

DISEGNO DI LEGGE

Disposizioni in materia di utilizzo dei dati sanitari

d'iniziativa dei senatori:

LORENZIN, BOCCIA, GIORGIS, PARRINI, VALENTE, BASSO, BAZOLI, CRISANTI,
D'ELIA, DELRIO, FINA, FRANCESCHELLI, FRANCESCHINI, IRTO, MALPEZZI,
MANCA, MARTELLA, MELONI, MISIANI, NICITA, TAJANI, SENSI, VERDUCCI,
VERINI, ZAMBITO, ZAMPA

Onorevoli senatori. – Il disegno di legge intende adeguare le regole per la gestione dei dati sanitari al fine di favorire l'avanzamento della ricerca scientifica e, in tal modo, il conseguimento di risultati utili per il miglioramento della salute dei cittadini.

L'adozione di tali disposizioni dovrebbe avvenire in modo da consentire una sperimentazione delle attività di ricerca basate sui dati sanitari. In particolare, si intendono affrontare, in un ambiente protetto, i limiti posti all'utilizzo dei dati sanitari da parte delle autorità amministrative e di vigilanza e delle strutture di controllo interno alle entità impegnate nella ricerca scientifica (nello specifico, il *Data Protection Officer*).

Queste disposizioni si propongono di sviluppare uno strumento agile, che permetta di sperimentare anche in sanità trattamenti automatizzati dei dati garantendone la sicurezza. La sperimentazione, infatti, deve tener conto del diritto alla riservatezza, senza pregiudicare le esigenze di celerità, di urgenza, di garanzia di salute del paziente.

La procedura utilizzabile per avviare la predetta sperimentazione è quella di *sandbox*, facendo tesoro dell'esperienza maturata in un altro contesto fortemente disciplinato, quale è quello della finanza. Il modello *sandbox* non risponde alla logica regola-eccezione, non è pensato per derogare o addirittura per deregolare la materia in oggetto, ma configura soltanto uno spazio controllato e limitato, nel tempo e nello spazio, dove poter sperimentare quale possa essere la migliore soluzione regolativa in un contesto di innovazione digitale. L'obiettivo è quello di permettere la medicina di iniziativa e di prevenzione, garantendo, allo stesso tempo, adeguata protezione dei dati sanitari degli assistiti.

Le autorità responsabili del controllo e della gestione dei dati sanitari, tramite la partecipazione alla *sandbox*, potranno perseguire la ricerca scientifica e, in particolare, testare prodotti e servizi innovativi in costante dialogo e confronto con le autorità di vigilanza, richiedendo anche eventuali deroghe normative nella fase di sperimentazione per poter ottimizzare l'utilizzo di servizi di medicina automatizzati.

Non si pregiudicano il diritto alla riservatezza del paziente, né l'anonimato, ma si tutela la salute avverso i ritardi dovuti alla rigidità di applicazione del Regolamento europeo 2016/679 sulla privacy (GDPR). Ed invero, in assenza di una *sandbox*, non sono oggi possibili iniziative a carattere preventivo e terapeutico, in situazioni che richiedono interventi in tempi ristretti per rispondere a condizioni emergenziali o epidemiche per le quali i tradizionali canali di richiesta di autorizzazione a procedere all'uso dei dati sanitari per finalità di ricerca e di salute pubblica non sono adeguati. Si tratta di una condizione già verificatasi durante l'emergenza pandemica da Covid-19 durante la quale per tutelare la salute delle persone si è dovuto ricorrere a soluzioni di emergenza in un contesto privo di norme adeguate ad affrontare la situazione.

L'articolo 4, n. 15, GDPR prevede che i dati relativi alla salute: “sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”. Più in particolare, il Considerando 35 GDPR prevede che “Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono [...] 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”. Il legislatore europeo ha prestato una specifica attenzione ai dati relativi alla salute e li ha inseriti tra le “categorie particolari di dati personali” per cui, in linea di massima,

è vietato il trattamento ai sensi dell'art. 9, par. 1, GDPR. Al par. 2, il Regolamento prevede una serie di deroghe al divieto del trattamento dei dati relativi alla salute che, in ambito sanitario, il Garante privacy ha ricondotto in genere ai casi per cui:

“g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri” (art. 9, par. 2, lett. g) GDPR) individuati dall'art. 2-sexies del Cod. Privacy;

“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” (v. anche Cons. 54). È il caso, ad esempio, delle emergenze sanitarie conseguenti a sismi e sicurezza alimentare;

“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 [di seguito “finalità di cura”] sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità”. In particolare, è bene specificare che per le finalità di cura i dati sanitari possono essere trattati esclusivamente da un professionista soggetto al segreto professionale, ovvero sotto la sua responsabilità, o ancora da persone in ogni caso soggette all'obbligo di segretezza (art. 9, par. 3, GDPR e Cons. 53; art. 75 del Cod. Privacy).

In questa prospettiva, il Garante ha specificato che laddove i trattamenti di dati relativi alla salute non siano strettamente necessari per la finalità di cura di cui alla lett. h) dell'art. 9, par. 2, anche se effettuati da professionisti della sanità, il titolare dovrà individuare un'altra base giuridica, ovvero eventualmente il consenso dell'interessato (artt. 6 e 9, par. 2, GDPR). Appare evidente che una lettura restrittiva della norma non permette alcuna azione di medicina di iniziativa e realmente preventiva, soprattutto in periodi di urgenza di azione, e limita eccessivamente l'azione sanitaria in opposizione con le finalità del diritto comunitario (art.35 Carta dei diritti fondamentali dell'UE e artt. 11 e 13 della Carta sociale europea) e con le esigenze di migliorare le cure ai pazienti favorendo, allo stesso tempo, l'attività di ricerca da parte degli istituti clinici pubblici.

È importante sottolineare che all'interno dei percorsi di prevenzione si può compiere una medicina di iniziativa e convocare il paziente per controlli sanitari, una medicina di attesa, ossia se il paziente si presenta presso lo studio medico o l'istituto di cura si possono fare i relativi controlli e una medicina di opportunità nel caso in cui il paziente si presenta per determinati motivi e si coglie l'occasione per effettuare ulteriori controlli. In ciascuna fase è applicato un diverso tipo di medicina. La più efficace è proprio la medicina di iniziativa, perché riesce a seguire le tempistiche necessarie per la *follow-up* o a contattare i pazienti, che non sono consapevoli del loro bisogno di salute. La medicina preventiva, inoltre, per essere realmente efficace deve permettere che il paziente venga contattato o richiamato e, banalmente, essere inserito in elenchi con possibilità di richiamo. Affinché il paziente possa essere inserito in una determinata lista c'è bisogno di una valutazione dei suoi dati sanitari, che non necessariamente si ha il diritto di analizzare, e questo limita fortemente le possibilità degli istituti di ricerca e cura. I termini prevenzione e iniziativa, del resto, possono parzialmente sovrapporsi. È evidente

la necessità di anticipare il bisogno di salute del paziente, realizzata anche attraverso la correlazione ed elaborazione dei dati relativi alle condizioni di salute dei pazienti di un determinato territorio per ottenere una stratificazione degli stessi pazienti in profili di rischio. Nel GDPR, il legislatore pone una particolare attenzione al trattamento automatizzato dei dati personali che possa sfociare in decisioni che sono proprie della macchina e non dell'uomo. L'art. 22 ribadisce come principio generale che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona. Tale disposizione non si applica quando la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, oppure b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, oppure c) si basi sul consenso esplicito dell'interessato. Al di fuori di tali ipotesi si pone l'articolo 22, par. 4, del GDPR che, come principio generale, vieta la profilazione dei dati sanitari. La stessa, eccezionalmente, può avvenire se: c'è un consenso esplicito dell'Interessato; va perseguito un interesse pubblico rilevante nell'ambito della sanità pubblica; il Titolare (o Responsabile) abbia adottato idonee e adeguate misure di sicurezza per tutelare i diritti, le libertà e i legittimi interessi del paziente. Se un Titolare (o Responsabile) decide di usare i dati sanitari dei pazienti per attività di profilazione, allora questi deve concedere agli interessati il diritto di rinunciare all'attività (il cd. diritto di "opt-out") e di revocare il consenso. In ogni caso, il Titolare (o Responsabile) sarà onerato dell'obbligo di adottare idonee misure di sicurezza che garantiscano all'interessato la tutela dei propri diritti e delle libertà fondamentali.

Rileva, come esempio esemplificativo, il caso in cui il Garante per la privacy nel dicembre 2022 ha sanzionato tre Asl friulane che, attraverso l'uso di algoritmi, avevano classificato gli assistiti in relazione al rischio di avere o meno complicanze in caso di infezione da Covid-19. Secondo l'Authority, le aziende sanitarie avevano elaborato i dati presenti nelle banche dati aziendali per attivare, nei confronti degli assistiti, opportuni interventi di medicina di iniziativa e individuare per tempo i percorsi diagnostici e terapeutici più idonei.

In particolare, l'istruttoria, avviata in seguito alla segnalazione di un medico, ha verificato che le aziende sanitarie avevano trattato i dati dei pazienti senza fornire agli interessati l'informativa prevista per legge. Il Garante, in questi provvedimenti, fornisce un'interpretazione della medicina di iniziativa stabilendo che questa è ulteriore e autonoma rispetto alle ordinarie attività di cura e prevenzione per poi affermare che non rientra nelle finalità del FSE, nelle quali sono previste la prevenzione, la diagnosi e la cura. Eppure, Agenas chiarisce (DM 77) che "La sanità di iniziativa è un modello assistenziale di gestione delle malattie croniche fondato su un'assistenza proattiva all'individuo dalle fasi di prevenzione ed educazione alla salute fino alle fasi precoci e conclamate della condizione morbosa." La sanità o medicina di iniziativa è, quindi, un modello assistenziale che riguarda la prevenzione e la gestione (la cura) delle malattie croniche. È certamente vero che non è menzionata esplicitamente tra le finalità del FSE ma può rientrare nelle voci prevenzione, diagnosi e cura. Dopo l'affermazione di tale orientamento da parte del garante ed in assenza di una *sandbox* sui dati sanitari, la salute dei pazienti è a rischio.

Attualmente è in discussione l'*European Health Data Space* (EHDS), una proposta di Regolamento del Parlamento Europeo e del Consiglio sullo spazio europeo dei dati sanitari, che potrebbe giungere alla fine del suo lungo iter legislativo non prima della primavera 2024. Si propone di introdurre disposizioni, norme e prassi comuni, infrastrutture e un quadro di *governance* per l'uso primario e secondario dei dati sanitari elettronici e in particolare: favorire il controllo dell'utente sui propri dati sanitari; regolamentare l'uso dei dati sanitari ai fini di miglioramento dell'erogazione delle prestazioni di assistenza sanitaria, ricerca, innovazione e definizione di politiche comuni; consentire all'Unione Europea di sfruttare appieno il potenziale offerto da uno scambio, un uso e un riutilizzo sicuri e protetti dei dati sanitari.

Dal quadro sommariamente descritto emerge che già oggi il diritto eurounitario segna una chiara traiettoria nell'impiego dei dati sanitari, pur garantendone la protezione, sulla base di piattaforme tecnologiche *compliance by design*. Tuttavia, come già accaduto per il GDPR sulla sperimentazione clinica, l'Italia è ben lontana da una applicazione coerente con le finalità perseguite dal legislatore comunitario. Un'iniziativa legislativa coerente con le finalità del diritto comunitario e con le esigenze di migliorare le cure ai pazienti favorendo l'attività di ricerca da parte di istituti di ricerca pubblici e privati deve confrontarsi: con la prassi applicativa e considerare che anche le fonti primarie sono spesso interpretate alla luce dei precedenti delle autorità amministrative e giurisdizionali, senza contare le strutture di controllo (DPO) collocate all'interno dei predetti istituti, primo vero limite all'impiego dei dati sanitari; con lo sviluppo tecnologico, che ha subito una profonda accelerazione negli ultimi anni, e che pertanto offre soluzioni che non sono neppure contemplate dalle autorità, né tantomeno lo possono essere dalla legge; con l'esigenza di proporre uno strumento agile che permetta di "sperimentare" trattamenti automatizzati dei dati garantendone la sicurezza, e valutando solo *ex post* la soluzione adottata, sterilizzando qualunque forma di potere interdittivo delle autorità preposte (Garante e DPO in primis).

Con la modifica proposta, attraverso la sperimentazione della *sandbox*, viene chiarito che lo svolgimento di attività di medicina d'iniziativa e di prevenzione, nell'ambito della sperimentazione e nel rispetto dei limiti stabiliti dai provvedimenti di ammissione, che rientrano nei diversi livelli di prevenzione (primaria, secondaria, terziaria e quaternaria), non necessita del rilascio di autorizzazioni e/o del consenso ove sia prevista una durata massima di sei mesi, salvo il maggior termine della sperimentazione, che non può superare complessivamente il limite massimo di diciotto mesi, nei casi in cui sia concessa una proroga.

La procedura *sandbox* garantirebbe, quindi, il trattamento e lo scambio dei dati sanitari, definendo *ex ante* gli istituti di ricerca coinvolti e le autorità preposte al controllo, con la preventiva costituzione di un comitato di gestione della sperimentazione composto dal Ministro della salute, dal Garante per la protezione dei dati personali, dall'Agenzia per l'Italia digitale, da quattro professori ordinari, di cui almeno uno di diritto dell'economia e uno di igiene, e da un esperto negli ambiti sanitario e sociosanitario nazionale, della ricerca scientifica e nei rapporti con gli *stakeholder* del settore sanitario.

L'obiettivo è quello di garantire alle autorità di vigilanza di poter operare grazie ad un percorso sperimentale, sotto la vigilanza rafforzata del Garante della privacy e dell'Agenzia per l'Italia digitale, al fine di assicurare il bilanciamento del diritto alla riservatezza con il diritto alla salute.

Il presente disegno di legge, fortemente innovativo, si propone l'ambizioso obiettivo di utilizzare le opportunità offerte dalle "nuove" tecnologie sull'analisi dei dati nel rispetto del diritto alla riservatezza e alla sicurezza.

Art. 1.

(Disciplina della sperimentazione dei dati sanitari)

1. Al fine di promuovere e sostenere la salute dei cittadini, la ricerca in materia sanitaria e di assicurare la protezione adeguata dei consumatori e del loro diritto alla riservatezza, nonché di favorire il raccordo tra le istituzioni, gli enti di ricerca, i presidi sanitari, le autorità e gli operatori del settore, il Ministro della salute, sentito il Garante per la protezione dei dati personali, adotta, entro novanta giorni dall'entrata in vigore della presente legge, uno o più regolamenti per definire le condizioni e le modalità di svolgimento di una sperimentazione relativa all'utilizzo dei dati sanitari volte al perseguimento, mediante nuove tecnologie, della tutela della salute, dell'innovazione dei prodotti e dei servizi sanitari, nonché le modalità di funzionamento del Comitato dati sanitari di cui all'articolo 2.
2. La sperimentazione di cui al comma 1 si conforma al principio di proporzionalità previsto dalla normativa dell'Unione europea ed è caratterizzata da:
 - a) una durata massima di diciotto mesi prorogabili per un massimo di ulteriori dodici mesi;
 - b) requisiti ridotti;
 - c) adempimenti semplificati e proporzionati alle attività che si intende svolgere;
 - d) tempi ridotti delle procedure autorizzative;
 - e) definizione di perimetri e limiti di operatività.
3. Nel rispetto della normativa inderogabile dell'Unione europea, i regolamenti di cui al comma 1 stabiliscono i criteri per determinare:
 - a) i requisiti di ammissione alla sperimentazione;
 - b) i casi in cui è ammessa la proroga;
 - c) gli adempimenti semplificati e proporzionati alle attività che si intende svolgere;
 - d) i perimetri di operatività;
 - e) gli obblighi informativi;
 - f) i tempi per il rilascio di autorizzazioni;
 - g) le eventuali garanzie;
 - h) l'*iter* successivo al termine della sperimentazione.
4. Le misure e i criteri di cui ai commi 2 e 3 possono essere differenziati e adeguati in considerazione delle particolarità e delle esigenze dei casi specifici; essi hanno carattere temporaneo e garantiscono adeguate forme di informazione e di protezione a favore dei cittadini, nonché del corretto funzionamento del Sistema sanitario nazionale. L'operatività delle misure cessa al termine del relativo periodo, ovvero alla perdita dei requisiti o al superamento dei limiti operativi stabiliti, nonché negli altri casi previsti dai regolamenti di cui al comma 1.
5. Nel rispetto della normativa inderogabile dell'Unione europea, l'ammissione alla sperimentazione può comportare la deroga o la disapplicazione temporanee degli orientamenti di vigilanza o degli atti di carattere generale emanati dalle autorità di vigilanza, nonché delle norme o dei regolamenti emanati dalle medesime autorità di vigilanza.
6. Il Garante per la protezione dei dati personali redige annualmente una relazione d'analisi sul settore sanitario, riportando quanto emerge dall'applicazione del regime di sperimentazione di cui al comma 1 e segnalando eventuali modifiche normative o regolamentari necessarie per lo sviluppo del settore, la tutela della salute e la riservatezza.

Art. 2

(Istituzione e compiti del Comitato dati sanitari)

1. Presso il Ministero della salute è istituito il Comitato dati sanitari, di seguito denominato Comitato, con i compiti di individuare gli obiettivi, definire i programmi, formulare proposte per favorire l'utilizzo dei dati sanitari in un'ottica di sviluppo della ricerca, della prevenzione e della assistenza sanitaria, anche in cooperazione con soggetti esteri.
2. Sono membri permanenti del Comitato il Ministro della salute, il Garante per la protezione dei dati personali, l'Agenzia per l'Italia digitale, quattro professori ordinari, di cui uno di diritto dell'economia e uno di igiene e medicina preventiva, e un esperto negli ambiti sanitario e sociosanitario, della ricerca scientifica e nei rapporti con gli *stakeholder* del settore della sanità. Per le attività svolte dal Comitato relative alla sperimentazione, i membri permanenti collaborano tra loro, anche mediante scambio di informazioni.
3. Dall'attuazione delle disposizioni della presente legge non devono derivare nuovi o maggiori oneri per la finanza pubblica.