, sarà necessario modificare il trattamento o consultare preventivamente l'autorità di controllo.

La DPIA, quindi, non è un adempimento puramente burocratico, ma uno strumento concreto di prevenzione, che incoraggia una gestione consapevole dei dati e rafforza la fiducia tra organizzazioni e cittadini. Al centro, ancora una volta, ci sono la persona, la sua dignità e il rispetto dei suoi diritti fondamentali.

L'art. 35, comma 1, del GDPR stabilisce che "*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".

Per quanto attiene alla metodologia utilizzata, il GDPR non indica delle modalità predeterminate per eseguirla, tuttavia, il considerando 90 fornisce alcune indicazioni utili, precisando che *"La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento".*

Il Gruppo di lavoro Articolo 29 (WP29), ora sostituito dal Comitato europeo per la protezione dei dati (EDPB), ha elaborato specifiche linee guida sulla Valutazione d'Impatto sulla Protezione dei Dati (DPIA). All'interno di queste linee guida, sono stati identificati nove criteri la cui ricorrenza congiunta o disgiunta rende raccomandabile l'effettuazione di una DPIA. Basandosi su queste indicazioni, il Garante per la Protezione dei Dati Personali italiano ha a sua volta stilato un elenco dettagliato di dodici tipologie di trattamenti per i quali la DPIA è considerata obbligatoria o fortemente consigliata.

La logica sottostante a queste indicazioni risiede nella necessità di valutare preventivamente la rischiosità dei trattamenti sui diritti e le libertà degli interessati, al fine di implementare misure adeguate a mitigare tali rischi.

Di seguito, si presentano le tipologie di trattamenti individuate dal Garante italiano che richiedono una DPIA:

1. trattamenti di profilazione e scoring su larga scala
2. trattamenti automatizzati con effetti giuridici o significativi sugli interessati
3. monitoraggio sistematico e capillare degli utenti, anche online o tramite applicazioni
4. trattamenti su larga scala di dati altamente sensibili o a rischio per i diritti fondamentali
5. controllo a distanza in ambito lavorativo tramite sistemi tecnologici
6. trattamenti non occasionali di dati di soggetti vulnerabili
7. uso di tecnologie innovative
8. scambio massivo di dati tra più titolari attraverso strumenti digitali
9. combinazione o raffronto di dataset per finalità diverse
10. trattamento di dati particolari o giudiziari con interconnessione con altri dati
11. trattamenti sistematici di dati biometrici
12. trattamenti sistematici di dati genetici

Questi criteri e le indicazioni del Garante italiano sottolineano l'importanza di un'attenta valutazione del rischio per la privacy prima di intraprendere determinate operazioni di trattamento dati.

Il GDPR attribuisce un ruolo centrale al Responsabile della Protezione dei Dati (DPO) nel processo di Valutazione d'Impatto sulla Protezione dei Dati.

Nello specifico, l'articolo 35, paragrafo 2, del GDPR stabilisce che il Titolare del trattamento deve consultare il DPO quando intende condurre una DPIA, qualora ne sia stato designato uno. Questa consultazione è fondamentale per garantire che la valutazione sia approfondita e che vengano presi in considerazione tutti gli aspetti rilevanti relativi alla protezione dei dati.

A sua volta, l'articolo 39, paragrafo 1, lettera c), del GDPR definisce uno dei compiti primari del DPO: "*fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento*". Ciò significa che il DPO ha anche la responsabilità di monitorare l'intero processo della DPIA, assicurando che venga eseguito correttamente e che le raccomandazioni emergenti siano implementate in modo efficace.

In sintesi, la collaborazione tra il titolare del trattamento e il DPO è essenziale per condurre una DPIA conforme al GDPR, rafforzando la tutela dei dati personali e la conformità normativa.

La DPIA, si configura come un pilastro fondamentale del sistema di protezione dei dati delineato dal GDPR., in particolare, in ambiti ad alto rischio come quello sanitario dove il trattamento di dati particolari è continuo e spesso supportato da tecnologie innovative, la DPIA si configura come uno strumento essenziale non solo per adempiere agli obblighi di legge, ma per progettare trattamenti etici e sostenibili, allineati con i principi di *privacy by design* e *by default*.

IV.3.3. Codici di condotta e certificazioni

Nel contesto della *governance* della protezione dei dati, strumenti come i codici di condotta e i meccanismi di certificazione, previsti dagli articoli 40 e 42 del GDPR e dai considerando 77[117] e 78[118], assumono un ruolo sempre più rilevante, fungendo da mezzi

[117] Il Considerando 77, in omaggio al principio di responsabilizzazione di cui all'art. 5, par. 2 del Regolamento stabilisce che "*Gli orientamenti per la messa in atto di opportune misure per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati (…)*"

[118] Il Considerando 78, prevede che "*Le associazioni o altre organizzazioni rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero essere incoraggiate a elaborare codici di condotta, nei limiti del*

concreti per tradurre i principi del Regolamento in prassi operative settoriali.

Sebbene siano di natura volontaria, rappresentano strumenti qualificati per agevolare l'adeguamento delle aziende ai requisiti normativi.

I codici di condotta consistono in regole o pratiche uniformi e condivise, elaborate da vari organismi internazionali o anche da singoli Stati.

Queste regole, in particolare potrebbero riguardare: il trattamento corretto e trasparente dei dati, i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici, la raccolta dei dati personali, la pseudonimizzazione, l'informazione fornita al pubblico e agli interessati, l'esercizio dei diritti degli interessati, la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore, le misure di sicurezza, la notifica dei *data breach* e la relativa comunicazione agli interessati, il trasferimento di dati personali verso paesi terzi, le procedure stragiudiziali di composizione delle controversie.

Prima dell'approvazione il codice dovrà essere sottoposto all'Autorità garante e questa esprimerà un parere. Se il parere è positivo e l'applicazione riguarda solamente lo Stato membro in cui è presentato, l'Autorità registrerà e pubblicherà il Codice realizzato.

Nel caso in cui si riferisca a trattamenti realizzati in vari Stati membri, prima che ci sial' approvazione definitiva, occorrerà un secondo con il coinvolgimento del Che vedrà coinvolto il Comitato europeo per la protezione dei dati. Qualora anche a seguito di tale controllo, il progetto ottenga un parere favorevole, sarà registrato e pubblicato.

La Commissione ha il potere di decidere se il codice di condotta avrà validità generale all'interno dell'Unione: in tal caso, il codice verrà applicato a tutto il settore di riferimento, in tutto il territorio dell'Unione Europea.

Tutti i Codici di condotta sono raccolti in un apposito registro.

Per quanto riguarda il settore sanitario è stato adottato il "Codice di condotta per l'utilizzo ai fini l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica**"** predisposto dalla Regione Veneto[119], approvato dal Garante e inserito nell'apposito registro[120]. L'esistenza di questo specifico codice dimostra come il GDPR, pur essendo una normativa generale, incoraggi lo sviluppo di strumenti settoriali che adattino i suoi principi alle peculiarità dei diversi contesti, come quello sanitario, per bilanciare l'innovazione con la tutela dei diritti fondamentali.

---

presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori (…). In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche"

[119] ASL Scaligera, https://www.aulss9.veneto.it/index.cfm?action=mys.news&news_id=1438.

[120] GARANTE DELLA PRIVACY, provvedimento del 14 gennaio 2021 (Doc Web 9535354)

Passando all'analisi delle certificazioni[121], nelle *faq* del Garante vengono definite come attestazioni rilasciate da una parte terza (organismo di certificazione - OdC) relative a un oggetto sottoposto a valutazione della conformità rispetto a requisiti contenuti in una norma tecnica o in un disciplinare specifico.

Il GDPR all'art. 42 promuove attivamente l'istituzione di meccanismi di certificazione, nonché l'introduzione di sigilli e marchi di protezione dei dati, come strumenti utili a dimostrare la conformità dei trattamenti ai requisiti del Regolamento e a rafforzare la fiducia degli interessati. Questi strumenti hanno una duplice funzione: da un lato, favoriscono la trasparenza, offrendo ai cittadini un'indicazione immediata e comprensibile sul livello di protezione dei dati garantito da un'organizzazione; dall'altro, supportano il titolare o il responsabile nel dimostrare il rispetto dei principi di *accountability* e *privacy by design*.

Tuttavia, la sola conformità normativa non è più sufficiente a garantire la credibilità di un'organizzazione: è necessario, infatti, disporre di competenze specifiche, processi e sistemi adeguatamente strutturati per affrontare in modo sistemico i rischi connessi alla privacy.

In ambito privacy vengono rilasciate diverse tipologie di certificazione, in base alle esigenze e alle prescrizioni del GDPR[122].

I requisiti per la certificazione sono definiti dagli Enti di Normazione (UNI e CEI in Italia, EN, ISO e IEC a livello europeo e internazionale) attraverso le norme tecniche o Prassi di Riferimento (PdR) o dagli schemi proprietari appartenenti a categorie private.

In conclusione, è opportuno evidenziare che l'aver aderito ad un codice di condotta o l'essersi certificato, non esonera il titolare dalla responsabilità di conformità al Regolamento e non lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti.

IV.3.4. Gli Audit privacy

L'audit sul rispetto della normativa in materia di protezione dei dati personali è uno strumento di verifica della conformità dell'azienda dal punto di vista del trattamento dei dati personali.

---

[121] Le certificazioni sono accreditate quando viene dimostrata, da parte dell'ente unico nazionale di accreditamento istituito ai sensi del Regolamento (CE) n. 765/2008, della terzietà, competenza, imparzialità e adeguatezza dell'OdC.

[122] PONTI C., *Certificazioni privacy, è tempo di "bollini": come ottenerli e le FAQ del Garante* in Agenda Digitale, in Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/certificazioni-privacy-e-tempo-di-bollini-come-ottenerli-e-le-faq-del-garante/

Si è soliti individuare tre categorie di audit: di prima, di seconda e di terza parte. Questa distinzione si riferisce a chi esegue l'audit e al rapporto che ha con l'organizzazione che viene sottoposta al controllo dell'auditor[123].

L'audit di prima parte è condotto dall'azienda stessa, ad esempio dal Titolare del trattamento o dal Responsabile, con l'obiettivo di:

- verificare la conformità alle politiche interne e alle procedure privacy adottate (es. informative, registri, DPIA, gestione consensi);
- valutare l'efficacia delle misure tecniche e organizzative adottate (art. 32 GDPR);
- prepararsi a controlli esterni o certificazioni;
- migliorare il sistema di governance privacy, anche in ottica di privacy by design e by default.

Questo tipo di audit è spesso svolto dal DPO o da un team privacy interno, e costituisce uno strumento essenziale per l'attuazione del principio di *accountability*.

L'audit di seconda parte è eseguito da un'organizzazione su un terzo con cui ha un rapporto contrattuale o collaborativo, come:

- un fornitore (es. cloud provider, società di gestione paghe, software house);
- un Responsabile del trattamento ex art. 28 GDPR designato da un Titolare;
- un sub-responsabile incaricato da un Responsabile primario.

Lo scopo è verificare che il partner esterno rispetti le clausole contrattuali, le istruzioni ricevute e le normative applicabili in materia di protezione dei dati.

L'audit di terza parte è condotto da un soggetto indipendente e accreditato, che non ha alcun interesse diretto con l'organizzazione. Rientrano in questa categoria:

- gli organismi di certificazione accreditati secondo l'art. 43 GDPR;
- autorità di controllo come il Garante Privacy (in caso di ispezioni o accertamenti);
- enti terzi che rilasciano certificazioni ISO/IEC 27701 o sigilli privacy europei.

Questi audit hanno l'obiettivo di valutare oggettivamente la conformità dell'organizzazione agli standard normativi o volontari, rilasciando una certificazione di conformità.

È di fondamentale importanza, maturare piena consapevolezza del ruolo e delle responsabilità dell'auditor, in particolare nell'ambito degli audit interni, al fine di promuovere un contesto di lavoro improntato alla collaborazione e alla trasparenza.

L'auditor non deve essere percepito come una figura antagonista o punitiva, né come un mero "ispettore", ma piuttosto come un alleato strategico dell'organizzazione. Il suo

[123] LINFANTE A., "*L'audit come strumento di compliance privacy: tipologie, procedure e norme di riferimento"* in Cibersecurity360, https://www.cybersecurity360.it/legal/privacy-dati-personali/laudit-come-strumento-di-compliance-privacy-tipologie-procedure-e-norme-di-riferimento/

compito si colloca infatti in una dimensione propositiva e costruttiva: egli condivide con l'organizzazione l'obiettivo comune di garantire un adeguato livello di protezione dei dati personali trattati e di favorire un'efficace conformità alla normativa vigente, in particolare GDPR.

In questa ottica, l'attività dell'auditor assume una funzione di supporto: attraverso l'identificazione di criticità, la verifica delle misure adottate e la proposta di azioni correttive, egli contribuisce al miglioramento continuo del sistema di governance della privacy, favorendo al contempo l'adozione di buone pratiche e la diffusione di una cultura della responsabilizzazione a tutti i livelli dell'azienda.

Per le aziende, predisporre una procedura specifica dedicata agli audit interni rappresenta un passaggio fondamentale, in quanto consente di definire con precisione le modalità operative, i criteri e le responsabilità con cui tali verifiche devono essere condotte. Solo attraverso una struttura metodologica chiara è possibile garantire che l'audit si svolga in modo efficace, coerente e in linea con i principi del GDPR.

A conclusione dell'audit dovrà essere redatto un rapporto contenente l'analisi delle risultanze: sulla base dei rilievi effettuati e contenuti nel rapporto, il titolare del trattamento, dovrà adottare le opportune azioni correttive.

La valorizzazione dell'audit interno come strumento di monitoraggio e miglioramento continuo della compliance rafforza l'efficacia del sistema di governance, promuovendo una visione non punitiva ma collaborativa e partecipativa del controllo. Solo attraverso una sinergia tra cultura organizzativa, innovazione tecnologica e rigore normativo sarà possibile affrontare con successo le sfide poste dal trattamento dei dati personali.

CONCLUSIONE

La presente tesi ha inteso analizzare il complesso percorso intrapreso dall'Unione Europea per la costituzione di un European Health Data Space (EHDS), delineandolo quale strategico volano per l'edificazione di un modello di sanità pubblica rinnovato, caratterizzato da digitalizzazione, sicurezza e interoperabilità.

Questo sforzo progettuale, promosso dalla Commissione Europea, riflette l'ambizione di forgiare un ecosistema dei dati sanitari capace di facilitare l'accesso, la condivisione e il riutilizzo dei dati clinici, preservando, al contempo, la piena tutela dei diritti fondamentali degli individui.

La pervasiva trasformazione digitale del settore sanitario, la cui urgenza è stata amplificata dalla crisi pandemica, rende inderogabile la creazione di un contesto normativo e infrastrutturale comune che, pur incentivando l'innovazione e il progresso medico, si fondi su un impianto robusto di garanzie.

In tale quadro, il Regolamento (UE) 2016/679 (GDPR) si erge a pilastro normativo cardine, fornendo un lessico condiviso per la protezione della privacy a livello europeo e imponendo una responsabilizzazione attiva a tutti i soggetti coinvolti. I principi di *privacy by design*, *data minimisation* e *accountability* si riconfermano quali strumenti essenziali per garantire una sanità digitale etica e sostenibile.

L'analisi dell'Ecosistema dei Dati Sanitari (EDS) in Italia ha rivelato una fase di implementazione avanzata, sebbene caratterizzata da una significativa disomogeneità.

Le marcate disparità regionali nell'accesso da parte dei cittadini e nella partecipazione attiva dei professionisti sanitari suggeriscono che, pur riconoscendo il potenziale del Fascicolo Sanitario Elettronico (FSE) 2.0 come strumento di *empowerment* del paziente e di ottimizzazione delle cure, la sua piena efficacia è subordinata a una governance più incisiva e a un quadro tecnico-normativo più omogeneo a livello nazionale.

Gli strumenti di governance e compliance previsti dal GDPR, quali il Sistema di Gestione della Privacy (SGP), le pratiche di gestione dei rischi, i registri delle attività, le valutazioni d'impatto (DPIA) e i codici di condotta, non devono essere ridotti a meri adempimenti burocratici, costituiscono, piuttosto, meccanismi cruciali per l'instaurazione di una cultura della responsabilità e della trasparenza.

Un ruolo di preminente importanza è stato riconosciuto al Data Protection Officer (DPO), figura ormai imprescindibile nelle realtà sanitarie.

Il DPO non è più un semplice garante formale della normativa, ma un attore strategico, capace di fungere da interfaccia dialettica tra le direzioni aziendali, i responsabili IT e i clinici, al fine di progettare trattamenti di dati che siano al contempo rispettosi dei diritti e innovativi.

L'esperienza della Sardegna, con il coordinamento tra i DPO delle aziende sanitarie, si configura come un esempio virtuoso di governance condivisa e pragmatica, attestando il potenziale di una collaborazione strutturata per superare le criticità e garantire un'applicazione omogenea delle norme e una tutela efficace dei diritti degli interessati.

L'analisi condotta rivela inequivocabilmente che la digitalizzazione della sanità non rappresenta unicamente un traguardo tecnologico, bensì un profondo mutamento culturale che coinvolge istituzioni, operatori e cittadini.

L'uso secondario dei dati sanitari per finalità di ricerca, prevenzione e pianificazione deve necessariamente essere bilanciato con il diritto all'autodeterminazione informativa, valorizzando il consenso, la trasparenza e il controllo da parte dell'interessato.

Nonostante i progressi teorici e normativi, la piena realizzazione di un ecosistema dei dati sanitari realmente efficiente e rispettoso della privacy incontra ancora diverse criticità.

La disomogeneità implementativa e l'enigma dell'adozione civica persistono, come evidenziato dalla limitata percentuale di cittadini che accedono al proprio FSE (circa il 18% nel trimestre giugno-agosto 2024 a livello nazionale) e dalle marcate differenze nell'abilitazione dei medici specialisti, il che suggerisce che le attuali strategie di informazione e sensibilizzazione non sono ancora sufficientemente incisive. Si rende imperativo, pertanto, l'implementazione di campagne nazionali di sensibilizzazione e alfabetizzazione digitale di ampia portata, che illustrino i benefici tangibili del FSE e le modalità di accesso in una veste semplificata e inclusiva. Contestualmente, è indispensabile razionalizzare le procedure di accesso e utilizzo per i cittadini, auspicabilmente attraverso l'adozione di interfacce utente più intuitive e un potenziamento del supporto tecnico a livello locale.

La complessità del contesto normativo e la delicata armonizzazione del consenso rappresentano un'altra area critica.

Sebbene il GDPR stabilisca il quadro di riferimento, l'intersezione con normative nazionali e settoriali, come il Regolamento EHDS e la Direttiva NIS 2, genera un ambiente giuridico di notevole complessità.

La previsione di meccanismi di opt-out per l'uso secondario e di opt-in per categorie di dati particolarmente sensibili costituisce un passo progressivo, ma la sua interpretazione e la sua applicazione pratica possono ancora generare incertezze.

Le autorità di controllo nazionali e l'European Data Protection Board (EDPB) dovrebbero impegnarsi nella produzione di linee guida chiare e operative, arricchite da esempi concreti, al fine di dirimere le interazioni tra le diverse normative e di definire modalità precise per la gestione del consenso e dell'obiezione, in particolare per i dati sanitari più sensibili.

Un ulteriore elemento di criticità risiede nel divario tecnologico e nella vulnerabilità cibernetica delle strutture sanitarie.

La tesi ha posto in luce la persistenza di sistemi legacy eterogenei in molte strutture ospedaliere, rendendole intrinsecamente vulnerabili agli attacchi informatici.

Il dato allarmante del 100% di incidenti informatici registrati nel settore sanitario italiano nel 2024 con impatti gravi o gravissimi sottolinea l'impellenza di investimenti mirati

e un radicale cambio di approccio. Si configura come cruciale l'implementazione di un piano nazionale di ammodernamento infrastrutturale e tecnologico per il settore sanitario, con l'obbligo di adottare sistemi certificati e interoperabili. Concomitantemente, la formazione continua e obbligatoria del personale sui temi della cybersecurity deve assumere carattere prioritario, estendendosi non solo agli specialisti IT ma a tutti gli operatori, per trasformare la sicurezza informatica da mero adempimento a cultura operativa diffusa.

Infine, la limitata integrazione del DPO e l'esigenza di proattività strategica meritano attenzione. La figura del DPO è, in taluni contesti, ancora percepita come un mero adempimento formale, coinvolta prevalentemente ex post, in situazioni di emergenza.

La sua funzione strategica di consulenza preventiva, intrinseca al principio di privacy by design, non è ancora pienamente valorizzata. È indispensabile, dunque, promuovere un coinvolgimento proattivo e strutturale del DPO in tutte le fasi di progettazione e implementazione di nuovi trattamenti di dati e sistemi in ambito sanitario.

L'incentivazione della creazione di reti regionali e nazionali di DPO nel settore sanitario può favorire la condivisione di buone pratiche, la risoluzione coordinata delle criticità e un'applicazione più omogenea della normativa sul territorio.

In ultima analisi, il successo dell'EHDS e, più in generale, della sanità digitale europea, non si misurerà unicamente in termini di efficienza tecnologica, ma sarà strettamente correlato alla capacità di mantenere al centro la persona: non come mero oggetto di trattamento dati, bensì come soggetto consapevole e partecipe del proprio percorso di salute, in un ambiente digitale sicuro, accessibile e rispettoso della dignità umana.

Le sfide future, dal consolidamento dell'interoperabilità all'affinamento delle misure di sicurezza e alla promozione di una cultura della protezione dei dati, richiederanno un impegno costante e una collaborazione sinergica tra tutti gli attori coinvolti, per garantire che i dati sanitari siano una risorsa preziosa per la salute collettiva, gestita con la massima responsabilità e rispetto per l'individuo.

BIBLIOGRAFIA

Arcuri, M. A., *EHDS ed EDS: la tutela della salute migliora attraverso la digitalizzazione della sanitò e la ricerca scientifica,* Agenda Digitale.https://www.altalex.com/documents/news/2025/05/05/ehds-eds-tutela-salute migliora-attraverso-digitalizzazione-sanita-ricerca-scientifica, 2025

Bacchieri, S., *Direttiva NIS 2: requisiti e impatti per il settore sanitario*, in *Cybersecurity360*, https://www.cybersecurity360.it/legal/direttiva-nis-2-requisiti-e-impatti-per-il-settore-sanitario/, 2024

Bassan F., *Dati non personali e regolazione europea: Il Data Act tra accesso e competitività*. in Diritto dell'economia digitale, n. 2. 2023

Buttarelli, G., *Privacy 2030: Una nuova visione per l'Europa*. IAPP., 2019

Califano, L., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*. Napoli: Editoriale Scientifica, 2017

Caggìa, F., *Il trattamento dei dati sanitari sulla salute.* Cuffaro V., D'Orazio R., & Ricciuto V., (Eds.), *Il codice del trattamento dei dati personali*. Torino: Giappichelli, 2007

Cataletta, A., *Data Governance Act ora applicativo: così cambia l'economia digitale.* Agenda Digitale. https://www.agendadigitale.eu/sicurezza/privacy/la-data-economy-alla-prova-del-data-governance-act-lo-scenario/, 22. 2023

Comandé, G., Nocco, M., & Peigné, G., *Il fascicolo sanitario elettronico: uno studio multidisciplinare.* Rivista Italiana di Medicina Legale, 2012

Corso, S., *Il fascicolo sanitario elettronico 2.0: spunti per una lettura critica. Le Nuove Leggi Civili Commentate*, 2024

D'Alessi, F., *Il ruolo del Registro delle Attività di Trattamento nelle aziende.* Mondo Privacy. https://mondoprivacy.it/blog/accountability/registro-delle-attivita-ditrattamento/, 2025

De Pretis, G.*, DPO in Sanità, un ruolo essenziale: come sceglierlo*. Agenda Digitale. https://www.agendadigitale.eu/sanita/sanita-il-ruolo-essenziale-del-dpo-come-sceglierlo/2025

Di Giacomo, L., *La Direttiva europea NIS2 per punti essenziali*. Diritto.it. https://www.diritto.it/la-direttiva-europea-nis2-per-punti-essenziali/2025

Dhoor Singh, D., *Cibersicurezza, la Direttiva NIS 2*. Altalex. https://www.altalex.com/documents/news/2023/01/24/cibersicurezza-direttiva-nis-2, 2023

Finocchiaro G., *Privacy e protezione dei dati personali. Commentario al GDPR e al Codice della privacy*, Bologna, Zanichelli, 2019

Finocchiaro, G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi* (1ª ed.). Zanichelli. ISBN 9788808065650, 2012

Giannone, G., *Risk-based approach e trattamento dei dati personali*. In S. Sica, V. D'Antonio, & G. M. Riccio (Eds.), *La nuova disciplina europea della privacy*. Cedam. 2016

Gorgoni, G., *EHDS: verso l'unione sanitaria europea: cos'è, le cautele, i vantaggi per i cittadini*. Agenda Digitale. https://www.agendadigitale.eu/sanita/ehds-verso-lunione-sanitaria-europea-cose-le-cautele-i-vantaggi-per-i-cittadini/

Licheri, G., *EHDS ed EDS: al via la rivoluzione dei dati sanitari in Europa e in Italia.* I-Com.,https://www.i-com.it/2025/03/14/ehds-ed-eds-al-via-la-rivoluzione-dei-dati-sanitari-in-europa-e-in-italia/. 2025

Linfante, A., *L'audit come strumento di compliance privacy: tipologie, procedure e norme di riferimento*. Cybersecurity360. https://www.cybersecurity360.it/legal/privacy-dati-personali/laudit-come-strumento-di-compliance-privacy-tipologie-procedure-e-norme-di-riferimento/. 2021

Magagna, F*., Soggetti "essenziali" e "importanti" secondo la NIS 2: differenze e implicazioni.* Lex Tech Hub. https://www.dataprotectionforum.eu/post/soggetti-essenziali-e-importanti-secondo-la-nis-2-differenze-e-implicazioni

Maggiolini, M., *Interoperabilità dei dati della pubblica amministrazione: novità in materia di dati sanitari.* Amministrativ@mente, (13665). Università Foro Italico, Roma. 2023

Mantelero, A., In G. Finocchiaro (Ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (pp. 287–330). Zanichelli. 2017

Mantelero, A., & Poletti, D. (Eds.). *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*. Pisa: Pisa University Press. 2018

Pavel V., *Rethinking data and rebalancing digital power. Report training data*, in Ada Lovelace Institute. https://www.adalovelaceinstitute.org/report/rethinking-data/

Pizzetti, F. (2016). *Privacy e il nuovo diritto europeo dei dati personali*. Torino: Giappichelli.

Ponti, C., & Castroreale, R. *Certificazioni privacy, è tempo di "bollini"*: https://www.agendadigitale.eu/sicurezza/privacy/certificazioni-privacy-e-tempo-di-bollini-come-ottenerli-e-le-faq-del-garante/. 2021

Posteraro, N., *Parere del Garante privacy sullo schema di decreto sul Fascicolo Sanitario Elettronico (FSE). Federalismi.it* (Osservatorio di diritto sanitario). https://www.federalismi.it. 2023

Rodotà, S., *Tecnologie e diritti*. Bologna: Il Mulino.1995

Rodotà, S., *Intervista su privacy e libertà* (P. Conti, Ed.). Roma-Bari: Laterza. 2005

Rodotà, S., *Il diritto di avere diritti*. Roma-Bari: Laterza, 2015

Rotolo, A., Longo, F., & Caccia, C. (2024). *Una visione sistemica per i silos digitali del PNRR*. *Mecosan*, 130, 19–47. https://doi.org/10.3280/mesa2024-130oa18956

Vicarelli, G., & Bronzini, M., *La sanità digitale: dimensioni di analisi e prospettive di ricerca*. *Politiche Sociali*, 5(2), 147–161. https://doi.org/10.7389/90591. 2018

Viola G*, Governare i dati in Europa. Dal GDPR al Data Act: nuove sfide normative*. Milano: Giuffrè Francis Lefebvre. 2024

Weber, K., Otto, B., & Österle, H., *One size does not fit all: a contingency approach to data governance*. Journal of Data and Information Quality, Article 4. https://doi.org/10.1145/1515693.1515696. 200

FONTI

Normativa e Documenti dell'Unione Europea

Carta dei Diritti Fondamentali dell'Unione Europea

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.*

Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 200*3, relativa al riutilizzo dell'informazione del settore pubblico.*

Direttiva 2007/2/CE del Parlamento europeo e dal Consiglio, del 14 marzo 2007, che istituisce l'infrastruttura per l'informazione territoriale nell'Unione europea (Inspire)

Direttiva 2013/37/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013*, che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.*

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016*, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).*

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018*, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.*

Commissione europea. *2019. Comunicazione della Commissione al Parlamento Europeo e al Consiglio:Empty, guidance on the Regulation on a framework for the free flow of non-personal data in the European Union: COM(2019) 250 final.*

Commissione Europea. 2020. *Strategia europea per i dati: COM(2020) 66 final.*

Parlamento Europeo. 25 marzo 2021. *Risoluzione su una strategia europea per i dati (2020/2217(INI)).*

Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022*, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Data Governance Act).*

Commissione Europea. *Proposta di Regolamento sull' Health Data Space, art. 3. COM(2022) 197 final*

Commissione Europea*, EHDS Impact Assessment, SWD(2022) 101 final, p. 22*

Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, *relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS 2).*

Commissione Europea. *2022. Health Data Access Bodies – Community of Practice.*

Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 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 (Data Act).*

Regolamento (UE) del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828. *Regolamento sull'intelligenza artificiale.*

Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, *sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.*

Parlamento Europeo. 22 novembre 2023. *Risoluzione sui progetti del Parlamento europeo intesi a modificare i trattati (2022/2051(INL)).*

Unione Europea. *Versione consolidata del Trattato sull'Unione Europea e del Trattato sul funzionamento dell'Unione Europea (2012/C 326/01).*

Consiglio dell'Unione Europea. 14 gennaio 2025. *Spazio europeo dei dati sanitari: il Consiglio adotta un nuovo regolamento che migliora l'accesso transfrontaliero ai dati sanitari dell'UE.* Comunicato stampa.

Normativa nazionale italiana

Costituzione della Repubblica Italiana

D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

D.lgs. 27 gennaio 2010, n. 32 di "*Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità Europea (INSPIRE)"*

L. 17 dicembre 2012, n. 221, Conversione in legge, con modificazioni, del D.L. 18 ottobre 2012, n. 179, *recante ulteriori misure urgenti per la crescita del Paese.*

L. 19 maggio 2020, n. 34, *Misure urgenti in materia di salute, sostegno al lavoro e all'economia (c.d. "Decreto Rilancio").*

D.lgs. 18 maggio 2018, n. 65, *Attuazione della direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (NIS).*

D.M. 20 maggio 2022*, Adozione delle Linee guida per l'attuazione del Fascicolo Sanitario Elettronico (FSE).*

D.P.R. 29 settembre 2015, n. 178, *Regolamento in materia di Fascicolo Sanitario Elettronico.*

Altre Fonti

Ministero della Salute e Dipartimento per la Trasformazione Digitale. *I dati di utilizzo del Fascicolo Sanitario Elettronico da parte di cittadini, medici e aziende sanitarie.*

Camera dei Deputati. *Il nuovo fascicolo sanitario elettronico.*

Agenzia per l'Italia Digitale (AgID), *2024, Guida operativa sulle serie di dati di elevato valore. Documento di orientamento per l'attuazione del Regolamento di esecuzione (UE) 2023/138 e delle Linee Guida per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico.*

Agenzia per la Cybersicurezza Nazionale (ACN). Determinazione del Direttore Generale del 14 aprile 2025 n. 164179, di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, recante *termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale*.

Provvedimenti e documenti del Garante per la Protezione dei dati personali

Garante per la protezione dei dati personali. 16 luglio 2009. *Linee guida in tema di Fascicolo Sanitario Elettronico (FSE) e di dossier sanitario.* Provvedimento n. 1634116.

Garante per la protezione dei dati personali. 26 luglio 2017. *Parere su uno schema di decreto del MEF di concerto con il Ministero della salute, concernente le modalità tecniche e i servizi telematici resi disponibili all'infrastruttura nazionale per l'interoperabilità dei FSE*". Provvedimento n. 341.

Garante per la protezione dei dati personali. 27 settembre 2018. *Parere su uno schema di decreto in tema di interoperabilità del Fascicolo Sanitario Elettronico (FSE).* Provvedimento n. 456.

Garante per la protezione dei dati personali. 7 marzo 2019. *Indicazioni per l'applicazione del GDPR in ambito sanitario,* Provvedimento n. 55.

Garante per la protezione dei dati personali. 22 agosto 2022. *Parere sullo schema di decreto sul Fascicolo Sanitario Elettronico (FSE),* Provvedimento n. 294.

Garante per la protezione dei dati personali. 22 agosto 2022. *Parere al Ministero della Salute sullo schema di decreto sull'Ecosistema Dati Sanitari (EDS)*. Provvedimento n. 295.

Garante per la protezione dei dati personali. *2023. Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali.*

Garante per la protezione dei dati personali. 26 settembre 2024. *Parere sullo schema di decreto del Ministero della salute sull'Ecosistema Dati Sanitari (EDS)*. Provvedimento n. 605.

Garante per la protezione dei dati personali. *Registro delle attività di trattamento. Faq*.

Giurisprudenza dell'Unione Europea

Corte di Giustizia dell'Unione Europea. 13 maggio 2024. *Sentenza Google Spain SL, Google Inc. contro Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, ECLI:EU:C:2014:317*.

Corte di Giustizia dell'Unione Europea. 16 luglio 2020. *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559*.