RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0247 • articolo sottoposto a peer review • pubblicato in anteprima il 21 nov. 2025

Stefano Corso

Il trattamento dei dati personali in ambito sanitario

Il trattamento dei dati personali in ambito sanitario è regolato da plurime disposizioni appartenenti a fonti di diverso livello. Uno dei principali aspetti che connota questa disciplina attiene alla tipologia di dati personali maggiormente trattati nella sanità, ossia i dati relativi alla salute. Da un esame complessivo della normativa, nazionale e sovranazionale, emerge la tensione fra gli interessi sottesi – di natura pubblica e privata – di cui il legislatore cerca di realizzare un bilanciamento. Elemento caratteristico del rinnovato quadro giuridico è il superamento definitivo della regola del consenso con l'approdo a paradigmi differenti di protezione dei dati, che possano valorizzare effettivamente la dimensione circolatoria del fenomeno. Nel cangiante panorama legislativo in materia di dati sanitari, permane la garanzia del diritto fondamentale della persona all'autodeterminazione. L'istituzione dello spazio europeo dei dati sanitari conferma l'assunto.

Protezione dei dati personali – Trattamento di dati relativi alla salute – Autodeterminazione
Fascicolo sanitario elettronico – Spazio europeo dei dati sanitari

The processing of personal data in healthcare

The processing of personal data in the healthcare sector is governed by multiple provisions from various sources. One of the main aspects of this regulation concerns the type of personal data most commonly processed in healthcare: data concerning health. An examination of national and supranational legislation reveals underlying tensions between public and private interests, which the legislator must balance. A defining feature of the updated legal framework is the definitive shift away from the consent rule, with different data protection paradigms now in place that can effectively enhance the circulation of data. Despite the changing legislative landscape regarding health data, individuals' fundamental right to self-determination remains guaranteed. The establishment of the European Health Data Space confirms this assumption.

Personal data protection – Processing of data concerning health – Self-determination
Electronic Health Record – European Health Data Space

L'Autore è assegnista di ricerca in Diritto privato presso il Dipartimento di Scienze politiche, giuridiche e studi internazionali dell'Università di Padova

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Autodeterminazione terapeutica e autodeterminazione informativa

"La dignità, l'identità, la libertà e l'autodeterminazione, la privacy nei suoi diversi significati sono prerogative da declinare con la specificazione '*nel corpo*'"[1]. Con queste parole Paolo Zatti si riferiva alle situazioni giuridiche pertinenti alla persona rapportandole al corpo. E Stefano Rodotà, citando queste stesse parole, aggiungeva: "dunque nella vita"[2]. Il ragionamento portava alla contrapposizione dell'autonomia del soggetto nei rapporti patrimoniali rispetto all'autonomia nelle scelte esistenziali. L'autodeterminazione come diritto della persona si declina così come autodeterminazione terapeutica. Ma non è questo l'unico modo possibile di concepire l'autodeterminazione.

Il 15 dicembre 1983, nel celebre *Volkszählungsurteil*, la Corte costituzionale tedesca[3] sancì, com'è noto, il diritto all'autodeterminazione informativa e tale diritto fu ancorato agli artt. 1 e 2 del *Grundgesetz*, riconducendosi direttamente all'istituto dell'*allgemeines Persönlichkeitsrecht*[4]. L'autodeterminazione informativa venne così intesa come il diritto fondamentale della persona di decidere autonomamente in merito alla divulgazione e all'utilizzo dei propri dati personali, derivante dal principio cardine della dignità e dalla garanzia del libero sviluppo della personalità, che richiede la protezione dell'individuo dalla raccolta, la conservazione, l'uso e la diffusione illimitati dei suoi dati personali.

Quando si parla di autodeterminazione in ambito sanitario, tuttavia, non è a quella informativa che si fa usualmente riferimento, bensì all'autodeterminazione terapeutica o meglio, e più in generale, all'autodeterminazione della persona sul proprio corpo. L'autodeterminazione accede, da questo piano, a un insieme di significati ampio e diversificato, una parte dei quali si rispecchia nei corrispondenti significati che stanno sul piano dell'autodeterminazione informativa e un'altra

1. Zatti 2009, p. 86.
2. Rodotà 2010, p. 211.
3. BVerfG, 15.12.1983, in "Neue Juristische Wochenschrift", 1984, p. 419.
4. Tale correlazione fu poi ribadita dall'art. 1 del *Bundesdatenschutzgesetz* del 1990 (e successive modifiche) nonché dalle normative dei singoli *Länder*. Resta 2006, p. 572.

parte, la più cospicua, vi è invece ignota. Nell'ordinamento italiano l'autodeterminazione, in questo senso, ma non solo, è considerata oggetto di un diritto fondamentale della persona, che trova il suo punto di sintesi con il diritto alla salute, nel consenso informato del paziente. Il consenso informato al trattamento sanitario è elemento fondamentale del diritto all'autodeterminazione terapeutica della persona, annoverabile fra i diritti della personalità, e la sua violazione determina il diritto al risarcimento del danno[5].

La consensualità nella relazione di cura, con l'abbandono dell'impostazione verticale e paternalistica del rapporto classico medico-paziente e con la centralità della persona in medicina, ha trovato riconoscimento normativo nella legge 22 dicembre 2017, n. 219[6]. Rubricata "Norme in materia di consenso informato e di disposizioni anticipate di trattamento", la legge 219/2017 è giunta a delineare una disciplina per la relazione di cura, dal momento attuale del dialogo fra medico e paziente a quello finale, in cui un'attualità di quel dialogo può venire a mancare, per le condizioni di fragilità dell'individuo. La legge non ha riempito un'area vuota di diritto, ma si è innestata su un terreno già abitato dal diritto vivente, nel fertile scambio di dottrina e giurisprudenza[7].

Il *consenso informato* – espressione di cui si fa uso anche nella legge 219/2017 – è l'elemento che connota tanto l'autodeterminazione terapeutica quanto l'autodeterminazione informativa, ritrovando l'autodeterminazione, come comun denominatore, il profilo della volontà del soggetto. All'interno del contesto sanitario, nel percorso di cura, l'autodeterminazione terapeutica supera e, per così dire, assorbe quella informativa. Infatti, nel momento in cui l'individuo esprime consapevolmente il proprio consenso al trattamento sanitario, non è necessario – come si ricava dall'art. 9 del Regolamento generale sulla protezione dei dati (reg. Ue n. 679 del 2016, c.d. GDPR)[8] – che egli manifesti pure il consenso al trattamento dei suoi dati, perché questo avvenga.

Uno degli aspetti critici della disciplina italiana in materia, prima che entrasse in vigore e fosse applicabile il GDPR, era proprio questo. Dover richiedere il consenso del paziente al trattamento dei suoi dati sanitari per l'esecuzione della prestazione sanitaria apriva, in astratto, all'aporia del soggetto che avrebbe potuto domandare la prestazione medica, quindi acconsentendo al trattamento sanitario, e allo stesso tempo negare il consenso al trattamento dei dati relativi alla propria salute. In concreto, per ottenere la prestazione medica, il paziente ovviamente acconsente anche al trattamento dei suoi dati sanitari e allora si comprende come il consenso possa dirsi del tutto apparente o necessitato[9].

L'autodeterminazione informativa in ambito sanitario non è stata tuttavia obliterata. Deve ritenersi, infatti, che essa sia recuperata proprio nella dimensione della relazione di cura, sul piano del rapporto medico-paziente, non più gerarchizzato secondo gli schemi del passato, ma costruito sul dialogo e orientato all'alleanza terapeutica[10].

Alla luce del ruolo che continua a svolgere il consenso informato tanto sul piano del trattamento sanitario quanto su quello del trattamento dei dati personali e, nella specie, nell'ambito sanitario, sembra potersi intravedere un parallelismo, seppure imperfetto, fra autodeterminazione come governo del corpo e autodeterminazione come controllo delle proprie informazioni: governo del corpo fisico e governo del corpo digitale. L'osservazione si arricchisce con riferimento alla protezione dei dati personali alla luce delle varie situazioni giuridiche riconosciute attraverso i c.d. "diritti dell'interessato".

L'autodeterminazione informativa nel contesto sanitario si connota specialmente per due aspetti: la sensibilità dei dati personali coinvolti e la qualifica prevalentemente pubblica dei

5. Pucella 2010. Cfr. Calderai 2015, p. 225 ss. Spec. con riferimento alla prospettiva del diritto sanitario, v. Pioggia 2011, p. 127 ss.
6. Su tutti, Zatti 2018, p. 247 ss.; Zatti 2019, p. 3 ss.
7. Mantovani 2019, p. 1447 ss.
8. Thiene 2021, p. 240 ss.
9. Finocchiaro 2008, p. 207 ss., spec. p. 213.
10. Senigaglia 2023, p. 470 ss., spec. p. 476. Cfr. Cacace 2025, p. 333 ss.; Foglia 2018.

soggetti che eseguono il trattamento e della loro funzione[11]. Partendo da tale constatazione, si coglie come proprio questo ambito sperimenti la tensione fra i valori e richieda un bilanciamento attento[12]. Là dove, infatti, si consideri la peculiare sensibilità delle informazioni, emerge la necessità di una più elevata difesa della persona, mentre, considerando l'interesse pubblico perseguito, si evince l'esigenza del limite al diritto individuale[13]: linee di tutela che sembrano muoversi in direzioni opposte.

2. Trattamento dei dati personali in ambito sanitario e trattamento dei dati relativi alla salute

La tutela della persona rispetto alla circolazione delle informazioni che la riguardano è stata affidata, in origine, al consenso dell'interessato. Il consenso era visto come lo strumento per mezzo del quale il soggetto poteva esercitare un controllo sul fenomeno circolatorio dei dati, nel suo duplice senso: in positivo, quando prestato, legittimando il trattamento dei dati personali e permettendo al titolare del trattamento di svolgere le relative operazioni; e in negativo, quando non prestato, rendendo illecito il trattamento che fosse comunque avvenuto e che non trovasse altra base giuridica e quindi attivando il meccanismo sanzionatorio[14].

La Direttiva UE n. 46 del 1995, che contemplava il consenso dell'interessato quale base giuridica del trattamento di dati personali al menzionato art. 7, lett. *a*, lasciava agli Stati membri il consueto margine di discrezionalità nell'attuare anche questa previsione, come disposto all'art. 5. La scelta del legislatore italiano fu quella di attribuire al consenso una funzione di perno della disciplina della protezione dei dati personali, attorno al quale far ruotare l'esercizio dei diritti dell'interessato.

Il panorama è mutato con l'entrata in vigore del GDPR[15]. Il consenso dell'interessato è solo una delle differenti condizioni di liceità del trattamento, ai sensi dell'art. 6 GDPR, e – qualificato come "esplicito" – è solo una delle ipotesi di deroga al divieto di trattamento delle categorie particolari di dati personali, ai sensi dell'art. 9 GDPR[16]. La novità non è tanto nel contenuto di queste disposizioni quanto nella tipologia di atto normativo adottato. Se la Direttiva, dovendo essere attuata, presupponeva la mediazione dell'intervento del legislatore nazionale, il Regolamento, invece, è direttamente applicabile e – pur se non elimina del tutto il margine di discrezionalità lasciato agli Stati membri, soprattutto alla luce di molteplici formulazioni normative volutamente ampie, che a loro volta richiedono un'attuazione da parte degli ordinamenti nazionali – trasferisce la sua impostazione nei sistemi giuridici europei in modo immediato.

Il discorso assume uno spessore maggiore se si considera che il trattamento di dati personali in ambito sanitario è forse quello che maggiormente ha ad oggetto i dati relativi alla salute. Com'è noto questa tipologia di dati personali rientra nel novero delle particolari categorie di dati personali per le quali si prevedono misure più rigorose in ordine al loro trattamento. Si tratta di quelle informazioni che tradizionalmente rientrano nel concetto di "dati sensibili" e il cui trattamento è in grado di mettere a serio rischio le libertà e diritti fondamentali della persona[17].

Come anticipato, l'art. 9, par. 1, GDPR vieta il trattamento di dati relativi alla salute, ma, al

11. Sandulli 2023, p. 1 ss. Cfr., per le linee di sviluppo del diritto sanitario, Sandulli–Aperio Bella 2021.
12. Evidenzia la centralità del rapporto fra privacy e attività della pubblica amministrazione P. Perlingieri 2003, p. 211 ss. Sul valore della persona e il principio personalista nel sistema ordinamentale italiano, nel rispetto del quale necessariamente deve compiersi ogni bilanciamento, v. P. Perlingieri 2020, vol. III, p. 1 ss.; nonché P. Perlingieri 1972.
13. C. Perlingieri 2022, p. 127 ss. Cfr. Di Ciommo 2002, p. 121 ss.
14. Cfr. Bygrave 2002, p. 150 e 154. Nel contesto italiano, *ex plurimis*, Iamiceli 2024, p. 76 ss., nonché Sica 2001, p. 621 ss.; Patti 1999, p. 455 ss.; Cuffaro 1997, p. 201 ss.
15. Cfr. P. Perlingieri 2018, p. 481 ss.
16. Thiene 2023, p. 7 ss.; Granieri 2017, p. 165 ss. Cfr. Georgieva–Kuner 2020, p. 365 ss.
17. Thiene–Corso 2023; Guarda 2019, p. 591 ss.; Riccio 2004, p. 247 ss.; Zambrano 1999, p. 1 ss.

contempo, il rigore del divieto è mitigato dall'elenco delle ipotesi eccezionali in cui tale trattamento è ammesso secondo il par. 2 dello stesso articolo. È proprio attraverso queste fattispecie derogatorie che il trattamento di dati sensibili, in ambito sanitario, è consentito. Oltre alle ipotesi riconducibili alla volontà della persona, ossia le eccezioni di cui alle lett. *a* ed *e* – cioè il consenso esplicito dell'interessato e la pubblicazione manifesta dei dati stessi da parte dell'interessato – giocano un ruolo di fondamentale importanza a tal fine le ipotesi enunciate alle lett. *c*, *g*, *h*, *i* e *j*.

Prima fra tutte, l'eccezione di cui alla lett. *h*, che si sostanzia nella c.d. "finalità di cura", permette il trattamento dei dati relativi alla salute, qualora necessario, per l'erogazione dei servizi e delle prestazioni di natura medica e sanitaria, non solo sulla base del diritto eurounitario o nazionale, ma anche "conformemente al contratto con un professionista della sanità". Viene così coperto il panorama del settore pubblico tanto quanto quello del settore privato. La disposizione è integrata dalla previsione dell'art. 9, par. 3, secondo cui il trattamento per finalità di cura di dati sanitari, oltre alle altre categorie particolari di dati personali, deve avvenire soltanto ad opera o sotto la responsabilità di un professionista vincolato al segreto professionale o di un soggetto comunque tenuto all'obbligo di segretezza. Va considerato che il trattamento di dati relativi alla salute in ambito sanitario è parte essenziale del rapporto medico-paziente ed è indispensabile per l'individuazione e l'esecuzione del trattamento sanitario e per lo svolgimento della funzione di un sistema sanitario[18].

Il trattamento di dati relativi alla salute in ambito sanitario è permesso, sotto altri aspetti, anche dalle altre ipotesi menzionate[19]. Così, con l'applicazione della lett. *c*, si consente il trattamento di dati sanitari che risulti necessario per un trattamento sanitario salvavita o richiesto in condizioni gravi di salute. Per la ricerca in ambito medico, la lett. *j* permette il necessario trattamento dei dati sulla salute. Mentre su un più generale versante amministrativo si colloca l'applicabilità delle eccezioni enunciate alle lett. *g* ed *i*. Se quest'ultima, infatti, viene in rilievo per i trattamenti di dati sanitari necessari per motivi pubblici legati alla sanità pubblica, quindi anche per garantire il buon funzionamento dei sistemi sanitari stessi, la lett. *g* si apre alle esigenze più ampie, non solo quelle che si prospettano come strettamente connesse alla sanità pubblica, ma anche le esigenze delle pubbliche amministrazioni, purché il trattamento di dati relativi alla salute sia necessario per "motivi di interesse pubblico rilevante".

L'importanza del trattamento dei dati sanitari – e delle altre tipologie di dati sensibili – a scopi legati alla tutela della salute è sottolineata anche dal considerando 53 del Regolamento, per cui "le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica".

Peraltro il settore sanitario non è l'unico in cui avviene il trattamento di dati relativi alla salute. Esso, infatti, si svolge in numerosi ambiti, anche per scopi più strettamente legati al mondo dell'economia. Anche per questo l'esigenza di delineare attentamente le eccezioni al divieto di trattamento si impone con forza, soprattutto nella rapida

18. "L'informazione è dunque al centro delle organizzazioni sanitarie forse anche più della conoscenza. Le informazioni sanitarie sono cresciute in numero e complessità e sono divenute forse la prima preoccupazione delle strutture sanitarie", Comandé 2008, p. 289.

19. Cfr. Greco 2019, p. 244 ss., spec. p. 249 ss.

evoluzione tecnologica che contraddistingue la società contemporanea[20].

Il GDPR rinuncia a una completa uniformazione delle discipline nazionali, lasciando alla discrezionalità degli Stati membri la possibilità di condizionare e anche limitare il trattamento dei dati relativi alla salute, così come quello dei dati genetici e biometrici, attraverso il mantenimento delle normative interne o l'introduzione di nuove regole, per certi versi seguendo una logica simile a quella armonizzante della direttiva: la disposizione di riferimento in questo caso è il par. 4 dell'art. 9[21].

Numerose altre regole dettate dal GDPR possono trovare applicazione con riguardo al trattamento dei dati personali in ambito sanitario, ma il ruolo principale è giocato proprio dall'art. 9, che definisce così uno statuto generale per i dati sensibili e quindi include le norme di base del trattamento dei dati relativi alla salute. La disciplina del trattamento di dati personali in ambito sanitario tuttavia non si esaurisce nel Regolamento generale sulla protezione dei dati, nonostante questo rimanga il più rilevante atto normativo di riferimento. Una parte delle norme in materia è al di fuori del diritto eurounitario e ricade nel diritto interno. Così, nell'ordinamento italiano, assumono rilievo al riguardo le disposizioni del Codice della privacy.

3. Le norme del Codice della privacy

Per adeguare l'assetto del proprio sistema all'avvento del GDPR, il legislatore italiano è intervenuto sul Codice della privacy apportando numerose ed estese modifiche mediante il d.lgs. 10 agosto 2018, n. 101[22]. Si è quindi inciso profondamente sulla struttura e sul testo delle disposizioni del Codice della privacy, abrogando interi blocchi di articoli, sostituendone e modificandone altri, introducendone di nuovi, con una tecnica legislativa che non è andata esente da critiche[23].

L'abrogazione dell'art. 4 ha comportato l'eliminazione della definizione di *dati sensibili*, contenuta alla lett. *d*, essendo ora assorbita dalla valenza dell'espressione "categorie particolari di dati personali" di cui all'art. 9 del GDPR. Il Titolo III della Parte I del d.lgs. n. 196 del 2003 è stato abrogato per intero, con tutti gli articoli che conteneva, compresi gli artt. 20 e 26 applicabili appunto ai dati sensibili. Una parte assai rilevante delle nuove disposizioni, introdotte nel 2018, si trova agli artt. 2-*bis* ss., distribuiti ora, nel Titolo I, "Principi e disposizioni generali", della Parte I. Fra questi, un ruolo di estrema importanza per il trattamento di dati personali appartenenti alle particolari categorie, anche e soprattutto per il trattamento dei dati relativi alla salute, è svolto dagli artt. 2-*sexies* e 2-*septies*[24].

L'art. 2-*sexies* precisa le condizioni di ammissibilità dei trattamenti necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lett. *g*, del GDPR[25]. Essi sono ammessi, ai sensi del comma 1, "qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"[26]. Tale disposizione è stata modificata

20. Richiamando il *mosaic of policies* di Westin 1976, p. 269, come necessità per gestire le problematiche sollevate dal trattamento di dati sanitari, Comandé 2008, p. 285, individua alcune aree in cui i dati sulla salute sono sempre maggiormente raccolti, usati e condivisi: "1. l'erogazione di servizi sanitari; 2. il pagamento delle prestazioni; 3. gli usi sociali dei dati sanitari per prevenire la diffusione di epidemie".
21. Cfr. Fares 2021, p. 23.
22. In argomento Pizzetti 2021, p. 3 ss.; Tosi 2019, p. 16 ss. Sullo spirito del Codice della privacy italiano, a seguito dell'avvento del GDPR, v. Alpa 2021, p. 995 ss.
23. Cuffaro 2018, p. 1181 ss., spec. p. 1183 s.
24. C. Perlingieri 2022, p. 130 s.
25. Cortese 2021, p. 1044 ss.
26. Il comma 2 dell'art. 2-*sexies* fornisce invece un elenco di materie in cui è considerato rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri. Tra le numerosissime ipotesi di questo elenco, si evidenziano, per la stretta connessione con i dati sanitari, quelle di cui alle lett. *t*, *u*, *v*, *z*, *aa* e *cc*.

dall'art. 9, comma 1, lett. *b*, n. 1, d.l. 8 ottobre 2021, n. 139[27] – c.d. "Decreto capienze" – convertito con modificazioni dalla legge 3 dicembre 2021, n. 205, che ha eliminato la fonte regolamentare della previsione come ipotesi di ammissibilità dei trattamenti nell'ordinamento interno e ha aggiunto invece quella degli atti amministrativi generali[28]. Il comma 1-*bis* dell'art. 2-*sexies* del Codice della privacy, introdotto dalla medesima lett. *b* dell'art. 9, comma 1, d.l. n. 139/2021, al n. 2, così come modificato dalla citata legge di conversione n. 205/2021, e specificamente dedicato al trattamento di dati relativi alla salute, è stato in seguito sostituito dall'art. 44, comma 1, del d.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla legge 29 aprile 2024, n. 56, il quale ha anche aggiunto all'art. 2-*sexies* un comma 1-*ter*. Queste nuove disposizioni individuano una serie di soggetti istituzionali che, nel rispetto delle proprie finalità, possono trattare i dati personali relativi alla salute, anche mediante interconnessione. Per poter essere trattati, i dati personali dovranno essere pseudonimizzati[29]. Si può notare, sin da subito, nel trattamento dei dati relativi alla salute, la centralità del fascicolo sanitario elettronico.

L'art. 2-*septies*, invece, si pone in attuazione del par. 4 dell'art. 9 del GDPR, prevedendo, come condizione per ammettere il trattamento di dati relativi alla salute, genetici e biometrici, la conformità alle *misure di garanzia* disposte dal Garante[30]. Un particolare rilievo ricopre il comma 5, per cui le misure di garanzia sono adottate in relazione a ciascuna categoria di dati personali di cui al comma 1, ossia dati relativi alla salute, dati genetici e dati biometrici, avendo riguardo alle specifiche finalità del trattamento. In tal senso, le misure di garanzia vengono ad essere l'elemento chiave, per coniugare la limitata circolazione dei dati appartenenti alle categorie particolari e la sicurezza nel trattamento, nell'ottica del rispetto dei diritti dell'interessato.

Espressamente dedicato al trattamento di dati personali in ambito sanitario è il Titolo V della Parte II del Codice della privacy, rubricato proprio in questi termini[31]. L'intervento di adeguamento al GDPR operato con il d.lgs. n. 101/2018 ha toccato, eccezion fatta per l'art. 93, tutte le disposizioni del Titolo V[32]. L'art. 75, d.lgs. n. 196 del 2003, ora recita: "Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-*septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore". La nuova disposizione, nel sottinteso riferimento all'oggetto del trattamento costituito dai dati sensibili, fa rinvio ad altre norme, prime fra tutte quelle di cui all'art. 9 del GDPR, soppiantando la precedente disposizione[33]. Ad essere richiamate sono quindi le eccezioni previste dal par. 2 dell'art. 9 che si traducono nella finalità di cura (lett. *h*) – con l'ulteriore precisazione normativa di cui al par. 3 – e nei motivi di interesse pubblico nel settore della sanità pubblica (lett. *i*).

Il trattamento di dati relativi alla salute – ma anche di dati personali appartenenti ad altre categorie particolari – quando avvenga per gli scopi menzionati, ricorrendo le necessità che sono alla base di dette deroghe, dunque prescinde dal consenso dell'interessato. Deve inoltre essere conforme alle misure di garanzia, *ex* art. 2-*septies*, e rispettare le "specifiche disposizioni di settore". Con tale formula l'art. 75 fa rinvio ad altre norme, anche di livello non primario, tracciate sempre con riguardo al trattamento di dati personali per finalità di tutela della salute. In questo caso, il

27. Per una prima analisi della norma, antecedente alle modifiche apportate dalla legge di conversione, v. Francario 2021.
28. Riportando il chiarimento del Garante, di cui alla nota del 27 novembre 2018, Cortese 2021, p. 1046, evidenzia come anche la prospettiva antecedente alle modifiche citate potesse aprire alla fonte di tipo amministrativo.
29. Si v. l'art. 4, n. 5), del GDPR.
30. Zanovello 2023, p. 129 ss., spec. 150 ss.; Zanovello 2021, p. 1051 ss.
31. Su questo assetto normativo, Riccio 2004, p. 247 ss. Cfr. Caggia 2007, p. 405 ss.
32. Molti degli articoli che componevano questo titolo sono stati abrogati: artt. 76, 81, 83, 84, 85, 86, 87, 88, 89, 90, 91 e 94.
33. Poletti 2007, p. 1195 ss.

riferimento può essere, ad esempio, alla disciplina del trattamento dei dati operato mediante il fascicolo sanitario elettronico. Per certi versi, l'art. 75 riveste un carattere programmatico, là dove, non menzionando il consenso, intende dare segno di un suo formale superamento, almeno nell'area del trattamento dei dati in ambito sanitario[34].

Il contenuto delle disposizioni "superstiti" del Titolo V, preannunciato dall'art. 77 del Codice della privacy, è costituito dalle modalità particolari per informare l'interessato e trattare i suoi dati. Dinanzi alla mutata prospettiva nei confronti del consenso, acquista un ruolo più pregnante l'informazione al paziente.

Posto che gli elementi dell'informativa sono quelli dettati agli artt. 13 e 14 del GDPR[35], l'art. 78 dispone che il medico di medicina generale, così come il pediatra di libera scelta, informi l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili detti elementi, conformemente al principio di trasparenza[36]. La tutela dell'interessato paziente è affidata a precetti che mirano a garantire un raggiungimento di consapevolezza in ordine al trattamento dei dati che lo riguardano, specialmente quando il trattamento avvenga con gli strumenti informatici, come oggi accade maggiormente. Le modalità descritte sono estese, dall'art. 79, alle strutture che erogano prestazioni sanitarie e socio-sanitarie, le quali, sulla base di adeguate misure organizzative, possono avvalersene "in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie" per più trattamenti di dati.

L'informazione al paziente sul trattamento dei suoi dati personali deve precedere la prestazione medica, eccezion fatta per i casi di emergenza e tutela della salute e dell'incolumità fisica enunciati all'art. 82. La regola contribuisce a confermare che nella prestazione sanitaria il trattamento dei dati relativi alla salute costituisce momento funzionale, per non dire coessenziale, alla sua esecuzione[37].

4. L'amministrativizzazione della protezione dei dati

Sin dalle prime riflessioni sulla protezione dei dati personali si è colta l'inconsistenza del consenso dell'interessato al trattamento come dispositivo di controllo nella circolazione dei dati[38]. È un'inappropriatezza che si riscontra su più fronti, se rapportata alle condizioni normali di un individuo, un utente medio dei servizi digitali.

Il più delle volte, infatti, il consenso è prestato senza alcuna consapevolezza, con disattenzione. La possibilità o la necessità di accedere velocemente a un servizio e le caratteristiche dell'ambiente digitale, alla portata di tutti, in qualsiasi luogo e in qualsiasi momento, su un computer, uno smartphone, un tablet, influiscono sui soggetti inibendo

34. Ogni riferimento al consenso è stato espunto dalle disposizioni di questo Titolo, "per effetto della mutata *ratio* normativa", Di Masi 2021, p. 1237.

35. Per la violazione degli obblighi informativi sanciti dal Regolamento e dal Codice della privacy, si è sostenuta in dottrina la configurabilità di una responsabilità contrattuale, in quanto si tratterebbe dell'inadempimento di obbligazioni derivanti *ex lege*, Piraino 2017, p. 389 s.

36. Vanno evidenziati, da parte sua, "analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato". E ciò, in particolare, nel caso di trattamenti effettuati: "a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; c-bis) ai fini dell'implementazione del *fascicolo sanitario elettronico* di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221".

37. Cfr. Finocchiaro 2008, p. 213 ss. Con riguardo, invece, al trattamento effettuato per la prescrizione di medicinali, l'art. 89 *bis* dispone che si adottino "cautele particolari" in relazione alle misure di garanzia del Garante, anche al di là della finalità di cura.

38. Cfr. Mirabelli 1993, p. 313 ss.

la considerazione che possono avere del valore della privacy e dei loro dati personali. Se l'interessato cercasse di comprendere ciò cui sta acconsentendo, spesso non sarebbe in grado di capirlo. La complicatezza delle operazioni di trattamento e la complessità tecnologica degli strumenti stessi pregiudicano l'intelligibilità delle attività e delle procedure messe in atto, la quale può richiedere conoscenze tecniche elevate e anche molto settoriali. Talvolta è l'informazione offerta all'interessato ad essere pregiudicata da questa complessità, di conseguenza ostacolando la comprensione del trattamento per cui si richiede il consenso, talaltra è anche solo il modo in cui l'informazione è resa che impedisce di comprendere. E, ancora, qualora tale consapevolezza vi fosse, la scelta sarebbe vincolata, poiché altrimenti il servizio correlato al trattamento potrebbe non essere erogato. In tal caso l'interessato avrebbe sì contezza delle operazioni di trattamento dei suoi dati personali e dei rischi connessi, ma acconsentirebbe ugualmente, per mancanza di alternative o per il bisogno di quel bene o di quel servizio[39].

Il pensiero giuridico si è, dunque, indirizzato verso altri strumenti, diversi dal consenso, per garantire la protezione dei dati personali – specie quelli sensibili – e, con essa, la protezione della persona. Le riflessioni sono approdate così ad una serie di misure e accorgimenti, soprattutto di natura tecnica, in grado di intervenire preventivamente rispetto alla possibile violazione di dati personali. E questi si sono poi tradotti in principi e regole, che possono, in larga parte, ricondursi al concetto di "sicurezza".

Così può intendersi la riservatezza per progettazione e per impostazione, cioè le nozioni di *privacy by design* e *privacy by default*[40]. Tali concetti impongono al sistema informatico di conformarsi alla protezione dei dati, sin dall'origine. L'ambiente digitale viene pensato sin dalla sua costruzione come un insieme di strutture atte a garantire la protezione dei dati personali e l'architettura dello spazio elettronico deve rispondere a questa logica[41]. In tal senso, la privacy non è più vista come un diritto corrispondente a mere pretese esercitabili dal singolo, bensì come un diritto che esige una tutela complessiva in quel contesto e da quel contesto e che quindi partecipa all'edificazione dell'ambiente digitale. Se il codice – informatico – diventa la nuova legge[42], allora il diritto modella questo codice affinché assicuri l'osservanza dei principi e delle regole, che al di fuori dello spazio elettronico è assicurata dalla legge[43].

Così può intendersi anche la tecnica della pseudonimizzazione, con cui viene impedita l'attribuzione del dato personale al soggetto cui si riferisce. L'impedimento non è irreversibile ed è sempre possibile restituire al dato pseudonimizzato la sua attribuibilità mediante l'utilizzo della specifica "chiave". In ciò la pseudonimizzazione si distingue dall'anonimizzazione, che invece spoglia irreversibilmente il dato personale della possibilità di essere attribuito alla persona e lo rende, appunto, dato anonimo[44]. La prima delle misure tecniche e organizzative che il GDPR, all'art. 32, prevede possa essere messa in atto da parte del titolare e del responsabile del trattamento per garantire un livello di sicurezza adeguato al rischio è proprio la pseudonimizzazione. Il dato pseudonimizzato è ancora dato personale e ne conserva il valore, perché l'individuo rimane identificabile, ma il trattamento che si svolge diviene più sicuro[45].

Allo stesso modo si possono intendere le procedure di valutazione del rischio[46]. Nelle

39. Cfr. Gatt–Caggiano–Montanari 2021.
40. Si v. l'art. 25 GDPR, rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".
41. Bravo 2022, p. 85 ss.; Bravo 2019, p. 775 ss. V. anche Calzolaio 2017.
42. Secondo la celebre formula *code is law*, Lessig 1999.
43. Maestri 2015, *passim*.
44. Irti 2022, p. 49 ss.
45. Pellecchia 2020, p. 360 ss., spec. p. 362.
46. Mantelero 2019, p. 473 ss.; Mantelero 2017, p. 287 ss. Cfr. Gruppo Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 ottobre 2017, WP 248 rev.01.

formulazioni del GDPR, la "valutazione dei rischi per i diritti e le libertà degli interessati" è inclusa nella "valutazione d'impatto sulla protezione dei dati", ai sensi dell'art. 35, par. 7, lett. c. Al titolare del trattamento è richiesta la valutazione d'impatto quando il tipo di trattamento da effettuare può presentare un rischio elevato per i diritti e le libertà degli interessati. La procedura contempla il coinvolgimento dell'autorità di controllo, ai sensi dell'art. 36 del GDPR: se la valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio, questi deve procedere con una consultazione preventiva dell'autorità. Peraltro, il par. 5 dell'art. 36 permette agli Stati membri di prescrivere che i titolari consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare, in relazione al corrispondente trattamento per l'esecuzione di un compito di interesse pubblico, come "il trattamento con riguardo alla protezione sociale e alla sanità pubblica2.

Ma soprattutto la funzione di garanzia in ottica preventiva è assegnata al principio di *accountability*, la responsabilizzazione dei soggetti che operano il trattamento dei dati[47]. In virtù di questo principio, ai sensi dell'art. 5, par. 2, del GDPR, il titolare del trattamento è competente per il rispetto di tutti i principi del trattamento dei dati personali, *ex* art. 5, par. 1, ed è in grado di comprovarlo. Nell'ipotesi in cui il trattamento si basi sul consenso dell'interessato, il GDPR, all'art. 7, par. 1, prescrive specificamente – come declinazione della più generale responsabilizzazione del titolare – che questi debba poter dimostrare che il consenso è stato prestato. Ai sensi dell'art. 24, il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, deve adottare le misure tecniche e organizzative che non solo ne garantiscano la conformità al GDPR, ma anche gli consentano di dimostrarla.

Il principio di *accountability* "costituisce il nucleo della riforma europea e realizza un nuovo sistema normativo nel trattamento dei dati personali e nella protezione dei diritti della persona"[48]. Mediante questo principio la tutela della persona, nell'ambito della protezione dei dati personali, si può trasferire dal piano rimediale successivo e della sanzione e dal piano singolare e puntiforme del consenso dell'interessato a quello più generale e preventivo della gestione del rischio. E così acquista nuova centralità la posizione del titolare del trattamento[49]: infatti, egli deve mettere in atto misure appropriate ed efficaci per assicurare la protezione dei dati, in conformità ai principi del GDPR, e deve documentare l'adozione di queste misure, per poter rispondere a una richiesta di dimostrazione[50]. Lungi dal restare una norma meramente programmatica, il principio di *accountability* ha notevoli ricadute pratiche e organizzative, in termini operativi, per le misure concretamente da prendere, e in termini precauzionali, come precostituzione della prova. Quindi vi è un obbligo di sicurezza, gravante sui soggetti che operano il trattamento, titolare e responsabile[51].

47. Camardi 2022, p. 25 ss.; Stanzione 2022, p. 1 ss.; Amram 2020; Finocchiaro 2019, p. 2778 ss. Cfr. Gruppo Articolo 29, *Parere 3/2010 sul principio di responsabilità*, 13 luglio 2010, WP 173.

48. Così Finocchiaro 2019, p. 2778; Finocchiaro 2012, p. 289 ss.

49. Cfr. Messinetti 2019, p. 146: "al ridimensionamento della volontà del titolare dei dati personali fa da contrappunto il rafforzamento di un potere del titolare del trattamento: il diritto – appunto – di trattare i dati personali altrui".

50. Sono i due elementi di cui si compone il principio di *accountability*. V. Gruppo Articolo 29, *Parere 3/2010 sul principio di responsabilità*, cit., 9.

51. In argomento Farace 2019, p. 731 ss. V. anche Sirgiovanni 2020, p. 1013: "In altri termini, la tutela del diritto alla protezione dei dati personali sta non tanto nel negare il consenso al trattamento – in quanto spesso negare il consenso significa non ottenere il servizio – ma piuttosto nel predisporre da parte del titolare del trattamento tutte le misure idonee perché il trattamento del dato sia eseguito nel rispetto dei principi di liceità, correttezza e trasparenza del trattamento, limitando il trattamento alla specifica finalità indicata". Nella prospettiva della legge n. 675 del 1996, Bozzi 1997, p. 97 ss., affronta i profili legati ai soggetti del trattamento, mentre Conte 1997, p. 225 ss., spec. p. 262 ss., mette in relazione gli obblighi di sicurezza con i diritti dei soggetti interessati.

Una buona parte dei trattamenti di dati personali effettuati ha luogo per le attività della pubblica amministrazione e ciò vale in particolar modo per i dati relativi alla salute, considerando che uno dei settori più importanti, forse il principale, in cui essi vengono trattati è proprio quello sanitario. E, se si parla di soggetti pubblici, allora, il campo delle regole non è più – o almeno non è più soltanto – quello del diritto privato, ma è quello del diritto pubblico o, forse, meglio, del diritto amministrativo. Come è stato messo in luce in dottrina, è possibile individuare una funzione amministrativa di protezione dei dati personali, alla quale rispondono le regole volte a disciplinare la pubblica amministrazione e la sua attività là dove vengano in gioco trattamenti di dati[52].

La norma di diritto pubblico che si cala nel contesto della sanità, nella garanzia del diritto alla salute, deve dunque includere la protezione dei dati personali e, specialmente, di quelli sanitari. Come espresso proprio dalla legge Gelli-Bianco, in apertura, all'art. 1, tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative contribuiscono a realizzare la sicurezza delle cure, che è parte costitutiva del diritto alla salute ed è perseguita nell'interesse dell'individuo e della collettività. Con ciò può comprendersi come nella tutela del diritto alla salute vadano ricompresi tutti quei requisiti organizzativi finalizzati a garantire trasparenza ed efficienza delle risorse e implicanti l'uso delle tecnologie[53]. La protezione dei dati personali partecipa quindi del diritto alla salute, come diritto della personalità e nell'orizzonte unitario – concettuale, giuridico – della persona umana.

Perciò si fa preminente la regolazione amministrativistica su quella privatistica. Questo superamento è l'*amministrativizzazione della protezione dei dati personali*[54]. Il fatto che le disposizioni non siano più – o non più tanto – di diritto privato, ma di diritto amministrativo non cambia il modo in cui vadano interpretate, alla luce del principio personalista e della dignità, che irradia l'ordinamento tutto.

5. Il fascicolo sanitario elettronico

Con lo sviluppo della sanità digitale si assiste a un aumento delle attività di trattamento di dati personali in ambito sanitario e quindi di dati relativi alla salute, mediante strumenti tecnologici e informatici. L'incremento delle operazioni di trattamento conferisce importanza maggiore alla normativa in materia di protezione dei dati sanitari.

Da questo punto di vista un plesso normativo in particolare assume grande rilevanza nell'ordinamento italiano, per il carattere applicativo e al contempo sistematico delle sue disposizioni rispetto alla materia della protezione dei dati personali, e cioè la disciplina del fascicolo sanitario elettronico (c.d. FSE)[55]. Si tratta peraltro di una disciplina in costante mutamento, mai assestatasi definitivamente, e anzi oggi in fase di rapidi aggiustamenti, per restare al passo con l'incessante innovazione tecnologica e con l'evoluzione del quadro normativo, specialmente su impulso del diritto eurounitario.

L'art. 12 del d.l. 18 ottobre 2012, n. 179, con cui il FSE fu formalmente istituito, è stato modificato dal legislatore finora per ben undici volte[56]. Le

52. Bombardelli 2022, p. 351 ss. V. anche Franca 2023. Cfr. Carullo 2018.

53. Amram–Comandé 2018, p. 1 ss. Cfr. Alpa 2022, p. 89 ss.

54. Corso 2024, p. 334 ss.; Corso 2023, p. 91 ss. Una amministrativizzazione della protezione dei dati si può osservare anche nel maggior peso dato all'atto amministrativo come fonte del diritto. A tal proposito, si considerino anche le modifiche apportate all'art. 2-*ter* del Codice della privacy ad opera del d.l. n. 139/2021, Francario 2021. Cfr. Francario 2022, p. 679 ss.

55. Sul FSE, senza pretesa di esaustività, v. Capilli 2025, p. 7 ss.; Catelani 2023, p. 423 ss.; Posteraro–Corso 2023, p. 187 ss.; Silvano 2023, p. 228 ss.; Posteraro 2022, p. 187 ss.; Posteraro 2021; Pioggia 2021, p. 215 ss.; Gambino–Maggio–Occorsio 2020; Bottari 2017, p. 65 ss.; Comandé–Nocco–Peigné 2012, p. 105 ss.; Finocchiaro 2012; Guarda 2011; Peigné 2011, p. 1519 ss. V. anche Corso 2020, p. 393 ss.

56. Dopo le modifiche dettate dall'art. 1, comma 1, l. 17 dicembre 2012, n. 221, in sede di conversione, l'articolo è stato ritoccato dall'art. 17, comma 1, lett. a, d.l. 21 giugno 2013, n. 69, convertito, con modificazioni, dalla l. 9 agosto 2013 n. 98. A queste hanno fatto seguito quelle di cui all'art. 1, l. 11 dicembre 2016, n. 232; art. 1, comma 558,

regole dettate dall'art. 12 sono completate da una normativa più dettagliata affidata a più decreti, principalmente del Ministero della salute. Il primo "regolamento" in materia di FSE, infatti, fu dettato dal d.p.c.m. n. 178 del 2015. Le disposizioni ivi contenute sono state poi abrogate dai decreti del Ministero della salute 7 settembre 2023, c.d. "decreto FSE 2.0", e 31 dicembre 2024, il decreto istitutivo dell'ecosistema dati sanitari (c.d. EDS). Nel frattempo, il decreto FSE 2.0 è stato già oggetto di modifiche ad opera del decreto del Ministero della salute 30 dicembre 2024.

Il FSE è un "contenitore" di dati personali e, come tale, di dati personali è alimentato. Ad alimentarlo sono i dati degli eventi clinici presenti e trascorsi riguardanti l'assistito, inerenti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale, in maniera continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie che hanno in cura l'assistito stesso nonché, su iniziativa di quest'ultimo, con i dati medici in suo possesso[57].

Da un esame complessivo delle disposizioni in materia, si evince come l'impiego del FSE consenta di raggiungere plurime finalità. La finalità di cura e assistenziale è solo una di queste, che si aggiunge alla finalità di ricerca e a varie finalità di carattere pubblico. Per il conseguimento degli obiettivi corrispondenti a queste varie finalità ora al FSE si affianca l'EDS, una banca dati in cui confluiscono le informazioni comprese nel FSE, che possono quindi essere gestite separatamente, soprattutto per gli scopi di carattere pubblico. All'assistito sono riconosciuti vari "diritti" ed è attraverso questi che egli vede garantita la propria autodeterminazione. Si pensi al diritto di accesso, che gli consente di avere contezza dei dati e dei documenti caricati nel FSE, o il diritto all'oscuramento, che gli permette di nascondere i referti presenti nel FSE ai professionisti che vi abbiano accesso. Il consenso dell'assistito rileva ai fini della consultazione: egli cioè può acconsentire o negare l'accesso al suo FSE agli esercenti le professioni sanitarie che intendano consultarlo per finalità di diagnosi, cura e riabilitazione, prevenzione, profilassi internazionale.

Ma la disciplina del FSE è emblematica del nuovo modo di intendere il consenso proprio perché consente trattamenti di dati personali e di dati sanitari a prescindere dal consenso dell'interessato stesso. Infatti, il comma 3-*bis*[58] dell'art. 12 d.l. n. 179/2012, secondo cui "il FSE può essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo", è stato abrogato dal d.l. n. 34/2020[59]. La scelta di procedere all'abrogazione cancellando il requisito del consenso è in linea con le affermazioni del Garante per la protezione dei dati personali, che nel provvedimento del 7 marzo 2019, n. 55 aveva ammesso, forse un po' frettolosamente, la possibile eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del fascicolo. La posizione del Garante si basava sul quadro normativo rinnovato, a seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati e del d.lgs. n. 101/2018, di adeguamento delle disposizioni contenute nel Codice della privacy[60].

Si può notare dunque come la previsione dell'interesse pubblico rilevante e dell'interesse pubblico nel settore della sanità pubblica, tra le eccezioni al divieto di trattamento di dati sanitari,

l. 30 dicembre 2018, n. 145; art. 3, l. 22 marzo 2019, n. 29; art. 11, d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77; art. 21, d.l. 27 gennaio 2022, n. 4, convertito, con modificazioni, dalla l. 28 marzo 2022 n. 25; art. 42, comma 1, lett. *a*, d.l. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56; art. 36, comma 2, d.lgs. 3 maggio 2024, n. 62. Invece la l. 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", all'art. 10 introduce l'art. 12-*bis* del d.l. 179/2012, per regolare aspetti dell'intelligenza artificiale nel settore sanitario.

57. V. art. 12, commi 1 e 3, d.l. n. 179/2012.

58. Introdotto dall'art. 1, comma 1, l. 17 dicembre 2012, n. 221, in sede di conversione.

59. Gambino–Maggio–Occorsio 2020. L'abrogazione, precisamente, si è avuta ad opera dell'art. 11, comma 1, lett. *d*, d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77. Al riguardo v. Miccú 2021, p. 11 ss.; Covino 2021, p. 66 ss.; Sorrentino–Spagnuolo 2020, p. 251.

60. Cuttaia 2021, p. 195 ss., spec. p. 200 s.; Foglia 2020, p. 43 ss. Sia concesso il rinvio a Corso 2019, p. 225 ss.

possa tradursi in una valvola di apertura, quasi una clausola generale, in grado di oltrepassare il divieto ex art. 9 par. 1 GDPR, al ricorrere del generale elemento pubblicistico. La protezione dei dati personali – e specialmente relativi alla salute – si connota, quindi, sempre più come materia di diritto pubblico e amministrativo, perdendo rilievo la connotazione privatistica che la descriveva sostanzialmente come un diritto dei singoli, come una questione di riserbo o un affare tra privati. La tutela della persona – e lo si può intendere anche dall'evoluzione del FSE – è affidata, dunque, al piano della sicurezza, che concretamente andrà garantita e implementata dai titolari del trattamento.

La garanzia dell'autodeterminazione permane – e con essa un'area di autonomia, che restituisce spazio al diritto privato – nel novero dei diritti dell'interessato e dell'assistito, pur con tutti i grossi limiti dell'attuale assetto normativo. Si pensi, ad esempio, ai limiti che incontra indistintamente il diritto alla cancellazione, sancito dall'art. 17 GDPR, là dove si tratti di trattamenti di dati necessari per motivi di interesse pubblico nel settore della sanità pubblica (par. 3, lett. c, dell'art. 17)[61]. L'assunto circa il rilievo dei diritti riconosciuti al singolo, in chiave di autodeterminazione rispetto al trattamento di dati relativi alla salute, trova riscontro nella nuova disciplina dello spazio europeo dei dati sanitari, dettata dal reg. Ue n. 327 del 2025.

6. Lo spazio europeo dei dati sanitari

Il Regolamento UE 2025/327 dell'11 febbraio 2025, pubblicato nella Gazzetta Ufficiale dell'Unione europea il 5 marzo 2025, ha istituito lo *European Health Data Space* (c.d. EHDS), lo spazio europeo dei dati sanitari. Nuova tappa del percorso del diritto della tecnologia, il Regolamento sull'EHDS rappresenta il frutto di un impegno che dura da anni per realizzare, sul piano giuridico, un ambiente digitale sicuro in cui trattare dati sanitari, essenziale per la digitalizzazione della sanità. Esso si colloca primariamente nell'ambito della strategia europea dei dati, ma al contempo rappresenta un elemento fondamentale dell'Unione europea della salute[62].

L'istituzione dell'EHDS si compie, come espresso dall'art. 1, par. 1, del reg. UE n. 327 del 2025, con la previsione di "disposizioni, norme e infrastrutture comuni e un quadro di governance al fine di facilitare l'accesso ai dati sanitari elettronici per l'uso primario dei dati sanitari elettronici e l'uso secondario di tali dati". La creazione dell'EHDS è diretta a garantire a ciascuno un accesso semplice e immediato ai propri dati sanitari in formato elettronico, un'agevole loro condivisione con i professionisti sanitari, anche in Stati membri diversi, e un controllo sui dati stessi, in una cornice di interoperabilità e sicurezza. Ha anche lo scopo di favorire un mercato unico per i sistemi di cartelle cliniche elettroniche e di delineare un quadro giuridico coerente, affidabile ed efficiente per riutilizzare i dati sanitari in ambito pubblico, come per la ricerca, l'innovazione, la determinazione delle politiche. Le finalità perseguite sono in realtà molteplici, ma possono simbolicamente raggrupparsi in due categorie, che strutturano l'intero Regolamento: l'*uso primario* e l'*uso secondario*. In estrema sintesi l'uso primario è l'utilizzo dei dati per l'assistenza sanitaria e i servizi connessi, mentre l'uso secondario è l'impiego dei dati per finalità diverse dalle finalità iniziali per cui i dati sono stati raccolti o prodotti.

Il Regolamento sull'EHDS si pone espressamente in relazione con il GDPR, a sua integrazione e specificazione, come enunciato all'art. 1. Inoltre, secondo il par. 3 dell'art. 1, esso "lascia impregiudicati gli altri atti giuridici dell'Unione relativi all'accesso ai dati sanitari elettronici, alla loro condivisione o al loro uso secondario o le prescrizioni dell'Unione relative al trattamento dei dati in relazione ai dati sanitari elettronici" e, in particolare, lascia "impregiudicato" il reg. Ue n. 679 del 2016. La disciplina dettata dal GDPR continua dunque a trovare applicazione, senza modifiche. Tuttavia, in relazione al trattamento di dati sanitari elettronici prende corpo un assetto normativo di dettaglio.

Le definizioni stesse, fornite dall'art. 2 del Regolamento sull'EHDS, poggiano, in buona parte, su quelle rese dal GDPR. Spicca, per il rilievo assunto nell'ambito dell'EHDS e in relazione alla protezione dei dati personali, la definizione di "dati sanitari elettronici personali", di cui all'art. 2, par. 2, lett. a, cioè "i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico". Non

61. C. Perlingieri 2022, p. 127 ss.

62. Catanzariti 2025; Morace Pinelli 2025-a, p. 1016 ss.; Morace Pinelli 2025-b; Slokenberga–Ó Cathaoir–Shabani 2025; C. Perlingieri 2024, p. 485 ss. Sia consentito di rinviare a Corso 2025, p. 563 ss.

vi è identità quindi tra la nozione di "dati sanitari elettronici" – che possono essere anche dati non personali – e quella di "dati relativi alla salute". Il formato elettronico, che è elemento attinente alla modalità di trattamento, individua una sottocategoria di dati personali sensibili ai quali si applica la specifica disciplina del reg. Ue n. 327 del 2025. Come espresso al considerando 7, l'impiego per via elettronica di dati sanitari è comune e funzionale ai sistemi sanitari nazionali, in cui vengono raccolti tramite le cartelle cliniche elettroniche, "che solitamente contengono l'anamnesi di una persona fisica, diagnosi e cure, medicinali, allergie e vaccinazioni, nonché immagini radiologiche, risultati di laboratorio e altri dati medici, distribuiti tra i diversi soggetti del sistema sanitario, quali medici di base, ospedali, farmacie o servizi di assistenza". Poiché i dati sanitari elettronici personali vengono definiti come un sottoinsieme di dati relativi alla salute ed essendo questi dati personali appartenenti alle categorie particolari, valgono per il loro trattamento le regole dettate dal GDPR per i dati sensibili, ossia il divieto generale, derogato nelle ipotesi espressamente previste. Si rinfrancano così l'incisività e l'estensione dell'interesse pubblico come legittimazione del trattamento dei dati personali, espressa dagli artt. 6, par. 1, lett. e, e 9, par. 2, lett. g, del reg. Ue n. 679 del 2016, esplicitamente menzionati dal reg. Ue n. 327 del 2025.

Tra le norme più significative del Regolamento sull'EHDS vi è il riconoscimento del diritto delle persone fisiche all'*esclusione*, verso il trattamento di propri dati sanitari elettronici personali. L'EHDS contempla quindi la possibilità che gli interessati esercitino un *opt-out*, rispetto allo spazio europeo stesso. Punto di equilibrio fra le esigenze della collettività all'utilizzo dei dati sanitari e le istanze di tutela del singolo, esso rappresenta un contemperamento funzionale tanto all'uso primario quanto all'uso secondario dei dati sanitari elettronici, nel rispetto delle libertà e dei diritti fondamentali della persona. Il diritto all'esclusione consiste nel diritto a che siano impediti l'accesso ai propri dati sanitari elettronici e la loro messa a disposizione per i servizi dell'EHDS. Aggiungendosi ai diritti dell'interessato[63], esso contribuisce sensibilmente a garantire l'autodeterminazione del soggetto rispetto ai trattamenti di dati sanitari che lo riguardino, pur se non comporta una cancellazione dei dati stessi, che invece sembrano permanere all'interno dell'EHDS.

Nodale, in ordine all'uso secondario dei dati sanitari elettronici, è il ruolo svolto dall'autorizzazione ai dati, che l'organismo responsabile rilascia, ai sensi dell'art. 68, sulla base della domanda e a seguito della valutazione di una serie di requisiti. Secondo la definizione dell'art. 2, par. 2, lett. v, la "autorizzazione ai dati", è "una decisione amministrativa": è chiaro qui il senso della amministrativizzazione della protezione dei dati.

Nel complesso, le nuove disposizioni raffigurano uno scenario ancora futuro – l'applicazione del reg. Ue n. 327 del 2025, infatti, è rinviata a partire dal 2027, con differenti scaglioni per più fasi temporali – per certi versi avveniristico – in quanto si coniuga con lo sviluppo delle tecnologie più nuove, come l'intelligenza artificiale, e quelle tuttora ignote che saranno fatte proprie dalla sanità digitale – ove trova valorizzazione il bisogno superindividuale legato al trattamento dei dati sanitari, di cui si fa portatrice l'amministrazione pubblica, ma sempre con l'osservanza dei diritti del singolo. L'EHDS si connota dunque, da un lato, per il rapporto diretto e speciale con la disciplina della protezione dei dati personali e, dall'altro, per la concezione del dato sanitario come di una informazione destinata a circolare e che *dovrà* circolare, eventualmente anche a prescindere dalla posizione del soggetto cui le informazioni stesse si riferiscono. L'avvento dell'EHDS conferma la fine del consenso al trattamento dei dati personali come strumento di tutela per eccellenza del soggetto dinanzi al fenomeno circolatorio dei dati e lo fa in relazione non a una categoria qualsiasi di dati, bensì rispetto proprio ai dati che più di tutti potrebbero astrattamente pregiudicare l'individuo stesso, se trattati. Le norme del GDPR non vengono toccate, ma trovano sviluppi proprio là dove ottimizzano la circolazione dei dati per ragioni di interesse pubblico. Ciò non significa che il consenso non svolga più alcun ruolo e non significa nemmeno che la volontà del soggetto non possa valere nell'esercizio dei suoi diritti soggettivi. Anzi, attraverso le norme nuove, che arricchiscono le situazioni giuridiche del soggetto interessato, si possono cogliere nuove sfumature dell'autodeterminazione della persona.

63. Cfr. Faillace 2025, p. 379 ss. V. anche Cacace 2025, p. 333 ss.

Il quadro giuridico che si staglia così all'orizzonte, seppur comunque perfettibile, racchiude il bilanciamento fra l'interesse di carattere pubblico, all'impiego dei dati sanitari, e quello di carattere privato, in capo ai singoli, che è anche interesse dei pazienti alla cura migliore. Spetterà all'interpretazione ricondurre queste disposizioni alla coerenza del sistema, conferendo ad esse il significato più corretto nel rispetto dei principi dell'ordinamento e illuminando il percorso ancora da seguire, verso la garanzia più effettiva della dignità della persona[64].

Riferimenti bibliografici

G. Alpa (2022), *Salute e medicina*, in G. Alpa (a cura di),"La responsabilità sanitaria. Commento alla l. 8 marzo 2017, n. 24", 2ª ed., Pacini, 2022

G. Alpa (2021), *sub art. 1, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

D. Amram (2020), *Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks*, in "Computer Law & Security Review", vol. 37, 2020

D. Amram, G. Comandé (2018), *Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla protezione dei dati personali UE/679/2016 e dalla legge n. 24/2017*, in "Rivista italiana di medicina legale", 2018

M. Bombardelli (2022), voce *Dati personali (tutela dei)*, in "Enciclopedia del diritto. I tematici. III, Funzioni amministrative", Giuffrè, 2022

C. Bottari (2017), *L'inquadramento costituzionale del Fascicolo Sanitario Elettronico*, in "Salute e società", 2017, n. 2

L. Bozzi (1997), *I soggetti coinvolti nell'attività di trattamento*, in V. Cuffaro,V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

F. Bravo (2022), *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

F. Bravo (2019), *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

L.A. Bygrave (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002

S. Cacace (2025), *Autodeterminazione, paternalismo e responsabilità: l'uso primario dei dati sanitari nella relazione di cura e di fiducia fra medico e paziente*, in "Responsabilità medica", 2025

F. Caggia (2007), *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "Il codice del trattamento dei dati personali", Giappichelli, 2007

V. Calderai (2015), voce *Consenso informato*, in "Enciclopedia del diritto, Annali VIII", 2015

64. "È indubitabile che i dati dei pazienti rappresentano una risorsa di valore inestimabile per la ricerca e per la migliore cura, ma è altrettanto palese che è necessario che vi sia un contesto, normativo e fattuale, all'interno del quale sia realmente possibile valorizzarli in tutta la loro potenzialità, salvaguardando nel contempo il rispetto dei diritti della persona. In questa prospettiva è dunque indispensabile perseguire e realizzare un corretto equilibrio tra i diversi diritti e interessi, individuando la loro possibile conciliazione non in termini astratti, ma sulla base delle esperienze concrete", Sandulli 2023, p. 4.

S. Calzolaio (2017), Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in "federalismi.it", 2017, n. 24

C. Camardi (2022), *Liability and Accountability in the 'Digital' Relationships*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

G. Capilli (2025), *Diritto privato sanitario. Fondamenti*, 2ª ed., Pacini, 2025

G. Carullo (2018), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018

M. Catanzariti (a cura di) (2025), *Lo spazio europeo dei dati sanitari: una riflessione interdisciplinare su diritto, etica e scelte pubbliche*, in "Notizie di Politeia", 2025, n. 158

E. Catelani (2023), *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in "Corti supreme e salute", 2023

G. Comandé (2008), *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, in F. Ruscello (a cura di), "Studi in onore di Davide Messinetti", I, Edizioni Scientifiche Italiane, 2008

G. Comandé, L. Nocco, V. Peigné (2012), *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in "Rivista italiana di medicina legale", 2012

G. Conte (1997), *Diritti dell'interessato e obblighi di sicurezza*, in V. Cuffaro, V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

S. Corso (2025), *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in "Nuove leggi civili commentate", 2025, n. 3

S. Corso (2024), *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in "Nuove leggi civili commentate", 2024, n. 2

S. Corso (2023), *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in A. Thiene, S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

S. Corso (2020), *Il fascicolo sanitario elettronico fra* e-Health, privacy *ed emergenza sanitaria*, in "Responsabilità medica", 2020

S. Corso (2019), *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali*, in "Responsabilità medica", 2019

F. Cortese (2021), *sub art. 2 sexies, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

F. Covino (2021), *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in "federalismi.it", 2021, n. 5

V. Cuffaro (2018), *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in "Corriere giuridico", 2018

V. Cuffaro (1997), *Il consenso dell'interessato*, in V. Cuffaro,V. Ricciuto (a cura di), "La disciplina del trattamento dei dati personali", Giappichelli, 1997

F.G. Cuttaia (2021), *The impact of EU Regulation 2016/679 on the Italian health system*, in G. Fares (ed.), "The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis", Giappichelli, 2021

F. Di Ciommo (2002), *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in "Danno e responsabilità", 2002

M. Di Masi (2021), *sub art. 75, d.lgs. 30 giugno 2003, n. 196*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

S. Faillace (2025), *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo Regolamento EHDS*, in "Contratto e impresa", 2025

D. Farace (2019), *Il titolare e il responsabile del trattamento*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

G. Fares (2021), *The processing of personal data concerning health according to the EU Regulation*, in G. Fares (ed.), "The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis", Giappichelli, 2021

G. Finocchiaro (2019), *Il principio di* accountability, in R. Caterina (a cura di), "GDPR tra novità e discontinuità", in "Giurisprudenza italiana", 2019

G. Finocchiaro (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012

G. Finocchiaro (2008), *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. Ferrari (a cura di), "La legge sulla privacy dieci anni dopo", Egea, 2008

M. Foglia (2020), *Patients and privacy: GDPR compliance for healthcare organizations*, in "European Journal of Privacy Law & Technologies", 2020, Special Issue

M. Foglia (2018), *Consenso e cura. La solidarietà nel rapporto terapeutico*, Giappichelli, 2018

S. Franca (2023), *I dati personali nell'amministrazione pubblica: attività di trattamento e tutela del privato*, Università degli studi di Trento, 2023

F. Francario (2022), *Protezione dei dati personali e pubblica amministrazione*, in C. Pisani, G. Proia, A. Topo (a cura di), "Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", Giuffrè, 2022

F. Francario (2021), *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse*, in "www.giustiziainsieme.it", 26 ottobre 2021

A.M. Gambino, E. Maggio,V. Occorsio (2020), *La riforma del fascicolo sanitario elettronico*, in "www.dimt.it", 22 luglio 2020

L. Gatt, I.A. Caggiano, R. Montanari (ed.) (2021), *Privacy and consent. A legal and UX&HMI approach for data protection*, Università degli Studi Suor Orsola Benincasa, 2021

L. Georgieva, C. Kuner (2020), *sub art. 9*, in C. Kuner, L.A. Bygrave, C. Docksey (eds.), "The EU General Data Protection Regulation (GDPR). A Commentary", Oxford University Press, 2020

M. Granieri (2017), *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in "Nuove leggi civili commentate", 2017

L. Greco (2019), *Sanità e protezione dei dati personali*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

P. Guarda (2019), *I dati sanitari*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

P. Guarda (2011), *Fascicolo Sanitario Elettronico e protezione dei dati personali,* Università degli Studi di Trento, 2011

P. Iamiceli (2024), *Consenso al trattamento e giurisprudenza europea: tra tutela dei diritti fondamentali e giustizia contrattuale*, in S. Orlando (a cura di), "Libertà e liceità del consenso nel trattamento dei dati personali", Persona e Mercato, 2024

C. Irti (2022), *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

L. Lessig (1999), *Code and Other Laws of Cyberspace*, Basic Books, 1999

E. Maestri (2015), *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*, Edizioni Scientifiche Italiane, 2015

A. Mantelero (2019), *La gestione del rischio*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

A. Mantelero (2017), *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

M. Mantovani (2019), *Introduzione l. n. 219/2017*, in A. Barba, S. Pagliantini (a cura di), "Delle persone. Leggi collegate", II, nel "Commentario del Codice civile", diretto da E. Gabrielli, Utet, 2019

R. Messinetti (2019), *Circolazione dei dati personali e autonomia privata*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam, 2019

R. Miccú (2021), *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in "federalismi.it", 2021, n. 5

G. Mirabelli (1993), *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in "Diritto dell'informazione e dell'informatica", 1993

A. Morace Pinelli (2025-a), *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in "Nuova giurisprudenza civile commentata", 2025, n. 2

A. Morace Pinelli (a cura di) (2025-b), *Sanità digitale – Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. I. Uso dei dati e assetti organizzativi*, Pacini, 2025

S. Patti (1999), *Il consenso dell'interessato al trattamento dei dati personali*, in "Rivista di diritto civile", 1999, n. 2

V. Peigné (2011), *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in "Rivista italiana di medicina legale", 2011, n. 6

E. Pellecchia (2020), *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in "Nuove leggi civili commentate", 2020, n. 2

C. Perlingieri (2024), *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici,* in "Tecnologie e diritto", 2024

C. Perlingieri (2022), *eHealth and Data*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

P. Perlingieri (2020), *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, 4ª ed., Edizioni Scientifiche Italiane, 2020

P. Perlingieri (2018), Privacy *digitale e protezione dei dati personali tra persona e mercato*, in "Foro napoletano", 2018, n. 2

P. Perlingieri (2003), *La pubblica amministrazione e la tutela della* privacy. *Gestione e riservatezza dell'informazione nell'attività amministrativa*, in "Annali della Facoltà di Economia dell'Università degli Studi del Sannio", 2003, n. 8

P. Perlingieri (1972), *La personalità umana nell'ordinamento giuridico*, Edizioni Scientifiche Italiane, 1972

A. Pioggia (2021), *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. Cavallo Perin (a cura di), "L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale", Università degli studi di Torino, 2021

A. Pioggia (2011), *Consenso informato ai trattamenti sanitari e amministrazione della salute*, in "Rivista trimestrale di diritto pubblico", 2011, n. 1

F. Piraino (2017), *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in "Nuove leggi civili commentate", 2017, n. 2

F. Pizzetti (2021), *Il procedimento italiano di adeguamento al GDPR e la struttura del Codice novellato*, in F. Pizzetti (a cura di), "Protezione dei dati personali in Italia tra GDPR e codice novellato", Giappichelli, 2021

D. Poletti (2007), *sub art. 75*, in C.M. Bianca, F.D. Busnelli (a cura di), "La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy", Cedam, 2007

N. Posteraro (2022), *Il fascicolo sanitario elettronico,* in V. Bontempi (a cura di), "Lo Stato digitale nel Piano nazionale di ripresa e resilienza", Università degli Studi Roma Tre, 2022

N. Posteraro (2021), *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in "federalismi.it", 2021, n. 26

N. Posteraro, S. Corso (2023), *The Italian Electronic Health Record (EHR)*, in "European Review of Digital Administration & Law", vol. 4, 2023, n. 1

R. Pucella (2010), *Autodeterminazione e responsabilità nella relazione di cura,* Giuffrè, 2010

G. Resta (2006), *Le nuove dimensioni dei diritti della personalità,* in G. Alpa, G. Resta, "Le persone e la famiglia", I, "Le persone fisiche e i diritti della personalità", nel *Trattato di diritto civile*, diretto da F. Sacco, Utet, 2006

G.M. Riccio (2004), Privacy *e dati sanitari*, in F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura di), "Il codice dei dati personali. Temi e problemi", Giuffrè, 2004

S. Rodotà (2010), *Il nuovo* habeas corpus*: la persona costituzionalizzata e la sua autodeterminazione*, in S. Rodotà, M. Tallacchini (a cura di), "Ambito e fonti del biodiritto", nel "Trattato di biodiritto" diretto da S. Rodotà e P. Zatti, Giuffrè, 2010

M.A. Sandulli (2023), *Introduzione*, in A. Thiene e S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

M.A. Sandulli, F. Aperio Bella (a cura di) (2021), *Shaping the Future of Health Law: Challenges for Public Law*, in "federalismi.it", 17 novembre 2021

R. Senigaglia (2023), *Telemedicina ed essenza fiduciaria del rapporto di cura*, in "Persona e mercato", 2023, n. 3

S. Sica (2001), *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in "Rivista di diritto civile", 2001, n. 2

C. Silvano (2023), *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in "federalismi.it", 2023, n. 26

B. Sirgiovanni (2020), *Dal consenso dell'interessato alla "responsabilizzazione" del titolare del trattamento dei dati genetici*, in "Nuove leggi civili commentate", 2020, n. 4

S. Slokenberga, K. Ó Cathaoir, M. Shabani (eds.) (2025), *The European Health Data Space. Examining A New Era in Data Protection*, Routledge, 2025

E. Sorrentino, A.F. Spagnuolo (2020), *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in "federalismi.it", 2020, n. 30

M.G. Stanzione (2022), *La protezione dei dati personali tra «consumerizzazione» della* privacy *e principio di* accountability, in "Comparazione e diritto civile", 2022

A. Thiene (2023), *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR*, in A. Thiene, S. Corso (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

A. Thiene (2021), *sub art. 9, reg. Ue n. 679/2016, I. Profili generali*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

A. Thiene, S. Corso (a cura di) (2023), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Jovene, 2023

E. Tosi (2019), *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del* nuovo *Codice Privacy*, in E. Tosi (a cura di), "Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy", Giuffrè, 2019

A.F. Westin (1976), *Computers, Health Records and Citizen Rights*, U.S. Government Printing Office, 1976

V. Zambrano (1999), *Dati sanitari e tutela della sfera privata*, in "Diritto dell'informazione e dell'informatica", 1999, n. 1

F. Zanovello (2023), *Misure di garanzia e rischio di* data breach *in ambito sanitario*, in A. Thiene, S. Corso, (a cura di), "La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza", Jovene, 2023

F. Zanovello (2021), *sub art. 2- septies, d.lgs. n. 196 del 2003*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e *data protection*", Giuffrè, 2021

P. Zatti (2019), *Brevi note sull'interpretazione della legge n. 219 del 2017*, in "Nuove leggi civili commentate", 2019, n. 1

P. Zatti (2018), *Spunti per una lettura della legge sul consenso informato e DAT*, in "Nuova giurisprudenza civile commentata", 2018, n. 1

P. Zatti (2009), *Maschere del diritto volti della vita*, Giuffrè, 2009