

FIDELIA CASCINI - MARIA ANASTASIA ARCURI

USO SECONDARIO DEI DATI PERSONALI RELATIVI ALLA SALUTE: PANORAMICA DELLA NORMATIVA EUROPEA E NAZIONALE

SOMMARIO: 1. Introduzione. — 2. Dati personali, sanitari e genomici. — 3. Trattamento dei dati sanitari personali. — 4. Cornice normativa europea e nazionale. — 4.1. Il Regolamento per la Protezione dei Dati Personali. — 4.2. La protezione dei dati personali in Italia. — 4.3. Il Data Governance Act. — 4.4. Il Regolamento sullo Spazio Europeo dei Dati Sanitari. — 5. Titolarità per finalità secondarie. — 6. Finalità d'interesse pubblico. — 7. Finalità di ricerca scientifica. — 8. D.L. 249/2023 in materia di Fascicolo Sanitario Elettronico. — 9. Riflessioni conclusive.

1. INTRODUZIONE.

L'esigenza di creare e sperimentare tecnologie per la salute sempre più all'avanguardia e il bisogno di sviluppo della ricerca clinica trovano soddisfazione nella disponibilità di dati personali sanitari (soprattutto quando si tratta di Big Data in sanità)¹, i quali assumono un ruolo primario per il miglioramento dei sistemi sanitari nell'erogare servizi di cura, nel fornire assistenza ai cittadini e nel sostenere attività di ricerca e sviluppo della scienza medica oltre che in ambito di medicina personalizzata².

* Fidelity Cascini, Università Cattolica del Sacro Cuore, Roma. Maria Anastasia Arcuri, Università degli Studi di Roma "Tor Vergata". Il lavoro è frutto della riflessione congiunta tra le due autrici, sebbene Fidelity Cascini abbia materialmente curato la stesura dei paragrafi 4, 4.3, 4.4, 5, 7 e 9 e Maria Anastasia Arcuri quella dei paragrafi 1, 2, 3, 4.1, 4.2, 6 e 8.

¹ Per la Commissione Europea « I Big Data in sanità si riferiscono a grandi set di dati raccolti periodicamente o automaticamente, che vengono archiviati elettronicamente, riutilizzabili allo scopo di migliorare

le prestazioni del sistema sanitario ». European Commission, *Study on Big Data in Public Health, Telemedicine and Healthcare*, December 2016 in [chrome-extension://efaidnbmnnnibpcajpcgglefindmkaj/https://health.ec.europa.eu/system/files/2016-12/bigdata_report_en_0.pdf](https://efaidnbmnnnibpcajpcgglefindmkaj/https://health.ec.europa.eu/system/files/2016-12/bigdata_report_en_0.pdf).

² La Commissione Europea, nel 2016, sostenne il lancio dell'International Consortium for Personalised Medicine (ICPerMed) per promuovere l'attuazione della medicina personalizzata. Per tutte le iniziative e le attività internazionali a supporto dello sviluppo della medicina personalizzata si rimanda a ICPerMed, *State of the Art Report*

Sotto il profilo legislativo, a partire dagli anni novanta l'UE si è adoperata per offrire garanzie e tutelare i dati che consentano di individuare le persone a cui sono riferiti (dati personali), intervenendo direttamente attraverso la promulgazione di raccomandazioni, direttive e regolamenti. A partire dagli stessi anni, anche l'Italia ha dedicato crescente attenzione al tema. Si sono così susseguiti importanti interventi normativi sia a livello europeo che nazionale, in materia del trattamento dei dati personali relativi alla salute delle persone fisiche ³.

Il primo intervento dell'UE si è avuto con la direttiva 95/46/CE ⁴, che all'art. 8 disciplina la materia riguardante le categorie particolari di dati, disponendo il divieto di trattamento dei dati che possono rivelare lo stato di salute di un soggetto, con l'eccezione per le finalità di cura. Lo stesso art. 8, al par. 3, ha infatti previsto una deroga particolare, in quanto statuisce che il divieto di trattamento dei dati sanitari non si applica “[...] quando il trattamento dei dati è necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando il trattamento dei medesimi dati viene effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale comprese le norme stabilite dagli organi nazionali competenti [...]”.

L'Italia, per adeguarsi alla direttiva europea, è intervenuta sulla tutela dei dati sanitari con la legge n. 675 del 31 dicembre 1996 ⁵, che agli artt. 22 e 23 disciplina i dati sensibili annoverando tra questi quelli “idonei a rivelare lo stato di salute”. Sulla base

2023, in *chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://www.icpermed.eu/media/content/SotA_report_2023.pdf*.

³ Per alcune riflessioni sulla disciplina dei dati personali sanitari, quali dati che rivelano l'identità e le condizioni di malattia delle persone, si v. A. THIENE, S. CORSO (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Jovene, Napoli 2023; C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, in *Dirittifondamentali.it*, 2019 in *chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://dirittifondamentali.it/wp-content/uploads/2019/07/Colapietro-Laviola-I-trattamenti-di-dati-personali-in-ambito-sanitario.pdf*; G. FARES, *I dati relativi alla salute e i trattamenti in ambito sanitario*, in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, pag. 444 e ss.; C. FILIPPI, S. MELCHIONNA, *I trattamenti*

di dati in ambito sanitario, in *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Aracne, Roma, 2016, pag. 469 e ss.; G. M. RICCIO, *Privacy e dati sanitari*, in *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004, pag. 247 e ss.; M. L. RIZZO, *La disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, in *La tutela dei dati personali in ambito sanitario*, Giuffrè Francis Lefebvre, Milano, 2020, pagg. 1-24; P. GUARDA, *I dati sanitari*, in *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, pagg. 591-626.

⁴ Per la normativa si v. <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A31995L0046>.

⁵ Viene considerata la prima legge italiana in materia di riservatezza. Per la normativa si v. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1996-12-31:675>. Per approfondimenti si v. C. M. BIANCA, F. D. BUSNELLI (a cura di), *Tutela dei dati personali. Commentario alla L. 31 dicembre 1996, n. 675*, CEDAM, Padova, 1999.

di tale disposizione normativa, vengono identificati come dati sensibili quei dati che possono intaccare la riservatezza di un individuo e che, per questo motivo, non possono essere trattati a meno che non ci sia un consenso espresso dal soggetto interessato. Dall'art. 23, comma 1, della legge 675/1996 emerge che sono autorizzati a procedere al trattamento di dati personali dai quali potrebbero evincersi informazioni sullo stato di salute di una persona fisica, coloro che esercitano professioni sanitarie nonché organismi sanitari pubblici anche senza l'autorizzazione del Garante per la protezione dei dati personali.

Successivamente, il d.lgs. n. 196 del 30 giugno 2003 (Codice Privacy)⁶ ha apportato modifiche alla legge 675/1996 e ha disciplinato espressamente la materia relativa al trattamento dei dati sanitari, rendendo lo stesso trattamento realizzabile sia per mano degli operatori del ramo sanitario e sia per mano degli organismi sanitari pubblici⁷. Il legislatore del 2003 ha, poi, attribuito un grande valore al consenso dell'interessato⁸, ritenendolo il presupposto legittimante e la condizione di liceità del trattamento dei dati personali. In virtù di ciò, è stato reso possibile il trattamento dei dati sensibili, e di conseguenza dei dati sanitari, previo consenso del soggetto interessato anche senza l'autorizzazione del Garante per la protezione dei dati personali.

La materia riguardante i dati personali e la loro protezione è stata poi unificata, a livello europeo, dal regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR)⁹, che ha abrogato la direttiva 95/45/CE e che è stato recepito in Italia con il d.lgs. n. 101 del 10 agosto 2018¹⁰, il quale ha, a sua volta, apportato modifiche al Codice privacy del 2003.

Attualmente, in Italia, il corpo normativo riguardante la protezione dei dati personali esprime le evoluzioni che, nel corso del tempo, si sono succedute, temperando al suo interno aspetti del trattamento dei dati differenti dall'originaria base europea e interpretazioni correlate agli interventi dell'Autorità Garante per la protezione dei dati personali, così esprimendo tratti giuridici propri.

⁶ Per la normativa si v. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196>. Per il commentario a questa normativa si v. 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, Padova, 2007.

⁷ Cioè coloro che, in base alla disposizione dell'art. 23 della L. 675/1996, erano destinatari del trattamento.

⁸ Per approfondire il tema del consenso dell'interessato al trattamento dei suoi dati personali si v. A. FICI, E. PELLECCIA, *Il*

consenso al trattamento, in *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003, pag. 469 e ss.; F. A. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, in *La circolazione dei dati personali. Persona, contratto e mercato*, Pacini Giuridica, Pisa, 2023, pag. 81 e ss.

⁹ Per la normativa si v. <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=cellex%3A32016R0679>.

¹⁰ Per la normativa si v. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018;101-art1>.

In particolare, si segnala la recente modifica italiana del comma 1 dell'art. 110 del Codice Privacy con il d.l. n. 19 del 2 marzo 2024, di cui scriveremo nei prossimi paragrafi, che rappresenta un'evoluzione per il tratta/mento dei dati personali sanitari in ambito di ricerca scientifica.

Altre norme europee hanno preso le mosse dal GDPR riguardando specificatamente il trattamento dei dati personali per finalità secondarie, con particolare riferimento ai dati sanitari: il regolamento (UE) 868 del 30 maggio 2022 (Data Governance Act — DGA) ¹¹ e il regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS) ¹², prossimo all'entrata in vigore.

2. DATI PERSONALI, SANITARI E GENOMICI.

Il regolamento n. 679/2016 (General Data Protection Regulation - GDPR) fornisce le definizioni ufficiali di dato personale, di dato relativo alla salute e introduce, per la prima volta, anche la definizione di dato genetico. Prima dell'emanazione del GDPR, in Europa, il dato genetico non veniva considerato quale dato sensibile, mentre, in Italia, il d.lgs. n. 196/2003 (Codice Privacy) ha sempre ricondotto il dato genetico al dato sanitario. Nello specifico, l'art. 4 del GDPR definisce dato personale “[...] qualsiasi informazione riguardante una persona fisica identificata o identificabile [...]”, dati relativi alla salute “[...] i dati personali attinenti alla salute fisica • mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute[...]” e dati genetici “[...] i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione [...]” ¹³.

I considerando 34 e 35 del GDPR, in relazione ai dati sanitari, ritengono che negli stessi “[...] dovrebbero rientrare tutti i dati

¹¹ Per la normativa si v. <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R0868>. Per una riflessione critica si rimanda al lavoro coordinato scientificamente da F. CASCINI, *Linee di indirizzo per l'applicazione al settore della Salute del Regolamento (UE) 2022/868 sulla Governance dei Dati: focus riutilizzo dei dati sanitari*, Atti del Progetto Net Health-Sanità in Rete 2030, 7 maggio 2024, Senato della Repubblica, Roma.

¹² Proposta di regolamento sullo spazio europeo dei dati sanitari (EHDS) COM (2022) 197, accompagnata dalla Comunicazione della Commissione dal titolo *Uno spa-*

zio europeo dei dati sanitari: sfruttare il potenziale dei dati sanitari per le persone, i pazienti e l'innovazione, COM (2022) 196 in <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197>.

¹³ Regolamento UE 2016/679 (GDPR), art. 4, numeri 1), 13), 15). Per un approfondimento sulla materia dei dati personali nel GDPR si v. M. MAGGIO, *Il regolamento europeo 2016/679 in materia di dati personali. Inquadramento generale e prospettive di sviluppo*, in *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento Ue 2016/679*, Maggioli, Santarcangelo di Romagna, 2017, pag. 55 e ss.

riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio [...]; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.” e, invece, in relazione ai dati genetici ritengono che “[...] si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.”¹⁴.

La definizione di dati personali fornita dal GDPR è ripresa anche all'art. 2 del regolamento n. 868 del 30 maggio 2022 (Data Governance Act — DGA)¹⁵ e all'art. 2, comma 1 (a) del regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS)¹⁶. In quest'ultimo regolamento in particolare, il riferimento ai dati genomici assume rilievo all'art. 51 riguardante le “Categorie minime di dati elettronici per l'uso secondario” ove i dati del genoma umano sono esplicitamente indicati tra quelli che devono essere messi a disposizione dai titolari dei dati per l'uso secondario.

¹⁴ Regolamento UE 2016/679 (GDPR), cons. 34 e 35. Per alcune riflessioni sui riferimenti specifici contenuti dal GDPR in merito all'applicazione di norme o istituti specifici al trattamento dei dati personali effettuati in ambito sanitario si v. M. S. BONOMI, *Privacy e dati sanitari: le principali novità introdotte dal GDPR*, 2018, in www.federalismi.it.

¹⁵ « [...] « dati personali »: i dati personali quali definiti all'art. 4, punto 1, del regolamento (UE) 2016/679 [...] ».

¹⁶ Il regolamento EHDS (CORRIGENDUM disponibile su: https://www.europarl.europa.eu/meetdocs/2024_2029/plmrep/COMMITTEES/ENV/DV/2024/12-04/2022_0140COR01_EN.pdf), all'art. 2 sulle definizioni richiama il concetto di dati sanitari elettronici personali, i dati relativi alla salute e i dati genetici così come definiti nell'art. 4, numeri 13) e 15) del regolamento (UE) 2016/679 e trattati in formato elettronico.

3. TRATTAMENTO DEI DATI SANITARI PERSONALI.

L'art. 4 del regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR) fornisce la definizione chiara di trattamento dei dati personali, con cui s'intende: "[...] qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione [...]"¹⁷.

Il trattamento dei dati personali è considerato lecito alle condizioni previste dall'art. 6 del GDPR ed è ammissibile se avviene per finalità determinate, esplicite e legittime¹⁸. Nel trattare i dati personali, il titolare del trattamento deve improntare il suo operato al principio di trasparenza, al quale è ispirato il GDPR. Il principio di trasparenza impone che le informazioni destinate al pubblico o all'interessato di un trattamento siano facilmente accessibili e comprensibili. Infatti, l'art. 12 del GDPR stabilisce che il titolare del trattamento debba adottare misure appropriate per fornire all'interessato tutte le informazioni necessarie e le comunicazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni che il titolare del trattamento deve fornire all'interessato sono elencate nei successivi artt. 13 e 14 del GDPR¹⁹.

L'art. 9 del GDPR, nell'individuare una categoria particolare di dati personali nei quali rientrano quelli sanitari e quelli genetici²⁰, dispone specificatamente il divieto di trattamento degli stessi in ragione della loro natura estremamente sensibile²¹. Il GDPR, però, prevede casi specifici di liceità del trattamento dei

¹⁷ Regolamento UE 2016/679 (GDPR), art. 4, numero 2).

¹⁸ Regolamento UE 2016/679 (GDPR), art. 5, comma 1 lettera b).

¹⁹ Per una riflessione sui principi a cui si deve ispirare il trattamento dei dati personali, ai sensi del GDPR, si v. L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018, pag. 1 e ss.

²⁰ Sul tema "trattamento dei dati genetici" si v. M. T. ANNECCA, *Il trattamento dei dati genetici*, in *Libera circolazione e protezione dei dati personali*, Tomo I, Giuffrè, Milano, 2006, pag. 1121 e ss.

²¹ Per un approfondimento sui dati sanitari e genetici quali categorie particolari di dati si v. A. BUSACCA, *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in *Ordine internazionale e diritti umani*, 2018, pag. 36 e ss.; A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pag. 204 e ss.; L. DURST, *Il trattamento di categorie particolari di dati in ambito sanitario*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n.*

dati, infatti il divieto è derogato quando sussistano alcune specifiche condizioni, ossia quando: l'interessato presti il suo consenso; il trattamento sia necessario ai fini di protezione sociale o per un interesse vitale dell'interessato e quest'ultimo non possa prestare il consenso; l'interessato abbia espressamente reso pubblici i suoi dati; il trattamento dei dati sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione Europea UE o degli Stati membri; il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro; il trattamento sia necessario per motivi di interesse pubblico in ambito di sanità pubblica, a fini di ricerca scientifica, storica o a fini statistici ²².

In Italia, il d.lgs. n. 101 del 10 agosto 2018, attraverso il quale è stato possibile l'adeguamento del Codice Privacy del 2003 al GDPR, all'art. 2 *sexties* ritiene ammissibile il trattamento di quelle categorie particolari di dati personali disciplinati all'interno dell'art. 9 del GDPR, per motivi di rilevante interesse pubblico. Proprio sulla base dell'art. 2 *sexies* si ritiene ammissibile il trattamento dei dati personali sanitari sia per uso primario (volto alla cura del singolo individuo) ²³, che secondario (riguardante altre finalità come ricerca scientifica, politiche sanitarie, sviluppi industriali) ²⁴. Con particolare riferimento all'uso secondario, il legislatore italiano è recentemente intervenuto con la nuova formulazione dell'art. 110 del Codice Privacy, in vigore dall'1 maggio del 2024, la quale consente il trattamento dei dati per finalità di ricerca medica, biomedica ed epidemiologica ²⁵ anche nell'impossibilità di raccogliere il consenso degli interessati se per particolari ragioni risulta impossibile informare i titolari dei dati del trattamento di questi ultimi oppure se implica uno sforzo sproporzionato o, ancora, se rischia di rendere impossibile o di pregiudicare — in modo grave — il conseguimento delle finalità della ricerca. Si ritornerà sul tema, con maggiori dettagli,

679/2016 e al d.lgs. n. 101/2018, Giuffrè, Milano, 2019, pag. 65 e ss.

²² Per alcune riflessioni sul trattamento dei dati sanitari si v. G. FINOCCHIARO, *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 *La legge sulla privacy dieci anni dopo*, EGEA, Milano, 2008, pag. 207 e ss.

²³ D.Lgs. 101/2018 art. 2 *sexies*, lettere t), u).

²⁴ D.Lgs. 101/2018 art. 2 *sexies*, lettere v), z -sub Cc-). Sul tema "uso secondario dei dati sanitari personali", per un approfondimento sul "quando", ai sensi del GDPR, questi dati possano essere utilizzati per finalità ulteriori, si v. R. BECKER, D.

CHOKOSHVILI, G. COMANDÉ, E. S. DOVE, A. HALL, C. MITCHELL, F. MOLNÁR-GÁBOR, P. NICOLÁS, S. TERVO, A. THOROGOOD, *Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?*, in *European Journal of Health Law*, 2022, in brill.com.

²⁵ Significative problematiche giuridiche emergono dai progetti che si mettono in campo sul trattamento dei dati per ricerca medica, biomedica ed epidemiologica come quelle esposte e commentate da E. Poddighe sul Progetto EINS per la regione Sardegna nel suo contributo *Piani epidemiologici regionali e raccolta, elaborazione e circolazione dei dati sanitari: il progetto EINS per la regione Sardegna*, in questa Rivista, 2024, pagg. 561-576.

nel par. 7, dedicato all'uso dei dati personali sanitari per finalità di ricerca scientifica.

4. CORNICE NORMATIVA EUROPEA E NAZIONALE.

Le principali, più recenti normative europee e nazionali che toccano il tema del trattamento dei dati per finalità di uso secondario prendono le mosse, anche per quanto riguarda l'ambito sanitario, dalle norme già in vigore sulla protezione dei dati personali. Il concetto di uso secondario del dato sanitario personale esprime tutto ciò che va oltre la cura individuale della persona, in modo coerente sia nella interpretazione offerta dal regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR), che in quella del regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA) e, da ultimo, in quella del regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS).

Nel GDPR, l'uso secondario dei dati personali sanitari è reso ammissibile dall'art. 5, in virtù del quale: “[...] *un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, par. 1, considerato incompatibile con le finalità iniziali [...]*”, per le quali i dati sono stati raccolti.

Il DGA prevede regole e salvaguardie per facilitare il riutilizzo di dati protetti ogniquale volta sia possibile in base ad altre normative e offre un quadro generale di governo dei dati protetti — senza limitazioni per una tipologia di dati o per un settore (per esempio, dei soli dati sanitari o genomici, o giudiziari, o politici, e così via) — ai fini del loro riuso.

In tema di trattamento dei dati personali sanitari, la differenza tra uso primario e uso secondario è meglio definita dal nuovo regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS), che dedica il Capo II e il Capo III all'uso primario mentre il Capo IV all'uso secondario. Specificatamente, ai sensi del regolamento EHDS, l'uso primario dei dati sanitari elettronici è strettamente legato all'erogazione della prestazione sanitaria nei confronti della persona fisica (attività di prevenzione, diagnosi e cura) anche a livello transfrontaliero, e comprende la raccolta e il trattamento iniziali dei dati personali del paziente²⁶. Di contro, l'uso secondario dei dati sanitari elettronici comprende utilizzi ulteriori, rispetto a quelli sottesi alla raccolta o al trattamento iniziali, finalizzati non solo ad attività di pubblico interesse, politiche sanitarie, ricerca, didattica, ma anche ad attività condotte da soggetti privati con carattere di impresa o senza scopo di

²⁶ Regolamento EHDS, art. 2, par. 2, lettera d).

luogo, quali attività per l'innovazione nel settore dei farmaci e dei dispositivi medici, lo sviluppo di algoritmi e sistemi di Intelligenza Artificiale (IA) nel settore medico-sanitario ²⁷. Come ben espresso al considerando 110, il regolamento EHDS garantisce un quadro coerente ed efficiente per il riutilizzo dei dati sanitari delle persone fisiche per la ricerca, l'innovazione, la definizione delle politiche e le attività normative (finalità declinate all'art. 53), di cui nel sotto-paragrafo 4.4. sarà illustrato il dettaglio.

4.1. *Il Regolamento per la Protezione dei Dati Personali.*

L'ammissibilità dell'uso secondario dei dati personali sanitari proviene dal regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR) che, all'art. 5, rende possibile il trattamento dei dati personali per finalità diverse da quelle per le quali sono stati raccolti, dunque per finalità di pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione che il trattamento avvenga in modo lecito, corretto e trasparente ²⁸.

Dal considerando 50 del GDPR si può evincere la disciplina più approfondita dell'utilizzo secondario dei dati. Nello specifico, il trattamento dei dati per finalità diverse da quelle per le quali sono stati raccolti è consentito solo se tali finalità sono compatibili con quelle per le quali i dati sono stati inizialmente raccolti e la base giuridica che ne regola l'utilizzo non differisce da quella che legittima l'utilizzo primario dei dati stessi, anche con riguardo a categorie particolari di dati personali. L'uso secondario dei dati sanitari è, allora, ammesso e soggiace alla disciplina prevista dall'art. 6 del GDPR e dall'art. 9, par. 2, del GDPR.

Se l'uso secondario dei dati sanitari è compatibile con le finalità per le quali si è proceduto all'uso primario ed è necessario per eseguire un compito di interesse pubblico o per esercitare pubblici poteri, la liceità e la compatibilità dell'ulteriore trattamento viene constatata in base alle finalità e ai compiti che possono essere stabiliti dal diritto dell'Unione Europea UE o degli Stati membri.

La compatibilità tra le finalità di un ulteriore trattamento dei dati e quelle per le quali — invece — gli stessi sono stati raccolti sussiste se il titolare del trattamento, ex art. 6 par. 4 del GDPR, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tiene anche conto di specifici elementi e in particolare:

— di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto;

²⁷ Proposta di Regolamento sullo spazio europeo dei dati sanitari, art. 2, par. 2, lettera e).

²⁸ Per una prima riflessione sulle problematiche collegate al complesso quadro

delle basi giuridiche dell'ordinamento italiano con le misure di soft law adottate con il GDPR si v. G. COMANDÈ, *Ricerca in sanità e data protection... un puzzle risolvibile*, in *Rivista italiana di medicina legale*, 2019.

- del contesto in cui i dati personali sono stati raccolti;
- delle aspettative dell'interessato, in base alla sua relazione con il titolare del trattamento, sull'ulteriore utilizzo dei dati;
- della natura dei dati personali;
- delle conseguenze dell'ulteriore trattamento previsto per gli interessati e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Il GDPR ritiene essenziale, per lo sviluppo della società europea ²⁹, creare un clima di fiducia che consenta la circolazione dei dati personali, e contribuisce a ciò fornendo garanzie per i diritti e le libertà delle persone fisiche.

4.2. *La protezione dei dati personali in Italia.*

Il regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR), in merito alla possibilità di utilizzare ulteriormente i dati personali, nello specifico quelli sanitari, prevede l'utilizzo degli stessi per finalità di interesse pubblico come la prevenzione e la gestione delle emergenze sanitarie, di ricerca scientifica, purché vengano rispettati i principi di proporzionalità, minimizzazione e finalità, e per finalità statistiche (art. 5 e cons. 50 ³⁰).

L'entrata in vigore del GDPR ha determinato in Europa, nella disciplina del trattamento — anche ulteriore — dei dati sanitari personali, il venir meno della centralità del consenso ³¹ laddove esistente, come in Italia. Infatti, dalla base giuridica che rende lecito l'ulteriore trattamento dei dati personali sanitari emerge che, ai sensi del GDPR, si possa procedere con il trattamento ulteriore dei dati personali sanitari anche senza che sia necessario il consenso dell'interessato. Se, però, l'interessato ha prestato il suo consenso, deve essere informato dell'utilizzo dei suoi dati personali sanitari per finalità diverse rispetto a quelle per le quali sono stati raccolti, deve ricevere indicazioni in merito alla diversa finalità ³² e può esercitare il suo diritto di opposizione in qualsiasi

²⁹ E. S. DOVE, *The EU General Data Protection Regulation: Implications for International Scientific Research in Digital Era*, in *The Journal of Law, Medicine & Ethics*, 2018.

³⁰ Art. 5: « 1. I dati personali sono: [...] b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, par. 1, considerato incom-

patibile con le finalità iniziali (« limitazione della finalità ») »;

Considerando 50: « [...] L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile [...] ».

³¹ Sul tema si v. C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, 2020, pag. 860 e ss.

³² Regolamento UE 2016/679 (GDPR), art. 13, par. 3 e art. 14, par. 4.

momento³³. Il titolare del trattamento può derogare al divieto di trattare ulteriormente i dati personali sanitari dell'interessato in presenza della sua opposizione all'utilizzo degli stessi, solamente se sussistono motivi legittimi cogenti per procedere al trattamento che prevalgono sui suoi interessi, sui suoi diritti e sulle sue libertà (dunque in condizioni di emergenza) oppure per l'esecuzione di un compito di interesse pubblico. Nel panorama europeo, quindi, il legislatore permette l'uso secondario dei dati sanitari personali, concedendo all'interessato il diritto di obiezione, che, in alcuni specifici casi, può anche essere ignorato³⁴.

In Italia, il d.lgs. n. 101 del 10 agosto 2018, che adegua il d.lgs. n. 196 del 30 giugno 2003 (Codice Privacy) alle disposizioni del GDPR, disciplina la materia dell'uso secondario dei dati personali sanitari partendo dal par. 4 dell'art. 9 del GDPR³⁵, che con riguardo al trattamento dei dati genetici, biometrici e relativi alla salute dispone che ogni Stato membro possa mantenere o introdurre ulteriori condizioni, comprese limitazioni.

In ragione di ciò, il legislatore italiano ha arricchito il quadro di riferimento europeo³⁶ ritenendo che il consenso sia necessario in determinate circostanze, che vengono espressamente previste dal Garante per la protezione dei dati personali³⁷. Il Garante per la protezione dei dati personali, con il provvedimento n. 9091942 recante "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"³⁸, ha fatto luce su alcuni aspetti critici relativi al trattamento dei dati personali sanitari per come disciplinati dal GDPR e dal d.lgs.

³³ Regolamento UE 2016/679 (GDPR), art. 21.

³⁴ Sul diritto di obiezione al trattamento dei dati personali, che può essere esercitato dall'interessato, si v. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, Tomo I, Giuffrè, Milano, 2006, pag. 993 e ss.

³⁵ « [...] 4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. [...] ».

³⁶ Ciò è ammissibile in virtù del par. 4 dell'art. 9 del GDPR che, con riguardo al trattamento dei dati genetici, biometrici e relativi alla salute, prevede la possibilità per ogni Stato membro di mantenere o introdurre ulteriori condizioni, comprese limitazioni. L'accesso per il riutilizzo dei dati personali è consentito solo se l'ente pubblico ha garantito l'anonimizzazione dei dati e se l'accesso stesso avviene in un ambiente di trattamento sicuro, fornito o controllato dall'ente (art. 5, par. 3, DGA).

³⁷ Il Garante per la protezione dei dati personali è l'autorità di controllo italiana individuata dall'art. 2 bis del Codice Privacy (così come modificato dal d.lgs. 101/2018), in virtù di quanto disposto dall'art. 51 del GDPR, che conferisce ad ogni Stato membro la possibilità di disporre che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del regolamento, con l'obiettivo di tutelare i diritti e le libertà fondamentali delle persone fisiche con riferimento al trattamento dei loro dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione Europea. Per una visione sull'attività dell'Autorità Garante per la protezione dei dati personali nella delicata ricerca di un equilibrio nella protezione dei dati a fronte dell'innovazione digitale si v. G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Aracne, Roma, 2016.

³⁸ Per il testo si rimanda a <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942>.

101/2018, che davano adito a dubbi interpretativi³⁹. In particolare, il Garante ha disposto espressamente che, a proposito dell'uso primario, il consenso del paziente per il trattamento dei dati relativi alla salute non debba necessariamente essere acquisito dal professionista sanitario quando il trattamento è necessario per perseguire finalità di cura, in linea con quanto disposto dall'art. 9, par. 2 lett. h) del GDPR⁴⁰. Mentre invece, per quanto attiene *“agli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari”*, che sono appunto i trattamenti ulteriori dei dati sanitari personali, il Garante per la protezione dei dati personali richiede che, anche se gli stessi siano effettuati da professionisti della sanità, debba essere individuata una distinta base giuridica nel consenso dell'interessato o in un altro presupposto di liceità.

L'altro presupposto di liceità si rinviene negli artt. 6 e 9 par. 2 del GDPR, in virtù dei quali il Garante ritiene ammissibile l'uso secondario dei dati personali sanitari senza il consenso dell'interessato, se l'utilizzo viene posto in essere per realizzare finalità di interesse pubblico o connesse all'esercizio di pubblici poteri⁴¹, finalità di interesse pubblico rilevante sulla base del diritto dell'Unione Europea UE o degli Stati membri⁴² o finalità di interesse pubblico nel settore della sanità pubblica⁴³.

Tra i trattamenti dei dati personali sanitari, che richiedono il consenso, sono ricompresi, secondo il Garante, quelli effettuati per inviare comunicazioni promozionali e quelli preordinati alla programmazione sanitaria e alla politica sanitaria. Pertanto, mentre il GDPR ha previsto per l'interessato la possibilità di obiettare all'utilizzo secondario dei propri dati personali sanitari, l'Italia ha dato priorità al consenso dell'interessato.

³⁹ Per alcune riflessioni sul trattamento dei dati in ambito sanitario si v. M. ALOVISIO, *Primi chiarimenti del Garante privacy sul trattamento dei dati in ambito sanitario*, 2019, in www.dirittoegiustizia.it.

⁴⁰ « [...] il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3. [...] ».

⁴¹ Regolamento UE 2016/679 (GDPR), art. 6, par. 1, lett. e): « [...] il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento [...] ».

⁴² Regolamento UE 2016/679 (GDPR), art. 9, par. 2, lett. g): « [...] il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. [...] ».

⁴³ Regolamento UE 2016/679 (GDPR), art. 9, par. 2, lett. i): « [...] il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale. [...] ».

Il d.lgs. 101/2018 ha però confermato, con gli artt. 6 e 7, quanto previsto dal GDPR in merito alla possibilità di trattare — per finalità di uso primario e secondario — i dati sanitari anche senza il consenso dell'interessato, incentrando tale facoltà sia sulle sei basi giuridiche del trattamento previste dall'art. 6 del GDPR ⁴⁴, sia sulle dieci condizioni per il trattamento delle categorie particolari di dati personali previste dall'art. 9, par. 2, del GDPR ⁴⁵.

L'art. 77 del Codice Privacy, così come modificato dal d.lgs. 101/2018, nel disciplinare modalità particolari di trattamento dei dati personali e di fornitura all'interessato delle informazioni di trattamento, non fa alcun riferimento al consenso per il trattamento dei dati personali.

⁴⁴ Regolamento UE 2016/679 (GDPR), art. 6, par. 1: « [...] Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. [...] ».

⁴⁵ Regolamento UE 2016/679 (GDPR), art. 9, par. 2: « [...] a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o

Il “Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici” è espressamente disciplinato dall’art. 110 *bis* del Codice Privacy. L’art. 110 *bis* prende in prioritaria considerazione il caso degli usi secondari da parte di “nuovi” titolari di trattamento rispetto a coloro che hanno originariamente raccolto per altre finalità i dati personali. Tali usi secondari di dati — compresi quelli dei trattamenti speciali di cui all’art. 9 del GDPR — a fini di ricerca scientifica o a fini statistici possono essere autorizzati dal Garante da parte di soggetti terzi, che svolgano principalmente tali attività quando, “(1) a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che (2) siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, in conformità all’art. 89 del regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati”.

Verificata quindi la sussistenza dei due requisiti appena citati, il Garante eventualmente autorizza entro quarantacinque giorni, se del caso imponendo specifiche condizioni e misure “*necessarie ad assicurare adeguate garanzie a tutela degli interessati nell’ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza*”.

Vi è inoltre la possibilità, data dal Garante, di adottare per le medesime finalità “*provvedimenti generali, adottati d’ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell’ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati*”.

Si tratta di provvedimenti che sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana e assumono valenza generale.

Tale opzione offerta dall’art. 110 *bis* comma 3, che consente di addivenire a provvedimenti generali in grado di offrire una solida base giuridica al trattamento dei dati sanitari in linea con la disciplina dei dati personali e nel pieno rispetto della tutela dei diritti e delle libertà cui essa è dedicata, non è stata, tuttavia, compiutamente espressa in Italia.

la garanzia di parametri elevati di qualità e sicurezza dell’assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell’Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell’interessato, in particolare il segreto professionale; 4.5.2016 L 119/38 Gazzetta ufficiale dell’Unione europea IT j) il trattamento è necessario a fini di archiviazione nel pubblico

interesse, di ricerca scientifica o storica o a fini statistici in conformità dell’art. 89, paragrafo 1, sulla base del diritto dell’Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l’essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato [...] ».

Il medesimo art. 110 *bis* al comma 4 ribadisce che: “*Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l’attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell’attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell’osservanza di quanto previsto dall’articolo 89 del regolamento*”. In tal caso, infatti, si tratta di un trattamento primario, autorizzato dalla normativa nazionale.

Un importante intervento legislativo in materia di uso dei dati personali sanitari si è avuto di recente con il D.L. n. 19 del 2 marzo 2024, che modificando l’art. 110 del Codice Privacy, non prevede più il requisito della consultazione preventiva del Garante all’utilizzo dei dati personali sanitari.

La nuova formulazione dell’articolo, infatti, stabilisce che se non è possibile ottenere il consenso dell’interessato all’utilizzo dei suoi dati, gli stessi possono essere trattati per finalità di ricerca medica, biomedica ed epidemiologica a condizione che vengano adottate le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato. Inoltre, il programma di ricerca scientifica, per cui si vuole procedere, deve essere oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere conforme alle specifiche misure di garanzia previste dal Garante ai sensi dall’art. 106 dello Codice Privacy. Il Garante deve così individuare misure di garanzie specifiche per il trattamento dei dati personali sanitari nei casi in cui si possa prescindere dal consenso degli interessati.

La consultazione preventiva del Garante, prima obbligatoria, diventa ora un’attività da realizzare solo se, a valle della valutazione d’impatto, risultano esserci dei rischi residui che non possono essere attenuati dall’adozione di adeguate misure di sicurezza da parte del titolare.

4.3. *Il Data Governance Act.*

Nel quadro legislativo generale dell’Unione Europea UE sull’uso secondario dei dati personali, una tappa importante è rappresentata dal regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA)⁴⁶. È una norma intersettoriale che regola il riutilizzo di dati pubblici (sia personali che non) conservati e protetti, e ne promuove la condivisione mediante il coinvolgimento di nuovi intermediari o l’incoraggiamento all’al-

⁴⁶ Per la normativa si rimanda a <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R0868>.

truismo ⁴⁷ prevedendo una serie di salvaguardie per incentivare la fiducia delle parti interessate.

Il DGA non offre un base giuridica in grado di legittimare autonomamente l'uso secondario dei dati personali, ma prevede regole e salvaguardie per estrarre, da dati protetti detenuti nel settore pubblico, grandi quantità di conoscenze utili per il raggiungimento di finalità diverse da quelle per le quali i dati sono stati originariamente raccolti, senza comprometterne la loro natura protetta e senza prevedere limitazioni per tipologie o settori specifici di dati, come quelli sanitari o genomici.

Il DGA non pregiudica quindi il diritto dell'UE in materia di protezione dei dati personali, né il diritto nazionale adottato conformemente a tale diritto ⁴⁸, neanche per quanto riguarda i poteri e le competenze delle autorità di controllo. Attraverso questo regolamento il legislatore europeo fornisce, allora, i requisiti tecnici per consentire al settore pubblico di gestire le fasi del processo che portano al riutilizzo dei dati, nel rispetto della privacy e della riservatezza degli stessi.

L'elemento maggiormente caratterizzante il DGA, in una prospettiva di implementazione della norma che abiliti — ai sensi della normativa vigente in materia di protezione dei dati personali — il riutilizzo efficiente dei dati personali sanitari (e di quelli non personali), può dunque ritenersi quello degli organismi competenti responsabili di gestire e governare il processo, che va dalla individuazione dei dati condivisibili alla loro condivisione effettiva, passando per i diversi sviluppi necessari per attuare la condivisione sul piano operativo, allo scopo di rendere tecnicamente abile il settore pubblico al riutilizzo di tali dati.

Il legislatore nazionale, nell'attuare la norma a livello di singolo Stato membro dell'UE, è conseguentemente chiamato ad individuare quali organismi competenti (uno o più di uno) debbono sostenere gli enti pubblici che concedono l'accesso ai dati sanitari per finalità secondarie ⁴⁹, assicurando anche la disponibilità di

⁴⁷ L'altruismo dei dati consiste nel dare il consenso o l'autorizzazione a rendere disponibili i propri dati — volontariamente e senza compenso — per utilizzarli nell'interesse pubblico.

⁴⁸ L'art. 1 comma 3 DGA precisa « [...] Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, anche per quanto riguarda i poteri e le competenze delle autorità di controllo. In caso di conflitto tra il presente regolamento

e il diritto dell'Unione in materia di protezione dei dati personali o il diritto nazionale adottato conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680 [...] ».

⁴⁹ Ai sensi dell'art. 7 DGA, gli Stati membri possono scegliere gli organismi competenti adatti per assistere gli enti pubblici nell'attività di concessione o rifiuto dell'ac-

ambienti sicuri per l'elaborazione dei dati e individuando le modalità per strutturare e archiviare al meglio i dati allo scopo di renderli facilmente accessibili. In tale operazione è, ai sensi del DGA, possibile avvalersi di intermediari di dati (anch'essi da individuare ad opera del legislatore nazionale), i quali funzionino come organizzatori affidabili della condivisione dei dati all'interno degli spazi comuni di dati europei. Un unico punto di informazione nazionale è richiesto agli Stati membri per aiutare gli utenti dei dati (i potenziali 'riutilizzatori') a reperire informazioni utili e pertinenti su quali dati siano detenuti da quali autorità pubbliche ⁵⁰.

In particolare, l'accesso ai dati personali per il loro riutilizzo è consentito solo se l'ente pubblico abbia garantito l'anonimizzazione di tali dati e quando vi sia garanzia di un ambiente sicuro per il loro trattamento rispettando rigorose norme di sicurezza ⁵¹. Dopo l'accesso nell'ambiente sicuro, il riutilizzo dei dati può avvenire solo laddove l'utente riutilizzatore rispetti l'obbligo di riservatezza che vieta la divulgazione di qualsiasi informazione che comprometta i diritti e gli interessi di terzi e che il riutilizzatore possa aver acquisito malgrado le misure di tutela adottate ⁵². È vietata la reidentificazione degli interessati cui si riferiscono i dati trattati: i riutilizzatori sono chiamati ad adottare le necessarie misure per impedire la reidentificazione e a notificare all'ente pubblico eventuali violazioni che rendano possibile la reidentificazione degli interessati.

D'altra parte, qualora l'ente pubblico non riuscisse a soddisfare tali requisiti e a consentire l'accesso a determinati dati per il loro uso secondario, lo stesso ente pubblico dovrebbe assistere i potenziali utenti riutilizzatori nel richiedere il consenso degli interessati o l'autorizzazione dei titolari dei dati i cui diritti e interessi possono essere implicati nel riuso ⁵³. Specificatamente, la previsione di cui all'art. 5 c. 6 del DGA stabilisce che è possibile riutilizzare il dato sanitario non anonimizzato, qualora: per i dati personali sussista una base giuridica ai sensi degli artt. 6 e 9 del regolamento UE) 2016/679 (GDPR); per i dati non personali sussista l'autorizzazione dei titolari dei dati, i cui diritti e interessi possono essere interessati da tale riutilizzo. Inoltre, la previsione di cui all'art. 5 precisa che è un dovere degli enti pubblici coinvolti di *“fornire assistenza ai potenziali riutilizzatori nel richiedere il consenso degli interessati o l'autorizzazione dei*

cesso ai dati per il loro riutilizzo (uso secondario).

⁵⁰ Ai sensi dell'art. 8 DGA, gli Stati membri mettono a disposizione elenchi di riserve di dati disponibili e condizioni per il loro riutilizzo attraverso gli sportelli unici.

⁵¹ Regolamento UE 2022/868 (DGA), art. 5, comma 3, lettere b), c).

⁵² Regolamento UE 2022/868 (DGA), art. 5, comma 5.

⁵³ Regolamento UE 2022/868 (DGA), art. 5, comma 6.

titolari dei dati, i cui diritti e interessi possono essere interessati da tale riutilizzo", a condizione che "ciò sia fattibile senza un onere sproporzionato per l'ente pubblico". Dunque, il riutilizzo del dato personale può essere legittimato dalle basi giuridiche previste dal GDPR incluso il consenso.

Un'importante novità del regolamento è infine rappresentata dalla possibilità di istituire servizi di intermediazione capaci di "[...] instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali [...]"⁵⁴. Ai nuovi intermediari di dati, il DGA consente quindi di agire come attori affidabili nell'economia dei dati. Tale scelta è coerente con l'obiettivo del DGA di facilitare la condivisione dei dati a vantaggio del progresso della società e dell'economia dell'UE, insistendo sul tema della fiducia nella condivisione dei dati attraverso il rafforzamento di meccanismi che incrementino la disponibilità di dati mediante il superamento di ostacoli tecnici e tramite la creazione di spazi comuni di dati in ambiti strategici quali la sanità, l'ambiente, la pubblica amministrazione⁵⁵.

4.4. *Il Regolamento sullo Spazio Europeo dei Dati Sanitari.*

Il regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS) si inserisce nell'ampia strategia europea per i dati⁵⁶, promossa dalla Commissione Europea a partire dal febbraio 2020 con l'obiettivo di costruire un mercato unico dei dati attraverso la creazione di spazi comuni europei in una serie di settori strategici tra cui sanità, pubblica amministrazione, agricoltura, industria manifatturiera, energia, mobilità, finanza⁵⁷.

⁵⁴ Regolamento UE 2022/868 (DGA), art. 2, numero 11).

⁵⁵ Il DGA è stato il primo traguardo normativo della recente strategia europea per i dati, volta a regolamentare i processi e le strutture di condivisione. A seguire, è stato introdotto il regolamento (UE) 2023/2854 (Data Act) che chiarisce chi può creare valore dai dati e in quali condizioni. Con quest'ultimo, l'UE vuole rendere disponibile un maggior numero di dati per il loro riutilizzo e stabilire norme su chi può utilizzarli e accedervi per quali scopi in vari settori economici dell'UE. L'impianto normativo punta, nell'insieme, a garantire un accesso ai dati affidabile e sicuro in modo da promuovere l'uso in settori chiave e in aree di

interesse pubblico come la sanità. Per la normativa si rimanda a https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL_2023%2854.

⁵⁶ A European strategy for data in <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>.

⁵⁷ Per approfondimenti sulla presentazione della proposta di regolamento da parte della Commissione europea si v. S. Corso, *European Health Data Space. La Commissione europea presenta la proposta di Regolamento sullo spazio europeo dei dati sanitari*, 2022, in www.rivistaresponsabilitamedica.it; S. CORSO, *Lo spazio europeo dei dati sanitari: la Com-*

Per il mandato politico 2024-2029, la neoeletta Commissione ha ribadito l'importanza di aumentare la produttività europea e le innovazioni sociali (dalla medicina personalizzata al risparmio energetico), mediante la diffusione delle tecnologie digitali sfruttando il potenziale inutilizzato dei dati. Il traguardo è quello di sviluppare nuovi servizi e modelli aziendali, anche supportati dall'intelligenza artificiale e da altre tecnologie di frontiera.

L'esigenza di progredire verso la costituzione di uno spazio comune di dati sanitari⁵⁸, idoneo ad assicurare un accesso tempestivo a dati sanitari elettronici non solo per finalità di cura individuale (uso primario), ma anche per facilitare la risposta alle minacce di salute pubblica e per agevolare lo sviluppo della ricerca scientifica, dell'innovazione in materia di servizi sanitari e la definizione delle politiche sanitarie (usi secondari), è stata dunque pienamente recepita dall'UE. L'unione dei dati viene ad essere basata su un quadro giuridico coerente affinché le aziende e le amministrazioni dell'UE possano condividere i dati senza soluzione di continuità e su larga scala, rispettando al contempo elevati standard di privacy e sicurezza.

Coerentemente con le basi giuridiche previste agli artt. 16 e 114 del Trattato sul Funzionamento dell'UE (TFUE) e nel rispetto dell'art. 168 TFUE, il regolamento sullo Spazio Europeo dei Dati Sanitari individua come obiettivo (considerando 110) quello di garantire un quadro coerente ed efficiente per il riutilizzo dei dati personali sanitari per la ricerca, l'innovazione, la definizione di politiche di governo, le attività normative e varie altre declinate all'art. 53⁵⁹. Tale obiettivo di un quadro comune non può, d'altronde, essere conseguito in misura sufficiente dagli Stati membri attraverso le sole misure di coordinamento, come dimostrato dalla valutazione degli aspetti digitali della direttiva 2011/24/UE⁶⁰. Di converso, in ottemperanza al principio di proporzionalità, può essere conseguito dall'UE (che interviene in base al principio di sussidiarietà di cui all'art. 5 del TFUE) attraverso le misure di armonizzazione per i diritti delle persone fisiche in

missione Europea presenta la proposta di regolamento, 2022, in www.federalismi.it.

⁵⁸ Per alcune riflessioni critiche sul tema si v. W. Li, P. QUINN, *The European Health Data Space: An expanded right to data portability?*, 2024, in <https://www.sciencedirect.com/science/article/pii/S0267364923001231>; P. QUINN, E. ELLYNE, C. YAO, *Limits to Health Data Access Body Discretion and a Need to Comply with the Gdpr - Enough to Protect Against Improper Sharing of Health Data Through the EHDS?*, 2023, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4662816.

⁵⁹ Per quanto riguarda l'EHDS, si fa

referimento al "CORRIGENDUM to the position of the European Parliament adopted at first reading on 24 April 2024 with a view to the adoption of Regulation (EU) 2024/... of the European Parliament and of the Council on the European Health Data Space P9_TA(2024)0331 (COM(2022)0197 - C9-0167/2022 - 2022/0140(COD)), già testo definitivo in iter di pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, ma non ancora disponibile al momento della redazione del presente lavoro.

⁶⁰ Per la normativa si rimanda a <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0024>.

relazione ai loro dati sanitari elettronici, per l'interoperabilità dei dati sanitari elettronici e quindi per un quadro comune per l'uso secondario dei dati sanitari elettronici.

In particolare, l'uso secondario dei dati sanitari elettronici (definito dall'art. 2, par. 2, lettera *e*) del regolamento EHDS)⁶¹ comprende utilizzi ulteriori rispetto a quelli riguardanti la raccolta e/o il trattamento iniziali dei dati. Si tratta quindi di utilizzi finalizzati a: interventi di sanità pubblica come ad esempio programmazione sanitaria, prevenzione o gestione di emergenze di salute della collettività; attività di innovazione, tra cui quelle condotte nel settore farmaceutico o dei dispositivi medici e delle tecnologie applicate alla salute anche da parte di soggetti privati (sia *for-profit* che *no-profit*); attività di ricerca scientifica e storica, e di medicina personalizzata; azioni per la sicurezza delle cure; iniziative formative e didattiche; finalità di natura legislativa e politica. In tal senso il Regolamento EHDS prevede (considerando 52) misure idonee e specifiche necessarie per salvaguardare i diritti fondamentali e gli interessi delle persone fisiche in conformità dell'art. 9, par. 2, lett. *g*), *h*), *i*) e *j*) del regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR), e dell'art. 10, par. 2, lett. *g*), *h*), *i*) e *j*), del regolamento (UE) 2018/1725⁶² sulla protezione dei dati nell'ambito delle istituzioni dell'UE. Il legislatore europeo sottolinea peraltro che la condivisione dei dati per uso secondario deve essere coerente con le disposizioni in materia di trasparenza previste dal diritto dell'UE (considerando 60 EHDS).

La struttura, a livello giuridico e di governance, del quadro comune per l'uso secondario si basa sull'istituzione di organismi responsabili dell'accesso ai dati sanitari (Health Data Access Body - HDAB), disciplinati dall'art. 55⁶³, cooperanti nell'UE attraverso una rete supportata da una infrastruttura tecnologica condivisa (HealthData@EU) che mira a sostenere lo scambio transfrontaliero e il riutilizzo dei dati sanitari elettronici. Il legislatore ha inteso che ciascuno Stato membro costituisca organismi responsabili dell'accesso ai dati sanitari, quali enti del settore pubblico, esistenti o di nuova costituzione, per consentire un accesso prevedibile e semplificato ai dati sanitari elettronici e un livello elevato di trasparenza, responsabilizzazione e sicurezza

⁶¹ L'EHDS definisce all'art. 2, par. 2, lettera *e*: « [...] secondary use of electronic health data' means the processing of electronic health data for purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced [...] ».

⁶² Per la normativa si rimanda a [http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018R1725#:~:text=Regolamento%20\(UE\)%202018%2F1725,il%20regolamento%20\(CE\)%20n.](http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018R1725#:~:text=Regolamento%20(UE)%202018%2F1725,il%20regolamento%20(CE)%20n.)

⁶³ Al comma 1, l'art. 55 dispone che gli Stati membri designano uno o più organismi responsabili dell'accesso ai dati sanitari per lo svolgimento dei compiti e l'adempimento dei doveri stabiliti agli artt. 57, 58 e 59.

nel trattamento di tali dati per le finalità di uso secondario legittimate dall'art. 53. Gli organismi di accesso ai dati (HDAB) sono gli organismi che, alla presenza dei requisiti prescritti dagli artt. 68, 69, e 73 del regolamento ⁶⁴, forniscono ai soggetti richiedenti i dati sanitari (utenti/utilizzatori dei dati o *data user*) l'accesso per usi secondari, in forma anonima o pseudonimizzata, così come esplicitato al considerando 72.

Se il richiedente i dati intende accedere ai dati sanitari elettronici personali in forma pseudonimizzata, congiuntamente alla domanda di accesso, egli è tenuto a fornire, ai sensi dell'art. 67 ⁶⁵, una descrizione di come il trattamento al quale procederebbe sarebbe conforme alla normativa nazionale e alla normativa dell'UE applicabile in materia di protezione dei dati e di privacy, in particolare dovrebbe descrivere come il trattamento sarebbe compatibile con il GDPR e, nello specifico con l'art. 6, comma 1, del GDPR. In caso di autorizzazione fornita dall'organismo di accesso ai dati (secondo le procedure previste agli artt. 68 e 69), i titolari di dati hanno l'obbligo di rendere disponibili i dati detenuti, al minimo nelle categorie previste dall'art. 51, salve ulteriori categorie individuate dalle legislazioni nazionali, per un periodo di tempo limitato allo svolgimento delle analisi per uso secondario.

I principali obblighi a carico dei titolari dei dati sanitari disciplinati all'art. 60 ⁶⁶ implicano che se vi è una richiesta dell'organismo di accesso ai dati sanitari o un permesso, il titolare dei dati è tenuto a rendere disponibili i dati sanitari elettronici e a comunicare una descrizione dell'insieme di dati in suo possesso, verificando, almeno su base annuale, che la descrizione dell'insieme di dati in suo possesso sia accurata e aggiornata negli insiemi di dati contenuti nel catalogo nazionale.

Con norma speciale e che prevale, per espressa previsione, sull'art. 6 del regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA), il Regolamento EHDS prevede (art. 62, dedicato alle tariffe o '*fees*') la possibilità per gli organismi di accesso ai dati di imporre tariffe per la messa a disposizione dei dati sanitari elettronici per un uso secondario, al fine di coprire i costi della procedura per valutare le domande di accesso ai dati o di richiesta di dati, concedere, rifiutare o modificare un permesso di dati, fornire una risposta a una richiesta di dati e, eventualmente, risarcire i costi sostenuti dal titolare dei dati sanitari per

⁶⁴ Si fa riferimento ai seguenti articoli: art. 68 '*data permit*', art. 69 '*health data request*', art. 73 '*secure processing environment*'.

⁶⁵ L'art. 67 disciplina le '*data access*

applications', appunto le domande di accesso ai dati

⁶⁶ L'art. 60 è dedicato a '*Duties of health data holders*'.

la compilazione e la preparazione dei dati sanitari elettronici da rendere disponibili per un uso secondario.

Il coordinamento degli organismi di accesso ai dati sanitari a livello dell'UE e l'inserimento dei loro compiti e delle loro attività in un disegno comune basato su analoghe funzioni, medesimi requisiti di interoperabilità e sovrapponibili modelli di governance, è stato infine pensato per garantire parità di condizioni così da spingere il riutilizzo anche transfrontaliero dei dati sanitari e la promozione del mercato interno dell'UE per i dati sanitari elettronici in linea con l'art. 114 del TFUE.

5. TITOLARITÀ PER FINALITÀ SECONDARIE.

Un raffronto tra le tassonomie (si veda la tabella che segue) previste nel regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR), nel regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA) e nel regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS), appare utile soprattutto per i risvolti che può avere sul piano applicativo per l'uso secondario, laddove le categorie dei Soggetti titolari dei dati e del loro trattamento sono riconducibili a nozioni non sempre sovrapponibili.

Nel nuovo regolamento sullo Spazio Europeo dei Dati Sanitari sono ad esempio contenute nozioni di titolare del dato e di titolare del trattamento del dato distinte tra gli ambiti dell'uso primario (che riprende le tassonomie del GDPR) e dell'uso secondario (ove sono introdotte nuove nozioni), pur rappresentando il GDPR la base normativa richiamata sia dal DGA che dal regolamento EHDS. Quest'ultimo, con riguardo agli usi secondari consentiti (previsti all'articolo 53) intende creare un ecosistema digitale gestito da enti o servizi interni ad enti nel settore pubblico, esistenti o nuovi, denominati *Health data access bodies* o *HDAB* (organismi responsabili dell'accesso ai dati sanitari - artt. 55 e 57) e individuati dagli Stati membri. Si tratta degli organismi che forniscono a soggetti richiedenti i dati sanitari (*health data applicant - health data user*), l'accesso ai dati sanitari per detti usi secondari consentiti (se in presenza dei requisiti prescritti), in forma anonima o pseudonomizzata (che può essere attuata dall'organismo di accesso ai dati *HDAB* o dal titolare dei dati - *data holder*), all'interno di un ambiente sicuro di trattamento (*Secure Processing Environment* - art. 73).

Se l'utente richiedente intende accedere ai dati sanitari elettronici personali in forma pseudonomizzata, congiuntamente alla domanda di accesso egli è tenuto a fornire informazioni aggiuntive tra cui una descrizione delle modalità con cui il trattamento si conformerebbe all'art. 6(1) del GDPR, nonché una valutazione d'impatto ex art. 35 GDPR ove ne ricorrano i requisiti. In caso di autorizzazione fornita dall'*HDAB* (secondo le procedure previste

agli artt. 68 e 69 del regolamento) i titolari di dati (*data holder*) hanno l'obbligo di rendere disponibili i dati detenuti, al minimo nelle categorie previste dall'art. 51.

TITOLARE DEL DATO PERSONALE

Regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR)

Data Subject: il GDPR (art. 4, par. 1) inquadra questa figura come la persona fisica cui appartengono i dati ('soggetto interessato') che può essere identificata, con riferimento al nome, al numero di identificazione, ai dati relativi all'ubicazione, a un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA)

Data Subject: il DGA (art. 2, par. 7) rimanda a definizione e funzioni sanciti nell'art. 4, num. 1, del GDPR.

Data Holder: ai sensi del DGA (art. 2 par. 8) è la persona giuridica (compresi enti pubblici e organizzazioni internazionali) o la persona fisica diversa dal soggetto interessato (*data subject*) cui appartengono i dati primari che, conformemente al diritto nazionale o dell'Unione Europea (UE) applicabile nella fattispecie, ha il diritto di concedere l'accesso a determinati dati personali (o non personali) o di condividerli.

Regolamento sullo spazio europeo dei dati sanitari (European Health Data Space - EHDS)

Health Data Holder: secondo il regolamento EHDS (art. 2, par. 2, lett. *t*) il titolare dei dati può essere qualsiasi persona fisica o giuridica (incluse autorità pubbliche, strutture sanitarie, industrie, agenzie, aziende) che ha la capacità di trattare o di rendere disponibili (registrare, fornire e limitare l'accesso, scambiare) determinati dati sanitari, assumendo nell'ultimo caso anche il ruolo di controller.

TITOLARE DEL TRATTAMENTO DEL DATO PERSONALE

Regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR)

Data Controller: il GDPR (art. 4, par. 7) determina le finalità e i mezzi del trattamento di dati personali. Se le finalità e i mezzi del trattamento sono determinati dal diritto dell'Unione Europea (UE) o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione Europea (UE) o degli Stati membri.

Regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA)

Data Holder: ai sensi del DGA (art. 2, par. 8) lo stesso titolare dei dati ha diritto al loro trattamento, diritto di concedere l'accesso a determinati dati personali o di condividerli.

Regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS)

Health Data Access Body: ai sensi del regolamento EHDS (art. 55 e 74.1) sono gli organismi responsabili del trattamento dei dati personali sanitari elettronici per finalità secondarie e

quello dell'accesso a tali dati e del loro trattamento quando gli utenti/utilizzatori ne facciano richiesta. Il trattamento deve avvenire negli ambienti sicuri di trattamento.

UTENTE DEL DATO

Regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR)

Recipient: è colui che riceve i dati personali ai sensi del GDPR (art. 4, par. 9). Le autorità pubbliche che possono ricevere dati personali nell'ambito di una particolare indagine conformemente al diritto dell'Unione Europea (UE) o degli Stati membri non sono considerate destinatari. Il trattamento dei dati personali da parte di tali autorità pubbliche dovrà avvenire nel rispetto delle norme sulla protezione dei dati applicabili in base alle finalità del trattamento.

Regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA)

Data User: il DGA (art. 2, par. 9) riconosce l'utente dei dati in colui che ha accesso legittimo a determinati dati personali o non personali e ha il diritto, anche ai sensi del GDPR, di utilizzarli per fini commerciali o scopi non commerciali.

Regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS)

Health Data User: l'EHDS (art. 2, par. 2, lett. u) riconosce l'utente dei dati sanitari in colui che ha accesso legittimo ai dati sanitari elettronici (personali e non personali) per uso secondario sulla base di un permesso o di una richiesta di accesso ai dati ai sensi del regolamento stesso.

Dal raffronto tra le tassonomie previste nel GDPR, DGA e EHDS si evince come la nozione di titolare di dati (data holder) fornita dall'EHDS riprende, specificandola, quella già utilizzata nel DGA, e richiama espressamente la nozione di titolare del trattamento ai sensi GDPR, con riguardo ai dati personali. Quanto ai dati anonimi/anonimizzati, ossia non personali, la nozione di titolare dei dati presente nell'EHDS fa, invece, riferimento ad una più ampia gamma di Soggetti, siano persone fisiche che giuridiche. In proposito occorre inoltre specificare che l'EHDS, esclude dagli obblighi generali previsti per i titolari dei dati sanitari (*health data holder*) le seguenti categorie di Soggetti: persone fisiche, singoli ricercatori e persone giuridiche qualificate come microimprese ai sensi dell'art. 2 dell'allegato della raccomandazione 2003/361/CE della Commissione delle Comunità Europee ⁶⁷.

⁶⁷ Commissione delle Comunità Europee, Raccomandazione della Commissione

del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie im-

6. FINALITÀ D'INTERESSE PUBBLICO.

Come più volte è emerso, il legislatore italiano, adeguandosi agli artt. 5, 6 e 9 e al cons. 50 del regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR), ha ritenuto ammissibile la possibilità di utilizzare ulteriormente i dati personali, e nello specifico quelli sanitari, per finalità di interesse pubblico ⁶⁸.

Il legislatore europeo, con l'art. 17, lett. c) del GDPR, ha previsto che il trattamento ulteriore (uso secondario) dei dati sanitari personali, in presenza dell'opposizione dell'interessato all'utilizzo degli stessi, possa avvenire se si deve eseguire un compito di interesse pubblico.

Nel concetto di interesse pubblico rientrano sicuramente, sulla base del considerando 52 del GDPR, il settore del diritto del lavoro e della protezione sociale, comprese le pensioni, la sicurezza sanitaria, la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute.

L'uso secondario dei dati personali per finalità di interesse pubblico deve limitarsi a ciò che è necessario per raggiungere l'obiettivo per il quale si procede, dovendo, quindi, come si deduce dagli artt. 6 e 9 del GDPR, rispettare i principi di proporzionalità e necessità.

In Italia, i motivi legittimanti il trattamento dei dati personali sanitari per finalità di interesse pubblico sono stati elencati nell'art. 2 *sexies* del d.lgs. n. 196 del 30 giugno 2003 (Codice Privacy) e corrispondono ad attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale; a compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di sicurezza e salute della popolazione; ad attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria; ad attività di vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; alla tutela sociale della maternità e interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili; ai trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, per fini di ricerca scientifica.

prese, in *eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32003H0361*.

⁶⁸ Per approfondire il tema dell'uso dei dati personali per finalità di interesse pubblico si v. G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in La protezione dei dati personali in Italia. Re-*

golamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, Zanichelli, Bologna, 2019, pag. 194 e ss.; F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giapichelli, Torino, 2021, pag. 357 e ss.

Questi motivi sono stati successivamente ampliati dal d.lgs n. 139 dell'8 ottobre 2021 (Decreto Capienze) convertito con modifiche nella Legge n. 205 del 2021 del 3 dicembre 2021 ⁶⁹, che ha aggiunto all'art. 2 *ter* del Codice Privacy il comma 1 *bis*, ai sensi del quale “[...]il trattamento dei dati personali da parte di un’amministrazione pubblica [...] è anche consentito se necessario per l’adempimento di un compito svolto nel pubblico interesse o per l’esercizio di pubblici poteri a essa attribuiti. [...]”.

La ragione per la quale il legislatore italiano ha provveduto ad ampliare i motivi che legittimano il trattamento dei dati personali sanitari per finalità di interesse pubblico risiede nella necessità di conformare la disciplina a quanto previsto dal GDPR, il quale dispone che il trattamento di dati personali, anche quello specifico dei dati sanitari, necessario per l’esecuzione di un compito di interesse pubblico, debba basarsi sul diritto dell’Unione Europea UE o dello Stato membro cui è soggetto il titolare del trattamento.

Il Decreto Capienze ha, inoltre, apportato modifiche alle basi giuridiche che legittimano il trattamento dei dati personali per finalità di interesse pubblico, prevedendo che la base giuridica stabilita dal diritto dello Stato membro cui è soggetto il titolare del trattamento (di cui all’art.6, par. 3, lett. *b*) del GDPR) di dati genetici, biometrici e dati personali relativi alla salute per motivi di interesse pubblico sia una norma di legge o di regolamento o un atto amministrativo generale a condizione che, con il medesimo strumento, si individuino:

- i tipi di dati che possono essere trattati;
- le operazioni eseguibili;
- il motivo di interesse pubblico rilevante;
- le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato.

Gli atti amministrativi generali sono *lex specialis*, regolamentano in modo generale un determinato evento giuridico e sono destinati ad una platea di soggetti determinabili solo *ex post*; ne sono esempi le direttive, i bandi, gli atti con i quali vengono fissati livelli di prestazione nei servizi pubblici.

In ambito sanitario, gli atti amministrativi generali sono documenti che regolamentano l’organizzazione e l’attività del Ministero della Salute e del Servizio Sanitario Nazionale.

L’inserimento degli atti amministrativi generali tra le basi giuridiche che legittimano il trattamento dei dati personali per finalità di interesse pubblico comporta, dunque, che anche un atto am-

⁶⁹ Per la normativa si rimanda a <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-10-08;139!vig=2021-10-11>. Per un approfondimento sulle conseguenze generate sulla pri-

vacy nel settore sanitario dal Decreto Capienze si v. M. ALOVISIO, *L’impatto della legge di conversione del decreto capienze sulla privacy nel settore pubblico e sanitario*, 2021, in www.dirittoegiustizia.it.

ministrativo possa legittimare il trattamento (e il riutilizzo) dei dati personali effettuato ai sensi dell'art. 6, par. 1, lett. c) ed e), attribuendo la facoltà alle pubbliche amministrazioni di abilitare e disciplinare in via generale, con proprio provvedimento, il trattamento di specifiche categorie di dati personali di cui all'art. 9 del GDPR.

Il che significa che, ove l'organizzazione degli organismi competenti fosse per esempio demandata *ratione materiae* a specifici ministeri o enti, questi stessi, restando in linea con le prescrizioni generali del GDPR e del Codice Privacy, avrebbero un potere normativo sufficiente per offrire idonea base giuridica al trattamento necessario per la predisposizione al riutilizzo dei dati. Del resto, il Decreto Capienze offre ad una ampia platea di enti pubblici e società a controllo pubblico una base giuridica — condizionata alle opportune cautele e fermo il rispetto dell'art. 6 GDPR — per i trattamenti necessari “per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a esse attribuiti”.

Il Decreto Capienze riconosce, dunque, negli atti amministrativi generali una base giuridica abilitante per l'uso dei dati personali per finalità di rilevanza sociale, incluso l'ambito sanitario, come la ricerca scientifica, la formazione e la sperimentazione.

Il Decreto Capienze ha, poi, apportato altre importanti modifiche in ambito di trattamento di dati personali, come l'abrogazione dell'art. 2 *quinquiesdecies* del Codice Privacy (che prevedeva, per l'esecuzione di compiti di interesse pubblico a rischio elevato, come quelli relativi ai dati sanitari, il potere del Garante per la protezione dei dati personali di prescrivere misure e accorgimenti a garanzia dell'interessato), la riduzione al termine di trenta giorni del potere entro il quale il Garante per la protezione dei dati personali deve intervenire per formulare ed esprimere un parere sulle riforme, le misure e i progetti riguardanti il Piano Nazionale di Ripresa e Resilienza - PNRR (decorso questo termine il Governo può procedere senza il parere).

Con il Decreto Capienze è stato, infine, introdotto anche il comma 5 *bis* all'art. 154 del Codice Privacy, che interviene sul potere consultivo che il Garante per la protezione dei dati personali deve esercitare se il trattamento dei dati personali presenta un rischio elevato. Questo articolo ha limitato le ipotesi di consultazione preventiva del Garante per la protezione dei dati personali ai soli casi in cui la legge o il regolamento in corso di adozione disciplinano espressamente le modalità del trattamento di dati personali.

Alla luce di tale intervento di modifica non sarà, per esempio, necessaria la consultazione del Garante per la protezione dei dati personali nel caso in cui si debba adottare un atto legislativo che non disciplina puntualmente un trattamento ma ne definisce solo le finalità e i motivi di rilevante interesse pubblico o nel caso in cui

un ente pubblico intenda disciplinare con un atto amministrativo generale dei trattamenti che contemplano dati personali comuni o dati di natura particolare.

Per gli atti legislativi che, invece, disciplinano espressamente il trattamento di dati personali, rimane necessario consultare il Garante per la protezione dei dati personali, poiché si possono produrre effetti negativi sugli interessati.

La *ratio* della consultazione preventiva del Garante per la protezione dei dati personali si sposta, quindi, su un piano di tutela sostanziale.

Anche se il Decreto Capienze non definisce in nessun caso le categorie dei dati personali sui quali interviene, si possono far rientrare, con un ragionamento per analogia, i dati genomici tra quelli ad alto rischio cui il Decreto Capienze fa indirettamente riferimento. Si può, quindi, intendere che le modifiche che il legislatore apporta con riferimento all'allargamento dei motivi legittimanti il trattamento dei dati personali per finalità di interesse pubblico e con riferimento alla limitazione del potere consultivo del Garante per la protezione dei dati personali da esercitare in caso di specifici trattamenti di dati personali, ricomprendano anche i dati genomici.

7. FINALITÀ DI RICERCA SCIENTIFICA.

L'uso secondario — ossia l'ulteriore trattamento — dei dati personali sanitari è basilare per numerose finalità di interesse pubblico, come le scoperte medico-scientifiche⁷⁰, tra cui la comprensione delle malattie e lo sviluppo di terapie mirate come nel caso della medicina personalizzata.

In Italia, quando l'uso secondario coincide con finalità di ricerca scientifica *“compatibili con le finalità per le quali i dati sono stati inizialmente raccolti”*⁷¹, tale ulteriore trattamento è considerato ammissibile dal momento che — ai sensi del regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation -

⁷⁰ Sull'uso dei dati personali per la ricerca scientifica nella sanità si v. S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 (GDPR) e al novellato d.lgs. 101/2018 (Codice Privacy)*, Giuffrè Francis Lefebvre, Milano, 2019, pagg. 579-620. Sulla volontà — o meno — di favorire la ricerca scientifica con la normativa europea, nazionale e con i provvedimenti del Garante si rimanda a un interessante contributo di M. LIOTTA, *Il favor per la ricerca scientifica e la sua*

effettiva applicazione nella normativa europea, nazionale e da parte dell'autorità garante, in questa *Rivista*, 2024, pagg. 363-384.

⁷¹ Si veda in proposito il considerando 50 del GDPR che recita: «[...] Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. [...]».

GDPR)⁷² e del d.lgs. n. 196 del 30 giugno 2003 (Codice Privacy) così come modificato dal d.lgs. n. 101 del 10 agosto 2018 (artt. 110 e 110 *bis*) — non è richiesta alcuna base giuridica separata da quella che ha consentito la raccolta dei dati personali, ossia il consenso dell'interessato⁷³. Nel caso in cui, invece, si presenti la necessità di trasferire i dati personali sanitari da un soggetto titolare del trattamento ad un altro, per finalità differenti da quelle originarie, in assenza del consenso dell'interessato, o quando si presenti la necessità di trattare i dati per attività di ricerca scientifica non identificate preventivamente, il GDPR chiarisce che quando non sia possibile individuare pienamente le finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati, “*dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica*”⁷⁴.

Il Garante per la protezione dei dati personali, con il provvedimento n. 9091942 del 7 marzo 2019 recante “Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario”, aveva fatto luce su alcuni aspetti critici relativi al trattamento dei dati sanitari, che davano adito a dubbi interpretativi per come disciplinati dal GDPR e dal d.lgs. 101/2018. In particolare, secondo la citata disposizione del Garante, il consenso del paziente per il trattamento dei dati relativi alla salute non deve necessariamente essere acquisito dal professionista sanitario quando il trattamento è necessario per perseguire finalità in linea con quanto disposto dall'art. 9, par. 2, lett. h) del GDPR⁷⁵. Mentre invece, per quanto attiene “*agli eventuali trattamenti attinenti, solo in senso lato alla cura, ma non stret-*

⁷² Per il trattamento dei dati personali sanitari per finalità di ricerca scientifica si v. N. BUSCA, *GDPR e ricerca scientifica: i requisiti al trattamento dei dati sanitari nel pubblico interesse*, in *Responsabilità medica. Diritto e pratica clinica*, 2020, pag. 417 e ss.

⁷³ Per alcuni approfondimenti sull'uso dei dati personali per finalità di ricerca scientifica si v. R. CIPPITANI, *Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali*, in *Cyberspazio e Diritto*, 2019, pag. 161 e ss.; F. DI TANO, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, in *BioLaw Journal - Rivista di BioDiritto*, 2022, pag. 71 e ss.

⁷⁴ Considerando 33 GDPR: «[...] In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, do-

vrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista. [...]».

Il legislatore ha — sempre — come obiettivo primario la protezione dei dati personali. Sul tema si v. A. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Le Nuove Leggi Civili Commentate*, 2020, pag. 175 e ss.

⁷⁵ «[...] il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o so-

tamente necessari”, anche se gli stessi siano effettuati da professionisti della sanità, deve essere individuata una distinta base giuridica nel consenso dell’interessato o in un altro presupposto di liceità.

Ai sensi delle Regole Deontologiche per trattamenti a fini statistici o di ricerca scientifica (provvedimento n. 9069637 del 19/12/2018 del Garante per la protezione dei dati personali ⁷⁶), le disposizioni del Garante prevedono che per tutti i trattamenti di dati che non risultino necessari ai fini della cura del paziente, è necessario il consenso del paziente quale ulteriore condizione di liceità, che, naturalmente, può sempre essere revocato. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso anche soltanto a determinati settori di ricerca o parti di progetti di ricerca che siano in linea con la finalità originaria del trattamento. Se, poi, i dati raccolti per finalità di ricerca in determinati settori specifici possono essere utili per ulteriori specifici studi, il titolare del trattamento dovrà procedere a raccogliere nuovamente il consenso degli interessati. Si parla, in questi casi, di consenso “a fasi progressive” ⁷⁷. Non si può dunque far rientrare, nell’informativa per l’ottenimento del consenso, la richiesta dello stesso anche per studi futuri e non ancora identificati con esattezza nelle loro caratteristiche, benché ritenuti idonei con le finalità dello studio originario.

Con successivo parere (n. 9791886 del 30/6/2022) ⁷⁸, il Garante ha poi ritenuto che il titolare del trattamento dovesse acquisire anche ulteriori e specifici consensi presso gli interessati “*in relazione a ciascuno degli studi di ricerca futuri che intenderà realizzare, all’esito dell’approvazione degli stessi progetti di ricerca da parte dei competenti Comitati etici*”.

Ci sono, però, delle possibili esimenti dal consenso per il trattamento dei dati personali sanitari dell’interessato per finalità di ricerca scientifica, che sono state individuate dal legislatore italiano nell’art. 110 del Codice Privacy, come modificato dal d.lgs.

ciali sulla base del diritto dell’Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3 [...] ».

⁷⁶ Provvedimento n. 9069677 del Garante per la Protezione dei Dati Personali del 19 dicembre 2018 in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069677>.

⁷⁷ Parere n. 9791886 del 30/6/2022 del Garante per la Protezione dei Dati Personali ai sensi dell’art. 110 del Codice e dell’art. 36 del GDPR in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9791886>.

⁷⁸ Richiesta di parere da parte dell’Azienda Ospedaliera Universitaria Integrata di Verona, Piazzale Aristide Stefani, 1 - 37126 Verona, Partita Iva/C.F. 03901420236, per il trattamento di dati personali per finalità di ricerca medica, biomedica ed epidemiologica, nello studio osservazionale interdipartimentale, prospettico e retrospettivo, su pazienti sottoposti a interventi del distretto toracico per patologie neoplastiche, infettive, degenerative e traumatiche denominato “DB Torax”.

101/2018⁷⁹. In particolare, il legislatore italiano ha ritenuto che il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea (UE), quando *“informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca”*. Al successivo art. 110 bis il legislatore ha poi previsto che, per il *“trattamento ulteriore dei dati sanitari da parte di terzi a fini di ricerca scientifica o a fini statistici”*, nel caso in cui *“informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca”*, si possa ricorrere all'autorizzazione del Garante per la protezione dei dati personali.

Tra i pareri espressi dal Garante, però, compaiono poche autorizzazioni al trattamento ulteriore per fini di ricerca scientifica da parte di terzi⁸⁰. Il motivo per il quale il Garante tende a non autorizzare l'uso secondario dei dati personali sanitari per ulteriori finalità di ricerca scientifica si può desumere bene dal provvedimento n. 9772545 del 7/4/2022⁸¹, mediante il quale l'Autorità di controllo fa emergere che la normativa applicabile in

⁷⁹ « [...] 1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'art. 9, par. 2, lett. j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12 bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'art. 36 del Regolamento.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca. [...] ».

⁸⁰ Ne è un esempio il Provvedimento n. 9731827 del Garante per la protezione dei dati personali del 1° novembre 2021 in <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9731827>.

⁸¹ Richiesta di parere da parte dell'Azienda Ospedaliero Universitaria di Parma, Via Gramsci 14 - 43126 Parma, Partita Iva/C.F. 01874240342, per il trattamento dei dati personali per finalità di ricerca medica, biomedica ed epidemiologica, riferiti alla coorte di pazienti arruolati nello studio no profit, multicentrico, osservazionale, retrospettivo, non farmacologico denominato “Effetti dell'infezione da SARS-CoV-2 sugli accessi al pronto soccorso e sui ricoveri della popolazione di età pediatrica e adolescenziale”. Provvedimento n. 9772545 del Garante per la Protezione dei Dati Personali del 7 aprile 2022 in <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9772545>.

seguito ad una richiesta di trattamento dei dati è l'art. 110 del Codice Privacy, come modificato dal d.lgs. 101/2018, in virtù del quale, nelle ipotesi in cui non è necessario il consenso degli interessati ⁸², il programma della ricerca deve essere sottoposto ad una valutazione preventiva da parte del Garante. L'istanza di consultazione preventiva (ex art. 36 GDPR) rappresenta, secondo il parere del Garante, *“una norma di chiusura per consentire che trattamenti di dati personali che si sarebbero dovuti fondare sul consenso degli interessati possano comunque essere svolti”*.

Con la legge n. 56/2024 (in conversione del D.L. n. 19/2024 c.d. “Decreto PNRR bis”), entrata in vigore il 1 maggio 2024 ⁸³, è subentrata la modifica dell'art. 110 del Codice Privacy in tema di trattamento dei dati personali sanitari, che ha riguardato essenzialmente la parte finale dell'articolo in quanto le parole: *“e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento”*, sono sostituite dalle seguenti *“Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice”*. Si fa dunque riferimento alle modalità di trattamento dei dati relativi alla salute ai fini di ricerca scientifica nei casi in cui non sia possibile raccogliere il consenso dell'interessato, ossia ai casi in cui, prima della modifica, era obbligatorio ottenere, oltre al parere favorevole del comitato etico territorialmente competente, anche un parere del Garante tramite l'istituto della consultazione preventiva ex art. 36 GDPR, che attualmente viene meno essendo sostituita da un generale provvedimento del Garante indicante le garanzie da osservare ai sensi dell'art. 106 c. 2 lett. d).

Con deliberazione del 9 maggio 2024, recante *“regole deontologiche per il trattamento dei dati a fini statistici o di ricerca scientifica ai sensi degli artt. 2 quater e 106 del Codice della Privacy”*, il Garante per la protezione dei dati personali ha dunque adottato le garanzie che i titolari del trattamento di dati sulla salute per finalità di ricerca dovranno osservare ai sensi del citato art. 110 Codice Privacy, in sostituzione della previgente obbligatoria consultazione preventiva. In particolare, il Garante ha stabilito che il titolare del trattamento, oltre ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca

[garanteprivacy.it/home/docweb/-/docweb-display/docweb/9772545](https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9772545).

⁸² Ossia quando « [...] informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare grave-

mente il conseguimento delle finalità della ricerca [...] ».

⁸³ Per la normativa si rimanda a <https://www.gazzettaufficiale.it/eli/gu/2024/04/30/100/so/19/sg/pdf>.

come previsto dall'art. 110 del Codice Privacy, deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso. Se acquisire il consenso risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, bisogna altresì documentare i ragionevoli sforzi profusi per tentare di contattarli. I titolari del trattamento di dati relativi alla salute riferiti a soggetti deceduti o non contattabili devono svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 del GDPR dandone comunicazione al Garante.

In pratica, fino al sopraggiungere dell'ultima modifica dell'art.110 del Codice Privacy, nei casi in cui vi era la necessità di procedere a una ricerca scientifica retrospettiva nell'impossibilità di ottenere il consenso del paziente, il ricercatore o il centro clinico interessato allo studio per conto del ricercatore, oltre al motivato parere favorevole del comitato etico e alla redazione di una valutazione di impatto sulla protezione dei dati (DPIA) ex art. 35 GDPR (la quale è ritenuta necessaria quando un trattamento *“può presentare un rischio elevato per i diritti e le libertà delle persone fisiche”*), doveva anche rivolgersi direttamente al Garante Privacy tramite lo strumento della consultazione preventiva (art. 36 GDPR). La modifica del citato art.110 permette invece, attualmente, che per finalità di ricerca scientifica in ambito medico, biomedico ed epidemiologico, i dati siano trattati anche nell'impossibilità di raccogliere il consenso degli interessati, non appena acquisito il parere favorevole del competente comitato etico e osservate le garanzie individuate dal Garante ai sensi dell'art. 106, c. 2, lett. d) del Codice Privacy. Dunque, la consultazione preventiva scompare come adempimento obbligatorio ritornando a essere, come nelle intenzioni originarie del GDPR, un'attività da compiere solo se, all'esito della valutazione d'impatto permangono rischi residui, che il titolare del trattamento (nella fattispecie il ricercatore) non è in grado di mitigare mediante l'adozione di adeguate misure di garanzia, così come prescritte dal Garante. Specificatamente, si fa riferimento alle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica* (allegato A5 al Codice) adottate dal Garante, ai sensi dell'art. 20, c. 4, del d.lgs. 10 agosto 2018, n. 101, con provvedimento n. 515 del 19 dicembre 2018⁸⁴, nonché alle *Prescrizioni relative al trattamento dei dati genetici e al trattamento dei dati personali effettuato per scopi di ricerca scientifica*, allegati 4 e 5

⁸⁴ Si veda in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637>.

al provvedimento del Garante n. 146 del 5 giugno 2019, recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, c. 1 del d.lgs. 10 agosto 2018, n. 101⁸⁵, su cui l'Autorità è intervenuta con modifiche nel provvedimento del 9 maggio 2024 recante *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2 quater e 106 del Codice*⁸⁶.

Per quanto riguarda l'evoluzione della normativa europea in materia di uso secondario dei dati per finalità di ricerca scientifica, il regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA) sulla governance dei dati, offre nello specifico sbocchi risolutivi limitati poiché segue il GDPR e non può intendersi come una normativa europea che disciplina il trattamento dei dati già legittimato dagli artt. 6 e 9 del GDPR⁸⁷. In materia di dati personali, quindi, il diritto nazionale di implementazione del GDPR prevale sul DGA e ogni normativa più restrittiva o permissiva nazionale — non in contrasto con il GDPR — prevale sul DGA, cosicché chiusure o aperture al riuso dei dati personali offerti dal diritto italiano — nella specie ai sensi del Codice Privacy — rimangono immutate, anche a valle del DGA. D'altro canto, il DGA favorisce un riutilizzo più efficiente — anche per finalità di ricerca scientifica — dei dati (personali e non personali, ivi compresi quelli personali relativi alla salute) detenuti nel settore pubblico⁸⁸, stabilendo l'obbligo per gli enti pubblici di creare le condizioni e la procedura per consentire l'uso secondario di questi dati⁸⁹, senza imporre la concessione dell'accesso ai dati per la realizzazione di finalità ulteriori alla cura. Dal considerando 15 del DGA si evince chiaramente che gli enti pubblici possono concedere il riutilizzo dei dati (anonimizzati) per finalità di ricerca scientifica solo se la base giuridica che legittima il trattamento è una di quelle previste dal GDPR, di conseguenza le autorità alle quali pervengono le richieste di accesso ai dati devono eseguire un controllo sulla base giuridica del trattamento.

Più rilevante nel panorama europeo della disciplina dell'uso secondario dei dati personali sanitari, si presenta invece la riforma prevista dal nuovo regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS), che all'art. 53 individua le finalità per le quali i dati sanitari elettronici

⁸⁵ Si veda in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9124510>.

⁸⁶ Si veda in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10016146>.

⁸⁷ Per una riflessione critica sull'evoluzione della normativa europea sull'uso dei dati personali sanitari per la ricerca scientifica si v. P. Hajduk, *A Walk in the Laby-*

rinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research, 2023, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4673534.

⁸⁸ Art. 3, par. 1 Regolamento UE 2022/868 (DGA).

⁸⁹ Art. 5, par. 1 Regolamento UE 2022/868 (DGA).

possono essere trattati per uso secondario, ivi compresa la ricerca scientifica. Si tratta in senso ampio di attività connessa ai settori della sanità o dell'assistenza, che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di avvantaggiare gli utenti finali, quali pazienti, operatori sanitari e amministratori sanitari, tra cui: attività di sviluppo e innovazione di prodotti o servizi; formazione, test e valutazione di algoritmi, anche in dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di intelligenza artificiale e applicazioni sanitarie digitali.

Questo nuovo regolamento, assegnando agli organismi di accesso ai dati sanitari (Health Data Access Bodies) compiti di interesse pubblico ai sensi dell'art. 6, par. 1, lett. e) del GDPR, visti i requisiti dell'art. 9, par. 2, lett. g), h), i), j) del GDPR, fa rientrare le finalità di ricerca scientifica tra quelle di interesse pubblico per la quali permane il diritto di obiezione, ma decade l'obbligo del consenso (considerando 50 del GDPR). Il regolamento EHDS istituisce inoltre nell'UE un meccanismo unico (regole, requisiti e infrastrutture comuni) grazie al quale accedere ai dati personali (e non personali) sanitari elettronici per l'uso secondario, laddove gli Stati membri, con riferimento al trattamento dei dati personali per uso secondario, potranno interpretare in modo diverso il diritto di obiezione del soggetto interessato (ossia la persona fisica del paziente), per quanto riguarda le categorie di dati e le finalità di uso secondario cui essi possono essere destinati ai sensi del citato art. 53 del regolamento stesso. Il legislatore europeo si è dunque espresso con una *lex specialis* per disciplinare il riutilizzo dei dati personali e non personali sanitari elettronici, che troverà applicazione in luogo delle norme generali nazionali.

8. D.L. 249/2023 IN MATERIA DI FASCICOLO SANITARIO ELETTRONICO. __

Il Fascicolo Sanitario Elettronico (FSE) è stato introdotto in Italia con l'art. 12 del D.L. n. 179 del 18 ottobre 2012, con l'obiettivo di dematerializzare i referti medici, le cartelle cliniche e favorire uno scambio di informazioni anche a livello transfrontaliero, per la realizzazione di progetti europei del settore sanitario ⁹⁰. Successivamente, con il decreto del Presidente del Consiglio dei Ministri n. 178 del 29 settembre 2015 è stato pubblicato

⁹⁰ Per la normativa si rimanda a <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012;179>. Per un approfondimento sull'introduzione del Fascicolo Sanitario Elettronico in Italia e sul

rapporto dello stesso con il trattamento e la protezione dei dati personali si v. G. COMMANDÉ, L. NOCCO, V. PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Rivista italiana di medicina le-*

il regolamento in materia di FSE e sono stati individuati i contenuti e gli elementi che avrebbero dovuto caratterizzarlo come strumento nazionale che assicurasse l'interoperabilità nei casi di ricoveri in regioni non di residenza del paziente⁹¹. Negli anni seguenti, si sono susseguiti tavoli tecnici sul tema, con l'obiettivo di definire le caratteristiche dei documenti dell'FSE⁹².

A luglio 2022 è stato pubblicato in Gazzetta Ufficiale un decreto-legge contenente le Linee Guida per il potenziamento dell'FSE (FSE 2.0)⁹³, il quale ha previsto che lo stesso potesse essere utilizzato, grazie ai dati custoditi al proprio interno, per effettuare analisi dei dati clinici e migliorare l'erogazione dei servizi sanitari⁹⁴.

Il Garante per la protezione dei dati personali ha reagito, però, con parere negativo⁹⁵ al decreto di luglio 2022, richiedendo più garanzie sulla banca dati denominata Ecosistema Dati Sanitari (EDS). L'EDS era stato previsto dalla riforma dell'FSE per *“garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale”*, comportando la duplicazione di dati e documenti sanitari già presenti nell'FSE e la costituzione della più grande banca dati sulla salute dei cittadini italiani.

In seguito al parere negativo, un gruppo di esperti è stato incaricato, insieme al Garante per la protezione dei dati personali, di lavorare a un nuovo decreto (D.L. n. 249 del 24 ottobre 2023), che è stato pubblicato in Gazzetta Ufficiale il 24/10/2023 e all'interno del quale sono stati individuati i contenuti dell'FSE 2.0, i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei

gale, 2012, pag. 105 e ss.; S. BOLOCNA, A. BELLAVISTA, P. P. CORSO, G. ZANCARA, *Electronic Health Record in Italy and Personal Data Protection*, in *European Journal of Health Law*, 2016, pag. 265 e ss.

⁹¹ Decreto del Presidente del Consiglio dei Ministri del 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico. (15G00192) (GU Serie Generale n. 263 del 11-11-2015) in <https://www.gazzettaufficiale.it/eli/id/2015/11/11/15G00192/sg>.

⁹² Per alcune riflessioni sull'inquadramento a livello costituzionale del Fascicolo Sanitario Elettronico si v. C. BOTTARI, *L'inquadramento costituzionale del Fascicolo Sanitario Elettronico*, in *Salute e società*, 2017, pag. 65 e ss.

⁹³ Sul tema si v. S. CORSO, *Le Linee guida di attuazione del fascicolo sanitario*

elettronico, 2022, in www.rivistaresponsabilitamedica.it; G. ESCUROLLE, *Le novità sul Fascicolo Sanitario Elettronico (FSE)*, in *Cyberspazio e Diritto*, 2020, pag. 427 e ss.

⁹⁴ Decreto del 20 maggio 2022, Adozione delle Linee guida per l'attuazione del Fascicolo sanitario elettronico. (22A03961) (GU Serie Generale n.160 del 11-07-2022) in <https://www.gazzettaufficiale.it/eli/id/2022/07/11/22A03961/sg>.

⁹⁵ Parere n. 9802729 del 22/8/2022 del Garante per la Protezione dei Dati Personali al Ministero della Salute sullo schema di decreto, da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sul Fascicolo Sanitario Elettronico (FSE) in <https://www.garanteprivacy.it/home/docweb/-/docweb-display/print/9802729>.

diritti dell'assistito e le modalità e i livelli diversificati di accesso ⁹⁶.

Nel D.L. 249/2023 vi sono diversi articoli dedicati al trattamento, alla gestione, all'accesso e alla conservazione dei dati e dei documenti dell'FSE di ogni assistito. Contenendo una vasta raccolta di dati sanitari, l'FSE rileva sotto il profilo del trattamento — primario e secondario — dei dati personali: infatti, è necessario che vengano garantiti la raccolta, la consultazione e la conservazione dei dati personali nel pieno rispetto della normativa nazionale ed europea in materia di trattamento dei dati personali.

Pertanto, nei tre mesi successivi all'entrata in vigore del decreto, il Ministero della Salute, le Regioni e le Province Autonome hanno dovuto fornire agli assistiti un'informativa idonea dalla quale comprendere le modalità e le finalità dei trattamenti dei loro dati nell'FSE, quale presupposto di liceità del trattamento stesso, in ottemperanza a quanto previsto dagli artt. 13 e 14 del regolamento n. 679 del 27 aprile 2016 (General Data Protection Regulation - GDPR) e secondo le modalità che gli stessi prescrivono.

La consultazione, da parte di terzi, dei dati e dei documenti contenuti nell'FSE per le finalità di diagnosi, di cura, di riabilitazione, di prevenzione e di profilassi internazionale potrà dunque avvenire solo dopo che l'assistito abbia preso visione dell'informativa privacy e dopo che abbia espresso un consenso esplicito, libero, specifico, informato ed inequivocabile ⁹⁷. In caso di situazioni emergenziali, nelle quali il paziente non possa prestare il consenso alla consultazione dei dati contenuti nel proprio FSE, gli operatori sanitari coinvolti potranno accedervi, solo per il tempo strettamente necessario e ad eccezione dei dati e dei documenti per i quali l'assistito abbia richiesto l'oscuramento ⁹⁸. I dati e i documenti dell'FSE possono essere consultati per finalità di cura dal personale sanitario autorizzato e vengono trattati secondo livelli diversificati di accesso, che assicurano il rispetto dei principi previsti dall'art. 5 del GDPR. Se gli interessati sono soggetti che necessitano di maggiore tutela (come donne che si sottopongono a interruzione volontaria di gravidanza o che decidono di partorire in anonimato o che sono vittime di atti di violenza sessuale), i rispettivi dati possono essere resi visibili a chi eroga la prestazione solo previo consenso (anche telematico) esplicito, informato e specifico dell'interessato, che potrà anche decidere, esercitando i diritti di cui all'art. 9 D.L. 249/2023, di non renderli visibili.

⁹⁶ Decreto del 7 settembre 2023, Fascicolo sanitario elettronico 2.0. (23A05829) (GU Serie Generale n. 249 del 24-10-2023) in https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto

[/originario?atto.dataPubblicazioneGazzetta=2023-10-24&atto.codiceRedazionale=23A05829&elenco30giorni=false](#).

⁹⁷ Art. 8, par. 1 D.L. 249/2023.

⁹⁸ Art. 20 D.L. 249/2023.

Per quanto riguarda l'alimentazione, i soggetti che concorrono all'alimentazione e all'aggiornamento dell'FSE sono le aziende sanitarie locali, le strutture sanitarie pubbliche del Servizio Sanitario Nazionale (SSN) e dei servizi socio-sanitari regionali e i Servizi di Assistenza Sanitari ai Naviganti (SASN), le strutture sanitarie accreditate con l'SSN e i servizi socio-sanitari regionali, le strutture sanitarie autorizzate, gli esercenti le professioni sanitarie (quando operano in autonomia), le regioni e le province autonome⁹⁹. Tutti coloro che concorrono all'alimentazione dell'FSE devono farlo entro cinque giorni dall'erogazione della prestazione sanitaria e rispondono dell'alimentazione intempestiva, inesatta o assente. Le regioni e le province autonome, che concorrono all'alimentazione dell'FSE, possono, previo parere del Garante per la protezione dei dati personali, utilizzare i dati contenuti nell'FSE anche per finalità secondarie che siano riconducibili all'interesse pubblico¹⁰⁰.

Il trattamento dei dati sanitari finalizzato all'alimentazione dell'FSE costituisce un trattamento diverso e ulteriore rispetto a quello necessario per la cura del paziente, per questo motivo la base giuridica che lo legittima non è l'art. 9, par. 2, lett. h) del GDPR per il trattamento delle categorie particolari di dati personali, ma l'art. 9, par. 2, lett. a), cioè il consenso esplicito dell'interessato. La compilazione dell'FSE non è un'azione necessaria che deve porre in essere il paziente, per questo motivo la base giuridica che la legittima è il consenso, ex art. 6, par. 1, lett. a) del GDPR.

Il soggetto, che eroga la prestazione sanitaria, deve informare l'assistito della possibilità di poter esercitare, ex art. 9 del d.l. 249/2023, il diritto all'oscuramento dei dati, non rendendoli disponibili per la realizzazione di altri documenti. Si tratta di un diritto che può essere esercitato o al momento dell'erogazione della prestazione o in qualsiasi momento successivo attraverso una specifica istanza. Anche l'oscuramento dei dati può essere revocato dall'assistito in ogni momento. Se l'assistito esercita il diritto all'oscuramento dei dati in un momento successivo all'erogazione della prestazione, viene informato che può esserci già stato un trattamento degli stessi per la realizzazione di altri documenti.

Il mancato consenso dell'assistito al trattamento dei suoi dati e la conseguente scelta di ricorrere alla prestazione in modo anonimo, determina l'impossibilità per l'erogatore di alimentare l'FSE.

I dati e i documenti contenuti nell'FSE possono essere trattati anche per finalità secondarie rispetto alla cura, quali le finalità di

⁹⁹ Art. 12, par. 1 D.L. 249/2023.

¹⁰⁰ Art. 13, par. 1 D.L. 249/2023.

prevenzione e di profilassi internazionale. I titolari del trattamento dei dati dell'FSE per finalità di prevenzione sono i soggetti dell'SSN e dei servizi sociosanitari regionali della regione di appartenenza, gli esercenti le professioni sanitarie che hanno in cura l'assistito o che comunque gli prestano assistenza sanitaria, le regioni attraverso gli uffici competenti in materia di prevenzione sanitaria e il Ministero della salute attraverso la Direzione generale competente in materia di prevenzione sanitaria ¹⁰¹.

Il trattamento dei dati personali sanitari per finalità di prevenzione è disciplinato dall'art. 17 del D.L. 249/2023 e deve avvenire nel rispetto dei principi di minimizzazione, necessità e pertinenza, sempre previo consenso dell'assistito. Inoltre, i dati oggetto di questo ulteriore trattamento devono essere privati degli elementi identificativi dei soggetti cui si riferiscono e pseudonimizzati. L'assistito, ex art. 9 del D.L. 249/2023, può decidere di oscurare i suoi dati e di non renderli disponibili per la realizzazione delle altre finalità di prevenzione e di profilassi internazionale.

Il trattamento dei dati personali sanitari per finalità di profilassi internazionale mira a fronteggiare eventi improvvisi di sanità pubblica inaspettati e il titolare di tale trattamento è la Direzione generale del Ministero della salute che è competente in materia di profilassi internazionale.

La Direzione generale del Ministero della salute che è competente in materia di profilassi internazionale può trattare, previo consenso dell'interessato, solo i dati e i documenti dell'FSE che possono contribuire a rilevare sintomatologie o circolazioni collegate “[...]a nuovi patogeni o all'emergere di sintomatologie sconosciute o fattori di rischio ambientale e/o alimentare, nuovi fattori di rischio legati a patologie correlate, come co-infezioni, lo sviluppo di nuovi casi di farmacoresistenza verso specifici gruppi di patogeni e, infine, possibili nuove complicanze non conosciute di alcune malattie infettive che possono portare al decesso del caso [...]” ¹⁰².

Tra i vari usi secondari dei dati contenuti nel FSE, inizialmente, con il decreto di luglio 2022, erano stati individuati, oltre a quelli di cura, di prevenzione e di profilassi internazionale, anche quelli di ricerca scientifica e di governo sanitario. Tuttavia, nelle tappe finali di approvazione del citato decreto, questi aspetti non sono stati inclusi rimanendo così in vigore i Capi III e IV del d.P.C.M. 178/2015.

Resta dunque inteso che, ai sensi dell'art. 12, c. 2, lett. b) del D.L. 18 ottobre 2012, n. 179 (convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come da ultimo modificato dal D.L. 27 gennaio 2022, n. 4, convertito, con modificazioni, dalla

¹⁰¹ Art. 16, par. 1 e 2 D.L. 249/2023.

¹⁰² Art. 19 D.L. 249/2023.

legge 28 marzo 2022, n. 25), il FSE è istituito dalle Regioni e Province autonome, anche a fini di “*studio e ricerca scientifica in campo medico, biomedico ed epidemiologico*”, ma per poter rendere possibili questi usi secondari, occorre ancora attendere l’adozione di decreti contenenti “*specifiche disposizioni per i trattamenti dei dati e dei documenti del FSE per le finalità di ricerca e di Governo*” (art 27 c. 5 del D.L. 249/2023).

9. RIFLESSIONI CONCLUSIVE.

I recenti sviluppi del panorama legislativo dell’UE e dell’Italia sono orientati alla piena valorizzazione dei dati personali (e non personali) relativi alla salute, soprattutto per finalità di pubblico interesse tra cui la ricerca scientifica, la programmazione sanitaria, il miglioramento dei sistemi sanitari. Si procede — speriamo in tempo utile per affrontare tempestivamente le crescenti sfide demografiche, sociali ed economiche — verso una visione sistemica dell’uso secondario dei dati sanitari, basata sull’implementazione armonizzata di infrastrutture tecnologiche, requisiti e regole comuni di trattamento, nonché su un disegno di *governance* condiviso e integrato non solo a livello europeo ma anche nazionale, affinché un riutilizzo efficiente dei dati diventi concretamente possibile ed estensivamente praticabile nel rispetto dei diritti soggettivi di riservatezza e protezione dei dati stessi.

Di grande interesse dal punto di vista applicativo saranno le interazioni del nuovo regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS), di prossima pubblicazione sulla Gazzetta Ufficiale dell’UE, con le altre norme già vigenti in materia di trattamento e *governance* dei dati. Si fa riferimento, in particolare al regolamento (UE) 2016/679 sulla protezione dei dati (GDPR), che continua a fungere da cornice sistematica garantita da previsioni di non derogabilità, e al regolamento 2022/868 (DGA), quale norma intersettoriale che mira a regolamentare il riutilizzo di dati pubblici conservati e protetti, promuovendone la condivisione mediante il coinvolgimento di nuovi intermediari o l’incoraggiamento all’altruismo, e prevedendo una serie di salvaguardie per incentivare la fiducia delle parti interessate.

I principali profili di attenzione nel rapporto tra regolamento EHDS e GDPR risiedono nelle tassonomie utilizzate (di cui si è detto nel precedente paragrafo 5 sulla titolarità), nonché nell’implementazione delle procedure e nell’esercizio degli ulteriori diritti degli interessati, complementari agli analoghi diritti già previsti dal GDPR (menzionati nei precedenti paragrafi 4.4. e 7). Il rapporto tra EHDS e GDPR trova espressione anche nella necessità che gli aspiranti utenti (richiedenti) dei dati dimostrino l’esistenza di una base giuridica ai sensi del GDPR per accedere ai dati per uso secondario. Dunque, per legittimare l’uso secondario, il nuovo regolamento EHDS, distinguendo le fattispecie in

ragione dei soggetti che intervengono e delle attività di trattamento, prevede che i richiedenti i dati dimostrino di possedere una base giuridica per il trattamento che richiedono ai sensi dell'art. 6 del GDPR. I richiedenti i dati, una volta ottenuto il permesso di accesso, diventano così utenti abilitati all'uso secondario dei dati da parte degli Organismi di Accesso ai Dati. Questi ultimi, a loro volta, sono titolari responsabili¹⁰³ dei trattamenti dei dati nello svolgimento dei propri compiti, quando il trattamento è necessario per generare una risposta a una richiesta di accesso ai dati¹⁰⁴, e per conto degli utenti di dati (che diventano tali quando abilitati dal permesso di accesso) nell'attività di fornire loro i dati attraverso un ambiente di trattamento sicuro. Gli utenti dei dati (*data user*) diventano, allora, titolari dei trattamenti dei dati sanitari personali elettronici sulla base del permesso di accesso (rilasciato dall'organismo di accesso ai dati) e purché il trattamento avvenga in un ambiente sicuro. I titolari dei dati (*data holder*) sono tenuti (obbligati) a loro volta a rendere disponibili i dati personali elettronici agli organismi responsabili per l'accesso ai dati, i quali li renderanno fruibili agli utenti con permesso ottenuto.

In generale, per i trattamenti autorizzati, l'EHDS fornisce una base giuridica espressa, qualificando l'esimente al divieto di trattamento in conformità all'art. 9, par. 2, lett. g), h), i), j) del GDPR. L'EHDS non include infatti il consenso dell'interessato quale base giuridica che legittima il trattamento per uso secondario dei dati sanitari elettronici. Esso fornisce una base giuridica conformemente ai regolamenti 2016/679 e 2018/1725 per l'uso secondario di dati sanitari elettronici personali, comprese le garanzie per consentire il trattamento di categorie speciali di dati, conformemente agli artt. 9(2), lett. g), h), i) e j) del regolamento 2016/679 e agli artt. 10(2), lett. g), h), i) e j) del regolamento 2018/1725, in termini di finalità legittime, *governance* affidabile per fornire l'accesso ai dati sanitari (attraverso il coinvolgimento di organismi di accesso ai dati sanitari) e trattamento in un ambiente sicuro, nonché modalità per il trattamento dei dati, stabilite nel permesso di accesso ai dati. Di conseguenza, gli Stati membri dell'UE non possono più mantenere o introdurre, ai sensi dell'art. 9(4) del regolamento 2016/679, ulteriori condizioni, tra cui limitazioni e disposizioni specifiche che richiedono il consenso delle persone fisiche, per quanto riguarda il trattamento per uso

¹⁰³ Art. 74 (controllership), par. 1, del testo di accordo provvisorio raggiunto il 24 aprile 2024 tra Parlamento europeo e Consiglio in https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_IT.html#title1.

¹⁰⁴ Art. 68 (data permit - autorizzazione ai dati), del testo di accordo provvisorio raggiunto il 24 aprile 2024 tra Parlamento europeo e Consiglio in https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_IT.html#title1.

secondario di dati sanitari elettronici personali, fatta eccezione per alcune categorie di dati. Più specificamente, essi possono introdurre misure più rigorose e garanzie supplementari a livello nazionale (in ogni caso con obbligo di notifica alla Commissione europea), volte a salvaguardare la sensibilità e il valore di quei dati che rientrano nell'art. 51, par. 1, lett. *f*), *i*), *q*), e *g*) ossia: dati genetici, genomici ed epigenomici umani; altri dati molecolari umani (proteomici, trascrittomici, metabolomici, e altri dati omici); dati delle applicazioni per il benessere; dati delle biobanche e relativi *database*. E per essi si procederà con un meccanismo di obiezione (*opt-out*)¹⁰⁵ da parte dell'interessato cui quelle specifiche categorie di dati appartengono.

Quanto ai profili di attenzione nel rapporto tra DGA ed EHDS, pur non essendo il primo specificatamente riferito ai dati sanitari personali né prevalente sul secondo, vi è coerenza nel centrare l'attenzione su organismi competenti responsabili di gestire e governare il processo che va dall'individuazione dei dati condivisibili alla loro condivisione effettiva, passando per i diversi sviluppi necessari per abilitare la condivisione sul piano operativo allo scopo di qualificare tecnicamente il settore pubblico al riutilizzo dei dati.

Nell'interpretazione del DGA, tale qualificazione può avvenire anche con il supporto di intermediari, i quali sono — per lo scopo — chiamati a interagire con le diverse categorie di titolari dei dati (enti pubblici, organizzazioni internazionali, ma anche persone fisiche che abbiano il diritto di concedere l'accesso a determinati dati personali, o dati non personali, o di condividerli) per facilitare l'implementazione di requisiti tecnici necessari a garantire il pieno rispetto della *privacy* e della riservatezza dei dati nelle situazioni di riutilizzo. Si spazia quindi dalle soluzioni tecniche, come l'anonimizzazione, la pseudonimizzazione o l'accesso ai dati in ambienti di elaborazione sicuri sotto la supervisione del settore pubblico, a mezzi contrattuali come gli accordi di riservatezza conclusi tra ente pubblico e riutilizzatore (utente dei dati). Il DGA definisce una serie di regole per i fornitori di servizi di intermediazione di dati (di cui al Capo III) per garantire che funzionino come organizzatori affidabili della condivisione o della messa in comune di dati all'interno degli spazi comuni di dati europei per aumentare la fiducia nella condivisione dei dati.

Diversa è invece l'interpretazione delle entità di intermediazione data dall'EHDS (considerando 59) laddove per ridurre l'onere amministrativo e alla luce dei principi di efficacia ed

¹⁰⁵ Disciplinato all'art. 35f del testo compromesso oggetto di accordo provvisorio "Right to opt-out from the processing of personal electronic health data for secon-

dary use" in <https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf>.

efficienza, gli Stati membri devono decidere (tramite legislazione nazionale) per quali categorie di dati è possibile (eventualmente necessario) che talune categorie di titolari dei dati (*data holder*) si avvalgano di entità di intermediazione di dati sanitari per adempiere ai propri obblighi di mettere a disposizione i dati. Tali entità di intermediazione di dati sanitari devono dunque essere, ai sensi dell'EHDS, persone giuridiche in grado di elaborare e rendere disponibili per uso secondario i dati sanitari elettronici forniti dai titolari dei dati. Le entità di intermediazione di dati sanitari previste dall'EHDS, le quali non possono intendersi come *trusted*, svolgono comunque compiti diversi dai servizi di intermediazione di dati di cui all'art. 10 del DGA, poiché sono persone giuridiche in grado di rendere disponibili, (ossia, registrare, fornire, elaborare, limitare l'accesso o scambiare) dati sanitari elettronici forniti dai titolari dei dati per l'uso secondario.

Alla luce di quanto sopra, tra gli svariati punti di contatto ma anche i possibili punti di distanza che emergono nel raffronto tra riforme in materia di dati, con particolare riferimento a quelli sanitari e al loro uso secondario, sarà allora necessario dedicare la massima attenzione all'integrazione nazionale ai fini della migliore implementazione di una normativa armonizzata.

Abstract

This work provides an overview of the current and main regulations concerning the secondary use of personal health data, starting from the European Union framework and examining the related regulatory actions implemented in Italy. It also includes a general presentation of personal health data (including genomic data) and their processing, as well as an in-depth analysis of the key figures involved in the processing of health data for secondary use purposes.

