IL DATO SANITARIO NELLA NUOVA NORMATIVA NAZIONALE E COMUNITARIA: DALLA DEFINIZIONE ALLE RAGIONI DELLA SUA TUTELA

di Marco Del Fungo e Francesco Giunti (*)

Sommario: 1. Introduzione – 2. Il dato sanitario: normativa e giurisprudenza. 2.1.Normativa – 2.2. Giurisprudenza 3. Le ragioni della tutela del dato sanitario – 4. Il dato sanitario nel GDPR - 5. Principi e rivoluzione del GDPR – 6. Modifiche al Codice Privacy: il decreto legislativo di adeguamento n. 101/2018 – 7. Ambiti e strumenti coinvolti dalle modifiche alla normativa nazionale e comunitaria (Fascicolo sanitario elettronico - Dossier Sanitario - Cartella elettronica - Referti online - Siti web – App e mHealth) - 8. Considerazioni finali

1. Introduzione

Lo scopo primario di questo contributo è quello di fornire in maniera sintetica e schematica il quadro giuridico vigente in ambito sanitario con riferimento alla protezione dei dati personali, soprattutto alla luce del Regolamento Europeo (GDPR) n. 679/2016 e del d.lgs. n. 101 del 10 agosto 2018 che ha adeguato la normativa nazionale a quest'ultimo.

Occorre prendere le mosse, innanzitutto, dalla definizione di dato sanitario. Prima di esaminare la portata normativa del GDPR in ambito sanitario, può essere utile ricapitolare sinteticamente il quadro normativo e giurisprudenziale di riferimento creatosi nel periodo antecedente all'entrata in vigore del Regolamento Europeo.
Come potrà notarsi, non vi è in nessun provvedimento una definizione precisa di dato sanitario: infatti, tutte le fonti di seguito riportate fanno generico riferimento ai dati relativi alla salute della persona o ai suoi dati genetici, ammettendo il loro trattamento solo in presenza di determinate condizioni.
In modo non organico ed anzi a volte incidentale sono intervenuti sia il legislatore che la giurisprudenza per definire e disciplinare il dato sanitario e la sua tutela.
La consapevolezza da parte del legislatore e della giurisprudenza della particolare importanza di questo genere di dati e della necessità di trattarli e proteggerli secondo modalità adeguate e talvolta predefinite ha determinato un susseguirsi di provvedimenti di natura legislativa ma soprattutto una copiosa produzione giurisprudenziale.

2. Il dato sanitario: normativa e giurisprudenza.
2.1. Normativa.

La prima fonte normativa da prendere in considerazione, in ordine

cronologico, è la Convenzione n. 108 del 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale[1].
L'art. 6 qualifica i dati personali relativi alla salute come "*speciali*": in base alla convenzione, essi non possono essere elaborati automaticamente a meno che il diritto di ciascuno stato aderente non preveda garanzia appropriate. Si nota, quindi, come già all'epoca il legislatore europeo avesse intuito che tale genere di dati dovesse essere trattati sulla base di adeguate misure di protezione.
Successivamente, la direttiva 95/46 del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, ha stabilito all'art. 8 il divieto di trattamento dei dati relativi alla salute, prevedendo, poi, una serie di condizioni di liceità al trattamento.
La normativa di riferimento, invece, nel panorama italiano è stata, fino all'entrata in vigore del GDPR, il d.lgs. n. 196/2003 o Codice Privacy.
Il decreto nella sua versione originaria non faceva alcuna menzione del "dato sanitario" ma all'art. 4 definiva i "dati sensibili" come i dati personali idonei a rivelare, tra l'altro, lo stato di salute.
Ciò precisato, emerge chiaramente l'importanza del ruolo della giurisprudenza comunitaria ed italiana sia di merito che, soprattutto, di legittimità nell'opera di definizione del dato sanitario.

2.2. Giurisprudenza.

Sono vari i provvedimenti giudiziari anche comunitari che hanno riguardato il trattamento dei dati personali sanitari.
Vale la pena citare in ambito comunitario la sentenza della CGCE del 6 novembre 2003 (c.d. caso Lindqvist)[2], la quale ha stabilito che la nozione di "*dati relativi alla salute*" (come riporta l'art. 8 della direttiva 95/46) deve essere intesa in senso ampio in modo da comprendere le informazioni riguardanti tutti gli aspetti, tanto fisici quanto psichici, della salute di una persona.
In Italia, la Corte di Cassazione si è pronunciata varie volte sull'argomento, trattando anche le questioni relative alle particolari modalità di trattamento ed alle misure di protezione da applicare ai dati sensibili.
In primo luogo, occorre dar conto della sentenza della Suprema Corte n. 14390 dell'8 luglio 2005 (la cui massima, sul punto, è stata ripresa successivamente dalla stessa Corte in altre sentenze) la quale assume particolare rilevanza nello stabilire che i dati personali riguardanti la salute appartengono alla species dei "*supersensibili*", dal momento

---

1 Convenzione di Strasburgo del 28 gennaio 1981 n. 108 *sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*.

2 Sentenza del 6 novembre 2003, Lindqvist, C-101/01.

che investono la parte più intima della persona nella sua corporeità e prevedendo che, in considerazione dei valori costituzionali posti a loro presidio (artt. 2 e 3 Cost.), debbano ricevere una tutela rafforzata e più incisiva rispetto agli altri, in quanto – in caso contrario – potrebbe essere arrecato un grave pregiudizio all'interessato.
Con la sentenza n. 15908/2016 la Suprema Corte, poi, analizza un'ipotesi di trattamento dati consistente nella raccolta di schede o di cartelle cliniche per ogni paziente, accessibile a diversi soggetti e consultabile on line.
La Corte, nel precisare e definire il raggio d'applicazione dell'art. 37 del Codice Privacy, con la propria decisione ha previsto che tra i soggetti obbligati alla notifica preventiva al Garante rientrino sia le strutture pubbliche e sia quelle private che effettuino trattamenti di dati idonei a rivelare lo stato di salute.
Nel caso specifico, la ragione per cui il tipo di trattamento in esame doveva essere subordinato alla preventiva consultazione del Garante è da ravvisarsi nella pericolosità intrinseca per i diritti e le libertà degli interessati del trattamento telematico dei dati sanitari, che necessita in via preventiva di adeguate misure di sicurezza, a differenza dei trattamenti sui dati sanitari effettuati manualmente mediante archivi cartacei (Cass. Civ. n. 8105/2016) per i quali non è previsto tale onere.
In altra occasione, sono intervenute le SS.UU della Suprema Corte che con la pronuncia n. 30981/2017 hanno statuito che i dati sensibili idonei a rivelare lo stato di salute possono essere trattati soltanto mediante modalità organizzative, quali tecniche di cifratura o criptatura che rendono non identificabile l'interessato.
Dal principio di diritto affermato dalle SS.UU. consegue, direttamente, che i soggetti pubblici o le persone giuridiche private, anche quando agiscano rispettivamente in funzione della realizzazione di una finalità di pubblico interesse o in adempimento di un obbligo contrattuale, sono tenuti all'osservanza delle predette cautele (cifratura o criptatura) nel trattamento dei dati in questione.
Infine, in una recente pronuncia del 2018 (Cass. Civ. n. 16816/2018) i giudici di legittimità, nel ribadire che la salute di un minore costituisce dato personale e sensibile, hanno sancito che esso è tutelabile non solo in relazione al minore ma anche in relazione agli altri familiari legati al minore medesimo da vincoli di comunanza di vita familiare o domestica.
L'assunto viene giustificato dal fatto che la diffusione delle informazioni sulle particolari condizioni di salute del minore si riflette sulla persona del genitore o altro familiare, atteso che la situazione del familiare congiunto a persona affetta da invalidità in ogni caso esprime una situazione di debolezza o di disagio sociale, di per sé potenzialmente idonea ad esporre la persona a condizionamenti o discriminazioni.
L'ostensione di tale dato conduce quindi ad una dolorosità e a rischi di

discriminazione sociale che certamente riguardano, accanto al minore, i suoi genitori e i suoi familiari (quali membri di un'intima comunità di vita).
Il quadro normativo e giurisprudenziale sopra esposto risulta evidentemente frammentario e non certo sistematico ma ha il pregio di far risaltare l'importanza della tutela e protezione dei dati relativi alla salute in considerazione dei valori costituzionali posti a loro presidio (artt. 2 e 3 Cost.).

3. Il dato sanitario nel GDPR.

Dopo aver esaminato brevemente il panorama giuridico precedente all'entrata in vigore del Regolamento UE n. 679/2016, il presente contributo non può che prendere le mosse dalla definizione di dato personale contenuta nel GDPR.
Ai sensi del GDPR, per "dato personale" si intende qualsiasi informazione relativa a soggetti identificati o identificabili, relativa alla sfera personale del soggetto declinata nei vari ambiti in cui coltiva la propria persona. All'interno di questa categoria rientrano i dati sanitari.
Se si considera – a fini prettamente definitori – il dato sanitario come quello idoneo a rivelare le caratteristiche più intime relative alla salute fisica, mentale e comportamentale complessivamente intesa e cronologicamente ricostruibile della persona, assume allora grande importanza quanto previsto all'art. 4 che al punto n. 15 definisce i *"dati relativi alla salute"* come i dati personali attinenti alla salute fisica o mentale di una persona fisica e le prestazioni sanitarie di cui ha usufruito. Al riguardo, il legislatore comunitario nel considerando 35 del Regolamento Europeo ha specificato che fanno parte di questa categoria "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 […] raccolte nel corso nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria": sono considerati tali non solo 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, 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, ma anche un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari.
Nel GDPR hanno grande rilevanza – per le medesime finalità definitorie – anche i *c.d. dati genetici* che – ai sensi del combinato disposto dell'art. 4 n. 13 e del considerando 34 del GDPR – sono

qualificabili come quelli relativi alle informazioni personali sui caratteri genetici ereditari dell'interessato, reperibili attraverso l'analisi di un campione biologico della persona fisica in questione, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti, ed i *dati biometrici* i quali – secondo l'art. 4 n. 14 – sono quelli derivanti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione mediante immagine facciale o dati dattiloscopici.
In termini generali possiamo far rientrare, dunque, nella definizione di dato sanitario – nel senso indicato all'inizio del paragrafo – ognuna delle tre tipologie di dati sopra richiamate.

4. Le ragioni della tutela del dato sanitario[3].

Con lo sviluppo delle nuove tecnologie, i dati sanitari rivestono sempre maggiore importanza, dal momento che, grazie ad esse, diventa estremamente semplice ricostruire e documentare la storia clinica dell'interessato; inoltre, la possibilità di scambiare le informazioni, contenute nelle banche dati, tra i vari istituti di ricerca e di analizzarne ingenti quantità attraverso algoritmi sofisticati consente di individuare cure sempre più precise e politiche sanitarie efficienti, aventi l'effetto visibile del miglioramento delle condizioni di salute della generalità.
Tuttavia, la "vocazione" dei dati sanitari travalica ormai l'ambito prettamente socio-sanitario: proprio le nuove tecnologie fanno sì che detti dati possano essere elaborati dagli operatori economici per finalità extra-sanitarie che possono ripercuotersi negativamente sui diritti e le libertà fondamentali della persona.
In generale, sono le stesse persone fisiche interessate che contribuiscono a rendere verosimile quest'ultimo scenario, giacché le loro scelte comportamentali spesso vanno nella direzione opposta rispetto alla tutela della propria riservatezza: infatti, senza porsi minimamente il problema, spesso rendono disponibili al pubblico, alle imprese e alle autorità pubbliche, su scala europea e mondiale, innumerevoli informazioni personali, tra le quali rientrano, appunto, i dati sanitari. Se è pur vero che la libera circolazione dei dati favorisce gli scambi, le relazioni sociali, la conoscenza, il confronto, essa cela non di meno anche considerevoli rischi.
E' quindi essenziale che ogni persona debba essere posta in grado di avere il controllo sui suoi dati, nel senso di conoscere come questi,

---

[3] Cfr. P. MUIÀ, *La tutela della privacy in ambito sanitario*, Santarcangelo di Romagna, 2018, p.

singoli o organizzati, vengono utilizzati, nell'ambito di un quadro europeo (e internazionale) di regole comuni.
Difatti, la possibilità di profilare i dati sanitari in direzione di interessi economici e privati e per plasmare forme di condizionamento delle persone nelle loro scelte economiche, politiche e sociale è tutt'altro che irreale.
Si pensi, ad esempio, all'elaborazione del dato sanitario per finalità legate al marketing delle case farmaceutiche oppure – dato che grazie ad essi è ricostruibile non solo la storia clinica dell'interessato ma anche prevedere l'andamento di certe patologie ed il loro carattere congenito – di utilizzarli per decidere se assumere un soggetto o – ad, esempio, in ambito assicurativo – se concludere un determinato contratto (come le polizze vita).
È, dunque, evidente che trattamenti del genere possono condurre a discriminazioni che si ripercuotono nella sfera economica e, soprattutto, intima e personale dell'interessato.
Al netto delle problematiche appena esposte, sono tuttavia innegabili le potenzialità intrinseche che i dati sanitari possiedono per gestire in maniera efficiente ed efficace la salute individuale e pubblica e che rendono manifesta la loro "*dinamicità*": in particolare, i progressi medici non sarebbero possibili se non fosse consentita o venisse limitata la loro circolazione, elaborazione, modificazione, confronto, comunicazione ed interconnessione tra i vari operatori sanitari. È chiaro, però, che un trattamento indiscriminato e privo di regole adeguate – soprattutto se la loro attitudine a rivestire un ruolo fondamentale nell'attuale mercato e contesto economico – può realmente condurre ad implicazioni negative sulla *"persona"* (intesa nel significato vero e proprio stabilito dall'art. 2 della Costituzione), come si è avuto modo di dire poco sopra.
L'esigenza, quindi, di trovare un bilanciamento necessita, da una parte, di forme di tutela più incisive legate soprattutto alla loro raccolta, analisi, comunicazione e conservazione e, dall'altra, che gli interessati siano informati adeguatamente dalle strutture o dai professionisti sanitari delle finalità e modalità del trattamento, nell'ottica di prevenire che soggetti terzi possano venirne a conoscenza indebitamente. È proprio questa linea che dovranno seguire i soggetti coinvolti: d'altronde, sono gli stessi Garanti degli Stai membri (considerando 39 del GDPR) a suggerire che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali.

5. Principi e rivoluzione del GDPR.

Abbiamo appena dato conto dell'importanza della tutela dei dati personali dei cittadini dell'Unione Europea, in particolare di quelli sanitari.
Al riguardo, il GDPR, in primo luogo, vuole garantire che il loro trattamento, e cioè l'utilizzo delle informazioni e notizie che li riguardano, si svolga nel rispetto dei diritti e delle libertà fondamentali, con particolare riferimento al diritto alla protezione dei dati personali (art. 1).
Più precisamente, il GDPR si propone soprattutto di far sì:
a) che i dati personali vengano utilizzati per scopi leciti e comunque per le finalità in base alle quali sono stati raccolti e non oltre il tempo necessario per raggiungere tali finalità;
b) che i dati conosciuti da estranei, che non vengano diffusi o comunque utilizzati contro la volontà o nell'ignoranza della persona cui si riferiscono;
c) che i dati personali non vengano distrutti o perduti.
Lungo queste tre direttrici si snodano i principi posti dal Regolamento. È l'art. 5 che li elenca:

- la lett. a) prescrive che il trattamento dei dati deve avvenire nel rispetto dei principi di liceità e correttezza. Ciò impone in capo al titolare l'obbligo di informare gli interessati sulla raccolta, l'utilizzo e la consultazione dei loro dati. La medesima norma prevede, sempre alla lett. a), il principio della trasparenza, che riguarda sia il contenuto delle informazione sui dati che le modalità con cui vengono veicolate, in termini di accessibilità, comprensibilità e consapevolezza dell'interessato;
- la lett. b) dell'art. 5 prevede il principio della limitazione delle finalità, secondo il quale i dati devono essere raccolti per finalità determinate, esplicite e legittime (cioè fondate su una base giuridica)[4];
- la lett. c) espone il principio della minimizzazione dei dati, per cui i dati raccolti devono essere solo quelli funzionali e necessari al perseguimento delle finalità predeterminate;
- la lett. d) manifesta il principio di esattezza, ai sensi del quali i dati devono essere trattati con un'organizzazione tale da garantire la loro accuratezza, il loro aggiornamento e, se del caso, il diritto di rettifica dell'interessato[5];
- alla lett. e) la disposizione enuncia il principio della limitazione della conservazione, secondo cui i dati possono essere conservati in modo tale da permettere l'identificazione

---

[4] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy Europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2018, p. 103.
[5] *Ivi*, pag. 109.

dell'interessato solo per il tempo necessario al perseguimento una determinata finalità, a meno che la loro archiviazione non sia sostenuta da ragioni di interesse pubblico, da finalità statistiche o di ricerca storica o scientifica;

- la lett. f) sancisce il principio dell'integrità e della riservatezza dei dati, per cui il trattamento deve garantire loro un livello di protezione adeguato in modo da scongiurare trattamenti illeciti, non autorizzati, la loro distruzione o un danno accidentale.

Da questi principi il Regolamento fa derivare una serie di misure ed adempimenti specifici che il titolare deve essere in grado di comprovare (art. 5 II° paragrafo: principio di "accountability" o di responsabilizzazione).

Passando, adesso, all'esame delle norme specifiche che disciplinano il trattamento dei dati sanitari, si nota che a differenza del nostro codice privacy il GDPR non riserva alcun capo per essi; ciò nonostante viene conferito loro un peso importante proprio per la loro fragilità rapportata alla protezione della persona. Infatti, per quanto riguarda le condizioni per la liceità del trattamento stesso (si veda il considerando 51 del GDPR), occorre prendere le mosse, in primo luogo, dall'art. 9 che definisce "categorie particolari di dati personali" una serie di dati personali che – come viene specificato sempre dal considerando 51 – per loro natura sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali stessi. Tra questi sono ricompresi i dati genetici e quelli biometrici intesi ad identificare in modo univoco una persona ed i dati relativi alla salute della persona stessa.

La norma sancisce, quindi, un principio di carattere generale che ne vieta il trattamento.

Al II° paragrafo, poi, l'art. 9 elenca le deroghe/basi giuridiche al ricorrere delle quali il divieto non opera. Se si esclude il consenso – che, come prevede la lett. a della norma, è condizione per il trattamento se rilasciato esplicitamente dall'interessato per una o più finalità specifiche – alcune di esse sono riconducibili alla prestazione sanitaria generalmente intesa, e cioè:

- tutela di 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 (lett. c);
- trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione Europea o degli Stati membri (lett. g): in tal caso, il trattamento è giustificato se risulta proporzionato alla finalità perseguita, rispetta i principi fondamentali in materia ed assicura misure appropriate e specifiche per proteggere i diritti fondamentali e

gli interessi dell'interessato[6];

- trattamento 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 il professionista della sanità (lett. h): in questa ipotesi, però, i dati possono essere trattati solo da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti;
- trattamento 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 (lett. i): in questo caso il trattamento è legittimo solo se prevede misure appropriate e specifiche per proteggere i diritti fondamentali e gli interessi dell'interessato).

Da quanto appena scritto, si nota immediatamente che il nuovo Regolamento UE segna un'accelerazione ed anzi un completo cambio di prospettiva nel campo della riservatezza e del trattamento dei dati sanitari rispetto al codice privacy: quest'ultimo, infatti, legittimava il trattamento dei dati sanitari solo previo consenso scritto dell'interessato o, in mancanza, previa autorizzazione del Garante, qualora il trattamento fosse giustificato da finalità di tutela della salute o dell'incolumità fisica di un soggetto terzo o della collettività (art. 76); mentre i dati genetici potevano essere trattati solo in seguito ad un'autorizzazione specifica del Garante (art. 92).

Nel GDPR, invece, aumentano le ipotesi di legittimità del trattamento svincolate dal consenso ma, nell'ottica della tutela rafforzata del dato sanitario, il legislatore europeo ha "corretto" questa scelta vincolando trattamenti del genere a misure appropriate e specifiche a tutela dei diritti fondamentali dell'interessato.

È proprio sulla base di questa "linea direttiva" e dell'autonomia che il paragrafo 4 dell'art. 9 del GDPR riconosce agli Stati membri che il nostro legislatore con il d.lgs. 101/2018 ha introdotto nel Codice Privacy l'art. 2-*septies*, il quale prevede che i dati sanitari dovranno essere trattati – oltre che nel rispetto dell'art. 9 del Regolamento – conformemente a misure di garanzia che dovranno essere emanate dal

---

[6] Quanto previsto alla citata lett. g), come vedremo in prosieguo, assume particolare rilievo atteso quanto disposto dal Legislatore italiano con il d.lgs. 101/2018 che ha introdotto nel Codice Privacy l'art. 2-*sexies* con il quale ha costruito un perimetro per delimitare il concetto di "interesse pubblico rilevante".

Garante con cadenza biennale.

6. Modifiche al Codice Privacy: il decreto legislativo di adeguamento n. 101/2018.

Riguardo alla normativa italiana, appare opportuno esaminare, sia pur brevemente, alcune delle modifiche al Codice Privacy riguardanti la sanità, introdotte dal d. lgs. 101/2018[7].
Come noto l'articolo 9 del Regolamento al paragrafo 1 pone un divieto generale di trattamento di alcune particolari categorie di dati.
Il paragrafo 2 del detto articolo contiene però delle significative eccezioni tra le quali assume particolare importanza, ai fini del presente elaborato, quella di cui alla lettera 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"*.
Il breve richiamo all'art. 9 del GDPR costituisce la base per illustrare l'ampia portata della prima norma degna di rilievo contenuta nel d. lgs 101/2018 ovvero l'art. 2-*sexies* che pone l'accento sul trattamento da considerarsi "necessario e legittimo" per motivi di interesse pubblico rilevante delle categorie particolari di dati personali (cfr. art. 9 GDPR).
Al I° comma la nuova norma stabilisce che deve essere la legge – o il regolamento, se previsto dalla legge stessa – a specificare quali dati personali particolari possono essere trattati, le operazioni eseguibili, i motivi di interesse pubblico e le misure di protezione a tutela dei diritti fondamentali dell'interessato.
La norma individua, poi, al comma 2 una serie di materie, in cui l'interesse pubblico si considera rilevante "*ex lege*".
Per quanto interessa ai fini del presente contributo tra le altre assumono particolare rilievo le lettere:
- *" .. t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;*
u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile,

---

[7] Decreto Legislativo 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, in *G.U.* n. 205 del 4 settembre 2018.

salvaguardia della vita e incolumità fisica;
v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili".
In relazione al trattamento di particolari categorie di dati viene quindi stabilita normativamente, per alcune sole materie, la liceità di trattamenti effettuati per "motivi di interesse pubblico rilevante" con la creazione, quindi, di una nuova base giuridica per il trattamento di dati particolari.

*

Altra norma di sicuro rilievo, già brevemente analizzata, è l'art. 2-*septies* che disciplina dettagliatamente il trattamento di dati genetici, biometrici e relativi alla salute con riferimento anche alle misure di garanzia.
La norma stabilisce che questi dati possono essere oggetto di trattamento, fermo quanto disciplinato dal GDPR all'art. 9, in conformità a misure di garanzia disposte dal Garante con proprio provvedimento.
Il provvedimento che stabilisce le misure di garanzia dovrà essere adottato con cadenza almeno biennale e dovrà tener conto:
a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.
Le misure di garanzia riguarderanno anche le cautele da adottare relativamente;
- ai contrassegni sui veicoli e accessi a zone a traffico limitato;
- ai profili organizzativi e gestionali in ambito sanitario
- alle modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute nonché la prescrizioni di medicinali.
Le misure di garanzia individueranno poi tra l'altro le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire

i diritti degli interessati.
Limitatamente ai dati genetici, le misure di garanzia potranno individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del Regolamento, o altre cautele specifiche.

*

Un'ulteriore novità è rappresentata dall'art. 2-*terdecies* che disciplina l'esercizio dei diritti di cui agli artt. da 15 a 22 GDPR, qualora l'interessato sia una persona deceduta; tali diritti potranno essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari e meritevoli di protezione.

*

Il capo II del Titolo V del Codice, come modificato dal d. lgs. 101/2018, contiene una serie di importanti disposizioni che individuano ipotesi in cui il legislatore italiano opera una significativa semplificazione delle modalità di informazione del paziente sul trattamento dati e delle modalità di rilascio e acquisizione del consenso al trattamento da parte dell'interessato.

*

Nella parte finale il d. lgs.101/2018 contiene norme "originali", ossia non modificative di articoli del Codice privacy e, nell'ottica che qui ci occupa, appaiono decisamente significativi l'art. 20 e l'art. 21.
L'art. 20 conferma la validità dei Codici di deontologia e di buona condotta già allegati al Codice; essi verranno rivisti dall'Autorità Garante per dare loro piena conformità alle norme del Regolamento Europeo e ripubblicati come "regole deontologiche" entro 90 giorni. Ove necessario le comunità scientifiche saranno invitate a definire le nuove regole.
Si segnala poi l'importanza dell'art. 21 in tema di autorizzazioni generali del Garante per la protezione dei dati personali.
Il Garante per la protezione dei dati personali, ai sensi del detto articolo, individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del Regolamento, che risultano compatibili con le disposizioni del medesimo Regolamento e del decreto di adeguamento e, ove occorra, provvede al loro aggiornamento.
Le autorizzazioni generali sottoposte a verifica che sono state ritenute incompatibili con le disposizioni del Regolamento (UE) 2016/679 cessano di produrre effetti dal momento della pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana del provvedimento di cui al comma 1.
Le autorizzazioni generali del Garante per la protezione dei dati personali adottate prima della data di entrata in vigore del decreto n.

101/2018 e relative a trattamenti diversi da quelli indicati al comma 1 cessano di produrre effetti alla predetta data.

7. Ambiti e strumenti coinvolti dalle modifiche al GDPR (Fascicolo sanitario elettronico - Dossier Sanitario - Cartella elettronica - Referti online - Siti web – App e mHealth).

È interessante, adesso, approfondire gli effetti che la nuova normativa ha prodotto sui principali sistemi di gestione elettronica delle pratiche sanitarie. Appare, quindi, opportuno, iniziare la trattazione partendo dal primo provvedimento che ha riguardato i principali sistemi, e cioè dalle Linee Guida del Garante in tema di **Fascicolo sanitario elettronico (Fse) e di Dossier sanitario** del 16 luglio 2009[8].
A livello pratico, il Fse e il Dossier venivano definiti come supporti contenenti diverse informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica. I dati personali sono collegati tra loro con modalità informatiche di vario tipo che ne rendono, comunque, possibile un'agevole consultazione unitaria da parte dei diversi professionisti o organismi sanitari che prendono nel tempo in cura l´interessato.
In particolare, secondo le Linee Guida, si parla di **Dossier sanitario** qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti. I Dossier sanitari possono anche costituire, ad esempio, l´insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in un'iniziativa di Fse regionale.
Si intende, invece, per **Fse** il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta).
Il Fse è costituito preferendo, di regola, soluzioni che non prevedono una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l´interessato.
Da queste caratteristiche il Garante individuava la necessità – specie perché i dati sanitari e i documenti riuniti nel Fse possono provenire da più soggetti – di adottare idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del Fse.

*

[8] Garante per la protezione dei dati personali, Linee Guida del Garante in tema di Fascicolo sanitario elettronico (Fse) e di Dossier sanitario del 16 luglio 2009, in *G.U.* n.178 del 3 agosto 2009.

Stante quanto sopra ed in assenza di una previsione legislativa che prevedesse l´istituzione di tali strumenti, le Linee Guida del 2009 ammettevano tra le finalità lecitamente perseguibili soltanto quelle riconducibili alla prevenzione, alla diagnosi ed alla cura dell'interessato, ovvero ad assicurare un migliore processo di cura dello stesso attraverso la ricostruzione di un insieme – di regola su base logica – il più possibile completo della cronistoria degli eventi di rilievo clinico occorsigli e relativi a distinti interventi medici.
L'utilizzo del FSE o del dossier per finalità ulteriori doveva essere escluso (in particolare, per le attività di programmazione, gestione, controllo e valutazione dell´assistenza sanitaria, che possono essere, peraltro, espletate in vari casi anche senza la disponibilità di dati personali), ferme restando eventuali esigenze in ambito penale.
Qualora – poi – attraverso il Fse o il dossier si intendessero perseguire anche finalità amministrative strettamente connesse all´erogazione della prestazione sanitaria richiesta dall´interessato (es. prenotazione e pagamento di una prestazione), tali strumenti devono necessariamente esser dotati di una struttura in grado di separare i dati amministrativi dalle informazioni sanitarie vere e proprie, prevedendo profili diversi di abilitazione degli aventi accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite sulla base delle mansioni svolte.
Il Garante non negava, inoltre, che il Fse o il dossier potessero essere utilizzati per fini di ricerca scientifica, epidemiologica o statistica ma subordinava il trattamento a specifiche cautele, come, ad esempio, la conformità alla normativa di settore.

*

Nella seconda parte delle Linee Guida il Garante chiariva alcuni diritti dell'interessato ed alcuni aspetti procedurali.
In particolare, venivano disciplinati il diritto – per i professionisti sanitari – alla costituzione di un Fascicolo sanitario elettronico e di un dossier sanitario, individuando i soggetti che abilitati al trattamento dei dati.
Le Linee Guida definivano le condizioni e le modalità di accesso ai dati personali contenuti nel Fascicolo sanitario elettronico e nel dossier sanitario ed elencavano i diritti dell´interessato sui propri dati personali.
Il Garante si occupava, poi, di porre dei limiti alla diffusione e al trasferimento all´estero dei dati nonché di individuare le misure di sicurezza a tutela degli stessi.
Infine, venivano disciplinate l'informativa e le modalità di rilascio del consenso nonché le modalità di comunicazione al Garante.

*

Svolto questo excursus sulle Linee Guida del 2009, appare opportuno dedicarsi sulle attuali normative di riferimento. Il fascicolo sanitario elettronico (FSE) è ora disciplinato principalmente da 4 atti, due di

carattere normativo e due di carattere eminentemente tecnico:
- il d.l. n. 179/2012[9], al cui art. 12 esso viene definito come l'insieme dei documenti e dei dati digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito. Si tratta, a ben vedere, di un mezzo – destinato ad implementarsi per sua stessa natura – idoneo a rappresentare la storia sanitaria di un paziente e può essere istituito dalle regioni o province autonome per finalità di (1) prevenzione, diagnosi, cura e riabilitazione, (2) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico e (3) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria;
- il Regolamento contenuto nel d.p.c.m. n. 178/2015[10];
- il Decreto 4 agosto 2017 del Ministero dell'Economia e delle Finanze recante "Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)"[11];
- l'art. 1, comma 382 della Legge di Bilancio 2017 (l'Informativa semplificata per gli assistiti)[12] e gli artt. 14-17 del Decreto del Ministero dell'Economia e delle Finanze del 4/8/2017 ("Disponibilità dei dati del Sistema Tessera Sanitaria nel FSE").

*

L'art. 6 del Regolamento (d.p.c.m. n. 178/2015) è una delle norme più importanti da interpretare alla luce delle novità normative intervenute, giacché il contenuto dell'informativa che deve essere messa a disposizione dei pazienti quando è istituito il FSE dovrà adeguarsi a quanto dispongono gli art. 13 e 14 del GDPR.
Anche l'art. 8 del Regolamento, che riconosce al paziente una serie di diritti, dovrà ampliare la sua platea a quelli previsti dal GDPR.
Vi è, però, una questione più rilevante da approfondire. Abbiamo visto nel secondo paragrafo che il consenso è diventato una base giuridica residuale per poter trattare legittimamente i dati, soprattutto dopo che

---

9 Decreto Legge del 18 ottobre 2012, n. 179, *Testo del decreto-legge 18 ottobre 2012, n. 179 (pubblicato nel supplemento ordinario n. 194/L alla Gazzetta Ufficiale 19 ottobre 2012, n. 245), coordinato con la legge di conversione 17 dicembre 2012, n. 221, recante: «Ulteriori misure urgenti per la crescita del Paese.»*, in *G.U.* n. 294 del 18 dicembre 2012.

10 Decreto del Presidente del Consiglio dei Ministri del 29 settembre 2015, n. 178, *Regolamento in materia di fascicolo sanitario elettronico*, in *G.U.* n. 263 dell'11 novembre 2015.

11 Decreto del Ministero dell'Economia e delle Finanze del 4 agosto 2017, *Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE) di cui all'art. 12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221*, in *G.U.* n.195 del 22 agosto 2017.

12 Legge 11 dicembre 2016, n. 232, *Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019*, in *G.U.* n. 297 del 21 dicembre 2016.

è stato introdotto al Codice Privacy l'art. 2-*sexies* che elenca una serie di materie in cui l'interesse pubblico rilevante è presunto.
Alla luce delle novità normative è d'obbligo chiedersi se il consenso sia da considerare ancora come la base per i trattamenti e le attività connesse svolte sulla base del FSE. Difatti, l'art. 9 alla lett. h) legittima i trattamenti dei dati particolari per finalità di diagnosi, assistenza o terapia sanitaria o sociale ovvero per la gestione dei sistemi e servizi sanitari, così come alla lett. j) legittima quelli finalizzati alla ricerca scientifica; mentre l'art. 2-*sexies* al II° comma considera materie in cui l'interesse pubblico rilevante è presupposto quelle relative ad attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale (lett. t), ai compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché ai compiti di sicurezza e salute della popolazione (lett. u), alla programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale (lett. v).
A ben vedere, si tratta di basi giuridiche cui corrispondono le finalità del FSE. Per cui, si può ritenere che l'alimentazione e la consultazione di esso costituiscano delle attività di trattamento la cui legittimità può ritenersi svincolata dal consenso preventivamente rilasciato dall'assistito.
Ammettendo questo, è opportuno allora domandarsi quale sia la sorte di alcuni diritti riconosciuti al paziente dal Regolamento sul FSE. Ad esempio, il diritto all'oscuramento – secondo cui alcuni dati o documenti possono esser resi inaccessibili su richiesta dell'interessato per coloro che, invece, avrebbero diritto di accedervi – contrasta con le basi giuridiche sopra riportate e dovrebbe, quindi, considerarsi caducato. Accettando questa ricostruzione, risulta fondamentale un nuovo bilanciamento tra queste ultime novità e le prerogative del paziente, soprattutto in considerazione dell'importanza dei dati sanitari. Potrebbe essere opportuno, allora, inviare all'interessato report periodici e comprensibili nei quali vengono specificati i soggetti che hanno "trattato" i dati contenuti nel FSE e per quali finalità: ciò non solo nell'ottica del rispetto dei principi di privacy by default e di accountability ma anche in funzione di educare i cittadini alla consapevolezza dell'importanza dei loro dati personali e di tutte le operazioni che li riguardano. Una misura del genere potrebbe benissimo rientrare tra quelle di garanzia previste dall'art. 2-*septies* introdotto dal d.lgs. 101/2018.
Se quanto appena scritto può ben riguardare i dati relativi alla salute, dei dubbi possono sorgere con riferimento, invece, ai dati genetici. Un approccio più cautelativo impone, infatti, di rendere questi ultimi ancora soggetti al requisito del consenso per le operazioni relative al

FSE, non foss'altro perché – oltre alla loro natura – sia il GDPR all'art. 9 paragrafo IV° che l'art. 2-*septies* al VI° comma prevedono che il consenso possa configurarsi per questa tipologia di dati ancora come misura di protezione dell'interessato.
Abbiamo scritto sopra che i dati contenuti nel FSE possono essere trattati anche per finalità di ricerca. Al riguardo è necessario coordinare questa finalità con le nuove prescrizioni normative di riferimento. L'art. 89 del GDPR stabilisce, infatti, che i dati personali a fini di ricerca scientifica dovrebbero essere trattati solo se sono state prese garanzie adeguate a proteggere i diritti e le libertà dell'interessato. Inoltre, prima di effettuare trattamenti del genere, il titolare deve aver valutato che sia fattibile raggiungere tale finalità in modo da non consentire l'identificazione dell'interessato. In casi del genere, la norma prescrive agli Stati membri di prevedere garanzie adeguate.
Da questo quadro, possiamo affermare che le previsioni normative del Regolamento sul FSE sono conformi all'art. 89 del GDPR: l'art. 16, infatti, prescrive che dal trattamento dei dati sanitari contenuti nel FSE per finalità di ricerca devono essere esclusi tutti i dati personali che possono costituire un riferimento idoneo per giungere all'identificazione del paziente. La disposizione elenca, quindi, espressamente i dati degli assistiti che non possono essere trattati.
Sfruttando la possibilità che il GDPR ha concesso agli Stati membri di prevedere garanzie adeguate per trattamenti indirizzati alla ricerca scientifica, il nuovo art. 106 del Codice Privacy demanda al Garante la promozione di regole deontologiche prescrittive per i soggetti interessati al trattamento per fini di ricerca scientifica. Si tratta di una norma il cui contenuto e la cui *ratio*, a ben vedere, sono stati ricalcati dall'art. 2-*septies*.

*

L'altro sistema di gestione dei dati sanitario è costituito come detto dal **c.d. Dossier sanitario**, il quale viene adesso definito dalle Linee Guida del Garante adottate con deliberazione del 4 giugno 2015[13] come l´insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l´interessato, che vengono condivisi tra i professionisti sanitari che lo assistono presso un´unica struttura sanitaria. Le Linee Guida disciplinano vari aspetti e questioni direttamente connesse al dossier.
In particolare trovano riferimento l'informativa e le modalità di espressione del consenso anche in casi di emergenza.
Vengono poi individuati i diritti dell'interessato in termini di limitato accesso di terzi ai propri dati ed esattamente il diritto all'oscuramento ed il diritto alla visione degli accessi al dossier.

---

[13] Garante per la protezione dei dati personali, Linee guida in materia di Dossier sanitario del 4 giugno 2015, in *G.U.* n.164 del 17 luglio 2015.

Il Garante definisce, inoltre, le modalità di accesso al dossier ed individua gli incaricati e responsabili del trattamento dei dati contenuti in esso.
Sul piano della sicurezza viene disciplinata una procedura dettagliata di Data breach e sono invitati i titolari alla nomina di un Data protection officer (referente per la protezione dati).
Anche la normativa che disciplina il dossier, come per il FSE, dovrà essere adeguata alle disposizioni del GDPR e del Codice Privacy modificato: così, l'informativa che deve essere fornita al paziente come stabilito dalle Linee Guida del Garante dovrà rispettare il contenuto prescritto dagli articoli 13 e 14 del Regolamento UE ed i diritti riconosciuti all'interessato saranno quelli elencati dal GDPR.
Le medesime considerazioni svolte per il FSE in merito al ruolo del consenso possono valere anche per il dossier sanitario.

*

La **cartella clinica**, normata dalle Linee Guida del Ministero della Salute del 17 giugno 1992[14], è definita come lo strumento informativo individuale finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente e ad un singolo episodio di ricovero. Ciascuna cartella clinica ospedaliera deve rappresentare l'intero episodio di ricovero del paziente nell'istituto di cura: essa, conseguentemente, coincide con la storia della degenza del paziente all'interno dell'ospedale. La cartella si forma dal momento dell'accettazione del paziente in ospedale, ha termine al momento della dimissione del paziente dall'ospedale e segue il paziente nel suo percorso all'interno della struttura ospedaliera. In definitiva, essa è una sorta di diario giornaliero contenente tutte le informazioni relative al paziente durante il periodo di ricovero.
Lo sviluppo delle tecnologie e la dematerializzazione è stato un processo che ha coinvolto anche questo strumento, per cui oggi possiamo parlare anche di cartella clinica elettronica come l'insieme logico delle informazioni cliniche, assistenziali e amministrative relative a un episodio di cura (es. episodio di Ricovero Ordinario, Day Hospital, Day Service, accessi ambulatoriali) o a un percorso di cura (es. PDTA, Percorsi di Cronicità, Percorso Gravidanza Fisiologica) gestito con modalità elettronica. Consente, quindi, la raccolta e la gestione semplice ed immediata delle informazioni cliniche del paziente su un supporto informatico a servizio dell'Azienda Ospedaliera[15].
Prima di esaminare gli effetti della novità normative su questo strumento, occorre chiarire che diverse cartelle cliniche afferenti lo

---

[14] Decreto del Ministero della Sanità del 17 giugno 1992, *"La compilazione, la codifica e la gestione della scheda di dimissione ospedaliera istituita ex dm 28.12.1991"*, in *G.U.* n.188 dell'11 agosto 1992.

[15] A. LOSITO, *Cartella clinica elettronica: cos'è e come funziona, costi e quali dati*, in www.guidafisco.it., 2018.

stesso paziente generate nel tempo in un ospedale o in una azienda sanitaria diventano, di fatto, un dossier sanitario.
In tal caso, la disciplina di riferimento sarà quella prevista per questo strumento, secondo quanto è stato sopra riferito.
Occorre prendere le mosse dal Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE) adottato il 15 febbraio 2007 dal WP 29[16]. In tale elaborato il Gruppo di lavoro Articolo 29 ha fornito degli orientamenti sull'interpretazione del quadro giuridico in materia di protezione dei dati applicabile alle CCE e spiegato alcuni principi generali. Il documento di lavoro ha dato altresì indicazioni sui requisiti relativi alla protezione dei dati richiesti per la costituzione delle CCE e sulle garanzie necessarie.
In primo luogo, il Gruppo di lavoro Articolo 29 ha ricordato il divieto generale di trattamento dei dati personali relativi alla salute sancito dall'articolo 8, paragrafo 1 della direttiva 95/46/CE sulla tutela dei dati, ed esaminato in seguito la fattibilità applicativa delle deroghe di cui all'articolo 8, paragrafi 2, 3 e 4 della stessa direttiva ai sistemi di CCE, sottolineando la necessità di interpretarle in modo restrittivo.
Inoltre, in merito al possibile quadro giuridico adatto ai sistemi di CCE, esso ha formulato undici raccomandazioni per gli ambiti in cui risultano particolarmente necessarie speciali garanzie per tutelare i diritti alla protezione dei dati dei pazienti e delle persone in genere.
Gli ambiti interessati sono i seguenti:
1. Rispetto dell'autodeterminazione
2. Identificazione e riconoscimento dei pazienti e del personale sanitario
3. Autorizzazione ad accedere alle CCE per leggerle e compilarle
4. Utilizzo delle CCE ad altri fini
5. Struttura organizzativa di un sistema di CCE
6. Categorie di dati contenuti nelle CCE e modalità di presentazione
7. Trasferimento internazionale di documentazione medica
8. Sicurezza dei dati
9. Trasparenza
10. Responsabilità
11. Meccanismi di controllo relativi al trattamento dei dati contenuti nelle CCE

*

Su un piano generale, il sistema informatico di supporto alla CCE deve permettere, secondo la logica dei nuovi principi di privacy by design e by default, l'implementazione di specifiche politiche di riservatezza e protezione dei dati dirette in primo luogo a garantire specifiche regole di accessibilità ai dati clinici dalla fase della

---

[16] GRUPPO DI LAVORO ARTICOLO 29, 00323/07/EN WP 131, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE).*

creazione a quella della cancellazione. Tali politiche – coerenti prima di tutto, quindi, con il GDPR e poi con la normativa italiana riformata – saranno oggetto di futuri provvedimenti del Garante che stabilirà misure di garanzia ad hoc per la tutela dei dati in caso di loro trattamento elettronico.

*

Passiamo adesso ad esaminare le problematiche attinenti al **referto on-line** che, nell'ambito della sanità digitale rappresenta la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale che viene trasmessa telematicamente. Il referto on-line è un servizio facoltativo ed è disciplinato dalle Linee Guida del Garante del 19 novembre 2009[17]. Il contenuto di tale provvedimento rivela, nonostante lo iato temporale, la piena conformità alle prescrizioni del GDPR e del nuovo Codice Privacy: basti pensare alle cautele prescritte per l'invio tramite mail del referto o per la sua consultazione sul sito web dell'azienda sanitaria oppure agli obblighi specifici relativi all'informativa che la struttura deve fornire all'utente in merito alla refertazione on-line. In quest'ultimo caso, vale quanto scritto sopra sul dossier e sul FSE: rispetto del contenuto prescritto dagli art. 13 e 14 del GDPR ed esposizione dei diritti previsti dal medesimo.

*

Lo sviluppo della tecnologia e di Internet unito all'implementazione dei mezzi di comunicazione telematica e digitale ha avuto un ruolo di primo piano nella diffusione delle informazioni sanitarie.
Il principale strumento di divulgazione e scambio dei dati sanitari – non solo tra professionisti sanitari ma anche tra semplici utenti della rete – è costituito dal **sito web** appositamente dedicato. Balzano immediatamente all'attenzione i pregiudizi che possono derivare alle libertà ed ai diritti fondamentali delle persone dall'uso improprio e incosciente di un tale strumento dedicato alle tematiche sanitarie. Ciò è evidente solo raffrontando la quotidianità: è, infatti, un dato di fatto che spesso gli utenti mettono a disposizione i propri dati sanitari in maniera del tutto acritica. Tali dati, come si è avuto modo di analizzare nel primo paragrafo, hanno una notevole potenzialità economica e strategica per determinati operatori del mercato. Si evince, quindi, che la maggior parte degli utenti sono privi di un'educazione e di una sensibilità tali da indurli a scegliere quali dati condividere, con chi ed in che modo. A fronte di queste problematiche il Garante ha emanato il 25 gennaio 2012 delle apposite Linee Guida[18].

---

[17] Garante per la protezione dei dati personali, *Linee guida in tema di referti on-line del 19 novembre 2009*, in *G.U.* n. 288 dell'11 novembre 2009.

[18] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute del 25 gennaio 2012*, in *G.U.* n. 42 del 20 febbraio 2012.

La portata delle Linee Guida riguarda tutti i soggetti che gestiscono siti web che svolgono un'attività divulgativa e conoscitiva delle informazioni relative alla salute: si pensi ai vari forum, ai blog, ai portali specializzati ed ai social network contraddistinti da una finalità di sensibilizzazione in tale ambito.
Il Garante, poi, distingue tra siti web che prevedono la registrazione dell'utente e siti che, al contrario, non la prevedono. Per i primi, le Linee prevedono una serie di adempimenti che vanno dall'informativa ad una specifica avvertenza dei rischi che possono derivare, dall'elenco dei diritti degli utenti fino all'implementazione delle misure di sicurezza preventive idonee ad evitare violazioni dei dati. Ebbene, se è chiaro che, anche in questo caso, il contenuto dell'informativa e l'elenco dei diritti riconosciuti all'interessato dovranno adeguarsi alle disposizioni di riferimento del GDPR, la validità delle altre disposizioni delle Linee Guida devono essere raffrontate con l'impostazione della normativa europea.
Difatti, stante quanto scritto sopra e nell'ottica dei principi di limitazione delle finalità, minimizzazione dei dati e di privacy by design e by default si possono considerare conformi alla normativa sovranazionale le disposizioni che prescrivono al gestore del sito di avvertire l'utente del rischio che l'inserimento dei propri dati relativi alla salute connessi a quelli identificativi può comportare l'individuazione della sua patologia o della possibilità di non inserire in fase di registrazione il suo nome e cognome? I medesimi dubbi possono sorgere riguardo agli avvertimenti che devono essere forniti all'utente in merito all'inserimento di dati o di video o foto idonei ad identificare lui o terzi?
Ebbene, se da un lato è indubbia la funzione divulgativa di questi siti web, è altrettanto indubbio, però, che alla luce dei sopra citati principi, le prescrizioni dettate dal Garante per tutelare gli utenti di tali siti non possono più tradursi in mere avvertenze sui rischi: sarebbe più opportuno prevedere strumenti che impediscono di base l'inserimento di determinati dati sanitari o che consentono soltanto la visione parziale o cifrata del dato, necessaria allo scopo per il quale viene inserito nel sito. In definitiva, si tratta pur sempre di informazioni rese a dei siti diversi da quelli "istituzionali" che, difatti, sono esclusi dalle Linee Guida.

*

Con il termine "sanità mobile" (di seguito **"mHealth"**) si fa riferimento alla "pratica della medicina e della sanità pubblica supportata da dispositivi mobili, quali telefoni cellulari, dispositivi per il monitoraggio dei pazienti, computer palmari (PDA) e altri dispositivi senza fili.
Nella sanità mobile rientrano anche le applicazioni (di seguito "app") come le app per il benessere e lo stile di vita che consistono principalmente in app destinate a mantenere o migliorare, in modo

diretto o indiretto, le abitudini sane, la qualità della vita e il benessere delle persone che possono connettersi a dispositivi medici o sensori (ad esempio, braccialetti o orologi), i sistemi di consulenza personalizzata, gli SMS con informazioni sanitarie e promemoria dei farmaci da assumere e la telemedicina attraverso comunicazioni senza fili.
La mHealth è un settore emergente e in rapido sviluppo che può contribuire a trasformare l'assistenza sanitaria, migliorandone la qualità e l'efficienza ed in tale ottica la Commissione Europea ha redatto in data 10 aprile 2014 un libro verde "mHealth" [19] di importanza fondamentale in tema di applicazioni delle nuove tecnologie al settore dei beni e servizi sanitari.
La sanità mobile comprende varie soluzioni tecnologiche che permettono, tra le altre cose, di misurare parametri vitali come il ritmo cardiaco, il livello di glicemia, la pressione sanguigna, la temperatura corporea e l'attività cerebrale. Alcuni importanti esempi di app sono gli strumenti di comunicazione, informazione e motivazione, come i promemoria dei farmaci da assumere o gli strumenti che offrono consigli dietetici e su come restare in forma.
La crescente diffusione degli smartphone e delle reti 3G e 4G ha dato un forte impulso all'uso delle app mobili che offrono servizi sanitari. La disponibilità di tecnologie di navigazione satellitare nei dispositivi mobili offre la possibilità di migliorare la sicurezza e l'autonomia dei pazienti. La mHealth permette di raccogliere, con l'ausilio di sensori e app mobili, un volume considerevole di dati medici, fisiologici, ambientali, sullo stile di vita e sulle attività quotidiane. Tali dati possono costituire la base per la prestazione di cure e la conduzione di attività di ricerca basate su dati empirici e nel contempo consentono ai pazienti di accedere più facilmente alle informazioni sulla propria salute, ovunque si trovino e in qualsiasi momento.
La mHealth può inoltre permettere di fornire un'assistenza sanitaria di alta qualità, con l'effettuazione di diagnosi più precise e la prescrizione di trattamenti più mirati. Gli operatori sanitari possono curare i pazienti con maggiore efficienza, grazie alle app mobili che invogliano a seguire uno stile di vita sano, consentendo di personalizzare le cure e i trattamenti terapeutici. La sanità mobile contribuisce a rafforzare la responsabilità personale del paziente, che può partecipare più attivamente alla gestione della propria salute, conducendo una vita più autonoma nel proprio ambiente domestico grazie a soluzioni di autovalutazione o di controllo a distanza e al monitoraggio dei fattori ambientali.
A tale riguardo, la mHealth è considerata uno strumento ausiliario nella gestione e nella prestazione dell'assistenza sanitaria, che non

---

[19] COMMISSIONE EUROPEA, *Libro verde sulla sanità mobile ("mHealth")*, COM(2014) 219 final.

intende sostituirsi ai professionisti del settore, i quali continuano a svolgere un ruolo centrale. La mHealth può avere un ruolo essenziale nel miglioramento della vita, ma è fondamentale offrire ai cittadini garanzie di sicurezza circa l'uso della tecnologia.
L'obiettivo del libro verde è stato di avviare un'ampia consultazione delle parti interessate sugli ostacoli esistenti e sulle questioni connesse alla diffusione della mHealth, nonché aiutare a individuare la strada giusta per sbloccarne il potenziale. Il Libro verde valuta il potenziale della mHealth e gli aspetti tecnologici connessi ed elenca le questioni sulle quali è sollecitato il parere delle parti interessate. Analizza, inoltre, le possibilità offerte dalla mHealth per mantenere e migliorare la salute e il benessere dei pazienti e rafforzarne il ruolo attivo e la responsabilità personale. Sebbene molte delle questioni affrontate possano non rientrare nelle competenze del diritto unionale, l'UE può in ogni caso fungere da camera di compensazione per lo scambio di buone prassi e contribuire a promuovere l'innovazione in un settore con un potenziale enorme.
Con particolare riferimento alle app mediche, il grado di rispetto della normativa sulla protezione dei dati personali è stato oggetto di un'indagine avviata a maggio 2014 (c.d. "Privacy Sweep 2014")[20] dalle autorità nazionali per la protezione dei dati personali che fanno parte del Global Privacy Enforcement Network (GPEN). I risultati di tale indagine hanno rivelato che metà delle app mediche oggetto di verifica, scelte a campione tra le più scaricate in Italia, non fornivano un'informativa agli utenti prima dell'installazione, oppure presentavano informazioni generiche o richiedevano dati eccessivi rispetto a quanto necessario per la fruizione del servizio offerto. Analoghi risultati insoddisfacenti sono stati riscontrati a livello internazionale. Anche il Privacy Sweep 2016 sul c.d. "Internet delle cose" [21] ha rivelato che, su oltre trecento dispositivi elettronici connessi a internet – come orologi e braccialetti intelligenti, contatori elettronici e termostati di ultima generazione – più del 60% non garantiscono una sufficiente tutela della riservatezza dei dati personali. Si pensi, ad esempio, alla cintura cardiaca – utilizzata frequentemente dagli sportivi – che trasmette le pulsazioni cardiache allo smartwatch o all'app installata sul cellulare: al termine dell'allenamento, i dati solitamente vengono scaricati dall'utente su un portale che li rende pubblici, senza preventiva richiesta di consenso.

---

[20] Garante per la protezione dei dati personali, *"Global Privacy Sweep 2014". I risultati dell´indagine svolta da 26 autorita´ per la privacy di tutto il mondo*, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3374906.

[21] Garante per la protezione dei dati personali, Privacy: *"Internet delle cose", utenti poco tutelati. I risultati dell´analisi internazionale svolta dalle Autorità garanti della privacy di 26 Paesi per il "Privacy Sweep 2016"*, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5443681.

Negli ultimi anni autorità nazionali ed europee hanno fornito raccomandazioni e linee guida per la configurazione delle app e l'implementazione di misure di gestione dei dati rispettose della normativa in materia.
Tra queste, il documento più recente è rappresentato dal Code of conduct on privacy for mobile health applications (il "Codice")[22], predisposto dalla Commissione europea con l'obiettivo di fornire indicazioni per gli sviluppatori di app mediche su come garantire la protezione dei dati personali, con particolare riguardo ai dati relativi alla salute.
La bozza di Codice è stata sottoposta all'esame dell'Article 29 Data Protection Working Party (WP29)[23] che, il 10 aprile 2017, ha comunicato le proprie osservazioni, nel complesso piuttosto negative[24].
Su un piano generale, infatti, il WP29 ha rilevato, da un lato, che il Codice non apporta un significativo valore aggiunto alla normativa esistente in quanto non vi sarebbero sufficienti spiegazioni ed esempi specifici dell'applicazione della normativa al settore della m-Health e, dall'altro, che il Codice non è totalmente allineamento alle previsioni del nuovo Regolamento Europeo sulla privacy.
Inoltre, il WP29 formula alcune critiche a specifici aspetti del Codice che dovranno debitamente essere riconsiderati dalla Commissione, tra cui:
- definizione di dati relativi alla salute: la bozza di Codice chiarisce che dati sensibili relativi alla salute non sono solo quelli che forniscono in via immediata un'informazione di carattere sanitario ma anche dati di natura diversa che, in combinazione con altre informazioni o in considerazione delle modalità e/o finalità concrete del trattamento, possono "diventare" dati sensibili (ad esempio una app che registra i passi o i battiti cardiaci non tratta dati relativi alla salute; se però tali dati sono utilizzati per misurare o predire un rischio per la salute o per consentire un follow-up medico, allora la app tratterà dati sensibili relativi alla salute). Tuttavia il Codice richiede che via sia un "clear and close link" o che i dati siano "inherently related" alla descrizione dello stato di salute di una persona, con l'effetto di limitare la tutela prevista per i c.d. "lifestyle data" che non sarebbero "inherently related" alla salute di una persona;
- poca chiarezza sul ruolo dello sviluppatore del software come

---

[22] COMMISSIONE EUROPEA, *Code of conduct on privacy for mobile health applications*, in https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised.

[23] Article 29 Data Protection Working Party, *Letter of the Chair of the Art.29 WP 10th April 2017*, in ec.europa.eu/newsroom/document.cfm?doc_id=44371.

[24] L. LIGUORI, E. STEFANINI, *M-Health e Privacy: parere negativo dei garanti europei sulla bozza di "Code of conduct on privacy for mobile health applications"*, in http://www.portolano.it/pcc_newsletters/m-health-e-privacy-parere-negativo-dei-garanti-europei-sulla-bozza-di-code-of-conduct-on-privacy-for-mobile-health-applications/.

titolare o responsabile del trattamento e sulla relativa informazione agli utenti;
- mancata considerazione di altre normative che hanno un impatto sulla protezione dei dati personali, come quella sui cookies;
- carenza di informazioni su come gli interessati possano esercitare i propri diritti, con particolare riguardo alle conseguenze della revoca del consenso, etc.

Su un punto, inoltre, il WP29 è particolarmente rigoroso: il trattamento dei dati da parte di terzi per fini di marketing.

Infatti, in base alla bozza di Codice:

(i) è consentita l'effettuazione di pubblicità nell'ambito di una app da parte dello stesso sviluppatore o di un terzo, a condizione che sia garantito: (a) l'opt-out dell'utente, se chi effettua la pubblicità non riceve alcun dato personale dell'utente e la pubblicità è strettamente connessa alla funzionalità e al contesto della app stessa; oppure (b) l'opt-in dell'utente, da acquisire in modo separato e specifico, se le condizioni precedenti non sono verificate; e ***(ii)*** è consentito rendere l'accettazione della pubblicità una condizione per l'utilizzo dell'app (ad esempio facendo sì che l'esercizio dell'opt-out comporti la rimozione dell'app).

Secondo il WP29, la previsione del Codice che consente di subordinare l'utilizzo dell'app da parte dell'utente all'accettazione della pubblicità non è conforme al regolamento sulla privacy in quanto mina il requisito della "libertà" del consenso. Inoltre, il WP29 chiarisce che non è sufficiente informare l'interessato se i suoi dati vengono comunicati e trattati da terzi, ma occorre acquisirne il consenso espresso (opt-in).

Le molte osservazioni ricevute dal WP29 richiederanno un significativo lavoro di ripensamento e approfondimento da parte della Commissione che ritarderà l'adozione definitiva del Codice.

Tuttavia, le indicazioni fornite in questa occasione dall'WP29 rappresentano, già da oggi, un utile ausilio per gli operatori del settore al fine di progettare health apps conformi alla normativa sulla protezione dei dati personali.

Risulta infatti strategico oltre che espressamente richiesto dal regolamento europeo sulla Privacy considerare le esigenze di protezione dei dati personali degli utenti già al momento della progettazione dell'applicazione, realizzando app in cui siano predeterminate le modalità e i limiti del trattamento dei dati personali ed incluse misure di protezione e minimizzazione del trattamento richieste dal regolamento stesso.

Il design del software, inoltre, può essere un aspetto decisivo per determinare se ed in quale misura una app sia soggetta alla normativa privacy (c.d. "privacy by design").

8. Considerazioni finali.

Alla fine di questa disamina sul dato sanitario, emerge, in primo luogo, che la sua definizione è ricavabile non solo dalle fonti normative e dalla giurisprudenza ma, soprattutto, dalla "dinamicità" del dato sanitario stesso intesa come l'atteggiarsi nelle realtà che lo interessano. Non è un caso, quindi, che i legislatori si sono preoccupati principalmente di definire, piuttosto, i caratteri della sua tutela; necessità – quest'ultima – diventata ancora più stringente se si pensa che dalla sua circolazione e dalle nuove forme di trattamento – sviluppatesi grazie alle nuove tecnologie – che lo riguardano derivano indubbi vantaggi per le persone interessate.
Alla luce di ciò, appare più che ragionevole che le normative di riferimento possano prevedere per i soggetti che trattano i dati sanitari delle ricadute pratiche gravose e più stringenti che in passato: il banco di prova sarà rappresentato dalle misure di garanzia che il Garante emanerà ai sensi del nuovo art. 2-septies del Codice Privacy.