ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

LA DIGITALIZZAZIONE DEI SERVIZI SANITARI, IL DIRITTO ALLA SALUTE E LA TUTELA DEI DATI PERSONALI
12 FEBBRAIO 2021

Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità

di Fabrizia Covino
Professore associato di Istituzioni di diritto pubblico
Sapienza - Università di Roma

Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*

di Fabrizia Covino
Professore associato di Istituzioni di diritto pubblico
Sapienza - Università di Roma

Abstract [It]: L'attuale situazione pandemica accentua l'utilizzo degli strumenti digitali in ambito sanitario. L'impatto delle innovazioni interessano sia il quadro normativo europeo, con l'introduzione di principi comuni e di uno standard europeo finalizzato allo scambio delle Cartelle cliniche elettroniche, sia quello nazionale. La natura delle innovazioni che investe direttamente la tutela della salute, pone problemi nuovi anche in relazione alla tutela dei dati personali. La sinergia tra normativa dell'Unione europea e nazionale fornisce un quadro di riferimento efficace per la tutela dei dati personali anche nel contesto dell'innovazione digitale.

Abstract [En]: The current pandemic crisis is emphasizing the use of digital tools also in the health sector. The impact of such innovations influences both the EU regulatory framework with the introduction of a European format on the exchange of electronic health records, and the national one. The core characteristics of these innovations, which directly affect health protection, create new problems related to privacy and personal data protection. An analysis of the EU regulations and of the national implementation provides an effective reference framework for the protection of personal data also in the context of digital innovation.

Parole chiave: Strumenti digitali; ambito sanitario; scambio di cartelle cliniche elettroniche; dati personali; innovazione digitale
Keywords: Digital tools; helth sector; exchang of eletronic health records; personal data protection; digital innovation

1. Uso della tecnologia, emergenza sanitaria e tutela dei diritti fondamentali: delimitazione del campo di indagine

Il contrasto alla pandemia da Covid-19 ha determinato da parte del legislatore la necessità di effettuare alcuni bilanciamenti, anche dolorosi, tra i diritti fondamentali sanciti dalla Carta costituzionale[1]. Non è

* Articolo sottoposto a referaggio.

[1] Sulla necessità che i bilanciamenti, da cui è scaturita la compressione di alcune libertà, possano essere realizzati "solo di fronte a beni supremi, come la salute pubblica", attraverso gli strumenti previsti dalla Costituzione e mantenendo viva la centralità del Parlamento, al fine di evitare che la pandemia ci lasci "in eredità una democrazia moribonda", cfr., tra gli altri, M. CALAMO SPECCHIA, *Principio di legalità e stato di necessità al tempo del "COVID-19"*, in *Osservatorio Aic*, n. 3/2020, p. 167 ss. Sulla necessità di realizzare "la piena riespansione di tutte le libertà", non appena "migliorata" la situazione emergenziale, cfr. G. AZZARITI, *I limiti costituzionali della situazione d'emergenza provocata dal Covid-19*, in *Questione giustizia*,

possibile in questa sede soffermare l'attenzione sulla molteplicità di atti normativi posti in essere per fronteggiare l'epidemia, nonché sulla pervasività degli atti amministrativi che hanno messo in discussione il principio di legalità e della riserva di legge (riverberandosi sul sistema delle fonti)[2]. E tuttavia alcuni elementi devono essere richiamati per delimitare il quadro di riferimento della presente analisi.

In primo luogo, l'emergenza sanitaria ha generato restrizioni alla libertà di circolazione, ritenute dal legislatore stesso compatibili con il quadro costituzionale, in quanto adottate per "motivi di sanità e di sicurezza", secondo quanto previsto dall'art. 16 Cost.[3]. La compressione della libertà di circolazione è stata finalizzata a garantire in effetti *l'ulteriore* diritto *fondamentale*, quello alla salute, declinato nella sua dimensione individuale e collettiva dall'art. 32 Cost.[4].

In secondo luogo, emerge come sebbene la lotta globale alla pandemia sia affrontata secondo modalità diverse nei vari ordinamenti[5], il dato comune è costituito dal massiccio incremento della tecnologia per proteggere la salute. Detto incremento si è determinato nel nostro ordinamento ricorrendo ad una pluralità di misure, tra cui figurano *in primis* le applicazioni digitali già impiegate in quei contesti dove

27 marzo, 2020. Sull'esistenza di solide basi di garanzia fornite dalla Carta costituzionale nella fase di emergenza si sofferma M. BIGNAMI, *Chiacchiericcio sulle libertà costituzionali al tempo del coronavirus*, in *Questione giustizia*, aprile 2020.

[2] Critico nei confronti del "profluvio" di d.p.c.m. per far fronte all'emergenza sanitaria G. SILVESTRI, *Covid-19 e Costituzione*, in *Unicost.eu*, che evidenzia come nell'attuale fase siano state "sospese" oltre alla rappresentanza parlamentare, anche la collegialità del Governo, "entrambe sostituite dalla comunicazione diretta tra vertice dell'Esecutivo e cittadini". L'incidenza sul sistema delle fonti da parte dei provvedimenti volti a contrastare, con particolare riferimento agli strumenti normativi utilizzati, è sottolineata, tra gli altri, da L. MAZZAROLLI, *"Riserva di legge" e "principio di legalità" in tempo di emergenza nazionale. Di un parlamentarismo che non regge e cede il passo a una sorta di presidenzialismo extra ordinem, con ovvio, conseguente strapotere delle pp.aa. La reiterata e prolungata violazione degli artt. 16, 70 ss., 77 Cost., per tacer d'altri*, in *Federalismi*, *Osservatorio emergenza Covid-19,* n. 1/2020.

[3] Sulla compressione di numerose libertà, da quella religiosa, alla libertà di iniziativa economica privata, per focalizzarsi poi sui provvedimenti restrittivi della libertà di circolazione cfr. MAZZAROLLI, *"Riserva di legge" e "principio di legalità" in tempo di emergenza nazionale*, cit., p. 2 ss.; L. CUOCOLO, *I diritti costituzionali di fronte all'emergenza Covid-19: la reazione italiana*, in ID. (a cura di), *I diritti costituzionali di fronte all'emergenza Covid-19. Una prospettiva comparata*, in *Osservatorio Emergenza Covid-19*, in *Federalismi*, n. 1/2020, p. 13 ss. Ritiene, invece, che i provvedimenti adottati per contrastare l'emergenza siano fondati non sullo stato di necessità, ma sulla Costituzione stessa, dal momento che sebbene "i Costituenti abbiano consapevolmente deciso di non normare esplicitamente lo stato di emergenza", la sua "positivizzazione" si rinviene in significative disposizioni: "nella previsione dell'indivisibilità (art. 5) e dell'unità (art. 87) della Repubblica, ma anche in quella dell'intangibilità dei princìpi supremi del vigente ordine costituzionale, quali argini alla negoziazione pattizia, alla revisione costituzionale, al diritto sovranazionale e al diritto internazionale (artt. 7, 10, 11 e 139)", M. LUCIANI, *Liber Amicorum per Pasquale Costanzo. Il sistema delle fonti del diritto alla prova dell'emergenza*, in *Consulta on-line*, aprile 2020, spec. p. 4. Adesivamente, E. GROSSO, *Legalità ed effettività negli spazi e nei tempi del diritto costituzionale dell'emergenza. È proprio vero che "nulla potrà più essere come prima"?*, in *Federalismi*, n. 16/2020, il quale ritiene che l'emergenza svela "il volto più "sincero" e vero della democrazia costituzionale", la quale, "essendo un sistema intrinsecamente fragile nella sua pretesa di controllare il potere attraverso la sua sottoposizione al diritto", scommette sulla capacità di quel sistema "di non andare in pezzi nel momento in cui l'emergenza lo mette alla prova". Ossia di non rompersi quando è costretto – nel senso letterale di oggettivamente forzato – a flessibilizzarsi, a rendersi "adattivo", *ibidem*, p. 5.

[4] Sulla complessità del diritto alla salute e sulle sue diverse declinazioni cfr. D. MORANA, *La salute come diritto costituzionale,* Giappichelli, Torino, 2018, 3^ ed., spec. p. 22 ss.; A SIMONCINI, E. LONGO, *Art. 32*, in R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, I, Utet, Torino, 2006, p. 655 ss.; B. CARAVITA, *La disciplina costituzionale della salute*, in *Dir. soc.*, 1984, p. 53 ss.

[5] Sull'impatto dell'emergenza sanitaria sugli ordinamenti costituzionali del diritto comparato, cfr. L. CUOCOLO (a cura di), *I diritti costituzionali di fronte all'emergenza Covid-19. Una prospettiva comparata*, cit., p. 1 ss.

maggiore è risultato il contagio come la Cina, la Polonia o Taiwan[6], al fine di realizzare il tracciamento delle persone, conservando i dati acquisiti sullo stato di salute in archivi digitali gestiti dallo Stato[7].

Accanto alle descritte misure di carattere straordinario, l'ordinamento ha potenziato gli strumenti della c.d. "sanità digitale" già esistenti a livello normativo. Si tratta di dispositivi quali il Fascicolo sanitario elettronico, le Cartelle cliniche elettroniche, ma anche la Tessera sanitaria e la Ricetta medica dematerializzata, che vengono ulteriormente valorizzati dal legislatore nel presente contesto congiunturale[8].

L'interconnessione tra vecchi e nuovi strumenti digitali consente la circolazione di informazioni di carattere sanitario, anche al fine di contenere e scongiurare ulteriori epidemie di portata globale come quella attuale. Si registra come l'impiego di dette risorse richieda al contempo un ulteriore bilanciamento tra i diritti fondamentali in gioco: rispettivamente il diritto alla salute collettiva e quello alla protezione dei dati personali dell'individuo.

Sebbene in periodi di crisi socio-sanitaria come quello attuale, ogni bilanciamento tra la protezione del diritto alla vita e il diritto inviolabile alla tutela dei dati personali diviene "ineguale", in quanto quest'ultimo diritto diviene recessivo davanti al superiore bene che è la *vita* stessa, messa in discussione dall'emergenza[9], il potenziale utilizzo dei dati personali su larga scala pone un tema di diritto costituzionale, determinando una potenziale ingerenza nella *qualità* della vita del soggetto stesso. In questo scenario in effetti il tema della protezione dei dati personali acquisisce una valenza ulteriore perché considerato all'interno del più ampio dibattito relativo al rapporto tra diritto e tecnica, in cui una delle prospettive prefigurate è la ricerca

[6] Si soffermano sull'impiego di alcuni di questi strumenti, G. BISCONTINI, M.E. COMBA, E. DEL PRATO, L. A. MAZZAROLLI, A. POGGI, G. VALDITARA, F. VARI, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *Osservatorio Emergenza Covid-19, Federalismi*, 2020, p. 1 ss., i quali palesano l'impatto che l'uso della tecnologia in ambito sanitario ha sulle istituzioni democratiche.

[7] Cfr. il decreto-legge 30 aprile 2020, n. 28, recante "Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19". Sul punto si rileva come, a fronte di un iniziale clamore e forti perplessità da parte della dottrina legate agli effetti sulle libertà fondamentali della potenziale geo-localizzazione delle persone, detta misura, progettata per essere utilizzata su base volontaria, è stata impiegata da un'esigua percentuale della popolazione senza sortire i risultati sperati. Evidenziano la compatibilità di detta applicazione sulla normativa a protezione dei dati personali C. COLAPIETRO, A. IANNUZZI, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in Diritti fondamentali, 2/2020, anche per l'ulteriore bibliografia.

[8] L'ulteriore impiego della tecnologia in Sanità, emerge anche dalle disposizioni del c.d. "decreto rilancio" (d.l. n. 34 del 2020), su cui v. *infra* par. 2 ss.

[9] Il presupposto è quello di salvaguardare il diritto alla vita, il quale gode di una "posizione privilegiata" nell'ordinamento costituzionale, come ha più volte messo in luce il giudice delle leggi . Sul tema del bilanciamento "ineguale" (riferito però ai diritti sociali e al costo per erogarli), M. LUCIANI, *Sui diritti sociali*, in *Scritti in onore di Manlio Mazziotti di Celso*, Cedam, Padova, II, p. 126 ss.

delle modalità da parte dell'ordinamento di forme di tutela dall'ingerenza eccessiva delle applicazioni della tecnologia nella sfera soggettiva[10].

Simile interconnessione di mezzi tecnologici e di dati si pone al crocevia di due situazioni giuridiche parimenti rilevanti. Se da un canto concretizza il diritto all'uso della tecnologia, quale forma della libertà personale nata dalla civiltà *post*-industriale, conosciuta come "libertà informatica"[11], dall'altro, pone il problema della circolazione di una mole enorme di dati definiti "supersensibili", come quelli idonei a rivelare lo stato di salute delle persone, chiamando in causa il sistema di garanzie a protezione di essi[12].

Obiettivo della presente analisi è l'indagine della disciplina degli strumenti di tutela dei dati personali relativi alla salute contenuti negli archivi elettronici, al fine di valutarne la portata garantistica[13]. L'osservatorio prescelto è costituito dal trattamento dei dati relativi alla salute all'interno del Fascicolo sanitario elettronico e del sistema di Cartelle cliniche elettroniche. Anticipando quanto si dirà nel prosieguo, l'analisi di questi specifici ambiti è dovuta alla circostanza per cui, al ricorrere di dati eventi - specificamente al fine di contenere le epidemie - la conservazione dei dati ivi contenuti può avere durata illimitata. Da ciò discende la possibilità di rivelare lo stato di salute del soggetto lungo tutto l'arco della vita.

L'analisi verterà dunque sulle garanzie messe a punto dalla normativa europea e le ricadute sull'ordinamento nazionale a salvaguardia dei dati ivi contenuti. Quello che si cercherà di mettere in luce è che l'attuale assetto normativo in tema di protezione dei dati relativi alla salute - esteso alla "sanità digitale" - elaborato nel contesto europeo e recepito nell'ordinamento nazionale, fonda un base giuridica in grado di tutelare adeguatamente le posizioni giuridiche soggettive anche in fasi di emergenza qual è quella attuale.

---

[10] Per i termini di questo dibattito cfr. P. COSTANZO, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, relazione al Convegno AIC del 2012, su *Costituzionalismo e globalizzazione*, Jovene, Napoli, 2014, il quale riflette sulla fisionomia del costituzionalismo di oggi e del suo rapporto con "una tecnologia di dimensioni globali", *ibidem* p. 43 ss.

[11] Su cui cfr. V. FROSINI, *L'orizzonte giuridico dell'internet*, in *Dir. inf. Inf.*, n. 2/2000, "non libertà da, ma libertà di, che è quella di valersi degli strumenti informatici per fornire ed ottenere informazioni di ogni genere", p. 275. Detta libertà informatica trova un fondamento anche nel corrispondente diritto sociale, come evidenzia P. COSTANZO, *Internet (dir. pubbl.)*, in *Dig. disc. pubbl.*, Appendice, Torino, UTET, 2000, p. 347 ss., ma v. anche L. CARLASSARE (a cura di), *La comunicazione del futuro e i diritti della persona*, Padova, Cedam, 2000.

[12] Secondo la Corte di Cassazione i dati riguardanti la salute sono dati "supersensibili" in quanto involgenti la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate. Come tali, essi beneficiano di una protezione rafforzata (*ex multis* Cass. civ., sez. VI, sent. dell'11 gennaio 2016, n. 222).

[13] G. BISCONTINI, M.E. COMBA, E. DEL PRATO, L. A. MAZZAROLLI, A. POGGI, G. VALDITARA, F. VARI, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *Osservatorio Emergenza Covid-19*, *Federalismi*, 2020, p. 2 ss., sottolineano come sul terreno giuridico ma non solo, si "paventa l'utilizzo di tali strumenti nel timore che la loro introduzione in situazione di emergenza possa poi inevitabilmente traslarsi anche in situazioni che non rivestano tale eccezionalità", il che induce a riflettere come "anche questa emergenza, come ogni emergenza, pone interrogativi di fondo sulle deroghe alle regole ordinarie di funzionamento del sistema democratico, sulla loro misura e inevitabilità, sulla loro forza di mutamento, sugli equilibri costituzionali, istituzionali, amministrativi e costringe a riflettere sull'equilibrio tra diritti individuali e bisogni collettivi, in termini fino ad ora inusuali", *ibidem*.

2. Gli strumenti della "sanità digitale"

Come si è anticipato, l'attuale fase di emergenza sanitaria ha indotto il Governo italiano a potenziare gli strumenti della "sanità digitale", al fine di consentire la circolazione efficace ed efficiente delle informazioni contenute nella documentazione elettronica. La tecnologia applicata alla salute ha finora percorso un veloce sviluppo, come mostrano gli strumenti esistenti, tra i quali emergono il Fascicolo sanitario elettronico (d'ara in avanti FSE), il *Dossier* sanitario, la refertazione *on-line*, l'ampio ricorso alla "Ricetta medica dematerializzata" e il sistema delle Cartelle cliniche elettroniche (CCE). Allo stesso tempo il loro impiego pone alcune criticità, come si vedrà nel prosieguo.

Tra gli strumenti su cui si è concentrata la normativa governativa nell'attuale fase di emergenza e su cui è opportuno focalizzare l'attenzione, figurano le innovazioni relative al FSE e alle CCE, quali strumenti valorizzati anche da parte dell'ordinamento sovranazionale[14].

Volendo dare una breve definizione di detti strumenti, il FSE è "l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito", secondo quanto indicato dal decreto-legge n. 179 del 2012, che lo ha istituito[15]. Il FSE permette la condivisione delle informazioni tra gli operatori della sanità con cui il soggetto viene a contatto, ai fini del coordinamento delle cure anche nel contesto interregionale, in un'ottica di maggior efficienza nell'erogazione dei servizi e di risparmio delle risorse. Secondo quanto indicato dal d.p.c.m. del 29 settembre 2015, n. 178[16], il FSE persegue tre finalità: di cura (prevenzione, diagnosi, cura e riabilitazione); di ricerca (studio e ricerca scientifica in campo medico, biomedico ed epidemiologico); di governo (programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria). Ha, inoltre, un contenuto obbligatorio e uno facoltativo, comprensivo anche dalle CCE[17]. L'infrastruttura per garantire l'interoperabilità dei FSE è prevista con decreto del ministro dell'economia e delle finanze del

[14] Al fine di garantire la circolazione dei dati in materia sanitaria ivi contenuti, come indicato dal'art. 14, rubricato "Assistenza sanitaria *on line*" della Direttiva 2011/24/UE del Parlamento Europeo e del Consiglio del 9 marzo 2011 concernente l'assistenza sanitaria transfrontaliera. V. *infra* par. 2.1.

[15] Come convertito in legge, 17 dicembre 2012, n. 221 e succ. modif. Il FSE ha preso le mosse nel 2008, attraverso la creazione di un tavolo interistituzionale presso il Ministero della salute e dalle successive Linee guida nazionali sul FSE, oggetto di Intesa Stato-Regioni, del 10 febbraio 2011.

[16] Recante "*Regolamento in materia di fascicolo sanitario elettronico*".

[17] Ai sensi dell'art. 2, commi 2 e 3, del d.p.c.m. n. 178, i documenti obbligatori fanno parte del c.d. "nucleo minimo"; quelli facoltativi servono ad arricchire il FSE dipendono dalle scelte compiute dalle strutture sanitarie sulla base delle indicazioni elaborate a livello regionale e dallo sviluppo digitale delle singole realtà ospedaliere. Il "nucleo minimo" del FSE comprende: i dati identificativi e amministrativi dell'assistito; i referti; i verbali pronto soccorso; le lettere di dimissione; il profilo sanitario sintetico; il dossier farmaceutico; il consenso o diniego alla donazione degli organi e tessuti. Tra i documenti facoltativi rientrano anche le Cartelle cliniche. Cfr. *Fascicolosanitario.gov.it*.

4 agosto 2017, e successive modificazioni; detto strumento mira a garantire all'assistito continuità nell'accesso *on-line* al proprio FSE "anche nei casi di trasferimenti di assistenza" infraregionale[18].

Il richiamato decreto "rilancio", n. 34 del 2020, innova il dato normativo estendendo la definizione di FSE a tutti i documenti digitali sanitari e socio-sanitari, riferiti alle prestazioni sia a carico del SSN che fuori di esso. L'obiettivo del legislatore è di potenziare l'efficacia del FSE ampliando la tipologia di informazioni trattate. In conseguenza di questo sviluppo si amplia altresì la categoria degli "esercenti le professioni sanitarie", quali soggetti abilitati a perseguire le finalità di cura (art. 12, comma 2, lett. *a*).

È inoltre prevista, con l'introduzione dell'art. 12, comma 15-*nonies*, del d.l. n. 179/2012, l'alimentazione del FSE con i dati già disponibili della donazione degli organi, vaccinazioni e prenotazioni. Il "decreto rilancio" incide anche sulla protezione dei dati personali ivi contenuti, semplificando la disciplina del consenso (*infra* par. 6).

Lo sviluppo normativo ha condotto ad integrare i dati contenuti nel FSE, non solo con i dati provenienti dai referti *on-line*[19], ma anche con quelli provenienti dalla Tessera sanitaria elettronica[20]. Sul punto, il richiamato decreto n. 34 prevede il potenziamento (art. 12, comma 15-*septies*, del d.l. n. 179) del flusso di informazioni provenienti dalla Tessera Sanitaria relativo alle prestazioni pagate del cittadino e i pagamenti elettronici delle spese sanitarie, reperite anche attraverso la fatturazione elettronica[21]. L'interconnessione dei documenti elettronici dovuti allo sviluppo della tecnologia nell'attuale fase di emergenza sanitaria è evidente anche nell'implementazione della c.d. "Ricetta medica dematerializzata" per le prescrizioni dei farmaci a carico del Servizio Sanitario Nazionale, dal momento che sono state estese le tipologie di ricette assoggettate a detta dematerializzazione[22].

[18] Cfr. il decreto 25 ottobre 2018 recante "*Modifica del decreto ministeriale 4 agosto 2017, concernente le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)*".

[19] Sul punto cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 6 dicembre 2012* e il d.p.c.m. dell'8 agosto 2013.

[20] Cfr. la legge n. 232/2016, che modifica l'art. 12 del d.l. n. 179/2012.

[21] Lo sviluppo normativo che caratterizza il FSE, coinvolge in parte anche il *Dossier* sanitario che raccoglie le informazioni "relative agli eventi clinici occorsi all´interessato esclusivamente presso un´unica struttura sanitaria". Detto documento si differenzia dal FSE per la circostanza che le informazioni accessibili sono generate "da un solo titolare del trattamento e non da più strutture sanitarie in qualità di autonomi titolari, come avviene proprio per il Fse" . Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento recante "*Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario"* del 2009.

[22] La Ricetta dematerializzata è stata originariamente introdotta con decreto del Ministero dell'Economia e delle Finanze del 2 novembre 2011, poi modificato dal decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 25 marzo 2020, recante "*Estensione della dematerializzazione delle ricette e dei piani terapeutici e modalità alternative al promemoria cartaceo della ricetta elettronica"*. Il d.m. ha formato oggetto del *Parere sulle modalità di consegna della ricetta medica elettronica*, adottato dal Garante per la protezione dei dati personali, il 19 marzo 2020.

2.1. segue: Il particolare ambito delle Cartelle cliniche elettroniche

Le prescrizioni introdotte sul FSE hanno un impatto anche sui sistemi di Cartelle cliniche elettroniche che, come si è evidenziato, possono costituirne parte integrante[23].

Il tema delle CCE nell'ordinamento italiano prende le mosse da un assunto di fondo, dato dall'essere dette Cartelle un atto pubblico, ai sensi dell'art. 2699 del Codice civile. Come tali, esse sono soggette ad un obbligo di conservazione illimitato nel tempo, secondo quanto previsto dalle circolari del Ministero della Sanità[24].

Nel nostro ordinamento, il passaggio e la preminenza della gestione elettronica rispetto a quella tradizionale nell'impiego delle Cartelle, è stabilita dall'art. 47-*bis*, 1 co., del d.l. 9 febbraio 2012, n. 5[25]. La disposizione prevede la conservazione, anche soltanto digitale, delle cartelle cliniche, determinando un decisivo passo in avanti nel processo di migrazione dei servizi sanitari per una gestione (prevalentemente o interamente) informatica.

Sul piano definitorio, già nel 1992 il Ministero della Sanità indicava la Cartella clinica quale "insieme di documenti che registrano un complesso eterogeneo di informazioni sanitarie, anagrafiche, sociali, aventi lo scopo di rilevare il percorso diagnostico-terapeutico di un paziente al fine di predisporre gli opportuni interventi sanitari e di poter effettuare indagini statistiche, scientifiche e medico-legali. È uno strumento informativo individuale finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente"[26]. Da questa definizione traspare una pluralità di finalità, non soltanto di cura, ma anche di ricerca scientifica e statistica. Emerge inoltre la tendenza a non limitare la Cartella clinica alla sola raccolta delle informazioni relative ad un singolo episodio clinico, dal momento del ricovero a quello della dimissione, con individuazione esatta del paziente, indicazione del motivo del ricovero, accertamenti diagnostici e specialistici, referti, terapie, ma di raccogliere, in senso più ampio, il complesso delle informazioni sanitarie disponibili in una struttura, riferite anche a più episodi clinici di un determinato paziente, tendenza quest'ultima favorita dal ricorso alle tecnologie informatiche. L'evoluzione della

[23] Cfr. l'art. 2, comma 3, del d.p.c.m. n. 178 del 2015.

[24] L'allora Ministero della Sanità ha stabilito che le cartelle cliniche siano conservate illimitatamente, perché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto: cfr. la Circolare n. 900 del 19 dicembre 1986. La Corte di Cassazione Penale, ss.uu., con sentenza 11 luglio 1992 n. 7958, ha precisato che quando il medico redige la cartella clinica opera in qualità di pubblico ufficiale. L'art. 7 del D.P.R. n. 128/1969 stabilisce la responsabilità della tenuta e conservazione della cartella clinica per tutta la durata del ricovero, nonché gli obblighi di conservazione della cartella da parte dell'archivio centrale della Struttura sanitaria che deve conservarla in luoghi appropriati, non soggetti ad alterazioni climatiche e non accessibili da estranei.

[25] Convertito con modificazioni dalla l. 4 aprile 2012, n. 35 e succ. modif.

[26] Cfr. MINISTERO DELLA SALUTE, *Sicurezza dei pazienti e gestione del rischio clinico - Manuale per la formazione dei Medici di Medicina Generale e dei Pediatri di Famiglia*, 2010, p. 24, reperibile sul sito istituzionale del ministero.

Cartella clinica, in altre parole, è sin dalle origini orientata a costituire un Fascicolo sanitario che registri la storia di un determinato paziente all'interno della struttura ospedaliera.

L'avvento della tecnologia recupera la prospettiva di utilizzare una pluralità di strumenti (il c.d. *electronic medical record* o *electronic patient record*), le cui definizioni assumono confini evanescenti. Non si rinvengono, inoltre, criteri univoci né ufficiali sulle modalità di strutturazione e compilazione della Cartella clinica, con la conseguente adozione di atti che differiscono notevolmente tra ospedali o tra diverse unità operative della stessa struttura sanitaria, da cui deriva il recente sforzo verso una standardizzazione[27].

A livello sovranazionale, infatti, si tenta un approccio paneuropeo all'impiego di tali strumenti elettronici, con il duplice intento di elevare gli *standard* di tutela della salute in termini di efficienza ed efficacia nel rispetto delle prerogative degli Stati membri, ma anche al fine di garantire la libertà di circolazione delle informazioni relative alla salute all'interno dell'Unione, in un'ottica di efficienza economica. Questo assunto è particolarmente evidente con riferimento alla necessità di definire un formato europeo di cartelle cliniche elettroniche al fine di scambiare i dati in esse contenuti, su cui si è recentemente focalizzata l'attenzione delle istituzioni europee.

Sin dalla Raccomandazione del 2 luglio 2008, sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche (punto 3, lett. *c*), queste sono definite come la "documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente di un individuo in forma elettronica, che consenta la pronta disponibilità di tali dati per cure mediche e altri fini strettamente collegati". Si tratta della versione elettronica della precedente cartella sanitaria che può includere dati clinici (anamnesi, problemi e patologie), farmaci e trattamenti, nonché risultati e relazioni di esami e laboratorio[28]. Tali documenti elettronici, che possono contenere interi fascicoli oppure semplici estratti o riassunti, sono accessibili al medico di medicina generale, al farmacista e ad altri operatori sanitari[29].

La recente Raccomandazione della Commissione del 6 febbraio 2019, n. UE/2019/243, relativa a un formato europeo di scambio delle cartelle cliniche elettroniche, evidenzia che i sistemi di CCE possono assicurare maggiore qualità e accuratezza dell'informazione medica rispetto agli strumenti tradizionali,

---

[27] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida sul FSE,* provvedimento del 19/7/2009, n. 25 (reperibile sul sito istituzionale), in cui viene distinto il *Dossier* sanitario, inteso come complesso di dati sanitari relativi a un paziente trattati all'interno di un'unica struttura sanitaria dal Fascicolo sanitario elettronico, nel quale convergono *dossier* elaborati da diverse strutture sanitarie e dunque rispetto al quale il singolo *dossier* sanitario rappresenta semplicemente una fonte di popolamento dei dati. La questione definitoria risulta abbastanza ambigua poiché da un canto la Cartella clinica elettronica tende a convergere nel concetto di Fascicolo sanitario elettronico; ciò si evince anche dal punto di vista della disciplina adottata, poiché il Garante formula le stesse prescrizioni per entrambi gli strumenti sanitari, ossia tanto per i *dossier* quanto per il FSE. Nel provvedimento però si afferma esplicitamente che l'ambito delle CCE è escluso dal provvedimento in questione sul FSE, in quanto già disciplinato a livello normativo.

[28] BUTTARELLI *et al*., *Manuale*, cit., p. 378 ss.

[29] *Ibidem*.

garantendo efficienza in termini di appropriatezza delle cure mediche e risparmi in termini economici; consente altresì l'uniforme elaborazione tra i diversi sistemi di informazione sanitaria, migliorando la qualità della fornitura dell'assistenza transfrontaliera[30]. Si ipotizza, inoltre, che attraverso la digitalizzazione delle cartelle si potrebbero configurare dati aggregati dando vita a grandi strutture di dati riferiti alla salute, le quali attraverso nuove tecnologie (*Big Data* e "intelligenza artificiale") potrebbero indirizzare la ricerca verso nuove scoperte scientifiche. Non si escludono, infine, ripercussioni positive di natura economica, come la riduzione dell'attuale frammentarietà del mercato.

Il richiamo al mercato mostra come l'informatizzazione, volta a garantire maggiore efficienza nell'uso dei dati, debba essere affrontata in riferimento anche all'utilizzo dei dati stessi da parte del personale medico e delle modalità della loro acquisizione/divulgazione. Si rendono necessarie, pertanto, particolari garanzie al fine di evitare l'abuso nell'utilizzo di simili informazioni riservate.

3. La tutela dei dati personali (cenni e rinvio)

La configurazione di strumenti di protezione dei dati personali relativi alla salute, resa necessaria anche dalle crescenti applicazioni della tecnologia in ambito sanitario come si è anticipato, costituisce una specificazione del più ampio diritto inviolabile alla tutela dei dati personali di matrice anglosassone (*right to privacy*) o per meglio dire alla tutela della "vita privata" secondo l'evoluzione concettuale avvenuta negli ordinamenti democratici[31].

L'elaborazione di detto "nuovo diritto" nell'ordinamento italiano, discende dallo sviluppo "convergente" del diritto costituzionale, della giurisprudenza e del diritto europeo su appannaggio di quello internazionale[32]. Pur se sottoposto ad una continua tensione, dovuta all'esistenza di diverse culture costituzionali presenti nell'ordinamento dell'Unione europea, il diritto in questione in effetti trova un elemento unificante nella protezione della sfera della persona e della sua dignità così come riconosciuto nel contesto sovranazionale (*infra* par. 3.1)[33]. Si tratta di una sfera di protezione riconducibile alle tradizioni

[30] Si rinvia per tutti gli aspetti specifici in merito alla definizione di un formato europeo di CCE, al contributo di M. FERRARA nel lavoro che qui si pubblica.

[31] Per una disamina generale delle origini di tale diritto v. A. BALDASSARRE, *Privacy e costituzione: l'esperienza statunitense*, Bulzoni, Roma, 1974.

[32] Cfr. sul punto le riflessioni e la ricostruzione del percorso giurisprudenziale e normativo, anche in chiave comparatistica, di A. DI MARTINO, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017, spec. p. 125 e 288 ss.

[33] Sul fondamento costituzionale di detto diritto, riconducibile al binomio libertà-dignità, cfr. F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, p. 20 ss. e p. 107; G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA e P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, 2006, II, p. 617 ss. Sul nesso tra diritto alla riservatezza e dignità umana cfr. U. DE SIERVO, *Diritto all'informazione e tutela dei dati personali*, in *Foro it.* 1999.

costituzionali comuni degli Stati membri dell'Unione, che ha un importante riflesso nelle pronunce della Corte di Giustizia e in quelle della Corte Europea dei Diritti dell'uomo.

Nel contesto nazionale, detto diritto, sviluppatosi inizialmente sul piano civilistico come diritto del soggetto all'autodeterminazione nello svolgimento della personalità, trova il suo punto di riferimento costituzionale in alcuni principi fondamentali, tra cui quello di solidarietà e di eguaglianza, di cui agli artt. 2 e 3 Cost., oltre che in una pluralità di disposizioni della Carta fondamentale contenute negli artt. 14, 15, 21 e 32, e soprattutto nel riferimento all'inviolabilità della libertà personale proclamata nell'art. 13, primo comma, Cost.[34]. Il dogma della centralità della persona umana nella Costituzione, in effetti, viene valorizzato anche dalla giurisprudenza costituzionale, attraverso il diritto alla riservatezza, quale riverbero del diritto della personalità ed espressione della dignità umana, tutelato "in forma analoga in tutti gli ordinamenti giuridici delle nazioni più civili"[35].

3.1. segue: Il contesto normativo di riferimento

Per cogliere appieno lo sviluppo del diritto alla protezione dei dati personali relativi alla salute, oggetto precipuo della presente analisi, è necessario cogliere le principali tappe compiute dall'ordinamento sovranazionale e internazionale - nonché le ricadute su quello nazionale - attraverso cui si è determinato il progressivo ampliamento della tutela.

L'attuale quadro normativo relativo alla protezione dei dati personali relativi alla salute trova la sua più alta espressione nel Regolamento Generale sulla Protezione dei Dati Personali dell'Unione europea (*General Data Protection Regulation*, d'ora in avanti GDPR), n. 2016/679/UE, divenuto applicabile nel maggio 2018[36]. Esso abroga la precedente Direttiva n. 95/46/CE e ha ripercussioni sui sistemi di protezione dei dati elaborati a livello nazionale chiamati ad allinearsi alla nuova normativa direttamente

[34] Il diritto alla *privacy* non è sempre stato accolto con favore dalla dottrina proprio anche a causa del dibattito sulla latitudine costituzionale del principio di riservatezza. Sul punto cfr. A. CERRI, *Riservatezza*, III, in *Enc. Giur. Treccani*, Roma 1995, p. 1 ss. Per il quadro di riferimento e l'evoluzione giurisprudenziale, a partire da un'iniziale diffidenza per la definizione costituzionale di detto diritto alla riservatezza, il quale avrebbe rappresentato un limite alla libertà di manifestazione del pensiero sancita all'art. 21 Cost., cfr. DI MARTINO, *ibidem*, p. 166 ss.

[35] Così la sentenza della Corte costituzionale n. 139 del 1990. Sulla centralità della persona e della sua dignità nella Costituzione cfr. N. OCCHIOCUPO, *Liberazione e promozione umana nella Costituzione*, Giuffré, Milano, 1995. La valorizzazione del diritto alla riservatezza da parte del giudice delle leggi si realizza attraverso un dialogo ideale con la Corte di cassazione soprattutto a partire dagli anni Settanta del 1900: cfr. sul punto la sentenza n. 2129 del 1975 della Corte di Cassazione e la sentenza n. 122 del 1970 della Corte costituzionale. Nei successivi anni Novanta il giudice delle leggi identifica in maniera sistematica il diritto alla *privacy* "riconducibile all'intangibilità della sfera privata negli aspetti più significativi e […] legati alla vita intima della persona umana", a partire dalla sentenza n. 366 del 1991.

[36] Per una ricostruzione dell'evoluzione del diritto alla tutela dei dati personali nel contesto europeo cfr. l'analisi di F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, spec. p. 56 ss.

efficace, pur nel rispetto di una parziale discrezionalità degli Stati membri[37]. Nell'ordinamento nazionale, infatti, si sono rese necessarie alcune modifiche significative al c.d. "Codice della *privacy*" (d.lgs. n. 196 del 2003), da parte della normativa di adeguamento, costituita dal d.lgs. n. 101 del 2018 (*infra* par. 6)[38].

Il grado di pervasività del Regolamento del 2016 rispetto alla precedente disciplina è reso possibile dallo sviluppo del processo di integrazione europea nel corso dell'ultimo ventennio[39]. Volendo tratteggiare a ritroso il cammino che ha condotto ad un si alto grado di tutela dei dati personali, prima, e di quelli relativi alla salute, poi, è necessario mettere in luce come il percorso compiuto dal legislatore sovranazionale sia avvenuto su impulso della normativa di diritto internazionale, accompagnata da alcune elaborazioni giurisprudenziali intervenute nei singoli Stati membri.

La richiamata Direttiva del 1995, in effetti, nasce con l'obiettivo di conciliare due esigenze contrapposte: rimuovere gli ostacoli alla circolazione dei dati personali finalizzata alla piena realizzazione del mercato interno e la necessità di prevedere idonee garanzie per salvaguardare i diritti fondamentali della persona, collegati alla circolazione dei dati stessi. L'art. 8 della Direttiva, infatti, delinea una serie di garanzie in assenza delle quali il trattamento dei dati è inibito. Atteso il divario esistente tra le discipline esistenti negli Stati membri, il fine della normativa è l'armonizzazione delle legislazioni attraverso il principio del mutuo riconoscimento, stando al quale la legislazione in materia di tutela dei dati personali è quella dello Stato su cui sussiste lo stabilimento principale del titolare del trattamento dei dati.

La Direttiva n. 46 (andando ancora a ritroso) pone le sue fondamenta nella protezione dei dati personali così come elaborati dal diritto internazionale. Al fine di delineare il diritto alla riservatezza nel contesto europeo, la Convenzione europea dei diritti dell'uomo, approvata nel 1950, all'art. 8, in effetti, sancisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, e specifica le condizioni alle quali detto diritto può essere soggetto a restrizioni[40].

---

[37] Con riferimento al trattamento dei dati personali, esso è consentito in presenza di taluni requisiti specifici individuati all'art. 9 del Regolamento (cfr. considerando n. 51), il quale ha previsto la possibilità per gli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni (cfr. art. 9, par. 4). Questi margini di apprezzamento sono stati riempiti dalla normativa nazionale, che ha rimesso all'autorità garante il compito di individuare i presupposti di liceità dei trattamenti, di adottare specifiche misure di garanzia e di promuovere l'adozione di regole deontologiche (cfr. artt. 2-*septies* e 2-*quater* del Codice).

[38] Il d.lgs. n. 196 del 2003, recante "Codice in materia di protezione dei dati personali" aveva, a sua volta, abrogato la legge n. 675 del 1996, adottata in attuazione della Direttiva n. 46.

[39] Sviluppo che ha inciso significativamente sulla protezione di alcuni diritti fondamentali, come nell'ambito della tutela dei dati personali, mentre è rimasto più indietro nello sviluppo delle politiche di coesione e nella solidarietà, come messo in luce da L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in L. CALIFANO, C. COLAPIETRO, *Innovazione tecnologica e valore della persona*, in ID., CALIFANO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, p. 204.

[40] La Corte ha chiarito che l'art. 8 della CEDU non solo richiede agli Stati di astenersi da azioni che possano violare detto diritto previsto dalla Convenzione, ma impone, in talune circostanze, l'obbligo di garantire attivamente il rispetto della vita privata e familiare: cfr. Corte EDU, *I c. Finlandia*, 17 luglio 2008.

L'art. 8 CEDU rappresenta la base per radicare la tutela della riservatezza, specificando la tipologia di dati e i trattamenti inibiti di pari passo con il progredire della società dell'informazione; detto sviluppo si realizza a partire dal rafforzamento del principio di autonomia della persona attraverso il superamento graduale di una concezione "difensiva" della vita privata e di un'apertura della nozione al contesto relazionale e sociale dell'individuo[41]. La disposizione in esame costituisce altresì il fondamento di ulteriori atti normativi volti a contrastare possibili ingerenze dovute all'abuso della tecnologia. Su di esso si innesta, infatti, l'importante "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*", n. 108 del 1981, adottata dal Consiglio d'europa, che all'art. 6 individua "categorie speciali di dati" tra cui quelli sulla salute, vietandone il trattamento automatizzato, salvi i casi assoggettati a particolari garanzie da parte della legislazione nazionale[42].

La normativa contenuta nella Convenzione del 1981 si applica a tutti i trattamenti di dati personali effettuati nel settore privato e pubblico; sancisce altresì il diritto dell'individuo di venire a conoscenza della conservazione di informazioni che lo riguardano e la facoltà di chiederne la rettifica[43]. Le limitazioni ai diritti stabiliti nella Convenzione sono possibili *solo* ove siano in gioco interessi superiori (come la sicurezza o la difesa dello Stato). Inoltre, la libertà di circolazione dei dati personali tra gli Stati che hanno ratificato la Convenzione è regolamentata attraverso restrizioni sui flussi di dati verso i paesi in cui non sussiste una protezione giuridica equivalente dei dati stessi[44]. La Convenzione del 1981 rappresenta tuttora il quadro normativo di riferimento a livello internazionale per il trattamento dei dati automatizzati e per questa ragione è stata più volte modificata e integrata. Nel 2018, infatti, è stata "modernizzata"[45] e, nel riaffermare alcuni principi in essa contenuti, garantisce nuovi diritti a vantaggio degli individui, ampliando le responsabilità dei soggetti preposti al trattamento dei dati personali[46].

---

[41] Cfr. Corte EDU, *Niemitz c. Germania*, 16 dicembre 1992. Sul punto v. DI MARTINO, *Profili*, cit., p. 261 ss., anche per l'ulteriore giurisprudenza.

[42] Tra i dati il cui trattamento è vietato figurano anche quelli relativi alla razza, ad opinioni politiche, alla religione, all'orientamento sessuale e al casellario giudiziale di un soggetto.

[43] È stata ratificata da tutti gli Stati dell'Unione europea e, dal 1999, dalla stessa organizzazione sovranazionale.

[44] Per quanto concerne il trattamento dei dati personali, i principi stabiliti nella Convenzione riguardano la correttezza e la liceità della raccolta e del trattamento automatizzato dei dati, per specifici scopi legittimi. Ciò significa che i dati non devono essere destinati a un uso incompatibile con tali scopi, né conservati oltre il tempo necessario. Tali principi riguardano anche la qualità dei dati, in particolare in riferimento alla loro adeguatezza, pertinenza e non eccessività (proporzionalità) nonché esattezza". Cfr. C. GIAKOUMOPOULOS, G. BUTTARELLI, M. ÒFLAHERTY, *Manuale sul diritto europeo in materia di protezione dei dati*, Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, Lussemburgo, 2018, pp. 27-28.

[45] Il 18 maggio 2018, il Consiglio d'Europa ha adottato un protocollo di modifica del testo della Convenzione, al fine di "fornire un quadro giuridico più consono ad un'epoca nella quale le violazioni del diritto alla protezione dei dati sono divenute una importante preoccupazione". Il protocollo è stato ratificato dall'Italia il 5 marzo 2019.

[46] Cfr. GIAKOUMOPOULOS, BUTTARELLI, ÒFLAHERTY, *Manuale*, cit., p. 29, che mettono in luce come ad esempio, "le persone i cui dati vengono trattati hanno il diritto di venire a conoscenza del motivo di tale trattamento dei dati e il diritto di opporsi allo stesso. Per contrastare l'aumento dell'attività di profilazione nel mondo *online*, la Convenzione

Lo sviluppo del diritto internazionale finora tratteggiato, si compie di pari passo rispetto all'elaborazione giurisprudenziale del concetto di vita privata, questa volta colto nel contesto dell'evoluzione tecnologica e delle prospettive da questa aperte[47]. Si tratta del diritto alla "autodeterminazione informativa", quale diritto di accedere ai propri dati personali a prescindere dal luogo in cui questi siano conservati, che discende dal diritto fondamentale al rispetto della personalità protetto dalla Costituzione tedesca, secondo la definizione data dal Tribunale costituzionale tedesco nel 1983, recentemente valorizzato dalla Corte EDU[48].

Un ulteriore impulso nella configurazione del diritto alla protezione dei dati personali proviene dalla giurisprudenza della Corte di giustizia dell'Unione europea, la quale, nel ritenere compatibile con la Direttiva n. 95/46 l'innalzamento della protezione di detti dati da parte degli Stati membri, ha ritenuto cogenti le disposizioni a tutela dei dati personali in relazione ad ogni trattamento, senza dover riscontrare di volta in volta un nesso effettivo con la corrispondente libertà di circolazione prevista nei Trattati[49]. In questa prospettiva, il diritto alla protezione dei dati personali gradualmente acquisisce autonomia propria rispetto al diritto alla tutela della vita privata. Entrambi i diritti, infatti, mirano a proteggere l'autonomia e la dignità umana, delineando una sfera del soggetto all'interno della quale sviluppare liberamente la personalità; come tali costituiscono un presupposto essenziale per l'esercizio di altre libertà fondamentali, quali la libertà di espressione, la libertà di riunione pacifica e di associazione, la libertà di religione. Per altro verso però i due diritti differiscono: il diritto al rispetto della vita privata delinea un divieto generale di ingerenza, derogabile nei casi in cui entri in gioco l'interesse pubblico, mentre la protezione dei dati

sancisce altresì il diritto dell'individuo a non essere assoggettato a decisioni fondate esclusivamente su trattamenti automatizzati, senza che siano prese in considerazione le sue opinioni".

47 Un concetto di vita privata che, come si è visto in alto, supera la prospettiva della semplice non ingerenza nella propria sfera personale (*right to be let alone*) di matrice statunitense.

48 Il Tribunale costituzionale federale tedesco ha affermato il diritto di autodeterminazione informativa nella sentenza *Volkszählungsurteil*, del 1983. Nel 2017 la Corte EDU ha riconosciuto che l'art. 8 della CEDU "prevede il diritto ad una forma di autodeterminazione informativa" nella sentenza *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, 27 giugno 2017, punto 137: "*The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article […]. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged*". Cfr. l'analisi di GIAKOUMOPOULOS, BUTTARELLI, ÒFLAHERTY, *Manuale*, cit., p. 18 ss.

49 La decisione più significativa è data dalla sentenza 6 novembre 2003 C-101/01, *Bodil Lindqvist*. Nei punti da 40 a 42 la Corte riafferma, a proposito della Direttiva n. 95/46, che il ricorso ad essa non presuppone l'esistenza di un nesso effettivo con la libera circolazione tra Stati membri, tale da rendere necessario verificare, caso per caso, "se l'attività specifica in questione incida direttamente sulla libera circolazione tra gli Stati membri"; un'interpretazione in senso contrario renderebbe incerti e aleatori i limiti del campo di applicazione della detta direttiva, in contrasto con il suo obiettivo essenziale, che è quello di ravvicinare le disposizioni degli Stati membri per "eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali". Cfr. anche le sentenze 20 maggio 2003, C-465/00 *Rechnungshof*; 9 novembre 2010, C-92/09 e 93/09 *Volker und Markus Schecke e Hartmut Eifert*.

personali è vista come un diritto "moderno e attivo" che instaura un sistema di controlli tesi a proteggere la persona quando vengano trattati i suoi dati personali[50].

Simile evoluzione giurisprudenziale costituisce la base di riferimento per l'ulteriore sviluppo normativo rappresentato dalla previsione contenuta nella Carta dei diritti fondamentali dell'Unione europea, la quale, nel Titolo II dedicato ai diritti di libertà, subito dopo la protezione della vita privata e familiare (art. 7), disciplina la protezione dei dati personali (art. 8) delineando l'esistenza di un'apposita autorità di garanzia a tutela di detto diritto. La successiva incorporazione della Carta nei Trattati nel 2009, come è stato sottolineato, contribuisce ad "innalzare" il rango della disciplina già contenuta nella Direttiva del 1995[51], la quale si applica alle istituzioni dell'Unione e agli Stati membri sulla base dell'art. 51 CDFUE.

La prospettiva garantista esplicitata nell'art. 8 CDFUE è altresì valorizzata in altre parti del Trattato di Lisbona, e in particolare nell'art. 16 TFUE, che fissa espressamente la competenza dell'Unione in materia di protezione dei dati personali. È su questa specifica disposizione che è stato adottato il Regolamento del 2016, il quale costituisce una normativa "impositiva e uniformante" che sposta a livello sovranazionale il sistema delle garanzie relativo alla protezione dei dati personali[52].

4. Dai dati personali ai dati "idonei a rivelare lo stato di salute"

Il Regolamento n. 2016/679, in continuità con la direttiva del 1995 sul piano dei principi, modernizza la normativa europea in materia di tutela dei dati al fine di proteggere i diritti fondamentali davanti alle sfide economiche e sociali dell'era digitale[53]. Poiché molti modelli commerciali si fondano sul trattamento dei dati personali, la normativa europea e nazionale così come supportata dalla giurisprudenza della CGUE, mira a restringere l'utilizzo di detti dati a fini economici[54].

---

[50] Cfr. GIAKOUMOPOULOS, BUTTARELLI, ÒFLAHERTY, *Manuale sul diritto europeo in materia di protezione dei dati*, cit., p. 20 ss., i quali mettono in luce come la giurisprudenza abbia delineato due distinti diritti: il diritto "classico" alla tutela della vita privata e il diritto più "moderno" alla tutela dei dati. Cfr. CGUE, cause riunite C-92/09 e C-93/02, *Volker und Markus Schecke GbR c. Land Hessen*, conclusioni dell'avvocato generale Sharpston, 17 giugno 2010, spec. punto 71.

[51] Cfr. L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in ID., C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 6.

[52] *Ibidem*, p. 12.

[53] Come sottolineato da GIAKOUMOPOULOS, BUTTARELLI, ÒFLAHERTY, *Manuale sul diritto europeo*, cit., p. 34 ss., il Regolamento "preserva e sviluppa i principi e i diritti fondamentali dell'interessato, previsti dalla direttiva sulla tutela dei dati". Introduce, inoltre, nuovi obblighi "che richiedono alle organizzazioni di attuare la protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita; nominare un responsabile della protezione dei dati in determinate circostanze; rispettare un nuovo diritto alla portabilità dei dati e rispettare il principio di responsabilizzazione".

[54] Cfr. l'art. 17 del GDPR che ha recepito la giurisprudenza della CGUE (caso c.d. *Google Spain*) in cui, nell'affermare che in presenza di alcune circostanze si possa richiedere la cancellazione di alcuni dati, ha stabilito che l'ingerenza del motore di ricerca nel diritto fondamentale alla protezione dei dati personali "non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca", evidenziano "in linea di principio" che detti diritti fondamentali stabiliti nella CDFUE prevalgono sia sull'interesse economico, sia sull'interesse dei privati a reperire informazioni attraverso ricerche aventi ad oggetto il nome dell'interessato. Cfr. causa C-131/12, *Google Spain SL, Google*

Nell'affermare il generale divieto di trattare i dati personali, salve le deroghe al principio provenienti da motivi tassativamente indicati, il Regolamento riconduce un ambito particolare di tutela ai dati sulla salute. In primo luogo definendoli e differenziandoli rispetto all'ampia compagine dei dati personali, trattati unitariamente dalla direttiva del 1995, che si limitava soltanto a richiamare i dati relativi alla salute e alla vita sessuale.

L'art. 4, n. 15 del GDPR, infatti, nel definire i dati "sensibili", conferisce un carattere preminente ai "dati relativi alla salute". Si tratta di quelli "suscettibili di rivelare informazioni attinenti allo stato di salute fisica o mentale", tra cui sono compresi i dati relativi alle prestazioni di servizi di assistenza sanitaria, rivolte alla persona "identificata" (l'i*nteressato*)[55].

Il *considerando* n. 35 del Regolamento stabilisce che tra detti dati sono compresi quelli idonei a rivelare informazioni connesse allo stato di salute fisica o mentale passata o futura; si tratta in particolare di "informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria", l'identificazione attraverso "un numero, un simbolo o un elemento specifico" per identificarla in modo univoco; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici, e qualsiasi informazione riguardante "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 di provenienza (ad esempio, un medico, un ospedale, un dispositivo medico o un test diagnostico).

Il Regolamento amplia quindi la nozione di dato relativo alla salute, anche alla luce della progressiva estensione del concetto di salute a livello internazionale, come emerge dalle indicazioni dell'OMS, per cui la salute va intesa come *stato completo di benessere psico-fisico*[56]. I dati in esame rappresentano, quindi, un complesso di informazioni che identificano la salute non soltanto come assenza di patologie, ma

Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, del 13 maggio 2014. La giurisprudenza della CGUE si è ulteriormente arricchita, come dimostrano le sentenze C-507/17, *Google LLC contro Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019 e C-18/18, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*, 3 ottobre 2019, su cui vedi O. POLLICINO, *L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi*, n. 9/2019.

[55] Ai sensi dell'art. 4, par. 1 del Regolamento sussistono varie modalità per identificare la persona: "direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

[56] Cfr. *Ottawa Charter for Health Promotion*, Ginevra, 1986, secondo cui "*Health is a positive concept emphasizing social and personal resources, as well as physical capacities. Therefore, health promotion is not just the responsibility of the health sector, but goes beyond healthy lifestyles to wellbeing*" (reperibile in *Euro.who.int.*).

descrivono il contesto di vita del soggetto, la promozione, il mantenimento e il recupero della salute fisica e psichica, nella prospettiva (peraltro) condivisa dal legislatore italiano[57].

Sotto tale impulso, anche il contenuto dei dati relativi alla salute viene ampliato dal Regolamento che annovera tra questi i dati genetici e quelli biometrici, "intesi a identificare in modo univoco una persona fisica", secondo quanto disposto dall'art. 9 del GDPR", che li assoggetta ad un particolare trattamento (*infra*).

4.1. In particolare le modalità di trattamento e il consenso

La progressiva incisività delle disposizioni a tutela dei dati relativi alla salute è legata anche all'accrescersi dell'utilizzo della tecnologia in ambito medico-sanitario, attraverso la nuova frontiera della "sanità digitale" e delle sue "sofisticate applicazioni", come si è anticipato[58].

La dottrina ha evidenziato, in effetti, che il potenziale utilizzo della tecnologia in maniera *a*-neutrale, minaccia concretamente il diritto all'autodeterminazione (fisica e informativa) del soggetto[59]. La maggiore facilità nel reperire le informazioni sulle persone fisiche, attraverso le moderne tecnologie, ha reso necessario modificare gli strumenti di protezione, in una prospettiva che considera la tutela della riservatezza non più solo come segretezza delle informazioni, ma come trasparenza delle informazioni possedute in capo ai soggetti pubblici e privati che vengono in contatto con la persona, la quale ha il diritto di accedere e modificare i documenti in possesso delle strutture sanitarie pubbliche e private[60].

È per questa ragione che il Regolamento diviene più stringente su alcuni punti.

L'evoluzione normativa tratteggiata sin qui evidenzia l'esistenza di norme cogenti a protezione dei dati relativi alla salute con particolare riferimento alle modalità di trattamento e al consenso.

Il "trattamento" è identificato dall'art. 4, ed è costituito da "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali […] come la raccolta, la registrazione, l'organizzazione […] la strutturazione, l'estrazione, la consultazione, l'uso, la

[57] Questa prospettiva è fatta propria anche dal legislatore italiano, come dimostra l'art. 1 della legge n. 883 del 1978, istitutiva del SSN. Cfr. sul punto anche G. FARES, *I dati relativi alla salute e i trattamenti in ambito sanitario*, in Califano, Colapietro (a cura di), *Innovazione tecnologica e valore della persona,* cit., p. 441 ss.

[58] Sul punto cfr. l'analisi di CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, cit., spec. p. 205.

[59] Sulla potenziale a-neutralità dell'impiego della tecnologia, cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, 14, nonché le riflessioni di V. FROSINI, *Il diritto nella società tecnologica*, Giuffré, Milano, 1981.

[60] Questo assetto vale per tutti i profili in cui siano coinvolti i dati personali e chiama in causa direttamente l'operato delle pubbliche amministrazioni, soggette ad un implicito obbligo costituzionale di trasparenza. Sul punto cfr. C. COLAPIETRO, *Trasparenza e democrazia: conoscenza e/è potere*, in ID., CALIFANO (a cura di), *Le nuove frontiere della trasparenza nell'ordinamento costituzionale*, Editoriale scientifica, Napoli, 2014, p. 30 ss.

comunicazione mediante trasmissione […] la cancellazione, la distruzione"[61]; da quanto si evince, viene ampliato in modo significativo l'elenco di operazioni che costituiscono detto trattamento. Il GDPR, subordina il trattamento dei dati all'esistenza di alcuni presupposti di liceità, primo tra tutti quello che fonda ogni trattamento in un'idonea base giuridica, come affermato nell'art. 6 del Regolamento e ribadito dalle modifiche al Codice della *privacy* intervenute nel 2018[62].

Posto questo elemento, dall'art. 9 del GDPR, letto insieme ai considerando nn. 51, 52, 53, 54, discende un *generale divieto di trattamento* dei dati relativi alla salute[63]. La norma implica che tutte le misure che permettono il trattamento sono poste in deroga a tale principio generale.

Ai sensi dell'art. 9, infatti, eccezioni al divieto sono ammesse ove si verifichi almeno una delle seguenti condizioni: l'interessato abbia prestato il proprio consenso esplicito al trattamento per una o più finalità specifiche; il trattamento sia necessario per assolvere gli obblighi ad esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto al lavoro e della sicurezza sociale e protezione sociale; il trattamento sia necessario per tutelare un interesse fondamentale dell'interessato o di un'altra persona fisica ove l'interessato sia incapace fisicamente o giuridicamente di prestare il proprio consenso; il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato; il trattamento sia necessario *per motivi di interesse pubblico rilevante* sulla base del diritto dell'Unione o degli Stati membri; il trattamento sia necessario per finalità di medicina preventiva, di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza e terapia sanitaria.

Nello specifico caso che prevede il trattamento per ragioni di interesse pubblico, il considerando 52 definisce il significato di "interesse pubblico" e richiede che siano previste adeguate garanzie, per proteggere i dati personali e altri diritti fondamentali. Le finalità di tutela di interesse pubblico sono volte a raggiungere "finalità di sicurezza sanitaria", come la prevenzione e il controllo di malattie trasmissibili e altre minacce gravi alla salute. La deroga al divieto di trattamento può avere luogo anche per gestire i servizi di assistenza sanitaria, "soprattutto al fine di assicurare la qualità e l'economicità delle procedure

[61] Anche la Direttiva n. 95/46/CE, nell'interpretazione datane dalla Corte di Giustizia forniva un'ampia accezione di trattamento dei dati relativi alla salute, estendendosi sia agli aspetti fisici, sia a quelli psichici: cfr. la richiamata sentenza *Bodil Lindqvist*, 6 novembre 2003, C-101/01.

[62] Il Codice della *privacy*, così come modificato dal d.lgs. n. 101 del 2018 (art. 2-*sexies*) stabilisce che il trattamento per motivi di interesse pubblico rilevante dei dati sensibili, sia ammesso solo ove previsto dal diritto Ue o da legge o regolamento che specifichino e motivino le finalità del trattamento stesso, introducendo una riserva di legge e di regolamento. Il d.lgs. n. 101, prevede, inoltre, all'art. 112, in maniera analitica, i casi per i quali si considera rilevante l'interesse pubblico relativo a tali trattamenti.

[63] Ai fini della cura del paziente anche la Direttiva prevedeva alcune deroghe generali al divieto di utilizzare i dati stessi: devono essere limitate, esaustive e interpretate in modo restrittivo. Tra le deroghe al divieto di trattamento quelle per motivi corrispondenti ad un "interesse vitale della persona interessata": ove il trattamento fosse necessario per somministrare una cura da cui dipende la vita del paziente. Secondo la Direttiva il trattamento poteva essere svolto solo se presenti alcune condizioni contestuali: necessario (cioè non solo utile); servire alla prevenzione o alla diagnosi, alla somministrazione di cure); effettuato da un professionista sanitario soggetto al segreto professionale.

per soddisfare le richieste di prestazioni e servizi nell'ambito del regime di assicurazione sanitaria", o "a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici".

Ai sensi dell'art. 9, par. 2, lett. h), il trattamento dei dati sanitari è consentito ove ciò sia necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura[64].

Il Regolamento dispone inoltre che il trattamento dei dati relativi alla salute e in particolare i dati genetici e biometrici, possa essere soggetto "a condizioni e/o limitazioni ulteriori, liberamente mantenute o introdotte dai singoli Stati membri"; sul punto il legislatore italiano ha introdotto una specifica normativa per bilanciare l'accesso ai dati dell'interessato e la situazione giuridica che si intende tutelare[65]. Sulla base delle indicazioni fornite dal GDPR, il Garante per la protezione dei dati personali, con Provvedimento del 7 marzo 2019, inoltre, specifica i casi in cui sia lecito il trattamento in ambito sanitario, integrando quanto già previsto nel d.lgs. n. 101 del 2018[66]. L'elenco delle fattispecie in deroga introdotte mostrano che si tratta di misure a tutela della salute pubblica, chiamando in causa il difficile bilanciamento con la protezione dei dati dell'interessato[67]. Dalla normativa in esame viene in evidenza, infatti, la difficoltà di integrare la dimensione individuale e collettiva del diritto alla salute, come risulta dalla fase attuale di contenimento dell'emergenza sanitaria. In tale difficile bilanciamento "l'elemento di chiusura" del sistema è dato dalla fiducia che il soggetto ripone nelle istituzioni[68].

Uno dei modi in cui si garantisce detta fiducia è rappresentato dall'istituto del "consenso".

---

[64] Il trattamento è autorizzato ove effettuato da un operatore professionista in campo sanitario e soggetto al segreto professionale o da un'altra persona soggetta a un obbligo equivalente.

[65] Una novità di rilievo introdotta nell'ordinamento circa il trattamento dei dati genetici e biometrici (oltre a quelli relativi alla vita o all'orientamento sessuale) è contenuta nell'art. 60, del d.lgs. n. 196 del 2003, come modificato dal d.lgs. n. 101 del 2018. La disposizione stabilisce che quando il trattamento concerne in particolare dati genetici relativi alla salute il trattamento è consentito *solo se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato ovvero consiste in un diritto della personalità o in altro diritto di libertà fondamentale*. La normativa, inoltre, prevede particolari misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute che identificano il soggetto (art. 2-*septies*).

[66] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*" del 7 marzo 2019, che definisce necessari i trattamenti per: motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. *g* del Regolamento), individuati dall'art. 2-*sexies* del Codice; 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 preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. *i* del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare); finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali.

[67] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute*, cit.

[68] Per un approfondimento, FARES, *I dati relativi alla salute*, cit., p. 460.

Sul punto va innanzitutto evidenziato come il consenso costituisca uno dei (sei) *fondamenti di liceità* del trattamento identificati dal GDPR[69]. Si tratta di "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato" che manifesta il proprio assenso "mediante dichiarazione o azione positiva" che i dati personali che lo riguardino siano oggetto di trattamento[70].

Nel nostro ordinamento la nozione di consenso è stata oggetto di ampia elaborazione giurisprudenziale da parte della Corte costituzionale, in riferimento normativa italiana che ha preso le mosse dalla direttiva del 1995. Il giudice costituzionale lo ha identificato quale diritto della persona che trova fondamento negli artt. 2, 13 e 32 Cost., come sintesi tra il diritto all'autodeterminazione e il diritto alla salute. Rappresenta una manifestazione di autodeterminazione (informativa) del soggetto, attraverso il quale esplicitare un potere di controllo (sentenza n. 438 del 2008)[71].

Come si anticipava, il GDPR innova la disciplina del consenso; il Considerando 54, infatti, evidenzia che possa essere necessario il trattamento di categorie particolari di dati personali *per motivi di interesse pubblico,* nei settori della sanità pubblica, senza il consenso dell'interessato.

Detto trattamento deve sottostare a misure specifiche di tutela dei diritti e delle libertà dei soggetti coinvolti. Le ragioni di detto trattamento vanno ricercate nella nozione di «sanità pubblica» richiamata dal GDPR, che si ricava dal Regolamento n. 1338/2008/CE e comprende tutti gli elementi relativi alla salute ("lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità"). Pertanto, posto che il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, come ad esempio i datori di lavoro, le compagnie di assicurazione e gli istituti di credito, il

[69] Considerando 40 e artt. 6-9 del GDPR.

[70] Art. 4, par. 11. Per essere valido il consenso deve essere: libero, specifico, esplicito e informato. Deve essere espresso, cioè manifestato anche con un comportamento concludente (non vale l'inazione o il silenzio). Deve essere dato liberamente, cioè frutto di una decisione volontaria; non è libero il consenso trasformato in condizione necessaria per la fruizione di un servizio (cons. 43). Deve essere specifico, cioè riguardare una situazione ben determinata e concreta e non un consenso generale al trattamento (tanti consensi quante sono le finalità del trattamento). Deve essere informato, basato cioè sulla conoscenza del titolare del trattamento e delle finalità dello stesso (cons. 42), nonché sulla comprensione e valutazione dei fatti (artt. 13 e 14 GDPR). In alcune situazioni deve essere esplicito, che non è sinonimo di espresso, poiché quest'ultimo è la regola generale mentre il primo è richiesto in tre soli casi: trattamento di dati sensibili (art. 9.2a GDPR); decisione basata su un trattamento unicamente automatizzato (art. 22, par. 2, lett. c); trasferimento dati verso paesi/organizzazioni non adeguati (art. 49 par. 1 lett. a). Può essere anche verbale (registrazione telefonica o via sms).

[71] Per un commento alla sentenza cfr. D. CEVOLI, *Diritto alla salute e consenso informato. Una recente sentenza della Corte costituzionale*, in *Forum dei quaderni costituzionali*, 2008. Come messo in luce dalla dottrina, la previsione della necessità del consenso "contribuisce a far uscire il malato dal cono d'ombra della soggezione al medico" per fargli "assumere consapevolmente ogni scelta, di tipo diagnostico e terapeutico, che coinvolga la propria salute e il proprio corpo". Cfr. B. PEZZINI, *Il diritto alla salute: profili costituzionali*, in *Dir. Soc.*, 1983, p. 87 ss.; B. CARAVITA, *La disciplina costituzionale della salute*, in *Dir. Soc.*, 1984, p. 31 ss.

considerando 54, pone il principio generale per cui è esentato dal consenso il trattamento dei dati relativi alla salute svolto da enti pubblici, in quanto vi sono ulteriori basi giuridiche di legittimazione, come la fonte primaria che disciplina la materia.

Diversamente, invece, come specificato anche dal provvedimento del Garante del 7 marzo 2019, il trattamento dei dati connessi solo in senso lato alla cura "ma non strettamente necessari" richiedono in ogni caso una base giuridica, da individuarsi nel consenso dell'interessato[72].

5. Protezione dei dati relativi alla salute e trattamento automatizzato del Fascicolo sanitario e delle Cartelle cliniche

La progressiva incisività delle disposizioni a tutela dei dati relativi alla salute è legata anche all'accrescersi dell'utilizzo della tecnologia in ambito medico-sanitario, attraverso la nuova frontiera della "sanità digitale" e delle sue "sofisticate applicazioni", come si è anticipato[73].

La dottrina ha evidenziato, in effetti, che il potenziale utilizzo della tecnologia in maniera *a*-neutrale, minaccia concretamente il diritto all'autodeterminazione (fisica e informativa) del soggetto[74]. La maggiore facilità nel reperire le informazioni sulle persone fisiche, attraverso le moderne tecnologie, ha reso necessario modificare gli strumenti di protezione, in una prospettiva che considera la tutela della riservatezza non più solo come segretezza delle informazioni, ma come trasparenza delle informazioni possedute in capo ai soggetti pubblici e privati che vengono in contatto con la persona, la quale ha il diritto di accedere e modificare i documenti in possesso delle strutture sanitarie pubbliche e private[75]. Per questa ragione il Regolamento diviene più stringente su alcuni punti.

Alla luce delle predette considerazioni, è necessario a questo punto dell'analisi, focalizzare l'attenzione sulle modalità di protezione dei dati personali contenuti nel FSE e nelle CCE, quali strumenti in grado di trattare una quantità maggiore di dati relativi alla salute, anche in via aggregata, determinando la potenziale disponibilità di detti dati in capo ad una vasta cerchia di persone, anche al di fuori del personale medico deputato a garantire le cure.

Il trattamento di detti dati pone altresì il problema della loro raccolta ai fini di eventuali profilazioni dei pazienti a fini commerciali e di ricerca scientifica, nonché alcune criticità con riferimento al trasferimento

---

[72] Cfr. il richiamato provvedimento "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", del 7 marzo 2019.

[73] Sul punto cfr. l'analisi di CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, cit., spec. p. 205.

[74] Sulla potenziale a-neutralità dell'impiego della tecnologia, cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, 14, nonché le riflessioni di V. FROSINI, *Il diritto nella società tecnologica*, Giuffré, Milano, 1981.

[75] Questo assetto vale per tutti i profili in cui siano coinvolti i dati personali e chiama in causa direttamente l'operato delle pubbliche amministrazioni, soggette ad un implicito obbligo costituzionale di trasparenza. Sul punto cfr. C. COLAPIETRO, *Trasparenza e democrazia: conoscenza e/è potere*, in ID., CALIFANO (a cura di), *Le nuove frontiere della trasparenza nell'ordinamento costituzionale*, Editoriale scientifica, Napoli, 2014, p. 30 ss.

dei dati digitalizzati in paesi terzi non sicuri ("non adeguati"). A queste questioni si affianca l'ulteriore tema del diritto di acquisire i propri dati da parte dell'interessato, di poterli controllare, esportare, trasferire ed eliminare.

Se si considera quanto si è precedentemente riferito circa la durata illimitata della conservazione di alcuni dati contenuti nelle cartelle cliniche, ci si rende conto di come tali questioni si amplificano nel passaggio dalle cartelle in formato cartaceo, conservate presso le singole strutture sanitarie, alla digitalizzazione che amplia notevolmente le possibilità di scambio e di circolazione dei dati[76]. L'utilizzo dei sistemi elettronici in sanità, dunque, pone alcune criticità, secondo quanto emerge anche dalla normativa di riferimento[77].

Al fine di comprendere quali norme garantiscono la protezione dei dati personali in detto contesto della sanità digitale, è necessario partire da un assunto di fondo. Secondo quanto indicato dal GDPR e dalla Convenzione n. 108 "modernizzata", che costituiscono le principali fonti di riferimento in materia, la disciplina a protezione dei dati relativi alla salute si applica anche al trattamento automatizzato di dati personali[78]. Ciò equivale a dire che si applicano a tale ambito, tutte le garanzie finora esaminate con riferimento alle modalità di trattamento e alla gestione consenso, nei casi espressamente indicati dalla normativa.

L'estensione della disciplina sulla protezione dei dati sulla salute anche all'utilizzo di detti dati ove digitalizzati, è un fattore costante nella disciplina in materia. Vigente la direttiva del 1995, infatti, detto principio si ricava già dall'importante e tuttora utile "*Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche*" del 2007, elaborato dai Garanti per la protezione dei dati europei, riuniti nel Gruppo di lavoro "*Articolo 29*" (c.d. "WP29")[79].

Attraverso il documento, il Gruppo di lavoro esprime un parere sull'opportunità di trattare i dati relativi alla salute, esplicitando quali garanzie dovessero corredare detto trattamento. Nel definire le CCE un "fattore di rischio", il "WP29" ha estrapolato una serie di principi da rispettare nel loro impiego, applicando le disposizioni generali sulla protezione dei dati relativi alla salute contenuti nella Direttiva n. 46 e adattandole al trattamento digitale di detti dati. Come si è evidenziato, sono principi che il Gruppo di lavoro evince dalla Direttiva, ma che restano validi anche dopo l'entrata in vigore del Regolamento del 2016, anche per la contiguità di intenti tra le due fonti normative e che rivestono pertanto notevole importanza per definire la disciplina di riferimento.

[76] *Infra* par. 2.1.
[77] Cfr. la richiamata Raccomandazione n. UE/2019/243, in tema di CCE.
[78] Cfr. GDPR, art. 2, par. 1 e art. 4, par. 2; Convenzione n. 108 "modernizzata", art. 2, lettere b), c).
[79] Gruppo di lavoro costituito ai sensi dell'art. 29 della Direttiva del 1995, sostituito dal Comitato Europeo Protezione Dati, con l'entrata in vigore del GDPR. Il documento del 15 febbraio 2007 (WP 131) è reperibile nel sito istituzionale del Garante per la protezione dei dati personali.

È necessario evidenziare sul punto che il Regolamento del 2016 ha razionalizzato a livello normativo alcune misure contenute nel parere del 2007, come si vedrà dettagliatamente nel prosieguo.

In linea generale, tra le prescrizioni generali sulla tutela dei dati personali contenute nella normativa e applicabili alle CCE, il Parere evidenzia le seguenti: innanzitutto l'applicazione al sistema di CCE dei principi generali in materia di trattamento. Tra questi si configurano i limiti all'utilizzo dei dati, ove non più necessari; l'impiego di dati di qualità e veritieri; altri presupposti di trattamento riguardano le corrette modalità di conservazione dei dati stessi, il diritto all'accesso da parte degli interessati in quanto dati personali e gli obblighi di sicurezza nella gestione degli stessi.

Con riferimento alle deroghe il Parere è molto puntuale quanto alle eccezioni al divieto di trattamento dei dati; sul punto il GDPR accoglie la prospettiva del Gruppo di lavoro, enfatizzando la deroga al divieto di trattamento per motivi di interesse pubblico[80].

Tra le segnalazioni del Gruppo di lavoro accolte dal Regolamento del 2016, figura altresì la prescrizione che i dati siano trattati sotto la responsabilità di un operatore sanitario soggetto al segreto professionale[81].

Un ulteriore elemento richiamato dal Gruppo di lavoro e recepito dal GDPR riguarda le modalità di trattamento dei dati contenuti nelle CEE che devono essere fondati sul consenso dell'interessato, come valorizzato dall'art. 4, par. 11 del GDPR. Deve trattarsi, come si è visto, di un consenso libero, specifico, esplicito e informato, secondo la prospettazione del GDPR, che definisce il consenso una delle basi giuridiche di legittimazione del trattamento. Allo stesso tempo, i Garanti avevano concluso che l'istituzione di un sistema di Cartelle cliniche elettroniche potesse basarsi sul principio che consente agli Stati membri di trattare i dati sensibili senza il consenso della persona interessata, purché ciò avvenga per motivi di "interesse pubblico rilevante" e siano fissate misure legislative o di altra natura che garantiscano la protezione dei dati. Tale norma era già contenuta nell'articolo 8, comma 4, della Direttiva n. 46, come ribadita dall'art. 9 del GDPR ed è applicabile anche ai dati contenuti nel FSE (*supra*).

Il documento delinea anche le garanzie da individuare attraverso un organico quadro normativo. Le garanzie mirano a preservare il rispetto del principio di autodeterminazione, che comporta la necessità di prevedere spazi e momenti diversi per consentire agli interessati (pazienti) di esprimere detta autodeterminazione attraverso strumenti, quali il consenso, ovvero forme di dissenso, secondo modalità opportunamente stabilite. Per i Garanti europei, è opportuno fissare idonee garanzie rispetto all'accesso ai dati da parte degli operatori sanitari, del paziente e di terzi, con riguardo alle misure di carattere tecnico quali l'identificazione, l'autenticazione e l'autorizzazione. Con particolare riferimento alla possibilità di accedere alle CCE per leggerle e compilarle, quale espressione del diritto all'autodeterminazione

[80] V. quanto si è detto *supra* circa il divieto di trattamento e le relative deroghe.
[81] Tale assunto è contenuto nel considerando n. 53.

informativa, essa viene evidenziata dal Parere del Gruppo di lavoro e valorizzata dal Regolamento. Sul punto, il WP mette in luce che l'accesso alle CCE in linea di principio dovrebbe essere consentito al paziente e al medico curante della patologia in corso. Allo stesso tempo, si segnala il diritto del paziente di poter impedire l'accesso ai propri dati ad altri soggetti e di accedere al contenuto della CCE. L'accesso deve essere garantito all'interessato senza difficoltà e l'interessato deve essere informato ove vi sia un accesso alla sua CCE. Questi aspetti sono stati recepiti dal considerando 63 del Regolamento, secondo cui ogni trattamento automatizzato deve sottostare ad alcune indicazioni. In particolare, il considerando dispone come l'interessato abbia diritto di accedere facilmente ai dati, ad intervalli ragionevoli; l'interessato deve, inoltre, essere consapevole del trattamento dei suoi dati e deve poterne verificare la liceità; deve, infine, avere comunicazione delle finalità di utilizzo dei dati da parte dei destinatari.

Altro elemento segnalato del WP riguarda la necessità di prevedere l'identificazione e il riconoscimento dell'interessato (paziente) e del personale sanitario che accede al SCCE. Tale identificazione deve essere affidabile. Sul punto è intervenuta la normativa di settore: l'utilizzo di mezzi sicuri di identificazione e autenticazione per accedere ai dati sanitari da parte dei soggetti interessati è definito dal Regolamento n. 2014/910/UE, in materia di identificazione elettronica[82], che fissa le condizioni a cui i mezzi di identificazione elettronica possono essere utilizzati dai cittadini per avere accesso a servizi pubblici *on-line* all'estero, compreso l'accesso ai dati sanitari; le norme indicate stabiliscono anche la disciplina della gestione e scambio sicuro di dati sanitari riducendo il rischio di alterazione e uso abusivo[83].

Il "WP29" segnala inoltre la necessità di prevedere appositi *standard* di sicurezza nella circolazione dei dati, soprattutto con riferimento ai trasferimenti verso paesi terzi, finalizzati a garantire maggiore efficienza nelle cure; su questo punto, in particolare, il Gruppo ha proposto il trasferimento dei dati in forma anonimizzata o pseudonimizzata, al fine di non rivelare l'identità del paziente se non quando assolutamente necessario (ad es. in caso di consulto medico). Anche eventuali utilizzazioni secondarie dei dati contenuti nella Cartella elettronica (per scopi di ricerca o di altra natura), secondo il Gruppo di lavoro, devono essere regolamentate specificamente a livello nazionale, nel rispetto di tutti i principi stabiliti in merito (dall'abrogata Direttiva n. 46). L'art. 14 del GDPR, valorizzando questa prospettiva, stabilisce che, se i dati vengano trasferiti in un paese terzo al di fuori del territorio UE, occorre che il titolare del trattamento verifichi l'esistenza di specifiche garanzie (indicate all'art. 46 del Regolamento). Il titolare del

[82] Cfr. il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[83] Nello specifico, la normativa prevede anche il controllo sui "destinatari". Ai sensi del regolamento del 2014, destinatario è "la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali". Nel nostro caso può trattarsi del personale medico che accede ai dati.

trattamento o il responsabile dello stesso, può trasferire dati verso un paese terzo solo in presenza di adeguate garanzie e se gli interessati dispongano dell'azionabilità dei diritti e di mezzi di ricorso effettivi. L'art. 36, commi 1 e 5, del GDPR, inoltre, conferisce agli Stati la facoltà di prescrivere un obbligo preventivo di consultare l'autorità di controllo da parte del titolare del trattamento dei dati ove i detti dati circolino in paesi non sicuri.

Ulteriori strumenti di protezione per garantire la liceità del trattamento previste dal GDPR sono contenute in ulteriori disposizioni del GDPR. Si tratta di forme di tutela che, se non sono direttamente rivolte alla digitalizzazione della sanità, rappresentano efficaci modalità di garanzia della tutela dei dati in questione. Il riferimento in generale è al principio dell'a*ccountability*, il quale nonostante la difficile traduzione in italiano, valorizza l'esistenza al suo interno di un principio della responsabilità e che implica un intervento consapevole del responsabile del trattamento anche attraverso l'ausilio di una figura di riferimento a supporto, data dal DPO (*data protection officer*), ai sensi dell'art. 37 del GDPR[84]. Altro ausilio è dato dal ruolo crescente dell'autorità di garanzia, che acquisisce il potere di sanzionare comportamenti illeciti da parte dei responsabili, secondo quanto stabilito dall'art. 57 del GDPR[85].

Accanto a questi principi di carattere generale valevoli per le diverse fattispecie, completa il quadro di riferimento anche l'ulteriore normativa sovranazionale. La direttiva n. 2016/1148/UE del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, stabilisce che i prestatori di assistenza sanitaria identificati come operatori di servizi essenziali dagli Stati e i fornitori di servizi digitali sono tenuti a rispettare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi sulla sicurezza delle reti e dei sistemi informativi. Sono previsti inoltre dei requisiti di c.d. «cybersicurezza» per minimizzare attraverso un'adeguata informazione agli organismi competenti gli incidenti a carico della sicurezza e i c.d. PBS (*Personal Data Breach*).

[84] Cfr. CALIFANO, *op. cit.* p. 13 ss. Il DPO è un consulente esperto che affianca il titolare del trattamento dei dati personali nella gestione delle varie problematiche, in considerazione della crescente complessità del settore. Il GDPR vuole garantire che un soggetto qualificato in ambito giuridico si occupi della materia aggiornandosi sui rischi e sulle misure di sicurezza.

[85] I poteri conferiti alle autorità si sostanziano nel costante controllo sull'operato e sulle attività poste in essere dal titolare e/o dal responsabile del trattamento. Il controllo non si esaurisce in una mera verifica delle attività, in quanto l'autorità opera in un rapporto di affiancamento, controllo e scambio di informazioni. I compiti delle autorità prevedono attività diversificate come, ad esempio, promuovere la consapevolezza riguardo agli obblighi imposti dal Regolamento, incoraggiare l'elaborazione di Codici di condotta ai sensi dell'art. 40, paragrafo 1, o l'istituzione di meccanismi di certificazione della protezione dei dati, a norma dell'art. 42, paragrafo 1. Si configura così non più una mera collaborazione e supporto di natura paritaria, ma di un vero e proprio controllo dell'operato e di intervento, facendo valere il proprio ruolo di autorità indipendente di controllo.

6. segue: "Sanità digitale" e protezione dei dati relativi alla salute nell'ordinamento italiano

Il Regolamento del 2016, come si è anticipato, lascia un margine di apprezzamento al legislatore nazionale sulla disciplina della protezione dei dati personali relativi alla salute, soprattutto in riferimento alle modalità di trattamento e al consenso. Nel riempire questo spazio di discrezionalità, il legislatore è affiancato dall'autorità di garanzia[86].

Riguardo alla "sanità digitale" l'intervento del Garante si è focalizzato sulla disciplina del consenso nell'ambito del trattamento di dati contenuti in *App* mediche e nel FSE (vedi *infra*).

Con riferimento al FSE e alla protezione dei dati relativi alla salute in esso contenuti, fino all'entrata in vigore dell'art. 12, comma 1, del d.l. n. 179/2012 (istitutivo del FSE), era rimessa alle *Linee guida* elaborate dal Garante della *privacy* nel 2009[87]. Queste sono state poi arricchite da fonti normative primarie e secondarie, tra cui figura l'art. 6 del d.p.c.m. n. 178. La disposizione prevede che il FSE sia soggetto all'informativa all'interessato da cui deve emergere, ai sensi dell´art. 13 del Codice della *privacy*, oltre al titolare e alle finalità del trattamento, anche che i dati che confluiscono nel Fascicolo siano relativi allo stato di salute attuale ed eventualmente pregresso dell'interessato.

Dopo l'entrata in vigore del GDPR, il Garante, nell'ambito della propria attività di verifica della compatibilità della normativa nazionale con le prescrizioni del Regolamento, ha modificato il suo orientamento circa l'espressione del consenso in talune applicazioni digitali. Ha, infatti, specificato che per i trattamenti effettuati attraverso il FSE, l'acquisizione del consenso (quale condizione di liceità del trattamento) richiesta dalle disposizioni precedenti all'applicazione del Regolamento Ue, deve essere rimodulata. Il Garante, infatti, si mostra favorevole "ad un'eventuale opera di rimeditazione normativa in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del Fascicolo", in quanto compatibile con il nuovo quadro giuridico in materia di protezione dei dati[88].

Questa prospettiva è stata fatta propria del "decreto rilancio" che, in un'ottica di semplificazione dovuta alla particolare situazione emergenziale, elimina il consenso all'alimentazione del FSE (abrogando l'art. 12, comma 3-*bis*, d.l. n. 179/2012) mentre lascia inalterata l'espressione del consenso dell'interessato per

[86] Il d.lgs. n. 101/2018, ha previsto, al riguardo, che il Garante completi l'individuazione dei presupposti di liceità dei trattamenti dei dati relativi alla salute, adottando specifiche misure di garanzia e promuovendo l'adozione di regole deontologiche (artt. 2-*septies* e 2-*quater* del Codice). Il legislatore ha, inoltre, previsto un periodo transitorio, affidando al Garante il compito di individuare ed aggiornare, le prescrizioni contenute nelle autorizzazioni generali sul trattamento dei dati sensibili che risultavano compatibili con le disposizioni del Regolamento e del decreto n. 101/2018, nonché di verificare la conformità dei codici deontologici al Regolamento (artt. 20 e 21 del citato decreto).

[87] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*, del 16 luglio 2009.

[88] Al punto 1, lett. e. Cfr. Garante per la protezione dei dati personali, "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", cit.

la consultazione del detto FSE da parte del personale medico, ai sensi dell'art. 12, comma 5, del richiamato decreto[89].

Riguardo invece all'accesso al FSE, il d.p.c.m. del 2015 dispone che per finalità di cura il FSE sia consultabile solo da parte del personale sanitario del SSN che prende in carico l'interessato. Possono accedere ad esso tutti quei professionisti che a vario titolo si occupano della cura dell'interessato, come il medico di medicina generale o il pediatra di libera scelta; il personale amministrativo operante nella struttura sanitaria, invece, può consultare solo le informazioni finalizzate ad assolvere alle funzioni amministrative correlate all'erogazione della prestazione sanitaria stessa. Per finalità di governo e di ricerca il FSE è invece accessibile da parte delle Regioni, del Ministero della salute e (limitatamente alle finalità di governo) da parte del Ministero del lavoro e delle politiche sociali.

La normativa prevede anche un'operazione di anonimizzazione dei dati poiché i trattamenti da parte di detti soggetti devono essere effettuati senza dati identificativi diretti dell'assistito e nel rispetto dei principi di indispensabilità, necessità, pertinenza e non eccedenza in relazione alle suddette finalità. È previsto inoltre il divieto di accesso al FSE per particolari categorie di soggetti[90].

L'interessato può decidere di non rendere accessibili alcuni dati nel FSE, richiedendo l'oscuramento dei dati e dei documenti in esso contenuti in ogni fase della vita del Fascicolo (art. 8 del d.p.c.m.). In questi casi, i dati oscurati potranno essere consultati esclusivamente dall'interessato e dai titolari che hanno generato i documenti[91]. L'assistito può comunque decidere di revocare in ogni momento l'oscuramento. La normativa prevede altresì che l'interessato possa accedere al proprio FSE in forma riservata e possa consultare l'elenco degli accessi eseguiti sul proprio Fascicolo (art. 9 del d.p.c.m.).

Riguardo invece alla disciplina dei dati relativi alla salute contenuti nelle CCE, il Garante esclude esplicitamente l'ambito delle CCE dalla disciplina contenuta nel provvedimento in tema di FSE, in quanto esse sono già oggetto di specifica regolamentazione[92]. La normativa di riferimento è costituita dagli artt. 75 ss. del Codice della *privacy*, così come modificata dal d.lgs. n. 10 del 2018, il quale stabilisce che ogni trattamento dei dati (e quindi anche quelli inseriti all'interno delle CCE) si effettua sulla base delle diposizioni del Regolamento, vale a dire sul richiamato art. 9 del GDPR.

---

[89] In caso di mancato consenso all'accesso al Fascicolo per gli operatori sanitari, il FSE potrà essere utilizzato solo per fini di governo e ricerca (adottando misure che non consentano di risalire all'identità dell'interessato). L'informativa deve precisare che il mancato consenso alla consultazione del FSE non incide sulla possibilità di accedere alle cure mediche richieste.

[90] Quali i periti, compagnie di assicurazione, datori di lavoro, associazioni scientifiche e gli organismi amministrativi pur se operanti in ambito sanitario.

[91] L'oscuramento deve avvenire con modalità tali da garantire che gli altri soggetti abilitati all´accesso al FSE per le finalità di cura non possano venire automaticamente a conoscenza del fatto che l´assistito ha effettuato tale scelta e che esistano dati "oscurati".

[92] Cfr. le richiamate *Linee guida in tema di FSE*, cit.

La disciplina italiana vigente interviene in un'ottica di semplificazione anche riguardo al regime dell'informativa connessa al trattamento dei dati, ivi compresi quelli contenuti in dispositivi digitali. Simile obbligo di informativa è finalizzato a rendere edotto l'interessato delle modalità di trattamento dei dati relativi alla salute (ai sensi degli artt. 13 e 14 del Regolamento), da parte di "strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie e dagli esercenti le professioni sanitarie", nonché dai soggetti pubblici (art. 80, d.lgs. n. 196). La semplificazione si realizza prevedendo ad esempio che l'informativa prestata dal medico di base copra automaticamente anche ulteriori trattamenti effettuati da altri operatori sanitari, ad esso collegati, ai sensi dell'art. 78 del Codice[93]. Sono fatti salvi quei trattamenti di dati personali che "presentano rischi specifici per i diritti e le libertà fondamentali", "per la dignità dell'interessato", ovvero nei particolari casi di trattamenti effettuati "nell'ambito della teleassistenza o telemedicina", nonché "per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica"[94], tra cui figura nello specifico l'implementazione del FSE (art. 78, comma 5, lett. c-*bis*)[95].

Con specifico riferimento alle modalità di redazione e di tenuta delle CCE, si ritiene che debba estendersi quanto esplicitamente affermato dal Codice in materia di Cartelle cartacee redatte dalle strutture (pubbliche o private) che erogano prestazioni sanitarie e socio-sanitarie, ai sensi dell'art. 92 del Codice. La loro compilazione deve essere effettuata sulla base di "opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri". Le richieste di presa visione o di rilascio di copia della cartella da parte di soggetti diversi dall'interessato possono essere accolte solo per motivi tassativamente indicati dalla disposizione[96].

---

[93] Il quale prescrive che il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in modo da rendere agevolmente comprensibili gli elementi indicati (negli artt. 13 e 14 del Regolamento). Le informazioni possono essere fornite "per il complessivo trattamento dei dati personali necessario per attività di (diagnosi, assistenza e terapia sanitaria), svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse". Possono riguardare, altresì, "dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto". Ove diversamente specificato, le informazioni riguardano "anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta che: a) sostituisce temporaneamente il medico o il pediatra; b) fornisce una prestazione specialistica su richiesta del medico e del pediatra; c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata; d) fornisce farmaci prescritti; e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile".

[94] Così l'art. 78, comma 5, del Codice.

[95] L'estensione automatica dell'informativa, in riferimento ad una pluralità di prestazioni erogate, è applicabile anche alle strutture pubbliche e private altresì nell'ambito di "distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate": art. 79 del Codice.

[96] L'art. 92, comma 2, prescrive che deve sussistere la documentata necessità: di esercitare o difendere un diritto in sede giudiziaria (cfr. art. 9, par. 2, lett. *f*, del Regolamento) di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale; di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

7. Alcune riflessioni conclusive

La normativa nazionale per far fronte alla pandemia ha potenziato gli strumenti della "sanità digitale" già esistenti, come il Fascicolo sanitario elettronico e le Cartelle cliniche elettroniche, che si affiancano alle nuove applicazioni tecnologiche messe in campo per combattere l'emergenza.

L'interconnessione tra vecchi e nuovi strumenti digitali consente la circolazione di informazioni, nel tentativo di scongiurare ulteriori eventi epidemiologici globali, come si è avuto modo di esaminare. L'impiego della sanità digitale richiede però il bilanciamento tra due diritti fondamentali in gioco: il diritto alla salute collettiva e quello alla protezione dei dati personali. L'oggetto dell'analisi riguarda proprio l'effettività della protezione dei dati relativi alla salute contenuti in detti dispositivi elettronici.

Il dato normativo nel quale si sviluppa sul piano dell'effettività la protezione dei dati relativi alla salute e il corrispondente diritto alla "autodeterminazione informativa" è caratterizzato dal Regolamento Generale sulla Protezione dei Dati personali, il quale rappresenta uno strumento normativo avanzato delineato a livello europeo. Ciò si evince in particolare dalla speciale attenzione rivolta ai dati relativi alla salute, e in particolare alla disciplina dei dati biometrici e genetici, di cui all'art. 9 del GDPR, nonché al generale divieto di trattamento dei detti dati, derogabile solo ove sussistano condizioni tassativamente indicate, tra cui figura l'interesse pubblico, come statuito del Regolamento del 2016. Altre forme di garanzia riguardano la procedura per l'espressione del consenso, oltre ad una serie di principi, quali la c.d. *accountability*, la previsione di un responsabile della sicurezza dei dati (DPO) e il ruolo pervasivo affidato alle autorità garanti.

L'estensione di questi principi alla c.d. "sanità digitale" rappresenta un'ulteriore forma di garanzia, secondo quanto emerge dal Regolamento. Proprio con riguardo all'impiego della tecnologia in ambito sanitario, infatti, il GDPR costituisce una forma di protezione efficace, facendo proprie alcune lungimiranti soluzioni in materia di protezione dei dati relativi alla salute contenuti nei documenti elettronici, proposte già dai Garanti europei riuniti nel richiamato Gruppo di esperti "WP 29".

Nonostante le perplessità derivanti da un utilizzo di dati potenzialmente illimitato attraverso le applicazioni tecnologiche in ambito medico-sanitario, ad avviso di chi scrive il contesto normativo di riferimento sovranazionale testé richiamato, a cui si è adeguato il legislatore italiano, mostra un complesso sistema di garanzie che appaiono funzionare proprio in virtù della loro dimensione multiordinamentale, la quale prefigura un'ottica collaborativa e dialogica tra il livello sovranazionale e gli Stati per mezzo delle singole autorità garanti. La delicatezza dell'ambito da proteggere, in definitiva, è garantita dal complesso impianto normativo, il quale si mostra solido ed evidenzia, in una prospettiva più generale, le potenzialità dell'ordinamento sovranazionale a fare da collante nella protezione di alcuni diritti fondamentali dei

cittadini europei; una protezione resa particolarmente necessaria nell'attuale fase di emergenza, fermo restando il rispetto delle peculiarità e delle prerogative costituzionali di ciascuno Stato membro.