Comparative Law Review

Vol. 17 · No. 2
2026

REGULAR ISSUE

ISSN 2038 – 8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.
Editor on the Register: Alessandro Somma

COMPARATIVE
LAW
REVIEW
VOL. 17/2 - 2026

Spazio europeo dei dati sanitari

SPAZIO EUROPEO DEI DATI SANITARI

IL SISTEMA SANZIONATORIO DELL'*EUROPEAN HEALTH DATA SPACE*: TRA ARMONIZZAZIONE E FRAMMENTAZIONE NORMATIVA

*Miriam I. Nigro Di Gregorio – Alessia P. Mangiacotti**

SOMMARIO:

l contributo analizza il sistema sanzionatorio delineato dal Regolamento (UE) 2025/327 istitutivo dello Spazio Europeo dei Dati Sanitari (European Health Data Space – EHDS), interrogandosi sulla sua effettiva idoneità ad assicurare un'applicazione uniforme della disciplina nei diversi ordinamenti degli Stati membri. L'indagine prende avvio dalla ricostruzione del ruolo degli Organismi responsabili dell'accesso ai dati sanitari, configurati dal regolamento quali nuovi snodi della governance europea dell'uso secondario dei dati sanitari, soffermandosi sulle funzioni di autorizzazione, controllo e vigilanza loro attribuite, nonché sui rapporti di coordinamento con le Autorità di sanità digitale e con le Autorità di controllo competenti in materia di protezione dei dati personali.

Su tali premesse, il contributo esamina la disciplina delle misure di esecuzione e del sistema sanzionatorio amministrativo prevista dal regolamento, evidenziando come l'ampio rinvio a profili rimessi al diritto nazionale possa incidere sull'effettivo conseguimento dell'obiettivo di armonizzazione perseguito dal legislatore europeo. In tale prospettiva, particolare attenzione è riservata alle possibili divergenze applicative tra gli Stati membri, anche attraverso l'analisi dell'esperienza danese, assunta quale caso di studio esemplificativo delle differenti soluzioni organizzative suscettibili di essere adottate nell'attuazione del regolamento.

In conclusione, si sostiene che l'effettività del sistema sanzionatorio dell'EHDS dipenderà dalla capacità di rafforzare i meccanismi di coordinamento a livello europeo mediante l'elaborazione di orientamenti interpretativi comuni, la definizione di standard applicativi condivisi e l'esercizio di un ruolo propulsivo da parte delle istituzioni dell'Unione, al fine di contenere i rischi di frammentazione applicativa e garantire un livello uniforme di tutela all'interno dello Spazio Europeo dei Dati Sanitari.

Keywords: Organismi responsabili dell'accesso ai dati sanitari - Governance dei dati sanitari - Apparato sanzionatorio EHDS - Frammentazione applicativa del sistema sanzionatorio EHDS - Armonizzazione del diritto dell'Unione Europea

I. IL RUOLO DEGLI ORGANISMI RESPONSABILI DELL'ACCESSO AI DATI SANITARI.

Il Regolamento che ha istituito l'*European Health Data Space* (EHDS) rappresenta un punto cardine nel passaggio verso l'ottimizzazione dell'accesso[1] e del controllo[2] dei dati sanitari[3] e introduce una significativa evoluzione ed estensione delle diverse possibilità di riutilizzo dei dati per finalità di interesse pubblico[4], ulteriori rispetto agli scopi posti alla base della raccolta iniziale[5].

In tale contesto emerge con forza il ruolo cruciale degli Organismi responsabili dell'accesso ai dati sanitari e, sebbene il nuovo regolamento non ne fornisca una definizione puntale, è chiaro il riferimento ad entità pubbliche con personalità giuridica[6], chiamate a garantire il conforme utilizzo secondario dei dati, promuovendone la condivisione[7]. Tali figure[8], ideate per soddisfare esigenze di interesse generale, dovranno disporre di risorse necessarie per dare attuazione ai poteri ad esse riconosciuti[9], collaborando alla creazione di un ambiente sicuro e affidabile per l'elaborazione dei dati sanitari elettronici a supporto della ricerca, dell'ideazione di politiche orientate all'innovazione e, in generale, per il perseguimento di molteplici finalità annesse[10].

Gli Organismi responsabili dell'accesso ai dati sanitari verranno designati da ciascuno Stato membro, che deciderà, tenendo conto delle esigenze nazionali, se individuare una figura

1* Il presente scritto si inserisce nell'ambito del progetto di ricerca di Ateneo PRA 2023 – Università di Foggia "*Health Data: protection and free movement in the digital age*".

** Nell'ambito del presente articolo, condiviso da entrambe le Autrici, la dott.ssa Miriam I. Nigro Di Gregorio ha redatto i §§ I. e II, mentre la dott.ssa Alessia Pia Mangiacotti i §§ III, IV e V.

1 Sul punto, v. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari, in G.U.U.E., 5 marzo 2025, art. 3. L'immediata disponibilità dei dati sanitari in formato elettronico è garantita dalla previsione di servizi gratuiti articolati su base nazionale, regionale o locale: v. Reg. (UE) 2025/327, cit., art. 4, par. 1. In particolare, ai pazienti è consentito l'accesso ai dati sanitari elettronici rientranti nelle categorie prioritarie, trattati per l'erogazione di servizi assistenziali: Reg. (UE) 2025/327, cit., art.14, par.1. Tale accesso viene garantito da un sistema di cartelle elettroniche che facilitano la consultazione dei dati clinici inseriti: Reg. (UE) 2025/327, cit., art. 3, par. 2. Per un puntuale approfondimento sul diritto di accesso relativo ai documenti informatici sanitari, cfr. ampiamente F. C. RAMPULLA, G. C. RICCIARDI, A. VENTURI, *Digitalizzazione delle amministrazioni e accesso ai dati e ai documenti informatici sanitari*, federalismi, 2024.

2 Il controllo e la condivisione dei dati costituiscono pilastri fondamentali dell'EHDS che mira all'interoperabilità delle informazioni cliniche: sul punto Reg. (UE) 2025/327, cit., Considerando 1, Considerando 110.

3 Per un approfondimento relativo al concetto di "dato sanitario", v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, Milano, 2018, 13 e ss.

4 Reg. (UE) 2025/327, cit., Considerando 53; sul punto, v. M. MAGGIOLINI, *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari* in *Rivista scientifica trimestrale di diritto amministrativo*, 2025, 397 e ss.

5 Sul punto, v. Reg. (UE) 2025/327, cit., art. 2, par. 2, lettera e); si rinvia al Capo IV del medesimo Regolamento per un puntale approfondimento relativo all'uso secondario dei dati.

6 La qualificazione di tali soggetti come enti pubblici è resa esplicita dal fatto che si tratta di Organismi designati direttamente dagli Stati membri che «possono istituire uno o più enti pubblici nuovi oppure fare affidamento su enti pubblici esistenti o su servizi interni di enti pubblici che soddisfano le condizioni di cui al presente articolo»: Reg. (UE) 2025/327, cit., art. 55, par. 1.

7 S. N. NAVARRO, *Datos sanitarios electrónicos, El espacio europeo de datos sanitarios*, Madrid, 2023, 231 e ss.

8 La *governance* adottata all'interno dello Spazio Europeo dei Dati Sanitari trae origine dal Regolamento (UE) 2022/868 relativo alla *governance* europea dei dati il cui articolo 7 prevede la designazione di uno o più Organismi competenti «per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo delle categorie di dati»: per un attento confronto v. Regolamento sulla *governance* dei dati (UE) 2022/868, 30 maggio 2022, in G.U.U.E., 3 giugno 2022, art. 7.

9 Reg. (UE) 2025/327, cit., art. 55, par. 2.

10 *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies,* 27 febbraio 2025, 8 e ss.

unica o ripartire l'incarico su più unità, mediante creazione *ex novo* o tramite l'attribuzione del ruolo ad entità già esistenti[11]. Nel caso di designazione di più Organismi, le funzioni verranno ripartite[12] e dovrà essere individuato un coordinatore che dovrà garantire un lavoro sinergico e armonizzato[13].

Ogni Organismo si impegnerà ad adottare condotte coerenti e strumenti operativi finalizzati all'applicazione uniforme del regolamento in tutto il territorio sovranazionale e per farlo collaborerà attivamente con le stesse entità degli altri Stati e con la Commissione Europea.

Al fine di assicurare un efficiente operato, gli Stati membri dovranno predisporre risorse umane, finanziarie e tecniche adeguate, con annesse infrastrutture, evitando qualsiasi conflitto di interessi tra le diverse aree; in tutte le fasi operative dovrà essere assicurata l'indipendenza, e ogni intervento dovrà mirare al perseguimento di finalità compatibili con l'interesse collettivo. Nella fase di gestione, gli Organismi competenti saranno, altresì, tenuti a coinvolgere i portatori di interessi, inclusi pazienti, titolari dei dati sanitari e ricercatori[14]. Ciascuno Stato informerà il pubblico dell'importanza del ruolo di questa figura embrionale, che, con cadenza bimestrale redigerà una relazione sull'attività svolta[15], successivamente resa pubblica tramite appositi siti *web* e presentata alla Commissione e al Comitato dello

11 Reg. (UE) 2025/327, cit., art. 55.

12 *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies,* cit., 11 e ss.

13 *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies,* cit., 8 e ss.

14 All'interno di ogni Organismo dovrebbe essere istituito un gruppo dedicato alla gestione dei metadati, composto da esperti, al fine di garantire la gestione coerente e accurata degli stessi. Sul punto, rileva l'esempio presente nel *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, del 27 febbraio 2025, dal quale emerge che alla domanda se avessero risorse umane sufficienti per implementare il catalogo di metadati per descrivere e gestire le attribuzioni dei dati, il 14% dei futuri organi che svolgeranno questa funzione ha dichiarato di aspettarsi un cambiamento moderato nelle proprie risorse umane, mentre il 79% ha dichiarato di aspettarsi un grande cambiamento. Ciò evidenzia la necessità di un'allocazione strategica delle risorse e di una pianificazione della forza lavoro per far fronte alle richieste previste: sul punto, v. Appendice 5 - Questionario HDAB, *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, cit., 19 e ss.

15 «Ogni due anni ciascun organismo responsabile dell'accesso ai dati sanitari pubblica una relazione di attività e la rende pubblicamente disponibile sul suo sito *web*. Se uno Stato membro designa più di un organismo responsabile dell'accesso ai dati sanitari, l'organismo di coordinamento di cui all'articolo 55, paragrafo 1, è responsabile della relazione di attività e richiede le informazioni necessarie agli altri organismi responsabili dell'accesso ai dati sanitari. Tale relazione di attività segue una struttura concordata dal comitato EHDS a norma dell'articolo 94, paragrafo 2, lettera d), e contiene almeno le categorie di informazione seguenti: a) informazioni relative alle domande di accesso ai dati sanitari e alle richieste di dati sanitari presentate, quali i tipi di richiedenti di dati sanitari, il numero di autorizzazioni ai dati rilasciate o respinte, le categorie delle finalità dell'accesso e le categorie di dati sanitari elettronici a cui si è avuto accesso, nonché se del caso una sintesi dei risultati degli impieghi dei dati sanitari elettronici; b) informazioni sull'adempimento degli impegni normativi e contrattuali da parte degli utenti dei dati sanitari e dei titolari dei dati sanitari, nonché sul numero e sull'importo delle sanzioni amministrative pecuniarie imposte dagli organismi responsabili dell'accesso ai dati sanitari; c) informazioni sugli audit effettuati sugli utenti dei dati sanitari per garantire la conformità del trattamento che questi effettuano in un ambiente di trattamento sicuro in conformità dell'articolo 73, paragrafo 1, lettera e); d) informazioni sugli audit interni e di terzi sulla conformità degli ambienti di trattamento sicuri alle norme, alle specifiche e alle prescrizioni stabilite, di cui all'articolo 73, paragrafo 3; e) informazioni sul trattamento delle richieste presentate da persone fisiche riguardo all'esercizio dei loro diritti alla protezione dei dati; f) una descrizione delle attività svolte dall'organismo responsabile dell'accesso ai dati sanitari in relazione al coinvolgimento e alla consultazione dei portatori di interessi pertinenti; g) le entrate derivanti da autorizzazioni ai dati e richieste di dati sanitari; h) il numero medio di giorni tra la domanda di accesso ai dati sanitari o la richiesta di dati sanitari e l'accesso ai dati; i) il numero di marchi di qualità dei dati rilasciati dai titolari dei dati sanitari, suddiviso per categoria di qualità; j) il numero di pubblicazioni di ricerca sottoposte a valutazione *inter pares*, documenti strategici e procedure di regolamentazione che utilizzano dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari; k) il numero di prodotti e servizi di sanità digitale, comprese le applicazioni di IA, sviluppati utilizzando dati a cui si è avuto accesso tramite lo spazio europeo dei dati sanitari»: Reg. (UE), 2025/327, cit., art. 59, par. 1.

spazio europeo dei dati sanitari entro sei mesi dalla fine del secondo anno del periodo di riferimento[16].

Le molteplici funzioni attribuite agli Organismi responsabili dell'acceso ai dati sanitari[17], ne evidenziano l'oggettiva centralità all'interno del contesto dell'uso secondario dei dati[18]: tra le principali responsabilità rientrano il rilascio delle autorizzazioni per l'accesso ai dati sanitari elettronici[19] e la valutazione delle richieste di dati per le finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario[20].

All'interno di ogni Stato, l'Organismo preposto si esprimerà concedendo o negando l'accesso ai dati sanitari, entro tre mesi dal ricevimento della domanda[21]; un eventuale diniego dovrà essere motivato[22]. Il rilascio dell'autorizzazione consentirà l'utilizzo dei dati[23]. Gli Organismi saranno incaricati anche di attività di monitoraggio e controllo; qualora si verifichino comportamenti o omissioni che compromettano la collaborazione, come un diniego ingiustificato di concessione dei dati o il mancato rispetto dei termini stabili[24], adotteranno misure sanzionatorie[25] improntate a criteri di proporzionalità e trasparenza. Tra queste, potrà essere applicata una penalità di mora giornaliera, calcolata in conformità alla normativa nazionale vigente, per ogni giorno di ritardo. Ripetute violazioni consentiranno all'Organismo di escludere, o avviare procedimenti per escludere il titolare dalla possibilità di accedere ai dati sanitari per un periodo non superiore a cinque anni[26].

Inoltre, l'autorizzazione ai dati rilasciata potrà essere revocata nei casi in cui gli utenti adottino condotte difformi alle prescrizioni; in tal caso, gli Organismi interverranno

16 Reg. (UE) 2025/327, cit., art. 59, par. 2.

17 Per un approfondimento, v. Reg. (UE) 2025/327, cit., art. 57.

18 Sul punto v. S.N. NAVARRO, *Datos sanitarios electrónicos, El espacio europeo de datos sanitarios*, cit., 234 e ss.

19 Reg. (UE) 2025/327, cit., art. 68.

20 Reg. (UE) 2025/327, cit., art. 69; relativamente alle finalità perseguibili, v. art. 53. Per un approfondimento esaustivo in merito alle attribuzioni e funzioni degli organismi preposti alla gestione e al controllo dei dati sanitari nel contesto dell'uso secondario, si rinvia a R. AMBROSINO, *Governance profiles of secondary use of health data in the EHDS,* in *Comparative Law Review*, vol. 17/1, 2026, 126 e ss.

21 Reg. (UE) 2025/327, cit., art. 68 par. 4: «In deroga al regolamento (UE) 2022/868 l'organismo responsabile dell'accesso ai dati sanitari rilascia o nega un'autorizzazione ai dati entro tre mesi dal ricevimento di una domanda completa di accesso ai dati sanitari. Se conclude che la domanda di accesso ai dati sanitari è incompleta, l'organismo responsabile dell'accesso ai dati sanitari informa il richiedente di dati sanitari, cui è concessa la possibilità di completare la domanda. Se il richiedente di dati sanitari non completa la domanda di accesso ai dati sanitari entro quattro settimane, l'autorizzazione non è rilasciata. L'organismo responsabile dell'accesso ai dati sanitari può prorogare di altri tre mesi il termine di risposta a una domanda di accesso ai dati sanitari, se necessario, tenendo conto dell'urgenza e della complessità della domanda di accesso ai dati sanitari e del volume di domande di accesso ai dati sanitari presentate per decisione. In tali casi l'organismo responsabile dell'accesso ai dati sanitari comunica quanto prima al richiedente di dati sanitari che è necessario più tempo per esaminare la domanda di accesso ai dati sanitari, indicando i motivi del ritardo».

22 Reg. (UE) 2025/327, cit., art. 68, par. 9.

23 Reg. (UE) 2025/327, cit., art. 68, par. 7.

24 Reg. (UE) 2025/327, cit., art. 60, par. 2: «Il titolare dei dati sanitari mette a disposizione dell'organismo responsabile dell'accesso ai dati sanitari i dati sanitari elettronici richiesti di cui al paragrafo 1 entro un termine ragionevole non superiore a tre mesi dal ricevimento della richiesta da parte dell'organismo in questione. In casi giustificati, l'organismo responsabile dell'accesso ai dati sanitari può prorogare tale periodo per un massimo di tre mesi».

25 Si segnala, in particolare, l'analisi condotta da M. CUCCOVILLO, *Uso secondario dei dati sanitari e tutela dell'interessato: tra rimedi e sanzioni,* in questo volume, par. V.

26 Reg. (UE) 2025/327, cit., art. 63, par. 4. Sul ruolo del titolare dei dati sanitari, v. M. NATALE, O. TROIANO, *L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari*, in questo volume, par. IX.

interrompendo senza ritardo il trattamento e adottando le soluzioni conformi a garanzia di un trattamento uniforme. In scenari di tal tipo dovranno essere adottate misure adeguate e proporzionate e, nel caso in cui risulti indispensabile, potranno essere avviati procedimenti di esclusione[27].

Le misure di esecuzione adottate dall'Organismo responsabile dell'accesso ai dati sanitari verranno condivise mediante l'utilizzo di uno strumento informatico integrato nell'infrastruttura DatiSanitari@UE (*HealthData@EU*) [28], al fine di garantire un'applicazione coordinata delle misure previste[29]. Tuttavia, poiché il regolamento non fornisce una definizione univoca delle misure di esecuzione da adottare, vi è il rischio che ogni Stato attribuisca al concetto di misura adeguata e proporzionata un significato autonomo. L'impiego di espressioni dal contenuto applicativo incerto potrebbe causare l'attuazione frammentata e non omogenea delle misure adottate a livello europeo, minando la coerenza del sistema sanzionatorio.

Inoltre, le misure di esecuzione prevedono la possibilità di avvio di procedimenti volti ad escludere l'utente[30] dallo spazio europeo, in conformità al diritto nazionale: anche in questo contesto emerge una possibile frammentazione applicativa. Differenti modalità attuative della disciplina europea, da Stato a Stato, potrebbero generare significative disparità di trattamento, con conseguenze potenzialmente dannose, aggravate dalle divergenze linguistiche e interpretative[31]. Tali lacune dovranno necessariamente essere colmate tramite puntuali interventi della Commissione, volti ad allineare l'attuazione regolamentare

---

[27] Gli Organismi responsabili dell'accesso ai dati sanitari, nel momento in cui svolgeranno attività di monitoraggio e controllo, precisamente in riferimento alla richiesta di dati sanitari elettronici di cui all'articolo 51 ai titolari dei dati sanitari, avranno il diritto di chiedere e ricevere dagli utenti e dai titolari tutte le informazioni che servono per accertare la conformità al IV capo. Nel caso in cui emergerà che un utente dei dati sanitari o un titolare non abbia rispettato le prescrizioni del Capo IV, gli Organismi responsabili dell'accesso informeranno immediatamente l'utente o il titolare e adotteranno le misure necessarie. Il titolare e l'utente coinvolti avranno la possibilità di esprimere un proprio parere entro un termine ragionevole non superiore a quattro settimane: sul punto, v. Reg. (UE) 2025/327, cit., art. 63, par. 3.

[28] Reg. (UE) 2025/327, cit., art. 75.

[29] Per un approfondimento delle misure di attuazione, v. Reg. (UE) 2025/327, cit., art. 63, il cui paragrafo 7 sancisce che: «La Commissione definisce, mediante atti di esecuzione, l'architettura di uno strumento informatico, quale parte dell'infrastruttura di DatiSanitari@UE (*HealthData@EU*) di cui all'articolo 75, volto a sostenere le misure di esecuzione di cui al presente articolo, in particolare le penalità di mora, la revoca delle autorizzazioni ai dati e le esclusioni, e a renderle trasparenti ad altri organismi responsabili dell'accesso ai dati sanitari. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.»

[30] Sul ruolo dell'utente dei dati sanitari, v. M. NATALE, O. TROIANO, *L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari,* cit., par. X.

[31] Per facilitare l'uso transfrontaliero dei dati, mantenendo al contempo un elevato standard qualitativo delle informazioni, gli Organismi preposti, noti anche come *Health Data Access Body* (HDAB), potranno valutare l'utilizzo della soluzione *open source* fornita dalla Commissione Europea, utilizzando *eTranslation*, per rendere disponibile il Catalogo Nazionale dei *dataset* anche in inglese, così come i moduli di richiesta dati comuni, tradotti in una qualsiasi delle lingue ufficiali dell'Unione Europea. Sebbene il Catalogo Nazionale sia disponibile solo in una lingua ufficiale dell'UE, gli utenti coinvolti nel Progetto Pilota hanno raccomandato agli Organismi di valutare modalità per fornire informazioni anche in inglese, ad esempio, implementando strumenti di traduzione, per facilitare l'uso transfrontaliero dei dati (Rapporto sul caso d'uso - WP9). Tuttavia, è stato osservato che ogni eventuale attività di traduzione dovrà essere condotta con grande attenzione per mantenere un'elevata qualità e usabilità del catalogo dei metadati. Inoltre, sebbene il modulo di richiesta comune per l'accesso ai dati sia stato sviluppato in inglese, la possibilità di renderlo disponibile in una delle 24 lingue ufficiali dell'Unione Europea e di consentire ai richiedenti di compilarlo nella lingua prescelta garantirà una migliore funzionalità e fluidità dei processi di accesso ai dati (WP7). Ciò richiederà la necessità di sviluppare di soluzioni linguistiche adeguate e/o di garantire la fornitura di servizi di traduzione per gli Organismi che si occupano dell'elaborazione delle domande: v. *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, cit., 39 e ss.

attraverso misure mirate e l'adozione di apposite norme tecniche di regolamentazione, che indichino con chiarezza le modalità di adempimento degli obblighi previsti.

In questa prospettiva, tanto a livello europeo che nazionale, sarà fondamentale assicurare un'azione sinergica orientata all'armonizzazione applicativa della disciplina. Un supporto costante e un impegno coordinato, declinato anche attraverso l'individuazione di tecniche da adottare per assicurare un proficuo uso secondario dei dati[32], costituiscono elementi chiave per definite misure atte a garantire un ambiente di trattamento sicuro.

L'analisi fin qui condotta consente di affermare che il perseguimento degli obiettivi delineati dal regolamento è funzionalmente collegato al rafforzamento della governance istituzionale e alla predisposizione di strumenti operativi a supporto della sua attuazione. In tale contesto si collocano le numerose iniziative già avviate dagli Stati membri, nonché gli orientamenti attesi dalla Commissione, che dovranno essere emanati entro il 26 marzo 2032[33].

Nella fase di "preparazione", gli Stati membri hanno evidenziato la necessità di implementare una piattaforma comune, utile per la condivisione delle eccellenze operative, l'esposizione delle problematiche e per il rafforzamento della collaborazione finalizzata alla creazione e gestione dello sviluppo degli Organismi. Per soddisfare questa esigenza, hanno scelto di creare una Comunità di Pratica *Health Data Access Body* (HDAB)[34], nota come HDABs-CoP, composta dalle Autorità competenti e dagli enti affiliati agli Stati europei e ai paesi SEE[35], destinata a supportare l'evoluzione dell'assetto istituzionale all'interno dello Spazio europeo dei dati sanitari[36]. La volontà di amplificare i vantaggi attendibili, tramite un approccio sinergico, rappresenta il risultato raggiunto a seguito delle discussioni tenutesi durante la preparazione delle domande per le sovvenzioni necessarie per la creazione degli Organismi, durante le quali gli Stati europei hanno espresso la volontà di facilitare l'istituzione e il rafforzamento di queste figure, promuovendo approcci standardizzati.

In questo contesto, assume particolare rilievo il ruolo degli Stati membri e, in particolare, delle Autorità nazionali per la protezione dei dati, le quali contribuiscono all'attuazione di un'interpretazione coordinata, per semplificare le procedure di richiesta e ridurre al minimo eventuali ritardi e revisioni dei protocolli di studio delle domande pervenute[37]. Tale approccio include anche la progettazione e l'erogazione di programmi di formazione, la

[32] Reg. (UE) 2025/327, cit., art. 57

[33] Reg. (UE) 2025/327, cit., art. 63.

[34] Per un ulteriore approfondimento v. *Health Data Access Bodies – Community of Practice* in *European Commission*.

[35] Lo Spazio economico europeo (SEE) è stato istituito nel 1994 allo scopo di estendere le disposizioni applicate dall'Unione europea al proprio mercato interno ai paesi dell'Associazione europea di libero scambio (EFTA), per ulteriori approfondimenti sul punto, v. A. RAZAUSKAS, *Lo Spazio economico europeo (SEE), la Svizzera e il Nord, Note tematiche sull'Unione europea* in *Note tematiche sull'Unione europea*, 2025.

[36] In particolare la missione della Comunità di Pratica degli Organismi responsabili dell'accesso ai dati sanitari riguarda la condivisione di conoscenze fra le autorità coinvolte nella definizione effettiva degli Organismi responsabili dell'accesso ai dati, al fine di sostenere l'istituzione degli stessi, rafforzarne la cooperazione, creare una piattaforma per coordinare le informazioni e le strategie da attuare, condividere informazioni di natura tecnica e conoscenze, ottimizzare l'operato, promuovere l'armonizzazione e l'interoperabilità, al fine di creare solide strategie di diffusione dei risultati. Per ulteriori approfondimenti, v. *Health Data Access Bodies – Community of Practice, European Commission.*

[37] Appare interessante sottolineare che dal questionario HDAB in materia di conformità legale e normativa, inerente alla sfida prevista per l'implementazione degli organismi nazionali, è emerso che: il 5% degli intervistati non prevede alcuna sfida, il 5% prevede una sfida lieve, il 35% prevede una sfida moderata e il 55% prevede una sfida significativa: sul punto, v. WP7, Appendice 5 - Questionario HDAB e D9, *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, cit., 37 e ss.

fornitura di risorse e la facilitazione di discussioni guidate da esperti, con l'obiettivo di dotare le autorità competenti degli strumenti e delle conoscenze necessarie per operare con la giusta consapevolezza[38].

L'incontro inaugurale della Comunità di Pratica delle Autorità competenti dello Spazio europeo dei dati sanitari si è tenuto il 25 gennaio 2024, con l'obiettivo di avviare le attività della Comunità stessa, di adottare il *Working Arrangements Document*[39] ed eleggere relatori e presidenti degli organi direttivi. Durante questo primo incontro, gli Organismi per l'accesso ai dati sanitari della Danimarca, Norvegia, Finlandia e Francia hanno presentato i propri modelli, condividendo la propria esperienza con i Paesi che non hanno ancora istituito tali figure[40]. La seconda riunione dell'Assemblea generale della Comunità di Pratica delle Autorità competenti si è svolta il 25 giugno 2024. In tale occasione sono state fornite informazioni su progetti di particolare rilievo, tra cui *Second Joint Action Towards the European Health Data Space* (TEHDAS2)[41] considerato fondamentale per favorire l'allineamento degli sforzi nazionali agli obiettivi europei, assicurando allo stesso tempo coerenza e supporto tra le diverse iniziative[42].

Dunque, la fase embrionale in attuazione richiede un dialogo costante con la *governance* dell'EHDS; non a caso, il Comitato dello spazio europeo dei dati sanitari, è stato istituito per facilitare la cooperazione e lo scambio di informazioni tra gli Stati membri e la Commissione Europea, svolgendo un ruolo centrale nella comunicazione strategica. Il Comitato è composto da due rappresentanti per Stato membro, uno assegnato per l'uso primario dei dati e uno per l'uso secondario[43]. Il Comitato ha il compito di coadiuvare le

---

[38] *EHDS Community of Practice for Secondary Use*, *Working Arrangements, CoP drafting Task Force*, 22 gennaio 2024.

[39] «*The WAD, prepared by a task force, sets out the CoP's mission and objectives, organization, procedures, roles, and responsibilities. It also identifies relevant stakeholders and outlines a roadmap of meetings and workplan for 2024. The WAD proposes the creation of six subgroups including the aim, objectives, results expected from each subgroup as well as the interdependencies between them. • Subgroup 1 Data Access Application systems (DAAM) • Subgroup 2 Health Datasets Metadata Catalogue (HDsC) and Data Quality and Utility (DQU) • Subgroup 3 Secure Processing Environments (SPEs) • Subgroup 4 Cross-border Gateways • Subgroup 5 Deployment and Operations • Subgroup 6 Stakeholder's Fora The WAD also includes a proposal for a set of collaborative tools (toolbox) to support the CoP to accomplish its goals. The WAD was adopted by consensus, and the chairs and rapporteurs for the General Assembly and Steering Board were elected. It was noted that this is the first version of the WAD which reflects the current needs of the CoP. A revision is welcome in one year, as the WAD acts as a "living" document which reflects the requirements at the time of production»:* European Health Data Space, *Kick-off meeting Competent Authorities – Community of Practice in secondary use of health data Meeting Summary,* 25 gennaio 2024.

[40] European Health Data Space, *Kick-off meeting Competent Authorities – Community of Practice in secondary use of health data Meeting Summary,* cit.

[41] Tale programma mira allo sviluppo di Linee guida concrete e alla definizione di tecniche per facilitare l'utilizzo dei dati sanitari in diversi Paesi, nonché al sostegno per l'attuazione armonizzata della legislazione relativa allo Spazio Europeo dei Dati Sanitari: sul punto, v. I. A. KESSISSOGLOU , S. M. COSGROVE, L. A. ABBOUD , P. BOGAERT, M. PEOLSSON, N. CALLEJA, *Are EU member states ready for the European Health Data Space? Lessons learnt on the secondary use of health data from the TEHDAS Joint Action* in *European Journal of Public Health*, 2024, 1102 e ss.

[42] Già nel febbraio del 2021 è stato avviato un primo progetto congiunto europeo dedicato alla costruzione dello Spazio Europeo dei Dati Sanitari, terminato a luglio del 2023, con l'obiettivo di supportare gli Stati membri dell'Unione Europea e la Commissione europea nella fase di sviluppo di principi per l'uso secondario transfrontaliero dei dati sanitari. Per ulteriori approfondimenti, visitare il sito *web* ufficiale: *Joint Action Towards the European Health Data Space – TEHDAS1*.

[43] «L'articolo 92 istituisce un meccanismo di coordinamento centrale tra gli Stati membri e la Commissione europea. La creazione del Comitato EHDS garantisce che le decisioni in materia di gestione e utilizzo dei dati sanitari elettronici siano condivise e basate su un processo partecipativo. Il sistema a doppia rappresentazione per Stato membro (uso primario e uso secondario) è un'innovazione importante, poiché consente di considerare le esigenze sia dell'assistenza sanitaria diretta che della ricerca e innovazione»: M. IASELLI, *Le nuove*

decisioni sull'uso dei dati sanitari elettronici, anche invitando esperti, autorità e organizzazioni pertinenti esterne; può creare sottogruppi specifici per affrontare tematiche dettagliate, mirando ad una efficace e ottimizzata operatività. La sua azione è finalizzata al perseguimento di interessi di natura collettiva[44].

Il Comitato opera in stretta collaborazione con altri Organismi, come il Comitato europeo per la Protezione dei Dati (EDPB)[45] e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), garantendo coerenza delle conclusioni avanzate per l'utilizzo dei dati nel settore della ricerca e dell'innovazione e assicurando il raggiungimento di obiettivi coerenti con i più recenti sviluppi tecnologici[46]. Tale attività è volta a garantire una coerente applicazione del regolamento, attraverso l'elaborazione di *best practices*[47] e la facilitazione del dialogo con i portatori di interessi coinvolti, inclusi pazienti, professionisti sanitari, ricercatori e responsabili politici[48].

In sintesi, il Comitato dello spazio europeo dei dati sanitari supporta gli Stati membri nel coordinamento e nell'attuazione del regolamento, promuovendo la cooperazione e lo scambio di informazioni tra tutti gli attori coinvolti[49]. Tale strategia organizzativa mira all'adozione di un sistema coordinato, caratterizzato da un operato coerente degli Stati e della Commissione, per una gestione dei dati in armonia con i sistemi di sicurezza informatici e di protezione dei dati personali[50].

Dunque, il coordinamento tra gli attori istituzionali coinvolti rappresenta un aspetto cruciale nell'attuazione applicativa del regolamento di recente adozione. Una governance armonizzata deve, infatti, costituire un obiettivo da perseguire già nella fase embrionale, dedicata all'individuazione degli Organismi responsabili dell'accesso ai dati sanitari in ogni Stato membro.

II. Equilibrio istituzionale all'interno dello Spazio Europeo dei Dati Sanitari

Nella fase dedicata all'attuazione del Regolamento sullo Spazio europeo dei dati sanitari, assume particolare rilievo la questione relativa all'individuazione degli Organismi

regole per l'uso primario e secondario dei dati sanitari, Reg. UE 11 febbraio 2025, n. 327 (EHDS), 2025, 130 e ss.; Reg. (UE) 2025/327, cit., art. 92, par. 1 ; sul punto, v. anche Reg. (UE) 2025/327, cit., Considerando 95.

[44] Reg. (UE) 2025/327, cit., art. 92, par. 5 e 6.

[45] Il Comitato europeo per la protezione dei dati garantisce la coerente applicazione nel territorio europeo del Regolamento generale sulla protezione dei dati personali, Regolamento (UE) 2016/679. Per un ulteriore approfondimento sul programma di lavoro del Comitato, v. *EDPB Work Programme 2024–2025*, 8 ottobre 2024.

[46] Reg. (UE) 2025/327, cit., art. 92, par. 8.

[47] Per un approfondimento delle *best practices* di gestione dei dati sanitari in altri paesi, v. M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari,* cit. , p. 165 ss.

[48] Reg (UE) 2025/327, cit., art. 94, par. 2; inoltre, il Comitato per lo Spazio europeo dei dati sanitari svolge un ruolo specifico in relazione all'uso primario dei dati sanitari fornendo assistenza agli Stati, per assicurare a questi ultimi il coordinamento con le pratiche adottate dalle autorità di sanità digitale, redigendo contributi volti a promuovere lo scambio delle migliori pratiche relative all'uso primario dei dati, facilitando la cooperazione tra le autorità di sanità digitale, condividendo informazioni volte ad ottimizzare la gestione del rischio legato ad eventuali incidenti che potrebbero riguardare la violazione di dati contenuti nelle cartelle cliniche e semplificando la consultazione dei portatori di interessi coinvolti: sul punto, v. Reg. (UE) 2025/327, cit., par. 94, par. 1.

[49] Sul punto v. M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, cit., 131 e ss.

[50] M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, cit., 130 e ss.

responsabili dell'accesso ai dati sanitari a livello nazionale. Come precedentemente illustrato, il regolamento offre agli Stati membri un margine di discrezionalità relativa alla creazione o individuazione dell'Organismo, purché vengano rispettati i requisiti di indipendenza, disponibilità delle risorse e competenze[51]. Ciò induce a interrogarsi sulla figura cui potrebbe essere affidato questo ruolo nel contesto dell'ordinamento giuridico italiano. Una possibile risposta potrebbe indurre a pensare che la soluzione riguardi l'individuazione di un ente pubblico già esistente, quale il Ministero della Salute, l'Istituto Superiore di Sanità o l'Agenzia per la Salute Digitale. Questa ipotesi sembra trovare riscontro nel recente decreto che ha istituito l'Ecosistema dati sanitari, che attribuisce al Ministero della Salute la titolarità dei trattamenti[52], mentre affida la gestione operativa dei dati all'Agenzia Nazionale per i Servizi Sanitari Regionali[53], che agisce in qualità di responsabile del trattamento[54], su designazione dello stesso Ministero[55]. La similitudine del modello organizzativo delineato dal decreto induce a ritenere che, in Italia, il ruolo di Organismo responsabile dell'accesso ai dati sanitari sarà verosimilmente attribuito al Ministero della Salute e alle figure istituzionali che lo coadiuvano nell'espletamento delle funzioni attribuite[56].

Questa ipotesi si inserisce in un contesto normativo complesso[57], che solleva interrogativi significativi in merito all'equilibrio tra le competenze istituzionali: in particolare, emerge il

[51] Gli Stati membri devono esaminare le loro strutture di *governance* nazionale per valutarne la coerenza con le funzioni degli Organismi e assicurare la conformità con i requisiti di rendicontazione e *governance* dell'UE secondo il Regolamento sullo Spazio europeo dei dati sanitari. È importante definire linee guida per il *reporting* e strumenti per la presa decisionale all'interno delle strutture nazionali, garantendo l'allineamento con il nuovo regolamento sullo spazio europeo dei dati sanitari. È anche fondamentale individuare e risolvere le lacune e sovrapposizioni di responsabilità tra ministeri, Organismo responsabile dell'accesso ai dati sanitari e altri attori coinvolti nella *governance* dei dati sanitari, mentre si stabiliscono processi per una rapida, accurata e conforme rendicontazione all'Unione Europea, ponendo particolare attenzione alla conformità, alle autorizzazioni e al coinvolgimento delle parti interessate: *Deliverable D4.1 Recommendations for establishing Health Data Access Bodies*, cit., 14 e ss.

[52] Per titolare del trattamento si intende «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri»: Reg. (UE) 2016/679, cit., art. 4, n. 7.

[53] Per un approfondimento, v. AGENAS, *Guida alle fonti normative, regolamentari e pattizie*, 30 giugno 2023, 11 e ss.

[54] Per responsabile del trattamento si intende «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»: Reg. (UE) 2016/679, cit., art. 4, n. 8.

[55] Decreto 31 dicembre 2024, *Istituzione dell'Ecosistema dei dati sanitari* in G.U. Serie Generale n. 53, 5 marzo 2025, art. 12.

[56] Nell'ambito dell'Ecosistema dei dati sanitari, i soggetti pubblici e privati che istituzionalmente perseguono finalità di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico potranno presentare all'Agenas una richiesta di estrazione di dati anonimizzati, corredata da un relativo progetto di ricerca redatto conformemente alle regole metodologiche ed etiche. Agenas, in qualità di responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, provvederà alla valutazione delle richieste: Decreto 31 dicembre 2024, cit., art. 17. Per ulteriori approfondimenti sulle misure di sicurezza, v. *Allegato B,* Decreto 31 dicembre 2024, cit.

[57] Non a caso, «il regolamento istitutivo dell'EHDS, come anticipato, si pone espressamente ad integrazione e specificazione del GDPR. La disciplina dettata dal reg. UE 2016/ 679, in quanto «impregiudicata» dal regolamento sull'EHDS, continua a trovare applicazione senza modifiche e, solo relativamente al trattamento di dati sanitari elettronici, prende corpo un assetto normativo di dettaglio.»: S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327, Le Nuove Leggi Civ. Comm.*,2025, 578 e ss.

rischio di sovrapposizione di competenze tra gli Organismi preposti alla gestione dei dati sanitari e l'Autorità garante per la protezione dei dati personali[58].

Le entità embrionali coinvolte nella gestione dell'accesso ai dati sanitari dovranno evitare sovrapposizioni o inutili duplicazioni di competenze, considerando l'eventuale esistenza di provvedimenti già adottati da altre autorità competenti. È essenziale che l'operato di tali Organismi sia coordinato con quello delle altre figure di vigilanza, nel pieno rispetto delle procedure giuridiche e del quadro normativo nazionale[59]. Per chiarire tale aspetto, appare rilevante sottolineare che la normativa europea riconosce agli individui e ai soggetti collettivi la facoltà di presentare un reclamo qualora ritengano che i loro diritti o interessi siano stati lesi o compromessi in modo significativo[60]. Nel caso in cui il reclamo riguardi diritti delle persone fisiche, compatibilmente con quanto previsto dall'articolo 71[61] del regolamento di recente adozione, la gestione del reclamo sarà deferita all'Autorità di controllo competente, in conformità con il Regolamento generale sulla protezione dei dati. In tale contesto, l'Organismo responsabile dell'accesso ai dati sanitari coinvolto sarà tenuto a trasferire tempestivamente tutte le informazioni rilevanti in suo possesso all'Autorità di controllo, al fine di agevolare la valutazione del reclamo e facilitare la relativa indagine, collaborando per garantire un'efficace tutela dei diritti degli interessati[62].

Sorge spontaneo chiedersi se le funzioni degli Organismi responsabili dell'accesso ai dati sanitari si sovrapporranno ai poteri delle Autorità nazionali per la protezione dei dati, o se si configureranno come complementari, senza interferenze dirette. Gli Organismi incaricati dell'accesso ai dati sanitari saranno deputati alla gestione delle richieste di accesso ai dati

[58] L'applicazione del Regolamento (UE) 2016/679 è di competenze delle Autorità designate che si occupano di protezione dei dati personali. In Italia l'Autorità di riferimento è il Garante per la protezione dei dati personali il Garante per la protezione dei dati personali, istituita dalla cosiddetta legge 31 dicembre 1996, n. 675, poi disciplinata dal Codice in materia di protezione dei dati personali (D.lg. 30 giugno 2003 n. 196), successivamente modificato dal Decreto legislativo 10 agosto 2018, n. 101. Sul punto, v. Regolamento generale sulla protezione dei dati (UE) 2016/679, 27 aprile 2016, in G.U.U.E., 4 maggio 2016, art. 51: «1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»). 2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII. 3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63. 4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica».

[59] Sul punto rileva la previsione sancita dall'art. 63, paragrafo 2, del Regolamento di nuova adozione, il quale stabilisce che nella fase di monitoraggio e controllo, gli Organismi coinvolti effettueranno puntuali comunicazioni all'Autorità per la protezione dei dati, qualora l'accertamento della non conformità riguardi una possibile violazione del Regolamento (UE) 2016/679, fornendo tutte le informazioni utili: Reg. (UE) 2025/327, cit., art. 63, par.2.

[60] Reg. (UE) 2025/327, cit., art. 81, par. 1.

[61] L'articolo 71, rubricato *"Diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali per l'uso secondario"*, disciplina il diritto delle persone fisiche di escludere, senza necessaria motivazione, il trattamento dei propri dati sanitari elettronici per l'uso secondario: Reg. (UE) 2025/327, cit., art. 71.

[62] In seguito a un adeguata attività istruttoria, l'Organismo competente dovrà informare il soggetto interessato sullo stato del reclamo entro un termine ragionevole: Reg. (UE) 2025/327, cit., art. 81, par. 2; Al fine di rendere maggiormente agevole la proposizione di reclami, ciascun Organismo sarà chiamato ad adottare misure di supporto adeguate, anche attraverso la predisposizione di appositi moduli e procedure semplificate per la proposizione dei reclami: v, Reg. (UE) 2025/327, cit., art. 81, par. 3.

per l'uso secondario, all'autorizzazione dell'accesso, alla predisposizione dei dati necessari e al monitoraggio del loro utilizzo. Tuttavia, resterà prerogativa delle Autorità incaricate per la protezione dei dati[63] assicurare il rispetto del Regolamento generale sulla protezione dei dati[64], che continua a rappresentare la cornice giuridica di riferimento all'interno della quale le Autorità preposte non perderanno la loro competenza, restando le uniche responsabili della sua corretta applicazione[65].

Queste considerazioni aprono ulteriori riflessioni sul ruolo delle Autorità di sanità digitale nella governance relativa all'uso primario dei dati sanitari, responsabili dell'attuazione del Capo II del Regolamento sullo Spazio europeo dei dati sanitari[66]. In caso di violazione dei diritti legati all'uso primario, le persone fisiche potranno presentare un reclamo alle Autorità di sanità digitale[67]. Ma se il reclamo riguarderà l'accesso ai propri dati sanitari elettronici personali[68], l'inserimento di informazioni nella cartella clinica elettronica[69], la rettifica dei dati[70], il diritto alla portabilità[71], la limitazione dell'accesso[72], la tracciabilità[73]e il diritto di

63 Reg. (UE) 2025/327, cit., art. 65: Le autorità di controllo incaricate dovranno verificare che sia rispettato il diritto delle persone a opporsi all'uso dei propri dati sanitari elettronici per scopi diversi da quelli di cura diretta (cioè per usi secondari, come ricerca o analisi statistiche). Se questo diritto non viene rispettato, le autorità potranno imporre sanzioni amministrative.

64 Il Regolamento sulla protezione dei dati personali stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, con l'obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali: Reg. (UE) 2016/679, cit. art 1. Per un approfondimento contestualizzato al tema oggetto di analisi, v. F. MATTEI, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie* in *Le nuove frontiere della medicina, Assetti istituzionali e gestione dei dati*, (a cura di) G. C. FERONI, Bologna, 2024, 125 e ss.

65 Si rinvia alle definizioni contenute nel Regolamento (UE) 2016/679. In particolare, si richiama l'attenzione sulla definizione di «violazione dei dati personali» intesa come «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»: Reg. (UE) 2016/679, cit., art. 4, par. 12.

66 «Ciascuno Stato membro designa una o più autorità di sanità digitale responsabili dell'attuazione e dell'applicazione del presente capo a livello nazionale. Gli Stati membri informano la Commissione in merito all'identità delle autorità di sanità digitale entro il 26 marzo 2027. Qualora uno Stato membro designi più autorità di sanità digitale o l'autorità di sanità digitale sia composta da più organizzazioni, lo Stato membro interessato comunica alla Commissione una descrizione della distribuzione dei compiti tra le diverse autorità o organizzazioni. Qualora uno Stato membro designi più autorità di sanità digitale, ne designa una che funga da coordinatore. La Commissione mette tali informazioni a disposizione del pubblico»: Reg. (UE) 2025/327, cit., art. 19, par. 1.

67 Reg. (UE) 2025/327, cit., art, 21, par. 1. In tema, v. A. ADDANTE, *Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari*, in questo volume, par. VI.

68 Reg. (UE) 2025/327, cit., art. 3, par. 3; La disciplina del diritto di accesso è contenuta nell'art. 15 del Reg. (UE) 2016/679, rubricato "Diritto di accesso dell'interessato". Inoltre, per un approfondimento relativo alla privacy e all'accesso civico in relazione alle strutture sanitarie pubbliche, v. G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità, Teoria e pratica del diritto*, Milano, 2018 101 e ss.

69 Reg. (UE) 2025/327, cit., art. 5.

70 Reg. (UE) 2025/327, cit., art. 6., conformemente all'articolo 16 del Regolamento (UE) 2016/679 il quale sancisce che: «L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa».

71 Reg. (UE) 2025/327, cit., art. 7; La disciplina del diritto alla portabilità dei dati è contenuta nell'articolo 20 del Regolamento (UE) 2016/679.

72 Il Regolamento prevede che le persone fisiche siano informate dei rischi legati alla scelta di limitare l'accesso ai propri dati e rimanda agli Stati membri l'effettiva regolamentazione e previsione di garanzie relative all'esercizio di tale limitazione: Reg. (UE) 2025/327, cit., art. 8.

73 «Gli Stati membri possono prevedere limitazioni al diritto di cui al paragrafo 1 in circostanze eccezionali, qualora vi siano indicazioni concrete che la divulgazione metterebbe a rischio gli interessi vitali o i diritti del professionista sanitario o le cure assistenziali fornite alla persona fisica»: Reg. (UE) 2025/327, cit., art. 9.

esclusione riguardo all'uso primario[74], l'Autorità di sanità digitale trasmetterà il reclamo all'Autorità per la protezione dei dati personali, fornendole tutte le informazioni necessarie[75]. Inoltre, all'interno dello Spazio europeo dei dati sanitari, le Autorità per la protezione dei dati personali saranno chiamate a svolgere un ruolo centrale di monitoraggio e garanzia di applicazione degli stessi diritti per i quali sono tenute ad intervenire in caso di reclamo[76].

Alla luce di quanto esposto, appare evidente che le diverse autorità opereranno in ambiti distinti: le Autorità per la protezione dei dati personali conservano la competenza esclusiva sulle violazioni del Regolamento generale sulla protezione dei dati, mentre le nuove figure della *governance* dello Spazio europeo dei dati sanitari interverranno in caso di violazioni espressamente previste dallo stesso Regolamento 2025/327, relative all'uso primario o secondario dei dati, a seconda dei casi[77].

Ne consegue che i diversi ruoli, pur operando in settori contigui, risultino complementari e non sovrapponibili. Gli Organismi incaricati dell'accesso ai dati sanitari si occuperanno della gestione dell'aspetto operativo e del monitoraggio inerente all'uso secondario dei dati, le Autorità di sanità digitale interverranno nel perimetro dell'uso primario, mentre le Autorità per la protezione dei dati personali che «*cooperano, se del caso, nell'applicazione del presente regolamento nell'ambito delle rispettive competenze*»[78], continueranno a vigilare sulla legittimità e la protezione dei dati personali[79].

Appare evidente che il quadro delineato dal Regolamento sullo Spazio europeo dei dati sanitari evidenzia un sistema di *governance* strutturato in maniera armonica, ove ciascuna autorità eserciterà le proprie funzioni in modo coordinato e sinergico, senza alterare l'equilibrio tra le istituzioni coinvolte. O almeno questo emerge da un'analisi meramente teorica della normativa europea vigente.

III. La potenziale frammentazione del sistema sanzionatorio.

Come visto finora, la Commissione Europea ha perseguito l'obiettivo di creare degli spazi europei dei dati settoriali, intesi come ecosistemi digitali interconnessi e fondati su regole condivise. Tale ambizione mira a realizzare un mercato unico dei dati sanitari integrato ed uniforme, in cui diritti, obblighi e garanzie risultino immediatamente operativi e coerenti in tutti gli Stati membri[80].

---

74 Reg. (UE) 2025/327, cit., art. 10.

75 Reg. (UE) 2025/327, cit., art, 21, par. 2

76 «L'autorità o le autorità di controllo responsabili di monitorare e assicurare l'applicazione del regolamento (UE) 2016/679 sono altresì competenti di monitorare e assicurare l'applicazione dell'articolo 3 e degli articoli da 5 a 10 del presente regolamento. Le pertinenti disposizioni del regolamento (UE) 2016/679 si applicano *mutatis mutandis*. Le autorità di controllo hanno il potere di infliggere sanzioni amministrative pecuniarie fino all'importo di cui all'art. 83, paragrafo 5, del regolamento (UE) 2016/679»: Reg. (UE) 2025/327, cit., art. 22, par.1.

77 Reg. (UE) 2025/327, cit., Considerando 65.

78 Reg. (UE) 2025/327, cit., art. 22, par. 2.

79 Per un approfondimento relativo al ruolo Garante Privacy, relativo al trattamento di dati sulla salute, v. G. Amarù, A. Fava, M. Fossi, F. Mainardi, *La privacy del dato sanitario, Manuale per operatori e professionisti che trattano dati relativi alla salute e per chi vuole saperne di più*, Milano, 2024, 91 e ss.

80 Così già M. Natale, O. Troiano, *L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari*, cit., par. II.

In quest'ottica, risulta particolarmente interessante e, sotto alcuni profili, problematico esaminare il sistema sanzionatorio dell'EHDS, il quale, pur presentandosi formalmente come un regolamento, adotta un approccio che lascia ampio margine di discrezionalità agli Stati membri. In effetti, sebbene l'adozione di tale atto sotto forma di regolamento evidenzi la volontà del Legislatore europeo di stabilire delle norme coerenti ed uniformi a livello unionale, dall'analisi del testo emergono diverse possibilità per i singoli Stati di adottare soluzioni flessibili, più vicine all'impostazione tipica delle direttive[81]. In questo senso, dunque, il Regolamento (UE) 2025/327 si colloca formalmente nel primo alveo, ma per quanto concerne la parte relativa alle sanzioni sembrerebbe assumere i tratti propri di una direttiva.

A tal proposito, appare utile analizzare in maniera sistematica l'art. 64 EHDS, il quale disciplina le conseguenze giuridiche per le violazioni delle norme in esso contenute, insieme poi all'articolo 99, relativo alle sanzioni previste per le violazioni non soggette a sanzioni amministrative pecuniarie.

In prima battuta, va subito osservato il richiamo che l'articolo 64 fa ai principi generali del diritto amministrativo: il Regolamento EHDS prevede, infatti, l'adozione da parte degli Stati membri di sanzioni «effettive, proporzionate e dissuasive»[82] per le violazioni contenute nelle disposizioni di cui ai paragrafi 4 e 5 dello stesso articolo[83]. Tali principi, già precedentemente espressi dall'articolo 2 del Regolamento (CE,Euratom) n. 2988/95[84] ed ormai ampiamente riconosciuti dagli Stati membri[85], non appaiono in grado di creare in

[81] Per esigenze di completezza si richiama la disciplina dei regolamenti che, come enunciato dall'art. 288, comma 2 del T.F.U.E., costituiscono fonti di diritto derivato dell'Unione Europea obbligatori, immediatamente vincolanti e direttamente applicabili in tutti gli Stati membri senza alcuna necessità di intervento da parte del legislatore nazionale; essi si impongono ai destinatari in modo uniforme, al fine di garantire una armonizzazione piena e la certezza che le stesse regole giuridiche siano osservate su tutto il territorio europeo. Al contrario, la disciplina della direttiva all'art. 288, comma 3 del T.F.U.E «vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere», lasciando la facoltà di scegliere i mezzi e la forma per conseguire l'obiettivo prefissato, tipicamente attraverso una legge nazionale di recepimento.

[82] Sul punto anche il Considerando 106, il quale, nel prevedere che gli Stati membri adottino tutte le misure necessarie per garantire l'attuazione del Regolamento EHDS, richiama, in caso di violazioni, la necessità di stabilire sanzioni «effettive, proporzionate e dissuasive». Come noto, il principio di effettività determina la capacità della sanzione e degli strumenti processuali di imporsi concretamente sul destinatario della sanzione. Il contenuto dissuasivo esige che la pena sia sufficientemente severa, in modo da scoraggiare potenziali violazioni future, sia del trasgressore, sia di altri soggetti. Il principio di proporzionalità richiede, invece, un bilanciamento tra la gravità dell'infrazione e l'entità della sanzione irrogata, prevedendo quindi che l'ammontare della sanzione sia commisurato al disvalore insito nell'azione stessa; nel delineare un concetto preliminare alla formulazione del principio di proporzionalità, Romagnosi descrive la necessità di contemperare i diversi interessi in gioco con una sublime perifrasi di seguito riportata: «Se dunque egli è vero che si deve scegliere un minor male per evitarne un maggiore, ed i calcoli dell'utilità devono essere regolati dall'antiveggenza, di leggieri si vede, che il preteso sagrificio in ultima analisi non è arbitrario, ma necessario, talchè l'uomo non serve all'uomo, ma alla necessità della natura e al proprio meglio». Si veda G.D. ROMAGNOSI, *Principi fondamentali di diritto amministrativo onde tesserne le istituzioni*, Prato, 1835, 16 e ss; S. DE NITTO, *La proporzionalità nel diritto amministrativo*, 2023, Roma, 9 e ss.

[83] Reg. (UE) 2025/327, cit., art. 64, par. 1.

[84] Secondo quanto dettato dall'articolo 2 del Regolamento (CE, Euratom) n. 2988/1995 del Consiglio del 18 dicembre 1995 relativo alla tutela degli interessi finanziari delle Comunità, i controlli, così come le misure e le sanzioni amministrative, devono essere previsti soltanto quando ciò risulti necessario a garantire la corretta applicazione del diritto dell'Unione. In tale prospettiva, ciascuno di questi strumenti deve presentare carattere «effettivo, proporzionato e dissuasivo», così da assicurare un'adeguata tutela degli interessi finanziari dell'Unione.

[85] Un aspetto caratteristico, e che nel caso di specie serve a sottolineare il processo di uniformazione normativa, è la capacità da parte del diritto dell'Unione Europea di assorbire principi giuridici già elaborati negli ordinamenti nazionali, trasformandoli in principi generali dell'Unione. In questo processo, la Corte di

maniera sufficientemente autonoma un impianto sanzionatorio uniforme[86], ma lasciano un certo margine di discrezionalità agli Stati membri circa la definizione e la concreta applicazione delle sanzioni. Un simile discorso potrebbe essere utilmente esteso anche al principio del «giusto processo» richiamato al successivo paragrafo 7 e la cui attuazione concreta è rimessa, anche in questo caso, agli Stati membri[87]; l'espressa previsione di tale principio appare, quindi, superflua in quanto ormai consolidato sia nel diritto dell'Unione Europea che nei diversi ordinamenti nazionali[88].

Risulta a questo punto necessario proseguire con la disamina dell'articolo 64 del Regolamento EHDS, il quale, sul piano strettamente sanzionatorio, si struttura in due articolazioni distinte.

La prima, contenuta nel paragrafo 4[89], fa riferimento alle violazioni degli obblighi posti a carico del titolare dei dati sanitari[90] o dell'utente dei dati sanitari[91]. In entrambi i casi, il Regolamento prevede espressamente l'irrogazione di sanzioni amministrative pecuniarie fino a 10 milioni di euro, oppure, nel caso in cui il soggetto responsabile sia un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se tale importo risulti superiore.

giustizia dell'UE svolge un ruolo centrale, selezionando e adattando quei principi che, per la loro natura e rilevanza, possono fungere da criteri comuni di legittimità. Il caso più significativo è quello del principio di proporzionalità, che trae origine dalla giurisprudenza amministrativa prussiana, in particolare dalla sentenza *Kreuzberg* del 14 giugno 1882. Successivamente, tale principio ha ricevuto pieno riconoscimento nella *Grundgesetz*, la Legge fondamentale della Repubblica Federale di Germania del 1949. In questo contesto esso è stato concepito come un limite intrinseco all'azione dei pubblici poteri, volto a garantire la salvaguardia del nucleo essenziale dei diritti fondamentali, secondo la cosiddetta *Wesensgehaltgarantie* prevista dall'articolo 19, paragrafo 2. La Corte di giustizia ha mutuato tale principio prima con la sentenza *Fédération Charbonnière* del 1956 e successivamente con la sentenza Società Acciaierie San Michele del 1962, elevandolo a parametro di validità degli atti delle istituzioni europee e delle misure nazionali adottate in esecuzione del diritto dell'Unione. Una volta riconosciuto come principio generale dell'Unione Europea, il principio di proporzionalità non solo prevale sul diritto derivato, ma vincola anche gli Stati membri, i cui giudici sono tenuti ad applicarlo e ad utilizzarlo come criterio di interpretazione delle norme interne. Ciò ha determinato un fenomeno di progressiva "tracimazione" (*spill-over effect*), per cui principi di origine nazionale, dopo essere stati "europeizzati", ritornano negli ordinamenti interni con una forza normativa accresciuta e con un ambito applicativo esteso anche a fattispecie prive di diretta rilevanza europea. Sul punto si veda D.U. GALETTA, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Rivista italiana di diritto pubblico comunitario*, 2019, 903 e ss.

[86] S. ANTONIAZZI, *Le sanzioni amministrative*, in *I dati personali nel diritto europeo*, cit., (a cura di) V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 1094 e ss.

[87] Secondo quanto dettato al paragrafo 7, l'esercizio dei poteri da parte dell'Organismo responsabile dell'accesso ai dati sanitari deve avvenire nel rispetto di garanzie procedurali adeguate, conformi al diritto dell'Unione e nazionale, comprese la possibilità di ricorso effettivo e il diritto al «giusto processo».

[88] Il principio dell'equo processo è stato più volte rimarcato a livello nazionale ed internazionale, si vedano ad esempio le norme contenute agli articoli 111 della Costituzione, 47 della Carta dei diritti fondamentali dell'Unione Europea e 6 della Convenzione Europea dei Diritti dell'Uomo.

[89] Reg. (UE) 2025/327, cit., art. 64, par. 4.

[90] Ricordiamo che l'articolo 60 del Regolamento (UE) n. 327/2025 disciplina gli obblighi in capo ai titolari dei dati sanitari: questi ultimi, oltre a fornire su richiesta i dati elettronici pertinenti agli Organismi responsabili, devono mantenere aggiornata la descrizione delle serie di dati, verificandone la correttezza almeno annualmente, giustificare l'eventuale marchio di qualità attribuito ai dati e, per i dati non personali, garantirne l'accessibilità tramite banche dati pubbliche, aperte e affidabili, gestite con trasparenza e responsabilità.

[91] I paragrafi 1, 5 e 6 dell'articolo 61 del Regolamento (UE) 2025/327 stabiliscono che gli utenti dei dati sanitari possano accedere e trattare i dati elettronici solo se abbiano ottenuto una specifica autorizzazione o approvazione, secondo quanto previsto dal Regolamento. Inoltre, hanno l'obbligo di informare l'Organismo responsabile nel caso in cui, durante il trattamento, emergano informazioni rilevanti per la salute delle persone coinvolte. Infine, sono tenuti a collaborare attivamente con gli Organismi responsabili nello svolgimento delle loro funzioni.

La seconda articolazione, prevista nel paragrafo 5[92], riguarda invece l'individuazione delle violazioni più gravi. Tra queste, vengono espressamente menzionate alcune condotte che minano le fondamenta del sistema di protezione dei dati sanitari europei: il trattamento di dati sanitari elettronici da parte di utenti che, seppur autorizzati[93], perseguono finalità espressamente vietate dall'articolo 54 – come ad esempio il marketing o l'utilizzo per fini assicurativi[94]; l'estrazione, da parte degli utenti, di dati sanitari elettronici personali da ambienti di trattamento sicuri[95]; la reidentificazione di dati pseudonimizzati, ovvero il tentativo di risalire all'identità degli interessati ex articolo 61, di cui al paragrafo 3[96]; ed infine la mancata conformità, da parte di utenti[97] e titolari[98], alle misure di esecuzione adottate dagli Organismi responsabili dell'accesso. Per la violazione di tale norma, l'articolo 64 prevede l'introduzione di massimali più elevati rispetto a quelli del paragrafo precedente. In particolare, gli Stati membri sono tenuti a prevedere sanzioni amministrative fino a 20 milioni di euro, oppure fino al 4% del fatturato mondiale annuo dell'impresa responsabile della violazione nell'esercizio precedente, con applicazione del maggiore tra i due importi.
Si tratta di due previsioni la cui finalità non è solo quella di garantire un effetto dissuasivo nei confronti delle grandi imprese, ma che mira a rafforzare la coerenza con il quadro regolamentare preesistente in materia di protezione dei dati personali, di cui il Regolamento EHDS rappresenta in parte una prosecuzione settoriale. Al tempo stesso, queste concorrono a rafforzare la responsabilizzazione degli operatori, i quali sono indotti a conformarsi alle disposizioni del Regolamento, anche alla luce della rilevanza economica delle sanzioni previste in caso di violazione[99].

[92] Reg. (UE) 2025/327, cit., art. 64, par. 5.
[93] Il procedimento attraverso il quale gli Organismi responsabili dell'accesso ai dati sanitari rilasciano l'autorizzazione ai dati per finalità di utilizzo secondario è disciplinato in modo dettagliato dall'articolo 68 del Regolamento (UE) n. 327/2025.
[94] Il secondo comma dell'articolo 54 chiarisce che i dati sanitari elettronici, una volta ottenuti tramite autorizzazione o richiesta formale, non possono essere utilizzati per fini che ledano i diritti delle persone. In particolare, oltre alle finalità di *marketing* già richiamate, è vietato impiegarli per assumere decisioni che abbiano effetti negativi giuridici, sociali o economici sui singoli o su gruppi, come accade in caso di discriminazioni sul lavoro, nell'accesso a beni e servizi, nelle condizioni di assicurazioni, prestiti o crediti. Parimenti, è escluso l'uso di tali dati per lo sviluppo di prodotti o servizi potenzialmente dannosi per le persone, la salute pubblica o la società, ad esempio droghe, alcol, tabacco, armi o beni che creino dipendenza o mettano a rischio l'ordine pubblico. Infine, non è consentito impiegarli per attività che risultino contrarie alle disposizioni etiche previste dal diritto nazionale.
[95] L'articolo 68 del Regolamento (UE) 2025/327 stabilisce che l'accesso ai dati sanitari elettronici da parte degli utenti sia consentito solo all'interno di ambienti di trattamento sicuri, sottoposti a rigorose misure tecniche e organizzative per garantire la sicurezza, la riservatezza e la tracciabilità. Nello specifico, gli ambienti sicuri devono: consentire l'accesso solo a persone autorizzate con credenziali individuali; prevenire copie, modifiche o estrazioni non autorizzate; registrare tutte le attività svolte al loro interno; permettere solo il *download* di dati anonimi o non personali; essere sottoposti ad *audit* periodici anche da terze parti; rispettare gli stessi *standard* anche se utilizzati da organizzazioni per l'altruismo dei dati.
[96] Reg. (UE) 2025/327, cit., art. 61, par. 3.
[97] Reg. (UE) 2025/327, cit., art. 63, par. 3.
[98] Reg. (UE) 2025/327, cit., art. 63, par. 4.
[99] In questo senso, il carattere deterrente della sanzione va letto insieme al principio di *accountability*. Tale principio, introdotto dall'articolo 5 comma 2 del GDPR, ha completamente sovvertito la visione sistemica dei dati personali: si tratta di un passaggio paradigmatico da un modello incentrato sul controllo formale *ex post* da parte delle autorità, a un sistema in cui la compliance deve essere integrata proattivamente nei processi decisionali e organizzativi dell'ente. Tuttavia, nell'EHDS il principio di *accountability* non è espresso, ma è facilmente desumibile dalla lettura di alcuni articoli relativi, ad esempio, agli obblighi di informazione e cooperazione degli utenti dei dati (articolo 67, paragrafi 5 e 6), alle richieste e autorizzazioni per l'accesso ai dati sanitari (articoli 68 e 69), ai poteri ispettivi e correttivi degli Organismi responsabili dell'accesso (articolo 63), nonché alla previsione di sanzioni particolarmente severe (articolo 64, paragrafi 4 e 5).

Al di là, dunque, dei principi generali e dei *plafond* menzionati, il testo del Regolamento non offre ulteriori indicazioni di natura vincolante, né al suo interno vengono definite modalità operative comuni o sanzioni direttamente applicabili. Appare limitata anche l'efficacia della lunghissima elencazione fatta nel paragrafo 2 del menzionato articolo, secondo il quale l'ammontare della pena deve essere fissato in base a criteri quali, ad esempio, la natura, la gravità e la durata della violazione – solo per citarne alcuni[100]. Occorre poi non sottovalutare un passaggio di particolare rilevanza che ritroviamo nella prima parte del suddetto paragrafo 2 e che appare alquanto vago nella sua formulazione; in esso si afferma, infatti, che le sanzioni saranno inflitte «in aggiunta […] o in luogo»[101] delle misure di esecuzione di cui all'articolo 63, paragrafi 3 e 4: ciò indica che spetterà a ciascun Organismo responsabile dell'accesso ai dati sanitari determinare la cumulabilità delle sanzioni, senza che venga espresso alcun criterio o indirizzo interpretativo uniforme circa l'orientamento da adottare, con la possibile, e forse addirittura probabile, divergenza valutativa e applicativa da Stato a Stato.

Da ultimo, vediamo come anche il paragrafo 6 dell'articolo 64 rimetta alla piena discrezionalità degli Stati membri la definizione del se ed in quale misura infliggere sanzioni amministrative pecuniarie alle autorità ed agli organismi pubblici[102], in linea con quanto già previsto dal Regolamento Generale sulla Protezione dei Dati[103].

In aggiunta a quanto appena esposto per l'articolo 64, un ulteriore margine di manovra viene riconosciuto dall'articolo 99 comma 1 del Regolamento EHDS il quale, invece di fungere da norma residuale a chiusura del quadro sanzionatorio, attribuisce a ciascuno Stato membro il potere di stabilire ulteriori sanzioni per le violazioni non soggette a sanzioni amministrative pecuniarie di cui agli articoli 63 e 64 del Regolamento[104]. Potrebbe apparire

[100] Reg. (UE) 2025/327, cit., art. 64, par. 2 : «[…] Gli Organismi responsabili dell'accesso ai dati sanitari decidono se infliggere una sanzione amministrativa pecuniaria e ne fissano l'ammontare in ogni singolo caso tenendo debito conto degli elementi seguenti: a) la natura, la gravità e la durata della violazione; b) se le sanzioni o le sanzioni amministrative pecuniarie siano state già irrogate da altre autorità competenti per la stessa violazione; c) il carattere doloso o colposo della violazione; d) le misure adottate dal titolare dei dati sanitari o dall'utente dei dati sanitari per attenuare il danno causato; e) il grado di responsabilità dell'utente dei dati sanitari, tenendo conto delle misure tecniche e organizzative da esso messe in atto ai sensi dell'articolo 67, paragrafo 2, lettera g), e dell'articolo 67, paragrafo 4; f) eventuali precedenti violazioni pertinenti commesse dal titolare dei dati sanitari o dall'utente dei dati sanitari; g) il grado di cooperazione del titolare dei dati sanitari o dell'utente dei dati sanitari con l'Organismo responsabile dell'accesso ai dati sanitari al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; h) la maniera in cui l'Organismo responsabile dell'accesso ai dati sanitari ha preso conoscenza della violazione, in particolare se e in che misura l'utente dei dati sanitari gli ha notificato la violazione; i) il rispetto delle misure di esecuzione di cui all'articolo 63, paragrafi 3 e 4, che siano stati precedentemente disposte nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto; j) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, tramite la violazione». Sul punto, v. M. CUCCOVILLO, *Uso secondario dei dati sanitari e tutela dell'interessato: tra rimedi e sanzioni*, cit., par. V.

[101] Si veda in proposito anche il Considerando 102.

[102] Reg. (UE) 2025/327, cit., art. 64, par. 6.

[103] Reg. (UE) 2016/679, cit., art. 83, par. 7.

[104] Reg. (UE) 2025/327, cit. art. 99 comma 1. Ricordiamo a tal proposito che in Italia, continuano ad operare gli articoli 167 (Trattamento illecito di dati), 167 *bis* (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala) e 167 *ter* (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala) del D.lgs. 30 giugno 2003, n. 196, il cd. Codice Privacy; per quanto riguarda l'ambito dei dati sanitari, potrebbe essere significativo richiamare il dettato del comma 2 dell'articolo 167 nel quale vengono sanzionate con la reclusione da uno a tre anni, salvo che il fatto costituisca reato più grave, le violazioni di cui agli articoli 2 *sexies* (Trattamento di categorie particolari di dati personali necessario per motivi

ridondante il riferimento ad alcuni dei criteri già menzionati dal paragrafo 2 dell'articolo 64 e che ritroviamo nuovamente nel secondo comma dell'articolo 99, in questo caso in relazione alle sanzioni nazionali[105]; tuttavia, il *discrimen* tra le due norme sembrerebbe essere l'espresso riferimento che l'articolo 64 fa riguardo al comportamento del trasgressore, alla sua cooperazione ed alle misure preventive adottate, riferimento non presente nell'articolo 99 il quale invece aggiunge, tra gli elementi da valutare per l'irrogazione delle sanzioni, la capacità economica del trasgressore.

Dall'analisi delle predette norme emerge, pertanto, un potenziale rischio di frammentazione applicativa: un atto concepito per garantire la piena armonizzazione potrebbe finire, invece, per produrre effetti disomogenei, in quanto, la regolazione della matrice sanzionatoria viene chiaramente lasciata alle scelte dei singoli ordinamenti nazionali[106]. La conseguenza potrebbe, quindi, essere un ampliamento significativo del grado di discrezionalità lasciato agli Stati membri, sia sotto il profilo normativo che procedurale. Tali criticità, che saranno opportunamente chiarite, evidenziano la necessità di una riflessione ulteriore sull'assetto sanzionatorio europeo e sulle sue possibili soluzioni.

IV. DIVERGENZE APPLICATIVE NELL'ORDINAMENTO DEI SINGOLI STATI MEMBRI: IL PECULIARE CASO DELLA DANIMARCA

Come poc'anzi sottolineato, sebbene l'articolo 64 del Regolamento sullo Spazio Europeo dei Dati Sanitari rappresenti un significativo tentativo da parte Legislatore europeo di delineare un quadro comune per l'applicazione delle sanzioni in materia di trattamento e accesso ai dati sanitari, la sua effettività si scontra, nella prassi, con l'elevata eterogeneità degli ordinamenti giuridici nazionali. Tale eterogeneità non riguarda solo le differenze terminologiche, ma riflette divergenze più profonde insite nei modelli culturali e istituzionali attraverso cui ogni Stato membro attua la funzione sanzionatoria, con conseguenze rilevanti sulla coerenza nell'applicazione delle norme europee.

A tal riguardo, il Regolamento EHDS propone una soluzione: stabilisce, infatti, al paragrafo 8 dell'articolo 64, che nel caso in cui uno Stato membro non preveda sanzioni amministrative pecuniarie, questo debba comunque garantire, secondo il proprio ordinamento, mezzi di ricorso effettivi ed equivalenti a tali sanzioni[107].

Pertanto, analizzare i diversi approcci nazionali all'applicazione delle sanzioni, specialmente in ambito amministrativo e penale, non costituisce un mero esercizio comparatistico, ma

di interesse pubblico rilevante) o le misure di garanzia di cui all'articolo 2 *septies* (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute). Sul punto si veda C. CUPELLI, F. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice Privacy dal d.lgs. n. 101/2018*, in *I dati personali nel diritto europeo*, cit., (a cura di) V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 1100 e ss; G. CARRO, S. MASATO, M. D. PARLA, *La privacy nella sanità*, cit. Milano, 2018, 113 e ss.

[105] Reg. (UE) 2025/327, cit., art. 99 comma 2.

[106] Il rischio di frammentarietà derivante dall'autonomia dei singoli Stati membri presenta ulteriori criticità che vengono messe in evidenza da A. ADDANTE, *Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari*, cit., parr. 4.1 6; R. AMBROSINO, *Governance profiles of secondary use of health data in the EHDS, cit., 133 - 137*; V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo dei Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, in questo volume, par. II.1.

[107] Reg. (UE) 2025/327, cit., art. 64, par. 8. Anche in questo caso il Regolamento sottolinea l'importanza di sanzioni effettive, proporzionate e dissuasive. Viene poi previsto che Stati membri debbano notificare alla Commissione le relative norme entro il 26 marzo 2029, nonché ogni successiva modifica.

risponde ad una esigenza metodologica fondamentale per comprendere i limiti concreti del processo di armonizzazione giuridica. Infatti, viste anche le molteplici similitudini riscontrate con il GDPR, l'esperienza acquisita evidenzia come i risultati normativi possano divergere sensibilmente a seconda del contesto giuridico interno.

Paradigmatico è, in tal senso, il caso della Danimarca[108].

Il sistema giuridico danese si distingue per una caratteristica di fondo che lo differenzia radicalmente dalla maggior parte degli ordinamenti europei: le autorità amministrative indipendenti danesi – tra cui la *Datatilsynet*[109], competente in materia di protezione dei dati personali – non dispongono del potere di irrogare direttamente sanzioni pecuniarie, così come evidenziato anche dal Considerando 23 EHDS[110]. La competenza in materia sanzionatoria è esclusiva delle corti penali, anche in presenza di illeciti che, in altri ordinamenti, sarebbero qualificati come amministrativi. Tale assetto, che affonda le sue radici in una lunga tradizione di tutela della propria giurisdizione[111], si applica anche a settori

[108] Il Considerando 66 *duodecies*, contenuto nella proposta emendata del 2 agosto 2024 (Emendamenti del Parlamento europeo, approvati il 13 dicembre 2023, alla proposta di regolamento sullo Spazio europeo dei dati sanitari), inizialmente menzionava espressamente non solo la Danimarca ma anche l'Estonia, riconoscendo formalmente la mancata previsione, da parte dei due ordinamenti, di sanzioni amministrative pecuniarie, come previsto dal Regolamento. In particolare, per quanto attiene l'Estonia, si stabiliva che tali sanzioni potessero essere applicate dall'autorità di controllo nell'ambito di una procedura d'infrazione, purché con effetto equivalente. In tal senso, l'ordinamento estone è emblematico: intatti, in tema di dati personali, pur prevedendo formalmente strumenti sanzionatori e di applicazione del GDPR – il PDPA (*Personal Data Protection Act)* e l'*Implementation Act* del 2019 – l'approccio prevalente è improntato ad un garantismo procedurale rigoroso e ad una marcata cultura della proporzionalità, con la necessaria imposizione di sanzioni notevolmente inferiori alle soglie previste dall'articolo 83 del GDPR. Anche in caso di violazioni rilevanti, le autorità hanno infatti adottato misure correttive e rieducative, anziché punitive in senso afflittivo. Fino al 2024, la sanzione più elevata nel contesto nazionale, ma comunque contenuta rispetto alle sanzioni comminate in altri ordinamenti europei, era quella del 13 febbraio 2023: il *Data Protection Inspectorate* estone aveva imposto nel caso di specie una sanzione di 200.000 euro all'*East Tallinn Central Hospital* per la divulgazione illecita di dati sanitari (sanzione successivamente annullata per decorso dei termini). Tale impostazione deriva da una tradizione giuridica rispettosa dei diritti individuali e fortemente orientata all'innovazione tecnologica, in linea con la vocazione digitale del Paese. L'Estonia, dall'approvazione del GDPR e con gli emendamenti al Codice penale del novembre 2023, ha iniziato un percorso di riforma il cui intento è quello di consentire sanzioni più severe ai sensi delle norme europee, al fine di favorire una maggiore armonizzazione con il quadro normativo dell'Unione. Pertanto, forse proprio alla luce di questo processo di riforma, il riferimento all'Estonia è stato rimosso dal nuovo Considerando 23 – che sostituisce l'antecedente Considerando 66 *duodecies* – del Regolamento (UE) 2025/327. Per una analisi delle sanzioni, si veda l'*Annual Report* 2023 sul sito dell'Autorità estone https://www.aki.ee/en/inspectorate-news-information-dpo-s/annual-reports.

[109] La *Datatilsynet* opera sotto la supervisione del Ministero della Giustizia e ha il compito di garantire l'applicazione del GDPR e della normativa nazionale. Tra le sue funzioni rientrano l'esame dei reclami, lo svolgimento di *audit* e indagini, l'emissione di provvedimenti e raccomandazioni, la sensibilizzazione degli enti pubblici e dei soggetti privati, la consulenza in materia di misure tecniche e organizzative, nonché la cooperazione con le altre autorità europee attraverso il Comitato europeo per la protezione dei dati.

[110] Reg. (UE) 2025/327, cit., Considerando 23.

[111] La Danimarca ha da sempre manifestato una forte propensione a mantenere la propria autonomia in ambito sanzionatorio rispetto al quadro giuridico dell'Unione Europea. Tale posizione trova fondamento nell'*opt-out* negoziato con l'Accordo di Edimburgo del dicembre 1992; interessante sul punto è la precedente Risoluzione del Parlamento Europeo sul Consiglio europeo straordinario di Birmingham del 16 ottobre 1992 in cui si «auspica, respingendo l'idea di un'Europa a due velocità, che dal Consiglio europeo di Edimburgo possa emergere un accordo atto a risolvere il problema della ratifica del Trattato da parte della Danimarca». L'Accordo di Edimburgo ha, infatti, consentito al Paese di recepire automaticamente strumenti relativi, ad esempio, alla definizione comune di reati e sanzioni previsti dagli articoli 82 e 83 del TFUE. Questa clausola permette alla Danimarca di escludersi dalle direttive europee che stabiliscono sanzioni minime o armonizzano le risposte penali a fenomeni come il terrorismo, il traffico di esseri umani o i crimini informatici. La Danimarca può decidere dunque, volontariamente e caso per caso, di recepire alcune norme secondo i criteri nazionali, mantenendo così un controllo diretto sulla propria politica sanzionatoria. La scelta danese non è

regolati da fonti europee come il Regolamento Generale sulla Protezione dei Dati e, ora, l'EHDS.

Di conseguenza, ogni violazione delle disposizioni dell'EHDS che dia luogo ad una sanzione pecuniaria deve essere sottoposta a procedimento penale, con tutte le implicazioni che ciò comporta. Occorre infatti rispettare, innanzitutto, le garanzie proprie del processo penale, tra cui l'onere della prova, il principio del contraddittorio o il diritto alla difesa[112]. I procedimenti penali poi, come accade tendenzialmente in ogni ordinamento, comportano tempi significativamente più lunghi rispetto a quelli amministrativi, anche per violazioni di modesta entità. Infine, la necessità di coinvolgere personale giudiziario, funzionari e avvocati comporta spesso un aggravio dei costi per l'amministrazione della giustizia, con ricadute economiche rilevanti sia per lo Stato che per i soggetti sanzionati.

Dal punto di vista del trasgressore, i costi non sono meno significativi: oltre alle spese legali e processuali, occorre considerare i tempi di incertezza e le ripercussioni reputazionali. L'impatto di tali fattori risulta particolarmente gravoso soprattutto per le piccole e medie imprese che, come noto, dispongono di minori risorse economiche e organizzative per affrontare contenziosi giudiziari complessi e prolungati.

In sintesi, il modello danese genera una sorta di paradosso normativo: se da un lato esso riesce a garantire un elevato standard di tutela dei diritti procedurali, dall'altro riduce fortemente l'efficacia del sistema sanzionatorio, soprattutto in relazione a violazioni che, in altri ordinamenti, sarebbero sanzionate in modo più rapido attraverso un procedimento amministrativo. Questa asimmetria si ripropone oggi in relazione al Regolamento EHDS, ma era già stata segnalata in merito al GDPR e poi parzialmente risolta con l'implementazione della normativa nazionale in materia di protezione dei dati[113]. Tuttavia,

---

solo tecnica, ma riflette una chiara opzione politica: quella di preservare la sovranità nazionale nella definizione e applicazione delle sanzioni penali, anche a costo di limitare l'integrazione giuridica con il resto dell'Unione, Vedi sul punto C. THORNING, *The Danish EU Opt-Outs, Their Legal Significance, Past and Present*, Oxford, 2024, 1 – 183.

112 Nel sistema penale danese, i principi del contraddittorio, del giusto processo e del diritto alla difesa, pur non essendo enunciati in forma solenne come in altri ordinamenti, sono pienamente garantiti e desumibili dal combinato disposto di una serie di norme contenute nella LBK n. 1101 del 22/09/2017, nota come *Retsplejeloven*. Si tratta del Codice di procedura danese, che disciplina il funzionamento del sistema giudiziario, sia in ambito civile che penale. È una legge organica che stabilisce le modalità di svolgimento dei processi, i diritti delle parti, le regole sull'assunzione delle prove, la nomina dei giudici e le principali garanzie procedurali. Il diritto alla difesa è tutelato tramite la possibilità per l'imputato di nominare un avvocato di fiducia oppure, nei casi previsti, di ricevere assistenza da un difensore d'ufficio (§§ 729a, 731–733). Il difensore ha diritto di accedere agli atti, partecipare agli interrogatori, mantenere il contatto con il proprio assistito e intervenire attivamente in tutte le fasi del procedimento. Il principio del contraddittorio si concretizza nella facoltà concessa alle parti di conoscere e contestare le prove, esaminare i testimoni e partecipare pienamente al processo (§§ 842–849). Le udienze devono essere comunicate con congruo preavviso e possono essere precedute da fasi preparatorie finalizzate all'organizzazione del dibattimento. Il giusto processo è garantito da norme che assicurano la ragionevole durata del procedimento, l'equilibrio tra accusa e difesa e l'accesso equo al materiale probatorio. Eventuali limitazioni a tali diritti sono ammesse solo per motivi gravi e giustificati, come la tutela della sicurezza nazionale o di terze parti (§ 729c).

113 Al fine di dare attuazione al Regolamento generale sulla protezione dei dati, il Parlamento danese ha approvato, il 17 maggio 2018, la Legge danese sulla protezione dei dati personali, la *Databeskyttelsesloven*, entrata in vigore il 25 maggio dello stesso anno, in concomitanza con l'applicazione del GDPR in tutta l'Unione Europea. Questa nuova normativa ha sostituito la precedente *Lov om behandling af personoplysninger* (la Legge n. 429 del 31 maggio 2000 sul trattamento dei dati personali in applicazione della Direttiva 95/46/CE), aggiornando il quadro giuridico nazionale per renderlo conforme alle disposizioni europee in materia di tutela della *privacy* e dei dati personali. Da notare che la legge non si applica ai territori autonomi della Groenlandia e delle Isole Færøer i quali, nonostante siano sotto il controllo danese dal 1397, non fanno parte dell'Unione Europea e dispongono di proprie normative in materia. La *Databeskyttelsesloven* prevede sanzioni di natura

in mancanza di una modifica strutturale della legislazione danese, sarà difficile ipotizzare una applicazione effettivamente armonizzata delle sanzioni sui dati, ed in particolare sui dati sanitari.

V. CRITICITÀ E POSSIBILI RIMEDI OPERATIVI

Alla luce di quanto sinora esposto, si può notare come l'intero apparato sanzionatorio dell'EHDS rappresenti il tentativo del Legislatore europeo di mediare tra due esigenze istituzionali e politiche profondamente diverse e, sotto alcuni profili, strutturalmente contrapposte: da un lato, l'obiettivo di garantire un livello minimo di uniformità sanzionatoria nell'intera Unione Europea; dall'altro, il rispetto dell'autonomia normativa e procedurale degli Stati membri, soprattutto in una materia così sensibile e tradizionalmente radicata nei diritti nazionali come quella delle sanzioni.

L'articolo 64, in particolare, tenta di delineare un quadro armonizzato nei principi generali, ma con ampi margini di flessibilità tali da non urtare contro la pluralità di modelli giuridici e culturali esistenti. Tale scelta discende non solo da valutazioni politiche legate al rispetto delle tradizioni giuridiche nazionali, ma anche dai vincoli sistemici che limitano la possibilità per il Legislatore europeo di intervenire in via diretta nella disciplina sanzionatoria[114]. Si tratta, dunque, di un equilibrio delicato, volto ad evitare sia una frammentazione totale, che avrebbe compromesso la funzione deterrente delle sanzioni e l'effettività del Regolamento, sia una uniformità rigida, potenzialmente in contrasto con il principio di sussidiarietà[115].

Resta però lecito domandarsi se tale compromesso sia davvero idoneo a garantire una uniformità applicativa. A parità di violazione, infatti, soggetti che operano in contesti giuridici diversi potrebbero essere sottoposti a regimi sanzionatori differenti, con effetti divergenti in termini di severità, tempi e procedure[116]. Ciò rischia di compromettere l'equità

penale che comportano fino a 6 mesi di reclusione o ammende, come stabilito all'articolo 41 sia dal comma 1 – per violazioni gravi quali il trattamento illecito di dati personali (punto 4), per la violazione dei diritti degli interessati (punto 5), per il mancato rispetto degli obblighi del titolare o del responsabile del trattamento (punto 1), per i trasferimenti illeciti verso paesi terzi (punto 6) – che dal comma 2 – per l'ostruzione delle attività dell'autorità di controllo (punti da 3 a 8). Le infrazioni di minore entità, come l'omessa collaborazione con l'autorità o il mancato rispetto di requisiti formali di cui all'articolo 42, possono essere sanzionate tramite contravvenzioni, le cd. *fixed penalty notices*, con la possibilità di evitare il procedimento giudiziario se si accetta di pagare la sanzione. Al seguente link la versione inglese della Legge: https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf.

[114] In materia penale, ad esempio, si veda l'articolo 83, comma 2 del Trattato sul Funzionamento dell'Unione Europea, secondo il quale l'Unione può intervenire per stabilire norme minime relative alla definizione dei reati e delle sanzioni, attraverso lo strumento della direttiva, quando ciò si riveli indispensabile per garantire l'attuazione efficace di una politica armonizzata. Un ragionamento analogo può estendersi anche alle sanzioni amministrative, le quali, pur non trovando una disciplina unitaria e compiuta, rappresentano lo strumento più frequentemente utilizzato dal Legislatore europeo per assicurare l'effettività delle proprie politiche settoriali, sebbene con caratteristiche meno tipizzate e connotate da maggiore elasticità rispetto al diritto penale.

[115] Ricordiamo come il principio di sussidiarietà sia stato inserito nell'articolo 5, paragrafo 3 del Trattato di Lisbona. In virtù di tale principio, nei settori di competenza non esclusiva, l'Unione europea interviene solo quando gli obiettivi non possono essere adeguatamente raggiunti dagli Stati membri, ma possono essere conseguiti meglio a livello dell'UE.

[116] Da una analisi delle prime applicazioni del GDPR si evince come le autorità garanti abbiano adottato approcci profondamente differenti all'irrogazione delle sanzioni, nonostante una cornice normativa comune. La Spagna, ad esempio, aveva emesso 73 sanzioni in 24 mesi, prevalentemente per violazioni del consenso e dell'informativa, con importi medi inferiori a 32.000 euro. Al contrario, il Regno Unito aveva emesso solo tre sanzioni, tutte per gravi carenze nella sicurezza dei dati, ma per importi milionari, tra cui quelle *contro British*

e la prevedibilità del sistema, oltre a incidere sulla concorrenza nel mercato unico. Non si può escludere, inoltre, che imprese particolarmente strutturate siano incentivate a delocalizzare le proprie attività [117] in Stati percepiti come *health data-friendly* [118], ossia caratterizzati da un approccio meno severo sul piano sanzionatorio. Tale fenomeno, oltre a svuotare la funzione deterrente del sistema e ad agevolare comportamenti opportunistici, rischierebbe di compromettere la parità di trattamento tra operatori economici e di falsare la concorrenza nel mercato unico europeo, generando effetti distorsivi difficilmente compatibili con la *ratio* stessa del Regolamento.

Il confronto con il modello del GDPR aiuta a comprendere meglio tali criticità. Infatti, anche il Regolamento Generale sulla Protezione dei Dati ha affidato agli Stati membri la concreta gestione delle sanzioni, ma ha introdotto strumenti di coordinamento che hanno gradualmente favorito una maggiore armonizzazione. La governance multilivello introdotta dal GDPR, e in particolare il ruolo attivo del Comitato Europeo per la Protezione dei Dati, ha consentito la promozione di una maggiore armonizzazione nell'interpretazione e nell'applicazione delle sanzioni, attraverso l'adozione di linee guida, decisioni vincolanti e meccanismi di cooperazione tra autorità nazionali. Al momento, il Regolamento EHDS non prevede strumenti assimilabili. In questo senso, l'assenza nel Regolamento EHDS di una autorità con funzioni analoghe a quelle esercitate dall'EDPB, rappresenta una carenza strutturale estremamente importante. Il GDPR, pur con i suoi limiti applicativi[119], ha infatti

Airways (183 milioni £) e *Marriott* (100 milioni £). In Francia, la CNIL ha sanzionato Google per 50 milioni di euro per violazioni relative alla trasparenza e al consenso, ma ha anche irrogato multe proporzionalmente molto elevate a imprese locali. Queste divergenze riflettono anche fattori strutturali come la disponibilità di risorse (personale, *budget*, capacità investigativa), il diverso grado di indipendenza delle autorità garanti e le differenze tra culture giuridiche nazionali, che influenzano l'approccio sanzionatorio: nei paesi di tradizione più formalista o autoritativa si tende a privilegiare la deterrenza attraverso sanzioni elevate, mentre in quelli di tradizione consensualista o cooperativa si predilige un *enforcement* meno punitivo e più orientato all'adeguamento progressivo da parte dei soggetti obbligati. Sul punto si veda l'analisi condotta da J. WOLFF, N. ATALLAH, *Early GDPR Penalties, Analysis of Implementation and Fines Through May 2020*, in *Journal of Information Policy*, 2021, 64 e ss.

[117] Si fa riferimento all'annosa questione del *forum shopping* sul quale l'EDPB si era già pronunciata con il "Parere 4/2024 sulla nozione di stabilimento principale di un titolare del trattamento nell'Unione ai sensi dell'articolo 4, punto 16), lettera a), GDPR" chiarendo che questa andava interpretata in modo sostanziale e non meramente formale. Il Comitato ha evidenziato il rischio che i titolari del trattamento possano manipolare la localizzazione dello stabilimento principale per scegliere una autorità capofila più permissiva. Ciò potrebbe riflettersi non solo sul piano del controllo, ma anche in ambito sanzionatorio, eludendo potenzialmente le sanzioni più severe. Il testo completo è disponibile al seguente link: https://www.edpb.europa.eu/system/files/2024-08/edpb_opinion_202404_mainestablishment_it.pdf.

[118] Sulla scorta del termine anglosassone *plaintiff-friendly*, l'uso provocatorio del neologismo *health data-friendly* vuole sottolineare, in mancanza di regole uniformi, la concreta probabilità che si instaurino, a livello unionale, regimi sanzionatori differenziati non solo tra gli Stati membri, ma anche tra settori distinti. L'Unione Europea è infatti impegnata nello sviluppo di quattordici Spazi europei dei dati settoriali – tra cui quelli relativi ad energia, finanza, agricoltura, media e mobilità – ciascuno disciplinato da propri atti normativi. Sul punto si veda la sezione dedicata alla Realizzazione di spazi comuni europei di dati, al link: https://digital-strategy.ec.europa.eu/it/policies/data-spaces. In assenza di un intervento coordinato, come ben potrebbe essere un regolamento quadro sui criteri sanzionatori ovvero la creazione di una autorità di coordinamento con poteri trasversali, la strategia europea rischia di tradursi in un mosaico di *enforcement* settoriali caratterizzati da livelli di tutela e rigore disomogenei, con il conseguente rischio di ingiustificate distorsioni competitive tra attori operanti in contesti nazionali e settoriali differenti. In tale ipotesi, potrebbero emergere veri e propri *hub* normativi specifici, con Stati che si distingueranno per un approccio più accomodante verso particolari ambiti, dando luogo a contesti *data-friendly* di qualsiasi genere. Queste differenziazioni, anziché riflettere scelte strategiche condivise, risponderebbero poi a logiche di attrattività regolatoria, con il rischio di incoraggiare dinamiche anticoncorrenziali e di compromettere la certezza giuridica a livello europeo.

[119] F. B. BASTOS, P. PAŁKA, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity*, in *European Constitutional Law Review*, 2023, 487 e ss; dall'analisi condotta si evidenzia con chiarezza il ruolo

potuto beneficiare di un apparato sanzionatorio progressivamente armonizzato, attraverso l'adozione nel 2018 e nel 2023 da parte dell'EDPB di Linee Guida in materia di calcolo delle sanzioni specificamente volte a disciplinarne il tema[120].

Il Regolamento EHDS, invece, non prevede in maniera puntuale un analogo meccanismo di coordinamento. Un parziale correttivo, come già visto, potrebbe derivare dall'adozione di orientamenti da parte della Commissione in cooperazione con il Comitato EHDS[121] ma nel contesto appena descritto, sembrerebbero mancare soluzioni evidenti. Tuttavia, il

dell'*European Data Protection Board* nell'ambito del meccanismo di enforcement del GDPR, mettendone in luce le potenzialità ma soprattutto i limiti strutturali. L'EDPB non opera come autorità sovranazionale autonoma, bensì come organo deputato alla risoluzione delle controversie tra autorità nazionali nel contesto del meccanismo di cooperazione e coerenza previsto dal Regolamento. Le sue decisioni hanno valore vincolante, ma sono circoscritte alle questioni sollevate dalle autorità nazionali. In tale prospettiva, il suo ruolo risulta più ausiliario che effettivamente direttivo. Tale assetto si rivela particolarmente inadeguato nei casi di interesse comune europeo, ossia in quelle situazioni in cui la portata transnazionale del trattamento e la complessità delle questioni interpretative richiederebbero un intervento centralizzato, rapido ed efficace. L'impossibilità per l'EDPB di agire autonomamente, unita alla frammentazione delle prassi procedurali nazionali, compromette l'uniformità della tutela dei diritti fondamentali dei cittadini europei. In questo contesto, pur accogliendo favorevolmente lo sforzo di armonizzazione procedurale dell'EDPB, si ritiene tale apparato ancora insufficiente a colmare le lacune sistemiche.

120 Si fa riferimento alle "Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 - WP253" entrate in vigore nel 2018 ed alle "Linee guida 4/2022 sul calcolo dell'ammontare delle sanzioni amministrative ai sensi del GDPR" adottate a maggio 2023. Entrambe mirano a garantire un'applicazione uniforme, proporzionata ed effettiva delle sanzioni amministrative previste dal GDPR. In questo quadro, le multe non sono considerate un rimedio eccezionale, ma uno strumento ordinario e fondamentale per assicurare il rispetto delle norme sulla protezione dei dati, da applicare con criteri chiari e motivazioni trasparenti. Le WP253 definiscono i principi generali che devono orientare le autorità di controllo nell'uso del potere sanzionatorio. Ogni decisione va presa caso per caso, valutando elementi come natura, gravità e durata della violazione, numero di interessati coinvolti, carattere doloso o colposo della condotta, adozione di misure tecniche e organizzative adeguate, recidiva e grado di cooperazione con l'autorità. Centrale è il rispetto dei principi di proporzionalità, efficacia e funzione dissuasiva, al fine di garantire uniformità di trattamento tra gli Stati membri. Al tempo stesso, le linee guida invitano a un uso prudente della sanzione pecuniaria: le multe non devono essere considerate né una *extrema ratio* da applicare solo in casi eccezionali, né uno strumento da utilizzare in modo indiscriminato, per evitare di svilirne l'efficacia. Ne risulta una cornice concettuale volta ad assicurare coerenza e responsabilità nell'applicazione del potere sanzionatorio. Le Linee guida 4/2022 introducono invece un metodo operativo per la determinazione dell'importo, con l'obiettivo di uniformare il calcolo tra le diverse autorità nazionali. Il processo prevede più fasi: l'individuazione delle operazioni di trattamento interessate e la verifica di eventuali violazioni autonome o collegate; la fissazione di un punto di partenza per la sanzione, basato su gravità della violazione, categoria normativa di riferimento e fatturato dell'impresa; l'analisi delle circostanze aggravanti e attenuanti, come recidiva, intenzionalità, cooperazione e misure correttive; la verifica del rispetto dei massimali previsti dal GDPR; infine, un controllo di coerenza con i principi di proporzionalità, effettività e dissuasività (sia generale che specifica), che può portare ad un aggiustamento dell'importo finale. In ogni fase, l'autorità è chiamata a motivare in modo trasparente le proprie scelte, dimostrando come le caratteristiche del caso abbiano inciso sulla decisione.

121 Reg. (UE) 2025/327, cit., art. 63, par. 8. Al Considerando 95 si afferma la necessità, nell'ambito dello Spazio europeo dei dati sanitari, di un Comitato che promuova una applicazione coerente della normativa in oggetto. Il Comitato EHDS, la cui disciplina è contenuta negli articoli 92 e 94 del Regolamento (UE) 2025/327, è quindi un organo tecnico-istituzionale istituito per garantire un'applicazione armonizzata del Regolamento sullo Spazio Europeo dei Dati Sanitari, promuovendo la cooperazione tra Stati membri e Commissione Europea sia nell'uso primario che secondario dei dati. È composto da due rappresentanti per ciascun Paese (uno per l'uso primario ed uno per l'uso secondario), opera in modo indipendente e nell'interesse pubblico, avvalendosi anche di sottogruppi tematici e del contributo di portatori di interesse. Tra i suoi compiti rientrano il coordinamento delle pratiche nazionali, lo scambio di buone prassi, la gestione dei rischi e la formulazione di orientamenti condivisi, con l'obiettivo di favorire l'interoperabilità, la qualità e la sicurezza del sistema EHDS in tutta l'Unione Europea.

Regolamento EHDS non lascia aperta la questione, ma propone una soluzione in grado di dipanare i diversi dubbi in merito.

A tal proposito, merita particolare attenzione l'articolo 22 del Regolamento EHDS[122]. Come si è avuto modo di osservare, a differenza del GDPR che all'articolo 70 attribuisce espressamente all'EDPB il potere di adottare linee guida, raccomandazioni e best practices al fine di favorire un'applicazione uniforme delle disposizioni, incluse quelle in materia sanzionatoria[123], il nuovo quadro normativo in materia di dati sanitari non contempla un analogo strumento di coordinamento interpretativo. Ne risulta, pertanto, un sistema in cui la coerenza applicativa non è attualmente garantita da una autorità centrale prevista dal Regolamento, ma sarà rimessa alla formazione progressiva di prassi orizzontali tra i futuri Organismi responsabili dell'accesso ai dati sanitari. L'espresso rinvio all'articolo 83, paragrafo 5, del GDPR, operato dall'articolo 22 EHDS, tuttavia, renderebbe applicabili al regime sanzionatorio dell'EHDS le Linee guida già adottate dall'EDPB in materia di determinazione delle sanzioni amministrative pecuniarie. Permetterebbe, inoltre, alle stesse autorità di controllo di infliggere sanzioni amministrative entro gli importi dettati dal paragrafo 5. In assenza, o comunque in attesa, di nuove fonti interpretative elaborate a livello europeo, la trasposizione di tali linee guida appare dunque lo strumento più idoneo a colmare le lacune del sistema e a ridurre il rischio di divergenze applicative, così da assicurare un minimo comune denominatore nell'azione delle autorità nazionali.

In definitiva, abbiamo visto come il modello sanzionatorio del Regolamento EHDS si discosti dal paradigma tradizionale dei regolamenti come fonti armonizzanti per eccellenza e presenti invece una forte impronta direttiva. Questa ambivalenza, che all'apparenza genera tensioni sistemiche tra l'aspirazione di uniformità e la persistenza delle discipline nazionali, trova la sua soluzione nella richiamata norma dettata dall'articolo 22. In questo modo si restituisce al Regolamento la tanto ambita funzione unificatrice che ne costituisce la *ratio* primaria, e si rende effettiva la promessa di integrazione dello Spazio Europeo dei Dati Sanitari, sulla scorta del grande lavoro interpretativo avviato per il GDPR dall'*European Data Protection Board*[124].

122 Reg. (UE) 2025/327, cit., art. 22, comma 1.

123 Reg. (UE) 2016/679, cit., art. 70, par. 1, lett. k).

124 Successivamente alla redazione del presente contributo, nell'ambito del progetto TEHDAS2 (*Second Joint Action Towards the European Health Data Space*), è stato pubblicato il deliverable D4.1 – *Guideline for health data access bodies on fees and penalties for non-compliance related to the EHDS Regulation* (27 febbraio 2026), contenente indicazioni operative rivolte agli *Health Data Access Bodies* in materia di applicazione degli artt. 62, 63 e 64 del Regolamento (UE) 2025/327. Il documento, elaborato anche sulla base degli esiti della consultazione pubblica svolta nel 2025, si propone di favorire un'applicazione armonizzata del regime dei corrispettivi e dei poteri di vigilanza e sanzionatori, formulando raccomandazioni in ordine ai criteri di determinazione delle sanzioni amministrative, alle procedure decisionali interne, all'impiego di strumenti di valutazione (*assessment tools e penalty matrices*), nonché al coordinamento con i quadri normativi nazionali. Lo stesso documento precisa, tuttavia, di costituire un documento di indirizzo tecnico, privo di efficacia giuridicamente vincolante, che non rappresenta la posizione della Commissione europea né costituisce una linea guida o specifica tecnica adottata ai sensi del Regolamento EHDS. Le conclusioni cui perviene il presente contributo risultano pertanto confermate, pur trovando nelle indicazioni elaborate da TEHDAS2 un significativo supporto interpretativo ai fini di una futura armonizzazione delle prassi applicative.