# Audizione, in videoconferenza, del Presidente del Garante per la protezione dei dati personali Soro nell’ambito dell’indagine conoscitiva in materia di semplificazione dell'accesso dei cittadini ai servizi erogati dal Servizio Sanitario Nazionale - 25 maggio 2020

**Audizione, in videoconferenza, del Presidente del Garante per la protezione dei dati personali Soro nell’ambito dell’indagine conoscitiva in materia di semplificazione dell'accesso dei cittadini ai servizi erogati dal Servizio Sanitario Nazionale**

*Commissione parlamentare per la semplificazione*

*(25 maggio 2020)*

Ringrazio la Commissione per quest’occasione di confronto sul rapporto tra diritto alla salute e protezione dati: tema di grande rilevanza, in particolare nell’attuale contesto emergenziale.

Questi due diritti fondamentali presentano, infatti, inattese analogie dovute essenzialmente alla dialettica che sottendono, tra libertà e dignità, persona e società.

In entrambi, in particolare, la libertà si esprime come autodeterminazione. Questi diritti vivono, poi, in costante dialettica tra garanzia individuale e tutela sociale, realizzando la prima nel bilanciamento con la seconda, spesso, persino in sinergia.

Il rapporto tra libertà e dignità, individuo e società, sotteso a questi due diritti, diviene ancor più articolato per effetto della tecnologia, che se da un lato offre possibilità straordinarie, dall’altro induce nuove vulnerabilità cui, tramite i nostri dati, esponiamo noi stessi.

Così, in ambito sanitario, la digitalizzazione è una componente essenziale di efficienza del governo clinico, tale da garantire anche un’assistenza sanitaria personalizzata, fondata sulla partecipazione consapevole del paziente al percorso terapeutico.

La pandemia ha dimostrato come il digitale-con la ricetta elettronica e con la telemedicina- possa consentire la prosecuzione delle cure anche in regime di distanziamento sociale.

Eppure una tecnologia non ben governata può aumentare esponenzialmente il rischio clinico in cui si riflette, in quest’ambito, il rischio informatico, ove ad esempio i dati su cui si fonda la diagnosi siano alterati.

Per altro verso, l’esfiltrazione o l’accesso indebito a dati sanitari possono violare, in modo talora irreversibile, quel diritto all’intangibilità della propria vita privata che costituisce la radice più antica della privacy.

Sul piano individuale, infatti, la conoscenza di dati così “sensibili” quali quelli genetici o sulla salute, può fondare discriminazioni (si pensi al rapporto lavorativo o assicurativo) o comunque pregiudizi rilevantissimi per l’interessato.

Ma il rischio cibernetico, in ambito sanitario, ha effetti importanti anche dal punto di vista collettivo.

Sul piano pubblico, infatti, gli attacchi a sistemi informativi di strutture sanitarie – parte significativa dei cyber attack nel nostro

Paese- possono avere effetti devastanti su tutti i cittadini, impedendo l'erogazione di prestazioni sanitarie o, nel caso di alterazione di dati dei pazienti, errori clinici su larga scala.

La vulnerabilità dei sistemi sanitari, rischia quindi di causare disservizi anche gravissimi, ingenerando errori diagnostici o terapeutici o paralizzando l'attività di cura.

E' un problema che riguarda il nostro Paese in modo particolare.

Recenti ricerche (Clusit, rapporto primo semestre 2019) hanno indicato, infatti, il settore sanitario come uno di quelli esposti ai maggiori rischi in termini di cybersecurity perché carente di un piano organico di sicurezza e protezione, che invece in questo campo sarebbe essenziale, soprattutto a fronte del sempre maggiore utilizzo del cloud computing e dell'intelligenza artificiale.

La sfida di oggi consiste, allora, nel rendere la digitalizzazione in ambito sanitario un processo organico, lungimirante e sicuro, promuovendo così l'efficienza del sistema e, con essa, l'effettività del diritto alla salute, superando le vulnerabilità della tecnica e minimizzandone i rischi, individuali e collettivi.

Il Fse è, in un certo senso, l'emblema di questa sfida, quale elemento imprescindibile di innovazione ed efficienza delle attività diagnostiche e terapeutiche, previsto dall'Agenda digitale italiana ed europea, dal Patto per la salute e per la sanità digitale, indicato quale piattaforma abilitante" dal Piano triennale dell'Agid.

Tuttavia, l'affidamento dell'intera storia clinica di milioni di pazienti a un'infrastruttura informatica rappresenta anche una non trascurabile fonte di vulnerabilità se priva di protezioni adeguate ad impedire accessi indebiti, esfiltrazioni o alterazioni dei dati.

Ciò spiega l'esigenza – da noi sollecitata in passato- di una cornice normativa tale da dotare uno strumento tanto irrinunciabile quanto delicato, di tutti i presidi necessari, in termini di misure di sicurezza ma anche di complessiva architettura del sistema.

La previsione legislativa ha anche consentito di ricondurre iniziative regionali disomogenee all'interno di un quadro di garanzie uniformi, tali da assicurare il pari trattamento dei cittadini.

Sin dal 2009 – tre anni prima dell'introduzione della relativa disciplina – il Garante ha fornito alcune importanti indicazioni sul fascicolo sanitario elettronico (come del resto sul dossier sanitario), rilevando in particolare la necessità di garantire:

- piena libertà al paziente sulle scelte essenziali relative al fascicolo, ivi incluse quelle inerenti la sua ampiezza e la possibilità di oscurare alcuni eventi clinici,

- la legittimazione selettiva e differenziata del personale autorizzato ad accedervi e il diritto del paziente di verificare gli accessi effettuati – restituendo così centralità all'interessato nel processo di gestione dei suoi dati –, nonché

- l'obbligo per il titolare di segnalare al Garante eventuali data breach occorsi nella propria struttura, quando ancora l'obbligo di notifica delle violazioni dei dati non era generale, al fine di contenere con misure tempestive i danni, individuali e collettivi, suscettibili di derivare da violazioni in quest'ambito.

Queste indicazioni hanno consentito di migliorare notevolmente la qualità delle prestazioni erogate, ponendo le condizioni necessarie per promuovere la fiducia dei cittadini in uno strumento diagnostico essenziale ma ancora troppo poco diffuso in quanto attivato nei confronti del solo 23% della popolazione.

Tale constatazione, unitamente al costante monitoraggio dell'applicazione normativa, ha quindi consentito di proporre, anche alla luce del sopravvenuto Regolamento europeo, misure di semplificazione e, al tempo stesso, di valorizzazione del fascicolo sanitario elettronico, poi introdotte proprio dal decreto legge rilancio.

In particolare, è stata ritenuta opportuna- e dall'Autorità condivisa - l'eliminazione del consenso all'alimentazione del Fascicolo, confermando invece quello (autenticamente espressivo di autodeterminazione informativa) relativo alla consultazione da parte dei professionisti sanitari.

Tale modifica contribuisce a semplificare notevolmente il processo di costituzione dell'fse rendendolo quindi automaticamente disponibile a prescindere da manifestazioni di volontà individuali, ma confermando il consenso del paziente quale fonte di

legittimazione dell'accesso ai dati, da parte del professionista sanitario.

Lo spettro del fascicolo è ampliato, sino a comprendere tutti i documenti, sanitari e socio-sanitari, riferiti alle prestazioni erogate, a carico o meno del SSN, includendo dunque tra i soggetti abilitati all'alimentazione la generalità degli esercenti le professioni sanitarie che seguano il paziente.

La prevista, ulteriore alimentazione del fse con i dati disponibili sulla scelta circa donazione degli organi, vaccinazioni e prenotazioni promuoverà poi l'efficacia delle prestazioni sanitarie se e nella misura in cui garantirà l'allineamento delle banche dati e, quindi, l'esattezza ed aggiornamento delle informazioni.

Si prospetta, inoltre, un notevole potenziamento- che dovrà essere oggetto di attento monitoraggio- del Portale e dell'infrastruttura nazionale per l'interoperabilità, necessario all'erogazione delle prestazioni sanitarie 'in mobilità' dei cittadini, ovvero nell'ambito di regioni diverse da quella di residenza.

Si prevede quindi l'istituzione dell'Anagrafe Nazionale dei consensi e relative revoche, da associarsi agli assistiti risultanti nella relativa anagrafe, comprensiva anche dei dati inerenti eventuali deleghe (ad esempio per le decisioni inerenti i minori).

La valorizzazione della funzione e l'estensione dello spettro del fse, prevista con il dl rilancio anche sulla scorta delle indicazioni fornite dall'Autorità, rappresenta certamente una sfida importante per il settore sanitario, da giocare fino in fondo senza però sottovalutare in alcun modo i rischi connessi all'affidamento, a una piattaforma informatica, dei dati sulla storia clinica, potenzialmente, di tutti gli assistiti.

Per un verso, infatti, il rischio informatico (suscettibile di risolversi fatalmente in rischio clinico) va contrastato con la più rigorosa osservanza del principio di responsabilizzazione e dei criteri di privacy by design e by deafult, razionalizzando il patrimonio informativo e la stessa architettura del trattamento, seguendone la dinamica lungo l'intera filiera.

Va anche inteso in senso rigoroso il vincolo di finalità, evitando l'accesso a dati del fse, di cui difficilmente può garantirsi la completa anonimizzazione, per fini di programmazione sanitaria da parte di amministrazioni titolari di competenze diverse.

Su questo aspetto, confido che le incomprensioni con il MEF siano risolte, anche perché quel dicastero già detiene i dati fiscali rilevanti al monitoraggio della spesa anche in ambito sanitario.

Del resto, già il Ministero della salute utilizza l'fse a fini (oltre che di ricerca, anche di) programmazione sanitaria, verifica delle qualita' delle cure e valutazione dell'assistenza sanitaria (finalità di "governo"), senza tuttavia l'utilizzo di dati identificativi, secondo livelli di accesso e modalita' di elaborazione dei dati definiti in conformita' ai principi di proporzionalita', necessita' e indispensabilita'.

Per altro verso, non va sottovalutato il rischio di accessi indebiti ai dati del fascicolo sanitario, resi possibili da una inadeguata definizione del perimetro e dei profili di legittimazione degli stessi professionisti sanitari.

Non rari sono stati i casi, sottoposti alla nostra attenzione, di consultazioni di fascicoli sanitari da parte di personale privo dei titoli, per fini ritorsivi o di semplice, patologica, curiosità.

La violazione della riservatezza derivante da tali condotte potrà essere, poi, persino più significativa ove nel fse confluiscano dati di particolare rilevanza sotto il profilo delle scelte esistenziali, quali quelli sulla donazione degli organi o, laddove dovesse prevedersi, sulle dichiarazioni anticipate di trattamento.

La protezione dei dati da accessi indebiti e l'esatta definizione dei soggetti legittimati alla consultazione costituiscono, del resto, un obiettivo ineludibile soprattutto nel contesto sanitario complessivamente inteso.

Si pensi alla delicatezza di dati, quali quelli (pur non presenti nel fse) sulla fecondazione eterologa, per i quali deve garantirsi, attraverso un sistema di codifica, tanto la tracciabilità del percorso dei gameti dal donatore (anonimo) al nato e viceversa, per consentire la reidentificazione in caso di eventi avversi, quanto la riservatezza delle madri.

La gestione, poi, di dati così delicati e in costante evoluzione quali quelli sanitari necessita di garanzie idonee ad assicurarne la

qualità.

In questo senso, le regole di protezione dati sono un presupposto di efficienza sanitaria, contribuendo alla garanzia di esattezza ed aggiornamento dei dati, in un ambito, quale quello in esame, in cui il ricorso a un'informazione obsoleta o alterata può determinare danni talora anche letali per il paziente.

L'aggiornamento costante deve, del resto, riguardare anche le manifestazioni di volontà dell'assistito, per poterne garantire l'effettivo rispetto nella loro attualità ed evoluzione.

E' un tema che riguarda molti degli archivi rilevanti in questo campo.

Esso coinvolge, infatti, il consenso alla consultazione del fse (la cui anagrafe comprende anche, appunto, le revoche), ma a maggior ragione, in ambito contiguo, le dichiarazioni anticipate di trattamento.

Rispetto alle scelte sul fine vita, infatti, la centralizzazione delle dichiarazioni è necessaria per evitarne il disallineamento e, quindi, garantirne il costante aggiornamento, necessario per il rispetto della volontà attuale del soggetto.

Il processo di digitalizzazione in ambito sanitario – di cui il fascicolo è una componente significativa – pone, del resto, altre questioni rilevanti dal punto di vista della protezione dati, cui accenniamo pur estendendo un minimo l'oggetto del nostro confronto di oggi.

Il ricorso sempre più frequente all'intelligenza artificiale a fini di ricerca in campo medico, ma anche diagnostici, evidenzia l'esigenza di garantire la correttezza del processo analitico fondato su dati, ove le scelte algoritmiche sono rese possibili dall'auto-apprendimento di cui è capace la macchina a partire dalle informazioni immesse.

Dall'esattezza dei dati utilizzati nella configurazione degli algoritmi dipende l'"intelligenza" delle loro scelte.

Se è errata la classificazione delle casistiche di riferimento fornita all'algoritmo per decidere, ad esempio, la natura di una patologia o per valutare un marker, sarà poi la conseguente diagnosi ad essere sbagliata, con effetti potenzialmente anche fatali per il paziente.

La protezione dei dati, dunque, è un presupposto di efficacia della big data analytics e va coniugata non certo con un arretramento ma, al contrario, con un ulteriore sviluppo di tecnologie "user-friendly" che incorporino in sé garanzie di sicurezza e confidenzialità dei dati.

Le misure di privacy by design e by default- da applicare ad esempio in modo rigoroso rispetto alla sempre più diffusa telemedicina- sono, in questo senso, un esempio determinante di come la tecnologia, se sostenuta da una "visione" lungimirante in termini sociali oltre che giuridici, possa rappresentare la soluzione, invece del problema e rafforzare la fiducia dei cittadini nel sistema sanitario.

Soluzione tanto più necessaria a fronte di ricerche sempre più fondate su dati e algoritmi idonei a incrociare quantità enormi di informazioni, con elevato rischio non soltanto di reidentificazione (che induce a ritenere i dati effettivamente anonimi solo in casi marginali) ma anche di discriminazione per gruppi (rischio tanto più elevato ove i dataset sui quali si fonda la decisione algoritmica non siano rappresentativi o sottendano comunque pregiudizi di genere, etnia, condizioni sociali o appunto di salute, ecc.).

La protezione dei dati può rappresentare tanto un elemento di garanzia del singolo quanto un fattore di appropriatezza della generale governance sanitaria.

Sotto questo profilo, questa disciplina offre importanti garanzie, esigendo in particolare trasparenza, contestabilità, non discriminatorietà del processo algoritmico, oltre che un approccio generale volto alla prevenzione del rischio, con la previsione di misure precauzionali e l'adozione di una strategia complessiva volta alla responsabilizzazione dei protagonisti del trattamento.

Abbiamo ricordato questi principi anche rispetto a sempre più frequenti, modelli di assistenza sanitaria fondati sulla medicina d'iniziativa e, quindi, sulla profilazione del rischio sanitario e che, sebbene volti alla "personalizzazione" della medicina e al miglioramento dell'offerta terapeutica, coinvolgono tuttavia aspetti delicatissimi dal punto di vista esistenziale.

Di qui l’esigenza non solo del consenso quale espressione di autodeterminazione (informativa e sanitaria ad un tempo) rispetto a un trattamento automatizzato non strettamente necessario per finalità immediate di cura dell’interessato, ma anche di un’adeguata supervisione della profilazione, che se fondata su dati o inferenze inesatti rischia di determinare gravi pregiudizi all’interessato e rilevanti errori sul piano complessivo del governo clinico.

Garanzie di correttezza andranno assicurate anche rispetto all’uso - promosso dal dl rilancio - di metodologie predittive del fabbisogno sanitario, per il quale le regole di protezione dati potranno rappresentare un prezioso presupposto di efficacia.

Anche questi esempi dimostrano, dunque, come sulla sinergia tra innovazione, governance sanitaria e protezione dati si giocherà una sfida sempre più determinante per le nostre società, che dobbiamo impegnarci a vincere nel segno, ancora una volta, della centralità della persona e della sua dignità: quei vincoli che, spiegò Aldo Moro in Assemblea Costituente, neppure l’interesse collettivo alla sanità pubblica può superare.