Focus on

Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona

Luigi Ferraro*

THE REGULATION (EU) 2016/679 BETWEEN THE ELECTRONIC HEALTH RECORD AND THE ELECTRONIC MEDICAL RECORD: THE PROCESSING OF HEALTH DATA AND THE INFORMATIONAL SELF-DETERMINATION

ABSTRACT: The Covid-19 pandemic has made the urgency of digital healthcare in Italy even more clear. In this perspective, the contribution examines the Electronic Health File and the Electronic Medical Record, as documentation that can help save on healthcare costs and more effectively protect people's health. However, this raises the issue of the protection of personal data and notably of the right to informational self-determination in its balance with the other rights here involved.

KEYWORDS: Regulation (EU) 2016/679; Electronic Health Record; Electronic Medical Record; health data; self-determination

SOMMARIO: 1. Introduzione: la sanità digitale – 2. Il Fascicolo Sanitario Elettronico (FSE) tra previsioni normative, attuazione regionale e suo effettivo utilizzo – 2.1 Lo sviluppo del Fascicolo Sanitario Elettronico nel Piano Nazionale di Ripresa e Resilienza (PNRR) – 3. La Cartella Clinica Elettronica (CCE): contenuto e caratteristiche – 4. Il trattamento dei dati in materia sanitaria alla luce del Regolamento UE 2016/679 – 5. Il problematico conflitto tra diritti e il loro bilanciamento – 6. Note conclusive.

1. Introduzione: la sanità digitale

In questo periodo la pandemia da Covid-19 ha drammaticamente posto in rilievo il valore della sanità digitale, che è emerso per l'adozione delle regole di distanziamento sociale, per la necessità di cura dei pazienti attraverso il ricorso alla telemedicina, o ancora per le difficoltà cui i cittadini sono andati incontro nel prenotare i tamponi presso le ASL, solo per citare taluni esempi.
L'Italia, invero, già da qualche anno ha incominciato a perseguire la strada della digitalizzazione sanitaria, come dimostra il d.l. n. 179/2012, la cui Sezione IV è per l'appunto rubricata la «Sanità digitale», ma ora, naturalmente, la pandemia richiede tempi molto più celeri nel portare a termine questo oneroso processo. La sanità elettronica, com'è noto, favorisce la riduzione delle spese per i costi contenuti nell'uso del digitale, un risparmio dei tempi per la rapidità dei servizi offerti, oltre che una loro efficienza, dal momento che gli stessi servizi si presentano come innovativi proprio a seguito della

* *Professore Associato di Diritto Pubblico Comparato presso l'Università degli Studi della Campania Luigi Vanvitelli. Mail: luigi.ferraro@unicampania.it.* *Contributo sottoposto a doppio referaggio anonimo.*

tecnologia impiegata[1]. È evidente che questi aspetti positivi della sanità digitale si sono ancora di più amplificati in forza delle esigenze emerse a seguito del Covid-19; basti richiamare la possibilità di ridurre drasticamente – se non addirittura eliminare – le file d'attesa, difficilmente compatibili in questo periodo pandemico con le regole del distanziamento sociale.

A questi innegabili vantaggi, tuttavia, corrispondono profili problematici non secondari. Si pensi a coloro che non hanno accesso ad Internet o che non sono in grado di utilizzare la tecnologia informatica (es.: le persone anziane), con il pericolo di un'evidente discriminazione «per l'eguaglianza dei diritti esercitabili online» in forza dell'avvento della società digitale[2]. A ciò si aggiungano, poi, le resistenze offerte da quella parte di operatori sanitari maggiormente abituati all'uso dell'analogico, piuttosto che al digitale, nonostante dispongano di sistemi informatici capaci di rendere i servizi sanitari più rapidi ed efficienti nel senso prima indicato[3].

La sanità digitale è diventata centrale nel Piano Nazionale di Ripresa e Resilienza (PNRR) predisposto dal Governo. Infatti, nell'ambito della c.d. Missione 6 dedicata alla salute sono stati previsti due settori d'intervento, tesi a rafforzare, ad esempio, la telemedicina per l'assistenza sanitaria territoriale e la digitalizzazione del Servizio Sanitario Nazionale[4]. Oltre al PNRR quale effetto del *Next Generation EU*, sempre dall'Europa provengono ulteriori sollecitazioni attraverso il Programma *EU4Health*, istituito dal Regolamento UE 2021/522. È significativo come in questo atto normativo, teso ad istituire un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027, ci si prefigga tra gli obiettivi specifici di

> «rafforzare l'uso e il riutilizzo dei dati sanitari per la prestazione di assistenza sanitaria e per la ricerca e l'innovazione, [di] promuovere la diffusione di strumenti e servizi digitali, nonché la trasformazione digitale dei sistemi sanitari, anche sostenendo la creazione di uno spazio europeo dei dati sanitari»

[1] Sul punto cfr. G. PELLICANÒ, *Sanità digitale, stato dell'arte e prospettive future*, in *Smart eLab*, n. 14, 2019, 1; D. GRECO, *Sanità digitale dopo la pandemia: lo scenario*, 25 maggio 2021, in https://www.agendadigitale.eu/sanita/sanita-digitale-dopo-la-pandemia-lo-scenario/, e L. CALIFANO, *Fascicolo sanitario elettronico (Fse) e dossier sanitario*, in *Sanità Pubblica e Privata*, 3, 2015, 12, che evidenzia anche i vantaggi offerti dalla sanità elettronica in tempi di *spending review*.

[2] Ancora, G. PELLICANÒ, *op. cit.*, 1. In modo significativo T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Il Diritto dell'informazione e dell'informatica*, 4, 2020, 467, richiama la «dottrina della cd. "libertà informatica", che soprattutto con Internet è diventata una pretesa di libertà in senso attivo […] che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di ogni genere. […]. Non è più soltanto l'esercizio della libera manifestazione del pensiero dell'individuo, ma piuttosto la facoltà di questi di costituire un rapporto, di trasmettere e richiedere informazioni, di poter disporre senza limitazioni del nuovo potere di conoscenza conferito dalla telematica». Su questo argomento, comunque, si ritornerà nella parte finale del contributo.

[3] Così S. CORONATO, *Gli strumenti necessari al processo di digitalizzazione del S.S.N.*, in *Il Diritto sanitario moderno*, 3, 2019, 169.

[4] Cfr. Piano Nazionale di Ripresa e Resilienza (PNRR), in *https://www.governo.it/sites/governo.it/files/PNRR.pdf*, 222 ss., che è stato definitivamente approvato in sede europea il 13 luglio 2021, con Decisione di esecuzione del Consiglio a seguito della proposta della Commissione. Più dettagliatamente, la Missione 6 relativa alla salute si articola in due Componenti: la prima (M6C1) che riguarda le Reti di prossimità, le strutture intermedie e la telemedicina per l'assistenza sanitaria territoriale, la seconda (M6C2) finalizzata allo sviluppo dell'Innovazione, della ricerca e della digitalizzazione del Servizio Sanitario Nazionale, come si dirà più avanti anche nel testo.

(art. 4, par. 1, lett. f)[5]. Tutto ciò a conferma del rilievo che la digitalizzazione della sanità ha ormai assunto a livello europeo, sicuramente in conseguenza anche dell'evento pandemico.

Alla luce di questo contesto il presente contributo intende allora soffermarsi sul Fascicolo Sanitario Elettronico (da ora in poi anche FSE) e sulla Cartella Clinica Elettronica (da ora in poi anche CCE), quale documentazione che esprime il processo informatico che si sta sviluppando in sanità. Al riguardo, il tema di indagine si concentrerà sul trattamento dei dati relativi alla salute – uno dei profili problematici conseguenti a questa trasformazione digitale – dal momento che la loro circolazione potrebbe da un lato tutelare il diritto alla salute nelle modalità che saranno analizzate, ma dall'altro anche violare il diritto alla riservatezza, in tutte le sue implicazioni, rispetto a dati che comunque rimangono sensibili. Al di là dei rilevanti interessi economici sottesi a quest'argomento, ma fuori dal nostro specifico campo di indagine per tutti gli aspetti di eventuale interferenza[6], l'analisi si presenta estremamente interessante non solo per le novità in sé rappresentate dal FSE e dalla CCE, ma anche per quanto introdotto dal Regolamento UE 2016/679 in tema di «protezione dei dati». L'obiettivo principale di tale disciplina, infatti, è quello di uniformare il trattamento dei dati e le relative garanzie a livello di tutti gli Stati membri dell'Unione europea, così che il grado di tutela della privacy – intesa nel caso come autodeterminazione informativa – possa essere omogeneo nei Paesi UE. In questo modo, «nell'assicurare un "quadro più solido" nei diversi settori di applicazione delle varie tecnologie, l'impegno regolatorio realizzato dall'UE potrà […] concorrere a "creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno"»[7], quale ulteriore volano di sviluppo per l'Unione.

Pertanto, il FSE e la CCE possono rappresentare, sotto il versante interno, un test probante circa gli effetti che sta producendo la normativa europea in tema di protezione dei dati sensibili a fronte di questo processo di ammodernamento della sanità, il che, per di più, porterà ad esaminare il livello di implementazione raggiunto in Italia soprattutto dal FSE, prestando una naturale attenzione anche all'esperienza regionale.

2. Il Fascicolo Sanitario Elettronico (FSE) tra previsioni normative, attuazione regionale e suo effettivo utilizzo

Ai sensi dell'art. 12, 1° co., d.l. n. 179/2012, «il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale»[8].

[5] Su tale Programma europeo, v. M. FERRARA, *Dalla mobilità dei pazienti alla interoperabilità dei sistemi sanitari. Spunti sull'adozione di un formato europeo di scambio delle cartelle sanitarie elettroniche (Raccomandazione (UE) 2019/243)*, in *federalismi.it*, 5, 2021, 24 s.

[6] In relazione a questo tema cfr., invece, L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *federalismi.it*, 4, 2018, 3 ss.

[7] Cfr. L. CHIEFFI, *op. cit.*, 4.

[8] Il Garante per la protezione dei dati personali, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*, deliberazione n. 25, 16 luglio 2009, già prima di quest'ultimo intervento normativo, ha sostenuto che il FSE favorisce «la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica». Ancora il Garante per la protezione dei dati

Il dettato normativo precisa, poi, che il FSE è istituito dalle regioni e dalle province autonome, in ossequio alla normativa vigente in materia di protezione dei dati personali, con il compito di: «a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria» (2° comma).

Per ciò che concerne i contenuti del FSE, è necessario richiamare il d.P.C.M. n. 178/2015, intitolato «Regolamento in materia di Fascicolo Sanitario Elettronico», che all'art. 2 prevede un «nucleo minimo» eguale per tutti i fascicoli sanitari regionali, costituito dai dati identificativi e amministrativi dell'assistito, dai referti, dai verbali di pronto soccorso, dalle lettere di dimissioni in caso di ricovero, dal profilo sanitario sintetico, dal dossier farmaceutico e dal consenso o diniego alla donazione degli organi e tessuti (1° e 2° comma). Invece, gli ulteriori dati e documenti che integrano il suddetto contenuto minimo del FSE sono stabiliti a livello regionale in funzione delle scelte di politica sanitaria territoriale e del grado di digitalizzazione cui è pervenuto ogni singolo ente sub-statale. Tra questi dati e documenti integrativi sono da ricordare: le cartelle cliniche, le prescrizioni specialistiche e farmaceutiche, le prenotazioni specialistiche e di ricovero, le vaccinazioni, le prestazioni di emergenza (118 e pronto soccorso), le prestazioni di assistenza ospedaliera in regime di ricovero, la partecipazione a sperimentazioni cliniche, i dati a supporto delle attività di tele-monitoraggio, etc. (3° comma).

Da quanto ora illustrato appare chiaro come l'obiettivo principale del Fascicolo, avendo quale «orizzonte temporale […] l'intera vita del paziente»[9], sia quello di offrire ai medici la storia sanitaria dell'assistito, tant'è vero che «tutte le informazioni e i documenti che costituiscono il FSE sono resi interoperabili per consentire la sua consultazione e il suo popolamento in tutto il territorio nazionale e non solo nella regione di residenza dell'assistito»[10]. Ne consegue che il FSE favorisce la raccolta e la condivisione di tutte le informazioni e di tutti i documenti sanitari che riguardano un paziente, così da favorire la ricostruzione della sua storia clinica[11]. In tal modo si ottiene una drastica riduzione della

personali, *Prescrizioni in tema di Fascicolo Sanitario Elettronico (FSE)*, deliberazione n. 26, 16 luglio 2009, ha imposto ai titolari di un trattamento «di comunicare al Garante i trattamenti dei dati personali effettuati tramite FSE, prima dell'inizio del trattamento e, nei casi di iniziative di FSE già in corso, entro il termine del 31 dicembre 2009», a dimostrazione dell'attenzione sempre riservata da tale Autorità nei confronti dei dati di salute all'interno del Fascicolo.

[9] In tal senso, v. S. CORONATO, *op. cit.*, 171.

[10] Cfr. Il Fascicolo Sanitario Elettronico (FSE), in *https://www.fascicolosanitario.gov.it/it/il-fascicolo-sanitario-elettronico*, 6 agosto 2021, laddove si continua affermando che la suddetta interoperabilità sull'intero territorio nazionale «permette all'assistito una maggiore libertà nella scelta della cura e nella condivisione delle informazioni». Sulle caratteristiche e funzioni del FSE, cfr. G. ESCUROLLE, *Le novità sul Fascicolo Sanitario Elettronico (FSE)*, in *Ciberspazio e Diritto*, 3, 2020, 429 ss., e P. ROSSI, A. MELE, *Cartella clinica, Fascicolo Sanitario Elettronico e dossier sanitario: tra tutela della salute e riservatezza dei dati. Riflessi in ambito medico-legale assicurativo-previdenziale*, in *Rivista degli infortuni e delle malattie professionali*, 3, 2018, 405 s. Inoltre, Y. PINEVICH, K.J. CLARK, A.M. HARRISON, B.W. PICKERING, V. HERASEVICH, *Interaction Timewith Electronic Health Records: A Systematic Review*, in *Applied Clinical Informatics*, 4, 2021, 796, evidenziano nel loro studio come il FSE aiuti ad ottimizzare i tempi di lavoro degli operatori sanitari.

[11] Per un'analisi attenta sulla migliore qualità della documentazione e sulla maggiore efficienza amministrativa garantita dai documenti sanitari elettronici, cfr. L. NGUYEN, E. BELLUCCI, L. THUY NGUYEN, *Electronic health records implementation: An evaluation of information system impact and contingency factors*, in *International journal of medical informatics*, 83, 2014, 780 ss.

ISSN 2284-4503

documentazione cartacea dell'assistito, senza alcun effetto negativo per la certezza delle notizie mediche, oltre alla possibilità di eliminare le prestazioni sanitarie superflue proprio per la presenza di tutti i dati nel FSE, il che evita ovviamente inutili aggravi per la spesa sanitaria. Nelle situazioni d'emergenza vi è ancora l'opportunità per i medici di pronto soccorso di acquisire tempestivamente le informazioni necessarie sull'interessato, con evidenti vantaggi per la sua salute[12].

Al fine di garantire la realizzazione di questi obiettivi e la loro piena operatività, è stato previsto che nel FSE siano riportati «i dati degli eventi clinici presenti e trascorsi» di un paziente e che lo stesso fascicolo sia «alimentato […] dai soggetti e dagli esercenti le professioni sanitarie che prendono in cura l'assistito sia nell'ambito del Servizio sanitario nazionale e dei servizi socio-sanitari regionali sia al di fuori degli stessi» (art. 12, 3° co., d.l. n. 179/2012, così come modificato dall'art. 11, d.l. n. 34/2020)[13].

C'è poi il profilo territoriale della questione, dal momento che «il FSE è istituito dalle regioni» ai sensi del già richiamato art. 12, 1° co., d.l. n. 179/2012. Va subito evidenziata la difficoltà delle regioni nel dare attuazione al disposto normativo, tant'è vero che solo nel triennio 2017-2019 sono cresciute del 90% le regioni che hanno attivato il Fascicolo Sanitario Elettronico[14]. Oggi, finalmente, è possibile registrare il dato positivo dell'attivazione di questo documento da parte di tutti gli enti sub-statali regionali (la regione Trentino-Alto Adige è stata scorporata nelle due province autonome di Trento e Bolzano), per cui si può dire che in ogni regione italiana vi è almeno un FSE attivato[15]!

Le difficoltà a livello regionale sono, però, ulteriormente dimostrate dagli altri dati relativi ai medici e alle aziende sanitarie che operano sui territori[16]. In particolare, relativamente alla categoria dei "medici" il riferimento è ai medici di medicina generale (MMG) e ai pediatri di libera scelta (PLS) che hanno utilizzato il FSE, mentre per la categoria delle aziende sanitarie il richiamo è al numero degli operatori sanitari abilitati al FSE all'interno di una azienda[17].

---

[12] Il FSE favorisce quanto sottolineato da L. CALIFANO, *Fascicolo sanitario elettronico (Fse) e dossier sanitario*, cit., 7, quando afferma che al fine di una piena effettività del diritto alla salute «è unanimemente riconosciuta la necessità di una sempre più fluida veicolazione delle conoscenze mediche: e con essa la necessità che anche i dati clinici e sanitari raggiungano un certo grado di facilità di circolazione». Sempre sui vantaggi del FSE è chiaro S. CORONATO, *op. cit.*, 171 ss.; cfr., ancora, G. COMANDÈ, L. NOCCO, V. PEIGNÈ, *Il Fascicolo Sanitario Elettronico: uno studio multidisciplinare*, in *Rivista Italiana di Medicina Legale*, 1, 2012, 112 ss. Infine, sulle finalità del Fascicolo Sanitario Elettronico, cfr. N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *federalismi.it*, 26, 2021, 197 ss.

[13] A.M. GAMBINO, E. MAGGIO, V. OCCORSIO, *La riforma del Fascicolo Sanitario Elettronico*, in *Diritto Mercato Tecnologia*, 22 luglio 2020, 5, evidenziano le novità introdotte dal decreto-legge n. 34/2020, dal momento che «l'impostazione adottata è quella di implementare – finalmente – in modo sostanziale lo strumento del FSE, che rischiava, […], di rimanere "lettera morta" fin tanto che in esso non fosse effettuato un invio massivo di dati».

[14] V. tutti i dati pubblicati dall'Agenzia per l'Italia Digitale (AGID), in https://www.agid.gov.it/it/argomenti/fascicolo-sanitario-elettronico.

[15] Cfr. Fascicolo Sanitario Elettronico, in *https://www.fascicolosanitario.gov.it/it*. In termini generali, cfr. V. ASSADI, K. HASSANEIN, *Consumer Adoption of Personal Health Record Systems: A Self-Determination Theory Perspective*, in *Journal of Medical Internet Research*, 19, 2017, 1 ss., sul rapporto tra paziente e documentazione sanitaria personale.

[16] Al momento in cui si licenzia il contributo, il sito ufficiale dell'AGID non ha pubblicato i dati relativi ai cittadini che, sulla base dell'appartenenza regionale, hanno attivato il FSE.

[17] Per queste precisazioni cfr. Fascicolo Sanitario Elettronico – Monitoraggio, in *https://www.fascicolosanitario.gov.it/it/monitoraggio*.

Ebbene, secondo i dati raccolti a livello governativo, per ciò che riguarda i medici abilitati che hanno effettivamente utilizzato il Fascicolo, si registrano dati lusinghieri in metà delle regioni italiane[18], mentre per altre il risultato è sicuramente negativo[19]; più deludente, invece, l'esito riguardante i medici che alimentano il FSE con il Profilo Sanitario Sintetico del paziente[20], in quanto questa categoria di professionisti è attiva a tal fine in meno della metà delle regioni italiane, per di più con dati tra loro disomogenei[21].

Passando ora alle aziende sanitarie i cui operatori sono abilitati al FSE, va detto che diverse regioni presentano numeri confortanti al riguardo[22], a fronte di altre in cui nessun operatore sanitario è abilitato al FSE[23]; infine, per le aziende che alimentano con i propri dati il Fascicolo Sanitario Elettronico, anche in questo caso si registrano regioni con risultati ragguardevoli[24], mentre per altre gli esiti appaiono particolarmente negativi[25].

In ragione dell'insieme di questi risultati, è possibile innanzitutto evidenziare che – dopo le difficoltà iniziali delle regioni nel dare attuazione ai servizi relativi al FSE (es.: servizi per l'accesso dei cittadini, dei MMG/PLS e delle aziende sanitarie) – oggi si registra, in via generale, un buono stato di avanzamento circa la realizzazione del Fascicolo da parte degli enti sub-statali[26]. Per ciò che concerne poi il

[18] È il caso, ad esempio, di Emilia-Romagna, Friuli-Venezia Giulia, Veneto, Puglia, Sicilia, Sardegna, etc., in cui oltre il 50% dei medici abilitati ha effettivamente utilizzato il FSE e in alcune di esse (es.: Sardegna) si è giunti al 100%.

[19] Es.: Liguria, Toscana, Abruzzo (nel 3° trimestre 2021 si registra un lieve miglioramento), Basilicata, Campania, Calabria e provincia autonoma di Bolzano.

[20] Secondo l'art. 3, d.P.C.M. n. 178/2015, «il profilo sanitario sintetico, o "patient summary", è il documento socio-sanitario informatico redatto e aggiornato dal MMG/PLS, che riassume la storia clinica dell'assistito e la sua situazione corrente conosciuta. La finalità del profilo sanitario sintetico è di favorire la continuità di cura, permettendo un rapido inquadramento dell'assistito al momento di un contatto con il SSN. I dati essenziali che compongono il profilo sanitario sintetico sono quelli individuati nel disciplinare tecnico allegato che costituisce parte integrante del presente decreto, di seguito denominato disciplinare tecnico». Per un suo ulteriore approfondimento, cfr. S. CORONATO, *op. cit.*, 171 s.

[21] Es.: Valle d'Aosta, Friuli-Venezia Giulia, Umbria e Sicilia. Per un esame di questi risultati relativi ai medici abilitati che hanno utilizzato il FSE o che lo hanno alimentato, con riferimento a tutte le regioni, v. https://www.fascicolosanitario.gov.it/it/monitoraggio/bm. È importante precisare che i dati sono riferiti al 3° trimestre 2021 o all'ultimo aggiornamento rilevato da ogni singola regione. In particolare, i medici che alimentano il FSE sono in numero tendenzialmente superiore al 50% solo in Valle d'Aosta.

[22] Es.: Lombardia, Toscana e provincia autonoma di Trento raggiungono il 100% degli operatori sanitari abilitati.

[23] Lazio e provincia autonoma di Bolzano.

[24] Es.: Veneto e Toscana con il 100% delle aziende sanitarie, cui fanno subito seguito Emilia-Romagna e Friuli-Venezia Giulia.

[25] Es.: Calabria e provincia di Bolzano. Per un esame di questi risultati relativi agli operatori abilitati al FSE o alle aziende sanitarie che lo alimentano, con riferimento a tutte le regioni, v. https://www.fascicolosanitario.gov.it/monitoraggio/ba. È opportuno precisare, pure in questo caso, che i dati sono riferiti al 3° trimestre 2021 o all'ultimo aggiornamento rilevato da ogni singola regione. In particolare, anche il Molise raggiunge il 100% delle aziende sanitarie che alimentano il FSE, ma tale percentuale riguarda solo il 2° trimestre 2017 e il 2° trimestre 2018 (ultimo dato disponibile). Passando ad una prospettiva comparata, sulla difficoltà negli USA di utilizzo della documentazione sanitaria elettronica da parte di taluni ospedali, v. C.S. KRUSE, C. KRISTOF, B. JONES, E. MITCHELL, A. MARTINEZ, *Barriers to Electronic Health Record Adoption: a Systematic Literature Review*, in *Journal of Medical Systems*, 12, 2016, 251 ss.

[26] Tale dato, sempre con riferimento al 3° trimestre 2021 o all'ultimo aggiornamento rilevato dalle singole regioni, è riportato in https://www.fascicolosanitario.gov.it/it/monitoraggio/a. Per una lettura di questi risultati, v. U. RESTELLI, S. SILVOLA, *Il Fascicolo Sanitario Elettronico in Italia*, in *Sanità Pubblica e Privata*, 2, 2021, 52 ss.

concreto uso del Fascicolo, la scarsa percentuale dei medici abilitati che hanno utilizzato lo stesso FSE si concentra soprattutto al meridione (Abruzzo, Calabria, Campania, ma invero anche la Liguria e la provincia di Bolzano), mentre i dati negativi circa i medici che alimentano il FSE attraverso il Profilo Sanitario Sintetico sono più equamente distribuiti sul territorio nazionale (es.: Lombardia, Piemonte, Lazio, Abruzzo e Campania). Passando poi alle aziende sanitarie, i risultati meno positivi per gli operatori abilitati al FSE riguardano anche in questo caso il Mezzogiorno (es.: Molise, Campania e Calabria), con talune eccezioni collocate nel centro-nord (Liguria, Umbria e Lazio), così come le stesse strutture sanitarie che alimentano di rado con i propri dati il Fascicolo sono tendenzialmente racchiuse nel centro-sud del Paese (es.: Umbria, Campania e Calabria).
Pertanto, a fronte di una ormai abbastanza omogenea attuazione del FSE da parte delle regioni, si registrano dall'altro lato dati differenziati circa il suo concreto utilizzo, per cui, seppure con qualche eccezione[27], appaiono tendenzialmente le regioni meridionali quelle meno sensibili ad impiegare il FSE, sia con riferimento alle aziende sanitarie, sia con riguardo ai professionisti di medicina generale, nonché ai pediatri di libera scelta di questi territori.

2.1 Lo sviluppo del Fascicolo Sanitario Elettronico nel Piano Nazionale di Ripresa e Resilienza (PNRR)

A ulteriore conferma dell'importanza del FSE, va registrata una specifica attenzione su di esso da parte del PNRR. In via preliminare, è utile rilevare che, in seguito alla pandemia da Covid-19, nel PNRR sono state evidenziate le seguenti criticità sanitarie nel Paese: importanti disparità territoriali nell'erogazione dei servizi sanitari; una scarsa sinergia tra assistenza ospedaliera, territoriale e sociale; elevati tempi di attesa per l'erogazione di talune prestazioni sanitarie, con effetti evidenti sul livello di tutela della salute.
A fronte di ciò sono stati previsti due indirizzi di intervento all'interno della Missione 6 in tema di salute: le Reti di prossimità, le strutture intermedie e la telemedicina per l'assistenza sanitaria territoriale (M6C1); l'innovazione, la ricerca e la digitalizzazione del Servizio Sanitario Nazionale (M6C2)[28]. Per la prima linea di intervento si prevede, tra gli altri, il rafforzamento dei servizi domiciliari, con un importante ruolo che può essere svolto dalla telemedicina a favore dei pazienti più anziani (over 65)[29], mentre la seconda linea di intervento si concentra sull'aggiornamento tecnologico e digitale del Paese. A tale ultimo riguardo, gli investimenti sono previsti per rendere più moderno il parco tecnologico e digitale degli Ospedali, poiché si registra un importante grado di obsolescenza delle infrastrutture tecnologiche e digitali dei nostri nosocomi, unitamente all'obiettivo del «rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione»[30].
Nell'ambito di quest'ultimo investimento è disposto il potenziamento del Fascicolo Sanitario Elettronico, che significativamente è valutato dallo stesso PNRR «quale pietra angolare per l'erogazione dei

[27] Tra queste possono annoverarsi la Puglia e la Sicilia che presentano, relativamente ai parametri adottati, risultati, a volte, davvero positivi.
[28] In riferimento alla necessità di implementare le competenze digitali e di sfruttare le tecnologie d'avanguardia, così come emerge dal PNRR, cfr. N. POSTERARO, *op. cit.*, 221 ss., il quale si sofferma in particolare sul FSE nel PNRR.
[29] Sulla telemedicina nel territorio dell'Italia meridionale, cfr. A.L. TARASCO, *La telemedicina per lo sviluppo della sanità del Mezzogiorno: una introduzione giuridica*, in *Rivista giuridica del Mezzogiorno*, 4, 2010, 1387 ss.
[30] Cfr. PNRR, cit., 230.

servizi sanitari digitali e la valorizzazione dei dati clinici nazionali»[31]. Il FSE dovrà svolgere tre diverse funzioni: «punto di accesso per le persone e pazienti per la fruizione di servizi essenziali forniti dal SSN»; «base dati per i professionisti sanitari contenente informazioni cliniche omogenee che includeranno l'intera storia clinica del paziente»; «strumento per le ASL che potranno utilizzare le informazioni cliniche del FSE per effettuare analisi di dati clinici e migliorare la prestazione dei servizi sanitari». Il fine, dunque, è quello di mettere meglio a fuoco e di implementare le funzioni già previste a carico del Fascicolo. In questo modo si punta all'integrazione di tutti i documenti sanitari del paziente, così da favorirne la ricostruzione della storia clinica, e, nello stesso tempo, si mira all'integrazione «dei documenti da parte delle regioni all'interno del FSE» e al loro supporto finanziario, almeno per quelle che adotteranno la piattaforma FSE[32].

È utile altresì ricordare come il PNRR – nella Missione 1 (Digitalizzazione, innovazione, competitività, cultura e turismo), con la Componente relativa alla Digitalizzazione, innovazione e sicurezza nella P.A. (M1C1) – preveda un investimento teso a favorire la interoperabilità dei dati e la nascita della Piattaforma Nazionale Dati[33]. Ciò è importante anche nell'ottica del Fascicolo Sanitario Elettronico in vista dell'obiettivo dell'interoperabilità dei FSE regionali. L'art. 12, comma 15-ter, d.l. n. 179/2012 (introdotto dalla l. n. 232/2016) prevede che l'Agenzia per l'Italia digitale curi, in accordo con il MEF e il Ministero della salute, «la progettazione dell'Infrastruttura Nazionale necessaria a garantire l'Interoperabilità dei FSE»; si tratta cioè dell'INI, con il compito per l'appunto di provvedere al dialogo tra i FSE regionali.

Tale possibilità di interazione tra sistemi informativi[34] è funzionale agli obiettivi del FSE, cioè di prevenzione, diagnosi, cura e riabilitazione, di studio e ricerca scientifica, oltre che di programmazione e di valutazione dell'assistenza sanitaria (art. 12, 2° co., d.l. n. 179/2012). In particolare, con riferimento alla finalità di cura, appare sicuramente necessario che i diversi sistemi regionali dialoghino tra di loro quando, ad esempio, un paziente emigri per «essere curato in una Regione diversa da quella di assistenza»[35], o addirittura sia costretto ad andare fuori dal territorio del proprio Paese, rendendo utile in questo caso il dialogo tra i diversi sistemi nazionali, sempre al fine di migliorare la prestazione sanitaria a favore dell'interessato. La stessa UE, infatti, ha predisposto il «Quadro europeo di interoperabilità» nella prospettiva di una Pubblica Amministrazione capace di fornire alle imprese e ai cittadini a livello nazionale e dell'Unione «servizi pubblici digitali chiave, interoperabili e incentrati sull'utente […], favorendo la libera circolazione delle merci, delle persone, dei servizi e dei dati in tutta l'Unione»[36]. In questo quadro, certamente, va richiamato il formato europeo di scambio delle cartelle cliniche elettroniche voluto da Bruxelles, di cui si tratterà a breve.

[31] Cfr. PNRR, cit., 17.

[32] Questo sottoparagrafo ricostruisce quanto riportato dal PNRR sulla Missione 6 Salute, per cui, anche con riferimento alle citazioni testuali, cfr. PNRR, cit., 222 ss., in particolare 230 s.

[33] Cfr., ancora, PNRR, cit., 89.

[34] Ai sensi dell'art. 1, 1° co., lett. dd), d.lgs. n. 82/2005 (Codice dell'amministrazione digitale), infatti, per interoperabilità deve intendersi «la caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi».

[35] Cfr. N. POSTERARO, *op. cit.*, 206, il quale precisa che l'emigrazione sanitaria è una «ipotesi non remota, nel nostro Paese, stando ai dati registrati sulla (sempre crescente) mobilità sanitaria interregionale».

[36] Comunicazione della Commissione, 23 marzo 2017, COM (2017) 134 final.

Il compito dell'Infrastruttura Nazionale per l'Interoperabilità (INI), come si è detto, è quello di dialogare con i sistemi regionali di FSE «al fine di collezionare, richiedere e trasmettere dati e documenti sanitari attraverso *modalità sicure* (corsivo nostro) e nel rispetto dei consensi stabiliti dagli assistiti»[37]. Da tale precisazione riportata nel portale ufficiale del Fascicolo Sanitario Elettronico emerge sicuramente il rischio per la privacy delle persone che può sorgere da un'ampia trasmissione di dati e di documentazione sanitaria, il che rende ancora più necessaria la normativa a tutela dei dati di salute[38].
In ogni caso, la volontà che si palesa dal PNRR di potenziare il Fascicolo Sanitario Elettronico, anche per il profilo dell'interoperabilità dei FSE regionali, è l'indicazione di un Piano ambizioso da parte del Governo per sfruttare in modo appropriato, sotto il versante sanitario, le risorse destinate all'Italia dal *Next Generation EU*. Il Piano richiederà una più fattiva collaborazione delle regioni, con tempi ben diversi da quelli impiegati per l'attuazione del FSE, che ha visto solo nel triennio 2017-2019 una sua importante accelerazione, cioè diverso tempo dopo il 2012, anno in cui lo stesso Fascicolo è stato previsto dal legislatore statale. Al contempo, sarà necessario superare le resistenze all'innovazione digitale in sanità, non a caso, sempre il PNRR prevede un opportuno investimento per lo sviluppo delle competenze tecniche, professionali e digitali degli operatori sanitari, così che i dati prima illustrati circa l'effettivo uso del FSE da parte di medici e aziende sanitarie possano concretamente migliorare.

3. La Cartella Clinica Elettronica (CCE): contenuto e caratteristiche

La Cartella Clinica Elettronica (CCE) è «un documento digitale, ossia la trasposizione digitale dei moduli cartacei che si adoperavano e, in molti casi ancora si utilizzano, per documentare le attività svolte nei reparti o negli ambulatori»[39]. La CCE permette di raccogliere tutte le informazioni relative alle indagini e alle visite mediche di un paziente effettuate dalla struttura sanitaria che lo ospita come degente, così da permettere al personale competente di accedere a questa documentazione.

---

[37] Cfr. il Fascicolo Sanitario Elettronico – Servizi di interoperabilità, in https://www.fascicolosanitario.gov.it/it/servizi-di-interoperabilit%C3%A0. Sull'INI è necessario ricordare la Circolare AgID n. 4/2017, cioè il «Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12, comma 15-ter – D.L. 179/2012)», così come il decreto del MEF (4 agosto 2017) sulle «Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)». Infine, in tema di interoperabilità tra sanità regionale e SSN, cfr. A.M. GAMBINO, E. MAGGIO, V. OCCORSIO, *op. cit.*, 10 ss.

[38] Tuttavia, A. PIOGGIA, *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. CAVALLO PERIN (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021, 221 ss., evidenzia non solo il rischio per la riservatezza delle persone, ma anche la possibilità, questa volta in termini positivi, «dei sistemi sanitari nazionali di interloquire da una posizione di minore debolezza con le grandi forze del mercato […] [come] Big Pharma. Soltanto sistemi pubblici che conoscono se stessi e la propria utenza effettiva e potenziale possono sperare di rapportarsi con le multinazionali farmaceutiche senza esserne sopraffatti».

[39] Cfr. Agenda Digitale, in https://www.agendadigitale.eu/sanita/cartella-clinica-elettronica-serve-una-riprogettazione/. Per C. INGENITO, *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, in *federalismi.it*, 5, 2021, 76, «la cartella clinica è, secondo il Ministero della Sanità, "il chi, cosa, quando e come dell'assistenza al paziente nel corso dell'ospedalizzazione, strumento informativo individuale, finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative, relative ad un paziente e ad un singolo episodio di ricovero"». Ancora sulla cartella clinica, v. F. FRÈ, *La cartella clinica nel sistema sanitario italiano*, in *Ragiusan*, 291-292, 2008, 352 ss.

Uno dei primi riferimenti normativi riguardanti la CCE si rinviene nell'art. 47-bis, 1° co., d.l. n. 5/2012, laddove si afferma che

> «nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, nei piani di sanità nazionali e regionali si privilegia la gestione elettronica delle pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica, così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini con la finalità di ottenere vantaggi in termini di accessibilità e contenimento dei costi».

Con l'art. 13, 5° co., d.l. n. 179/2012, è stato poi aggiunto il comma 1-bis al suddetto art. 47-bis, per cui «a decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche può essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche *solo* (corsivo nostro) in forma digitale».
Tali disposizioni normative di rango primario hanno, pertanto, segnato il passaggio dall'ordinaria cartella clinica cartacea alla corrispondente documentazione in formato digitale, evidenziandone subito i vantaggi in termini di accessibilità e contenimento dei costi, ai sensi dell'art. 47-bis, 1° co.
Per ciò che concerne il contenuto di una cartella clinica è necessario prestare attenzione, rispettivamente, al d.m. della Sanità 5 agosto 1977 «Determinazione dei requisiti sulle case di cura private», al d.P.C.M. 27 giugno 1986 «Atto di indirizzo e coordinamento dell'attività amministrativa delle regioni in materia di requisiti delle case di cure private» e alla Circolare del Ministero della Sanità, 14 marzo 1996, n. 900.2/2.7/1990. In particolare, all'art. 24, d.m. della Sanità 5 agosto 1977, si stabilisce che per ogni ricoverato si deve procedere alla «compilazione della cartella clinica, da cui risultino le generalità complete, la diagnosi di entrata, l'anamnesi familiare e personale, l'esame obiettivo, gli esami di laboratorio e specialistici, la diagnosi, la terapia, gli esiti e i postumi»[40].
Non di meno, è utile riportare quanto disposto pure dall'art. 26 del Codice di Deontologia Medica, secondo cui

> «il medico redige la cartella clinica, quale documento essenziale dell'evento ricovero, con completezza, chiarezza e diligenza e ne tutela la riservatezza; le eventuali correzioni vanno motivate e sottoscritte. Il medico riporta nella cartella clinica i dati anamnestici e quelli obiettivi relativi alla condizione clinica e alle attività diagnostico-terapeutiche a tal fine praticate; registra il decorso clinico assistenziale nel suo

[40] Circa il profilo problematico relativo alla natura giuridica della cartella clinica, secondo C. SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy*, in R. FERRARA (a cura di), *Trattato di biodiritto*, diretto da S. RODOTÀ, P. ZATTI, Milano, 2010, 586, «la giurisprudenza [citata dall'A. e a cui si rinvia] è abbastanza concorde nel classificare la cartella clinica come un atto pubblico, e ciò in ragione del fatto che essa è "esplicazione di potere certificativo e partecipe della natura pubblica dell'attività sanitaria cui si riferisce"». Invece, per F. BUZZI, C. SCLAVI, *La cartella clinica: atto pubblico, scrittura privata, o "tertium genus"?,* in *Rivista Italiana di Medicina Legale*, 1997, 1182 ss., la cartella clinica può essere classificata «come un "*tertium genus*", collocandosi in una posizione intermedia tra la scrittura privata e l'atto pubblico ed essendo ragionevolmente assimilabile ad una "certificazione amministrativa"»; infatti, «essendo […] la cartella formata in momenti assistenziali diversi […] e per di più da operatori con ruoli professionali, cultura e competenze assai differenti, né essendovi alcun obbligo normativo di un'individuale sottoscrizione delle annotazioni apportate da costoro, non può che scaturirne un atto dai requisiti formali e sostanziali molto lontani da quelli che l'atto pubblico deve possedere ai sensi degli artt. 2699 e 2700 c.c.».

contestuale manifestarsi o nell'eventuale pianificazione anticipata delle cure nel caso di paziente con malattia progressiva, garantendo la tracciabilità della sua redazione» [41].

Al contenuto tipico di una cartella clinica si devono aggiungere, nel caso di specie, le caratteristiche che deve avere questo tipo di documento informatizzato. È necessario, infatti, che lo stesso contenuto sia «organizzato come base per ogni successiva elaborazione e per garantire un adeguato livello di qualità», per cui sono utili «un insieme minimo di dati concordato», «un dizionario di dati comune predefinito», i «sistemi di codifica condivisi e il loro formato standard», così egualmente è opportuno «riportare le informazioni sull'esito delle terapie e sullo stato del paziente»[42].

Sempre nell'ottica della digitalizzazione di questo documento, è importante che il sistema di gestione delle cartelle cliniche permetta la connessione con altri sistemi, così da favorire lo scambio di informazioni, il collegamento con registri istituzionali e, se opportuno, anche con cartelle cliniche di familiari, naturalmente nel rispetto delle regole della privacy[43].

Da quanto ora brevemente illustrato appare subito evidente la differenza tra la CCE e il FSE, in quanto, mentre quest'ultimo è funzionale a rappresentare la storia clinica di una persona, per cui raccoglie le informazioni sanitarie che provengono da ospedali, ambulatori, studi medici, etc., lungo l'intera vita dell'assistito, al contrario la CCE è un documento digitale predisposto dalla singola struttura sanitaria presso la quale è in cura un paziente in un determinato momento della sua vita[44]. Ne consegue che la Cartella Clinica Elettronica è parte integrante del più ampio Fascicolo Sanitario Elettronico.

I vantaggi della CCE sono altrettanto evidenti, a partire dalla "dematerializzazione" del documento, poiché è necessario seguire un processo digitale di creazione e poi di gestione della cartella elettronica, per cui tutto ciò che la riguarda ha un carattere informatico. In questo modo si migliora la qualità del servizio offerto al paziente e si contribuisce a ridurne i costi[45], conformemente a quanto richiesto

[41] Per tali riferimenti normativi, cfr. P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, Trento, 2011, 150 s., e C. SARTORETTI, *op. cit.*, 583 s., la quale precisa altresì che «la compresenza all'interno della cartella clinica di informazioni anagrafiche (c.d. "dati comuni") e di dati riguardanti le condizioni di salute (c.d. "dati sensibili") di un individuo fa di questo atto il documento sanitario contenente il maggior numero di informazioni personali» (in particolare p. 579), da cui poi si ricava, come si vedrà a breve, il profilo problematico della gestione dei dati.

[42] Cfr. G. CIPRIANO, *La cartella clinica digitale*, in *Il Diritto sanitario moderno*, 1, 2008, 19 s., secondo cui è necessario prestare attenzione anche alle «prestazioni del sistema», nel senso di garantire un'agevole immissione di dati, un loro rapido recupero e una disponibilità della cartella clinica in ogni momento della giornata. Come evidenzia P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, cit., 153 s., diversa, rispetto a quanto si sta trattando, è la cartella infermieristica (art. 69, d.P.R. n. 384/1990), poiché si tratta di uno strumento «volto a contenere la registrazione dei dati e l'insieme dei documenti di pertinenza infermieristica sul caso oggetto di cura. Essa svolge anche funzioni di certificazione ed organizzazione di tutto il patrimonio informativo e delle attività assistenziali della persona, raccolte e/o eseguite dall'infermiere […]. Il nucleo centrale è caratterizzato dal piano di assistenza personalizzato».

[43] Cfr. G. CIPRIANO, *op. cit.*, 20.

[44] Sulla differenza tra il FSE e la CCE, v. N. POSTERARO, *op. cit.*, 194 ss., che si occupa anche della "dematerializzazione" delle ricette mediche.

[45] Cfr. S. CORONATO, *op. cit.*, 181 s. Il Gruppo di Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, 15 febbraio 2007, ha avuto modo di sostenere che «i sistemi di CCE possono assicurare maggiore qualità e sicurezza dell'informazione medica di quanto consentano le forme tradizionali di documentazione. Tuttavia, parlando della tutela dei dati, va sottolineato che i sistemi di CCE danno la possibilità non solo di trattare una quantità maggiore di informazioni di natura personale

dall'art. 47-bis, 1° co., d.l. n. 5/2012. Oltre alla "dematerializzazione" del documento, un ulteriore vantaggio della CCE è rappresentato dall'eliminazione del problema relativo alla sicurezza degli archivi tesi a custodire le informazioni sanitarie, poiché la digitalizzazione della cartella clinica evita il suo materiale deposito presso un luogo di quel tipo, così da scongiurare ogni pericolo legato ad eventi naturali o umani (incendi, alluvioni, etc.) che possano danneggiare o distruggere quest'importante documento sanitario, a favore invece di un archivio digitale. Allo stesso tempo va ricordata la possibilità di condividere la CCE con i medici specialisti e di famiglia, il che evita l'inutile ripetizione di analisi di laboratorio o di indagini cliniche, con evidenti vantaggi sia per la salute del paziente, sotto il profilo della rapidità di informazione per il medico, sia per il Servizio sanitario, sotto il versante del risparmio delle spese. Infine, la completezza delle informazioni presenti all'interno della CCE favorisce, anche in tal senso, la prestazione professionale del medico a beneficio del paziente[46].

Un ulteriore vantaggio della CCE è rappresentato dalla possibilità, già prima richiamata, della c.d. interconnessione tra i sistemi, tant'è vero che la Raccomandazione UE 2019/243 (6 febbraio 2019), relativa ad un formato europeo di scambio delle CCE, prevede tra i suoi obiettivi proprio «lo sviluppo di un formato europeo di scambio delle cartelle cliniche elettroniche al fine di consentire che, nell'Unione, i dati sanitari elettronici siano accessibili e scambiabili in maniera sicura, interoperabile e transfrontaliera». Si vuole, cioè, semplificare la vita dei cittadini in una serie di situazioni, giacché «ogni anno si registrano oltre due milioni di casi in cui un cittadino residente in uno Stato membro richiede assistenza sanitaria in un altro» (*considerando* 3). È ovvio che tutto ciò, predisposto tempestivamente, sarebbe stato di sicuro molto utile, già solo sotto il profilo informativo, nel fronteggiare in sede UE l'attuale stato pandemico[47]. Tuttavia, «le notevoli disparità nell'approccio seguito dai diversi paesi per

(ad es. in nuovi contesti o per aggregazione), ma anche di rendere i dati del paziente più facilmente disponibili ad una cerchia di destinatari più ampia di prima». Recentemente, la Commissione Europea, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*, 25 aprile 2018, ha affermato che, a fronte del costante aumento della spesa pubblica in materia di salute nei Paesi UE, «le soluzioni sanitarie e assistenziali digitali possono accrescere il benessere di milioni di cittadini e cambiare radicalmente il modo in cui i servizi sanitari e assistenziali vengono forniti ai pazienti».

[46] Cfr. G. CIPRIANO, *op. cit.*, 17 s., secondo cui gli studi degli «ultimi 30 anni hanno evidenziato, con dati quantitativi, che spesso la cartella clinica cartacea non è disponibile durante la visita (fino al 30% delle visite), e che per esempio gli esami di laboratorio vengono molte volte ripetuti perché i risultati non vengono resi disponibili al medico in modo tempestivo. Quando le cartelle sono disponibili, spesso alcuni dati essenziali non sono presenti. Ad esempio, in uno studio sui medici di medicina generale è stato riscontrato che l'età del paziente mancava nel 10% dei casi, che i farmaci non erano trascritti nel 30%, che la diagnosi mancava nel 40%».

[47] Tale Raccomandazione è in linea con la Commissione Europea, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*, cit., che un anno prima sosteneva la possibilità da parte dei cittadini europei di «poter godere di un accesso sicuro ad un registro elettronico completo dei propri dati sanitari ovunque si trovino nell'UE», sempre nel rispetto della disciplina relativa alla protezione dei dati. Sulla Raccomandazione UE 2019/243 del 6 febbraio 2019 v. C. INGENITO, *op. cit.*, 87 ss., la quale richiama anche l'utilità dello scambio delle CCE a livello europeo per affrontare la diffusione del virus. M. FERRARA, *op. cit.*, 33 ss., sottolinea la scelta per «un atto di soft law come la raccomandazione» al fine di regolare in modo unitario in sede UE un formato di cartella sanitaria, con il vantaggio per cui «ovunque il malato si trovi in Europa […] le informazioni passate e presenti sulla sua vita clinica sono destinate […] a confluire nella cartella sanitaria elettronica». Può essere opportuno ricordare come nel settembre 2020 (con durata di 24 mesi) sia partito «X-eHealth (*eXchanging electronic Health Records in a common framework*)», cioè «un progetto di rilevanza strategica per l'Unione europea che mira a sviluppare un framework condiviso per un formato di scambio di cartelle cliniche

sviluppare un sistema [integrato] di cartelle» hanno rappresentato un ostacolo importante alla realizzazione dell'obiettivo enunciato di implementare un formato europeo di scambio di CCE[48].

4. Il trattamento dei dati in materia sanitaria alla luce del Regolamento UE 2016/679

I contenuti e le caratteristiche del Fascicolo Sanitario Elettronico e della Cartella Clinica Elettronica svelano la gran quantità di informazioni che questa documentazione è in grado di veicolare, con evidenti ripercussioni sulla questione del trattamento dei dati in ambito sanitario.

Sotto il profilo normativo, è utile richiamare innanzitutto il Regolamento UE 2016/679 (da ora in poi anche GDPR), divenuto applicabile, com'è noto, dal 25 maggio 2018, il quale sancisce, all'art. 1, par. 2, il diritto alla tutela dei dati personali quale diritto fondamentale dell'individuo, in ossequio a quanto stabilito dall'art. 8 Carta di Nizza, per cui «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». Questa situazione soggettiva si concretizza, in particolare, nel diritto della persona, cui i dati si riferiscono, di esercitare un controllo su di essi[49]. In tale contesto è possibile il richiamo alla privacy, a condizione di intendere la tutela della riservatezza anche come diritto di ognuno a vedersi garantito il controllo sui propri dati, così da configurarsi un potere di autodeterminazione informativa[50]; se, invece, la privacy è interpretata unicamente nella sua accezione più tradizionale, cioè come libertà negativa di non subire indebite intrusioni nella sfera privata, allora la riservatezza – così staticamente intesa – non sarebbe in grado di accogliere l'esigenza, oggi molto avvertita, di proteggere e trattare i dati personali dinanzi alla possibilità di una loro circolazione. Del resto, anche a livello di Unione europea, mentre il diritto di tutelare i propri dati si richiama al già citato art. 8 della Carta di Nizza, al contrario la privacy, nella visione statica, si collega più direttamente all'art. 7 della medesima Carta, laddove è stabilito che ogni persona ha diritto al rispetto della propria vita privata e familiare, del domicilio e delle sue comunicazioni[51]. Non di meno, alla base del Regol. UE è da registrare

elettroniche, interoperabile, sicuro e transfrontaliero, al fine di gettare le basi per il progresso del settore dell'eHealth», in https://www.fascicolosanitario.gov.it/it/progetto-x-ehealth.

[48] In tal senso, cfr. ancora C. INGENITO, *op. cit.*, 94. Sempre la Raccomandazione UE 2019/243 precisa gli elementi costitutivi per un formato europeo di scambio delle cartelle cliniche elettroniche: profilo sanitario sintetico; prescrizioni/dispensazioni elettroniche; risultati di laboratorio; diagnostica per immagini e referti; lettere di dimissione ospedaliera.

[49] Così G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Id. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 5 ss., la quale precisa che il diritto in questione si estende dall'accesso alla rettifica dei dati.

[50] Tant'è vero che secondo C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, 2017, 100, «la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati». Sul modello di privacy proposto dal Regolamento UE, v. S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 3 ss.

[51] Sul punto è chiaro L. CHIEFFI, *op. cit.*, 21 s., quando sostiene che il Regolamento UE «consolida una interpretazione della riservatezza dell'individuo, […], che non potrebbe "più esaurirsi in uno *status* negativo, nel solo potere cioè di escludere le intromissioni non consentite", ma che si estende al riconoscimento in capo al soggetto sottoposto al trattamento di "conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano" […]. Da una protezione *statica* di questo diritto da interferenze provenienti dall'esterno, espressione di una pretesa di essere lasciati soli con sé stessi (*a right to be alone*), […], si è giunti progressivamente, […], ad

anche l'art. 16, par. 2, TFUE, secondo cui il Parlamento europeo e il Consiglio «stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale […] e le norme relative alla libera circolazione di tali dati»; in questo modo emerge chiaramente il compito dell'Unione di garantire il diritto alla protezione dei dati personali[52].

Con specifico riferimento ai dati di salute, è lo stesso GDPR, all'art. 4, par. 1, ad offrirne una definizione, cioè di «dati personali attinenti alla salute fisica o mentale di una persona […], compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». Tale ampia formula definitoria, da un lato, risponde ad una indispensabile esigenza di elasticità del dettato normativo, così da essere interpretativamente capiente sul tema rispetto al rapido incedere del processo digitale[53], ma dall'altro rende sempre più evidente la necessità di ogni persona – proprio a fronte di questa ampia formulazione – di controllare i propri dati personali, in particolare quelli di salute[54].

Nell'ambito dell'obiettivo perseguito da Bruxelles di uniformare la disciplina sull'intero territorio UE, il GDPR introduce quali principi generali applicabili al trattamento dei dati personali quelli di liceità,

un approccio di tipo *dinamico*, agevolato da una maggiore circolazione dei dati personali attraverso il ricorso alla comunicazione elettronica». Sulla «pluralità contenutistica» della riservatezza, cfr. G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, 2006, 632 s.; v., pure, L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., 3 ss. O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *federalismi.it-focus TMT*, 3, 2014, 3, con riferimento alla giurisprudenza della CGUE, sostiene che i giudici di Lussemburgo ricavano un diritto alla privacy digitale «fondandolo sulle due colonne portanti costituite dai diritti al rispetto della vita privata ed al trattamento dei propri dati personali, previsti, rispettivamente, dagli artt. 7 ed 8 della Carta dei diritti fondamentali dell'Unione europea». Per la giurisprudenza della Corte di Lussemburgo relativa alla sfera privata dell'interessato, *ex multis*, CGUE, causa C-203/15, 21 dicembre 2016, c.d. sentenza *Tele2 Sverige* (in tema di conservazione dei dati); CGUE, causa C-362/14, 6 ottobre 2015; CGUE, causa C-131/12, 13 maggio 2014, c.d. sentenza *Google Spain* (diritto di rimuovere informazioni personali). Su quest'ultima decisione, v., ancora, O. POLLICINO, *op. cit.*, 14 s., così come cfr. T.E. FROSINI, *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, 4-5, 2014, 563 ss. Infine, cfr. M. BRKAN, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, in *German Law Journal*, 20, 2019, 864 ss.

[52] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 8 s., richiama anche il *considerando* 11 del GDPR, laddove si afferma che «un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali». Ciò giustifica, a giudizio dell'A., il ricorso allo strumento normativo del Regolamento UE. Ancora sulla riservatezza, v. M. FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus Civile*, 1, 2021, 5 ss.

[53] Cfr. C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., 101 s.; v. anche G. CIACCI, *Problemi e iniziative in tema di tutela dei dati personali*, in *Politica del diritto*, 4, 1991, 688 ss. In proposito, L. CHIEFFI, *op. cit.*, 11, sottolinea come il GDPR arrivi a fissare una definizione molto estesa del dato sanitario «che abbraccia qualunque notizia che abbia uno stretto legame con l'integrità psico-fisica dell'interessato».

[54] Per S. SICA, *op. cit.*, 5, si tratta di «una nozione di dato personale persino al limite della genericità», ma, in realtà, l'opzione è «convincente: poche materie come questa necessitano di un difficile *mix* tra definizioni legislative "elastiche" e, ove occorra, di interventi regolamentari di dettaglio».

correttezza, trasparenza e sicurezza (art. 5, par. 1, lett. a) e f)[55]. In particolare, il trattamento può considerarsi lecito solo se ricorrono le condizioni previste dal successivo art. 6, tra cui ad esempio il consenso dell'interessato in relazione a «una o più specifiche finalità» del trattamento (art. 6, par. 1, lett. a), o quelle previste dall'art. 9, par. 2, relative a taluni trattamenti su particolari categorie di dati personali, tra cui ovviamente quelli di salute. Allo stesso tempo, il trattamento deve essere, da un lato, trasparente, nel senso che l'interessato va informato sulle operazioni che riguardano i suoi dati personali, dall'altro responsabile, in quanto è compito del titolare del trattamento rispettare tali principi che sono alla base della gestione dei dati personali (art. 5, par. 2)[56]. Tale ultimo principio di responsabilizzazione (c.d. *accountability*) rappresenta uno degli elementi di maggiore novità del Regolamento UE, segnando un mutamento di indirizzo rispetto al passato, in quanto si esige un atteggiamento di forte responsabilità a carico delle aziende e della pubblica amministrazione in qualità di titolari del trattamento dei dati, dal momento che nell'ottica del GDPR è fondamentale la prevenzione del danno, ancor prima della sua riparazione[57].

Tra gli ulteriori principi applicabili al trattamento dei dati personali vi è quello relativo alla loro sicurezza (art. 5, par. 1, lett. f, GDPR). Il Regolamento continua, infatti, sancendo all'art. 9, par. 1, il generale divieto

> «di trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [di] trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Naturalmente, ai fini del presente contributo sono importanti soprattutto i «dati relativi alla salute»[58], per i quali sono previste talune eccezioni rispetto al principio del divieto. Quanto disposto dall'art. 9,

[55] Cfr. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, Milano, 2018, 49 ss.

[56] Per un commento sui principi dell'art. 5 GDPR, v. S. SCAGLIARINI, *La tutela della* privacy *e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta online*, 2, 2021, 577 s. Cfr., altresì, G. CASSANO, V. COLAROCCO, G.B. GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR*, Milano, 2018, 29 ss. È ascrivibile, poi, al principio di trasparenza quanto stabilito dal Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, provvedimento n. 55, 7 marzo 2019, nel momento in cui sostiene che i titolari del trattamento impegnati ad effettuare nel settore sanitario una pluralità di operazioni complesse (es.: aziende sanitarie) debbano fornire all'interessato «in modo progressivo» le informazioni previste dal Regol. UE, nel senso che la generalità dei pazienti potrebbero essere informati solo relativamente «ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie», mentre per particolari attività di trattamento potrebbero essere informati, «in un secondo momento, solo i pazienti effettivamente interessati da tali servizi».

[57] Cfr. B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *dirittifondamentali.it*, 2, 2020, 353 s., che evidenzia, come obiettivo della nuova normativa, «il radicale mutamento di prospettiva, il passaggio da un approccio fondato sulla riparazione del danno (*ex post*) a uno basato sulla prevenzione dello stesso (mediante una valutazione *ex ante* della rischiosità del trattamento)». Cfr., anche, M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Responsabilità civile e previdenza*, 4, 2020, 1352 ss., e AA.VV., *Privacy e dati personali*, Milano, 2018, 65 ss.

[58] Secondo il *considerando* 35 del GDPR nei dati di salute rientrano «tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso […] le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza

par. 1, GDPR, non si applica nel momento in cui «l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche» (art. 9, par. 2, lett. a), o ancora quando «il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, […], diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri» (art. 9, par. 2, lett. h); in quest'ultimo caso, però, il principio del divieto non vale a condizione che i dati siano «trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale» (art. 9, par. 3). La funzione della deroga che permette il trattamento di questi dati è finalizzata alla tutela della salute delle persone e dell'intera società (cons. 53), con la possibilità, tuttavia, per gli Stati membri di mantenere o introdurre eventualmente ulteriori condizioni (art. 9, par. 4).

Egualmente, non si applica il divieto dell'art. 9, par. 1, GDPR, nel caso in cui il trattamento sia

> «necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri»

(art. 9, par. 2, lett. i)[59]. Tale disposizione, soprattutto nella sua prima parte, appare sicuramente appropriata al contesto pandemico che stiamo vivendo, il che dovrebbe ulteriormente sollecitare, pure sotto questo profilo, la realizzazione del formato europeo di scambio delle cartelle cliniche elettroniche[60].

In tale contesto normativo un ruolo fondamentale in termini di responsabilità, a seguito del GDPR, è stato assegnato ai titolari del trattamento dei dati, tanto nel settore pubblico quanto in quello privato, nel senso che dovranno dimostrare di avere adottato tutte le misure necessarie per l'applicazione del Regolamento UE. Il compito dei titolari del trattamento è indirizzato a valutare con ponderazione tutti

organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro». S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 105, qualifica i dati di salute come informazioni che esprimono da sé un bisogno di segretezza.

[59] In questo caso, come ricorda P. GUARDA, *I dati sanitari*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 599, il *considerando* 54 del GDPR stabilisce che il trattamento di categorie particolari di dati personali, necessario per motivi di interesse pubblico nell'ambito della sanità pubblica, non richiede il consenso dell'interessato.

[60] Un'ulteriore ipotesi di eccezione al divieto è prevista all'art. 9, par. 2, lett. g), quando cioè «il trattamento è necessario per motivi di *interesse pubblico rilevante* (corsivo nostro) sulla base del diritto dell'Unione o degli Stati membri». Tra le ipotesi di «rilevante interesse pubblico» – come stabilito in Italia dal Codice della privacy che espressamente richiama la disposizione normativa europea – vi è il caso del trattamento dei dati effettuato «da soggetti che svolgono compiti di interesse pubblico» in talune materie, come, ad esempio, «attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale», o «compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica», o come ancora «vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria» (art. 2-*sexies*, 2° co., Cod. privacy, in particolare si veda dalla lett. t) sino ad aa). Su tutti questi profili dell'art. 9, par. 2, GDPR, cfr. C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, in *dirittifondamentali.it*, 2, 2019, 13 ss.

i rischi legati alla circolazione dei dati e ad «avere una strategia articolata e trasparente» nei riguardi delle persone cui si riferiscono le informazioni. In breve, la disciplina adottata a Bruxelles «ha determinato un totale cambiamento […] [di] approccio […] nella regolamentazione della materia, mediante l'introduzione […] del principio di *accountability*, teso a responsabilizzare i titolari del trattamento nella loro attività di "manipolazione" di dati personali»[61].

Il GDPR riserva un corpo significativo di norme al tema della sicurezza dei dati personali, per cui il titolare e il responsabile del trattamento devono attivare – dopo averle opportunamente individuate – misure tecniche e organizzative funzionali a garantire un livello di sicurezza dei dati adeguato al rischio (art. 32, par. 1, GDPR). Tra queste merita di essere evidenziata la «valutazione d'impatto sulla protezione dei dati», che richiede da parte del titolare, prima di qualunque attività, «una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali» (art. 35 GDPR)[62]; così come è significativa, *ex* art. 42, par. 1, GDPR, l'istituzione «di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al […] regolamento dei trattamenti effettuati dai titolari […] e dai responsabili del trattamento». Non meno importante, come evidenzia pure il Garante per la privacy[63], è la figura del responsabile della protezione dei dati, che è designato dal titolare e dal responsabile del trattamento nei casi di gestione, su larga scala, dei dati personali di cui al già citato art. 9 GDPR, oppure designato quando «le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala», e quando, infine, il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (art. 37, par. 1, GDPR). I compiti affidati al responsabile sono quelli di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, di verificare la corretta attuazione della disciplina relativa alla tutela dei dati personali, di fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e, infine, di cooperare con l'autorità di controllo. Di poi, nell'eseguire i propri compiti il responsabile della protezione dei dati deve valutare i rischi inerenti al trattamento (art. 39, par. 1 e 2 GDPR)[64].

---

[61] Cfr. B. BORRILLO, *op. cit.*, 345 (prima citazione) e 333 (seconda citazione). Allo stesso modo, anche M. D'AGOSTINO PANEBIANCO, *Il trattamento dei dati nel Sistema Sanitario Nazionale italiano alla luce del Provvedimento del Garante del 7 marzo 2019*, in *Ciberspazio e diritto*, 1-2, 2019, 264, sostiene come il titolare del trattamento sia «il primo espressamente chiamato alla "responsabilizzazione" nonché a dimostrare la *compliance* e l'*efficacia* del trattamento». Secondo G. FINOCCHIARO, *op. cit.*, 14 s., il termine *accountability* «può essere tradotto in molti modi diversi, fra i quali: responsabilità, affidabilità, assicurazione, obbligo di rendicontare, attuazione dei principi concernenti il trattamento dei dati personali».

[62] La valutazione d'impatto sulla protezione dei dati, in particolare, è richiesta nei seguenti casi: a) «una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche»; b) «il trattamento, su larga scala, di categorie particolari di dati personali»; c) «la sorveglianza sistematica su larga scala di una zona accessibile al pubblico» (art. 35, par. 3, GDPR).

[63] Difatti, secondo il 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 designazione del responsabile della protezione dei dati agevola il rispetto della relativa disciplina.

[64] Altre previsioni importanti in tema di sicurezza sono, ad esempio, le notifiche a carico del titolare del trattamento ed effettuate all'autorità di controllo nel caso di violazione dei dati personali (art. 33), «l'istituzione di

Insomma, come è stato sottolineato, in forza del principio dell'*accountability* «il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali»[65].

Proprio i titolari del trattamento dei dati, in riferimento al Fascicolo Sanitario Elettronico, dovranno prestare attenzione a quanto sancito per l'Italia dall'art. 12, 5° co., d.l. n. 179/2012, per cui la consultazione dei dati e dei documenti presenti nel FSE, almeno con riguardo alle finalità di prevenzione, diagnosi, cura e riabilitazione, «può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria». In questo senso la disposizione normativa interna sembrerebbe coerente con il principio espresso dal GDPR, *ex* art. 9, par. 1, circa il divieto di carattere generale nel trattare i dati di salute, per cui la documentazione presente nel FSE è consultabile solo a seguito di consenso dell'interessato. È bene precisare, tuttavia, sempre ai sensi del sopra citato art. 12, 5° co., che l'eventuale mancato consenso comunque non pregiudica il diritto del paziente alla prestazione sanitaria, sicché, in questo caso, la persona non sarà costretta a sacrificare le garanzie nel trattamento dei dati a favore della tutela della salute[66].

Per l'altro documento oggetto della presente indagine, cioè la CCE, vale quanto disposto in generale per la cartella clinica dall'art. 92, 2° co., del Codice della privacy (d.lgs. n. 196/2003)[67], secondo cui la richiesta di questo documento da parte di un soggetto diverso dall'interessato può essere accolta solo se è giustificata dalla documentata necessità, da un lato di esercitare un diritto in sede giudiziaria di rango pari a quello dell'interessato (ovvero consistente comunque in un altro diritto o libertà fondamentale), dall'altro di tutelare una situazione giuridicamente rilevante di rango pari a quella dell'interessato (ovvero consistente sempre in un altro diritto o libertà fondamentale)[68].

---

meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al […] regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento» (art. 42) o, ancora, la c.d. protezione dei dati *by design* e *by default* (art. 25). Su questi temi, cfr. P. GUARDA, *I dati sanitari*, cit., 609 ss.; G.M. RICCIO, *Data Protection Officer e altre figure*, e R. D'ORAZIO, *Protezione dei dati by default e by design*, entrambi i contributi in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, cit., 45 ss.; nonché, F. PIZZETTI, *op. cit.*, 106 ss.

[65] Così si esprime G. FINOCCHIARO, *op. cit.*, 14. Nell'ambito del principio di responsabilità rientra anche la previsione dei registri delle attività di trattamento (art. 30 GDPR), che devono essere tenuti dal titolare/responsabile del trattamento. In particolare, per il Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, cit., tale previsione deve considerarsi un obbligo in sede sanitaria. «Ciò in coerenza con la circostanza che il registro delle attività del trattamento costituisce uno strumento di accountability e di gestione del rischio».

[66] Del resto, il Garante per la protezione dei dati personali, già nelle *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*, cit., con riferimento alla libertà di costituzione del FSE sosteneva che l'interessato dovesse godere della prestazione del Servizio Sanitario Nazionale anche nel caso di mancata attivazione del Fascicolo, così da garantire l'effettività di quel potere di scelta.

[67] Il d.lgs. 30 giugno 2003, n. 196, cioè il «Codice in materia di protezione dei dati personali», è stato novellato dal d.lgs. 10 agosto 2018, n. 101, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

[68] Sulla valutazione del pari rango, di cui all'art. 92, 2° co., del Codice, v. C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, cit., 21; cfr., altresì, C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *federalismi.it*, 14, 2020, 77 s.

È evidente che nelle diverse fattispecie normative ora proposte, le disposizioni individuano, ciascuna autonomamente, un bilanciamento tra diritti che eventualmente potrebbero entrare in conflitto, come nel caso ora esposto del diritto alla privacy del paziente e quello alla salute di un terzo, o, come nell'ipotesi particolare del FSE, in cui il consenso richiesto dalla disciplina interna favorisce la «giusta composizione degli interessi contrapposti dell'interessato e del titolare del trattamento […] nel conflitto fra le ragioni della riservatezza e quelle della libertà di essere informati»[69]. La problematica ponderazione tra situazioni giuridiche soggettive eventualmente contrapposte impone, allora, la precisa individuazione di queste fattispecie normative, tenendo comunque conto del principio, *ex* art. 22, 1° co., d.lgs. n. 101/2018, secondo cui le norme interne del Codice della privacy si interpretano e si applicano in funzione di quanto dettato dal Regolamento UE 2016/679[70].

Con riferimento al caso del trattamento necessario dei dati per finalità di cura (GDPR, art. 9, par. 2, lett. h), è utile ribadire, ad esempio, anche in ossequio alle indicazioni del Garante per la privacy, che il professionista sanitario soggetto al segreto professionale «non deve più richiedere il consenso del paziente», a prescindere dalla sua qualifica di libero professionista o di operatore all'interno di una struttura sanitaria pubblica o privata. Tale possibilità di fare a meno del consenso vale comunque solo per i trattamenti necessari per finalità di cura, «cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (cfr. considerando 53 del Regolamento)»[71].

La disciplina europea sembra esprimere un indirizzo diverso rispetto a quella italiana, tesa invece a richiedere il consenso, sempre per finalità di cura, quale condizione di liceità per i trattamenti effettuati attraverso il FSE (art. 12, 5° co., d.l. n. 179/2012). Tale ultima scelta appare comunque legittima in considerazione della facoltà offerta dal GDPR agli Stati membri di «mantenere o introdurre ulteriori condizioni, comprese le limitazioni» (art. 9, par. 4, Reg. UE 2016/679), oltre che, ovviamente, per il generale divieto fissato da Bruxelles nel trattare i dati di salute. Questo non esclude, però, la possibilità di immaginare – come rileva il Garante – «un'eventuale opera di rimeditazione normativa» circa l'indispensabilità del consenso dell'interessato per l'alimentazione dei dati del FSE, in quanto ciò sarebbe «ammissibile alla luce del nuovo quadro giuridico»[72].

[69] In tal modo si esprime, seppure in termini generali, C. SARTORETTI, *op. cit.*, 612.

[70] Anche l'art. 75, Cod. privacy, precisa che «il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafo 2, lettere h) ed i)».

[71] Per queste precisazioni, 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. Si tratta comunque di un'ipotesi derogatoria rispetto al consenso quale condizione di liceità per il trattamento dei dati di salute, secondo l'art. 9, par. 2, lett. a), che consente di superare il generale divieto stabilito nel precedente paragrafo 1. Secondo P. GUARDA, *I dati sanitari*, cit., 615, «ciò si traduce nel fatto che le scelte in ordine a quali informazioni immettere nel sistema, ai livelli di condivisione e alle varie applicazioni che una piattaforma di sanità elettronica permette di amministrare possono essere gestite direttamente dal paziente attraverso lo strumento tecnico-giuridico del consenso».

[72] Cfr., ancora, Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, cit., il quale precisa, altresì, che la richiesta del consenso per il trattamento dei dati presenti nel FSE è prevista non solo dall' art. 12, 5° co., d.l. n. 179/2012, ma anche «dalle disposizioni di settore».

5. Il problematico conflitto tra diritti e il loro bilanciamento

In questo contesto di circolazione delle informazioni è agevole immaginare un possibile conflitto tra diritti, in particolare tra il diritto fondamentale alla salute e quello alla tutela dei dati personali, dal momento che, per un verso, può sussistere l'interesse della persona a comunicare la sua condizione fisica al fine della prestazione sanitaria, ma, dall'altro, la medesima persona può nutrire un naturale sentimento di riserbo sulle proprie informazioni di salute[73]. A ciò, ovviamente, si può aggiungere l'ipotesi del terzo, nel senso del contrasto tra il diritto all'autodeterminazione informativa di un paziente e il diritto alla salute di altro individuo. È poi possibile configurare un ulteriore conflitto tra il valore della trasparenza – che permette «di preservare la libertà dei privati dagli abusi del potere» attraverso le informazioni sull'azione della Pubblica Amministrazione – e sempre la sfera di riservatezza di una persona, nei suoi diversi risvolti, che potrebbe essere coinvolta dalla stessa attività della P.A.[74].
Naturalmente, se vi sarà, come previsto dal PNRR con la Missione 6 sulla salute, una implementazione della sanità digitale, un ammodernamento delle strutture tecnologiche e una auspicabile maggiore diffusione del FSE, le eventualità di conflitto tra i diritti sono evidentemente destinate ad aumentare a fronte di una più rapida e intensa possibilità di diffusione di dati sensibili. Vale la pena ricordare come proprio i dati di salute costituiscano il c.d. «nucleo duro della privacy»[75], non a caso sono tutelati, oltre che dalla normativa già richiamata, cioè gli artt. 7 e 8 della Carta UE dei diritti fondamentali, anche da ulteriori disposizioni internazionali, come l'art. 10 della Convenzione di Oviedo unitamente all'art. 8 CEDU[76]. Si tratta, cioè, di un corpo di norme, tra la vecchia e la recente regolamentazione, che approfondisce «l'interdipendenza tra autodeterminazione fisica e autodeterminazione informativa poste a presidio della libertà e della dignità della persona»[77].
Sotto il profilo della disciplina di rango costituzionale, il diritto alla riservatezza, in tutte le sue implicazioni, è configurato come un nuovo diritto che, com'è noto, non ha un esplicito riconoscimento nella Carta italiana, come invece avviene in altre esperienze comparate[78]. Ciò, però, non pregiudica il c.d.

[73] C. SARTORETTI, *op. cit.*, 582; C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, cit., 7, evidenziano il diritto alla salute e quello alla privacy come «legati da un nesso indissolubile», anche se «tale relazione può alle volte mostrare diversi profili di conflittualità per la "pluralità di beni, valori e interessi che si contendono il campo"».
[74] Al riguardo è chiaro C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy*, cit., 64 ss., che configura l'ipotesi di «trasparenza *versus privacy*». L'A. richiama anche la recente sentenza della Corte costituzionale, n. 20/2019, che ha affrontato il tema della trasparenza (p. 90).
[75] Cfr. S. RODOTÀ, *op. cit.*, 105. Per un esame approfondito di tale diritto, cfr. anche A. CERRI, *Riservatezza (diritto alla)*, in *Enciclopedia Giuridica*, XXVII, Roma, 1995, 1 ss.
[76] Com'è noto, l'art. 10 Convenzione di Oviedo stabilisce che «ogni persona ha diritto al rispetto della propria vita privata allorché si tratta di informazioni relative alla propria salute. Ogni persona ha il diritto di conoscere ogni informazione raccolta sulla propria salute. Tuttavia, la volontà di una persona di non essere informata deve essere rispettata», mentre, con riguardo alla Carta UE, l'art. 7 è rubricato «Rispetto della vita privata e della vita familiare» e l'art. 8 è intitolato «Protezione dei dati di carattere personale». Infine, l'art. 8 CEDU disciplina il «diritto al rispetto della vita privata e familiare».
[77] Cfr. L. CHIEFFI, *op. cit.*, 5 s.
[78] Il riferimento è, ad esempio, alla Costituzione spagnola che richiama, in ragione della sua più recente formulazione rispetto a quella italiana, il diritto alla *privacy*, come nell'art. 18.4 CE, dove si afferma che «la legge limita l'uso dell'informatica per garantire l'onore, l'intimità personale e familiare dei cittadini ed il pieno esercizio dei loro diritti», o ancora l'art. 20.4 CE, allorquando si precisa che le libertà di manifestazione del pensiero, di

«tono costituzionale» del diritto e la sua relativa tutela, poiché quest'ultimo è comunque ricavabile in via ermeneutica dalla nostra Legge fondamentale, in particolare dagli artt. 2, 3, 13, 15, 21 e 32 Cost., applicati «ai fenomeni della tecnologia informatica»[79]. É doveroso allora il richiamo «al principio della dignità umana […] a presidio dei diritti della persona»[80], di cui è pervasa la nostra Carta e la cui capienza assiologica permette di abbracciare, anche in questo caso, i diritti della personalità, come quello alla riservatezza, conformemente al personalismo della Costituzione italiana. Questo indirizzo interpretativo, peraltro, è stato autorevolmente confermato anche dal *Bundesverfassungsgericht*, secondo cui il diritto alla privacy trova il suo fondamento costituzionale nei noti artt. 2, Abs. 1, e 1, Abs. 1, *Grundgesetz*, che sanciscono, rispettivamente, il diritto di ciascuno al libero sviluppo della personalità e il principio della intangibilità della dignità umana[81].

Proprio la Corte di Karlsruhe ha declinato la riservatezza come diritto di «rango costituzionale»[82] all'autodeterminazione informativa della persona, nel senso del diritto dell'individuo a determinare la divulgazione e l'utilizzo dei propri dati personali, il che segna un'evidente evoluzione rispetto all'originaria formulazione della riservatezza quale *the right to be let alone*. Attualmente, in sede scientifica, si è affermata la «dottrina della libertà informatica», per cui quest'ultima è configurata nella duplice dimensione, positiva e negativa. «La libertà informatica negativa esprime "il diritto di *non* rendere di dominio pubblico certe informazioni di carattere personale, privato, riservato […]; la libertà informatica positiva, invece, esprime la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della *privacy* per essere divenuti elementi di *input* di un programma elettronico"»[83]. In questa cornice teorica è evidente che nel prossimo futuro – nella prospettiva del deciso rafforzamento della sanità digitale voluto dal PNRR – si determinerà un

insegnamento e di comunicazione trovano il loro limite, in particolare, nel diritto all'onore, all'intimità e all'immagine. Tale indirizzo costituzionale è stato poi implementato con la *Ley Orgánica* 3/2018, di «Protección de Datos Personales y garantía de los derechos digitales», che nell'art. 1 precisa come il suo compito sia quello di garantire «los derechos digitales» conformemente a quanto stabilito dall'art. 18.4 della Costituzione, oltre che armonizzare l'ordinamento giuridico spagnolo al Regol. UE n. 2016/679. In particolare, per ciò che concerne i dati sanitari, in Spagna è stata prevista la *Historia Clínica Digital* tesa a raccogliere «la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en *el soporte técnico* (corsivo nostro) más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada», secondo quanto indicato dall'art. 15, *Ley* 41/2002, che disciplina «la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica». Allo stesso tempo, la *Ley* 16/2003, relativa al *Sistema Nacional de Salud*, all'art. 56 precisa che «el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, […], para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información».

[79] Per queste considerazioni v. T.E. FROSINI, *Internet come ordinamento giuridico*, in *Percorsi costituzionali*, 1, 2014, 17, e, per i disposti costituzionali impegnati, v. L. CHIEFFI, *op. cit.*, 22.

[80] Ancora, L. CHIEFFI, *op. cit.*, 23.

[81] BVerfG, 1 BvR 209/83, 15 dicembre 1983.

[82] Su questa giurisprudenza del BVerfG, cfr. S. RODOTÀ, *op. cit.*, 45.

[83] Sulla dottrina della libertà informatica, cfr. T.E. FROSINI, *Liberté Egalité Internet*, Napoli, 2015, 107 s.

ampliamento dell'«orizzonte giuridico di internet»[84], cui dovrà corrispondere una sempre maggiore attenzione in termini di tutela verso la libertà informatica.

Tuttavia, secondo il GDPR (cons. 4) il diritto alla protezione dei dati di carattere personale «non è una prerogativa assoluta […] e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». Lo stesso Reg. UE 2016/679, dunque, individua nella proporzionalità il criterio che deve guidare il bilanciamento nel caso di conflitti, come prima prospettati, tra il diritto alla privacy come autodeterminazione informativa, da un lato, e il diritto alla salute o il principio di trasparenza, dall'altro[85]. Ciò significa che la possibile limitazione del diritto alla riservatezza – secondo i noti criteri attraverso cui si articola il giudizio di proporzionalità – deve essere idonea, necessaria e strettamente proporzionale alla tutela della salute, volendosi prestare particolare attenzione nel presente contributo a questa situazione soggettiva[86]. Con riferimento ai due documenti sanitari oggetto di indagine – il FSE e la CCE per i quali la normativa nazionale richiede il consenso ai fini del trattamento dei dati – se ne deduce che sarà l'interessato, proprio attraverso il consenso, a procedere, prima, alla valutazione di idoneità circa la limitazione della privacy rispetto all'obiettivo stabilito di protezione della salute, poi al giudizio di necessarietà, teso a commisurare tale limitazione rispetto alla finalità perseguita, e, infine, alla valutazione di stretta proporzionalità, nel senso che non devono emergere effetti collaterali intollerabili per lo stesso interessato[87].

6. Note conclusive

Alla luce di quanto ora sostenuto, appare chiaro che il consenso prestato dall'interessato nel trattamento dei dati con riguardo al FSE e alla CCE favorisce il perseguimento del punto di equilibrio tra diritti eventualmente contrapposti; laddove invece il consenso non è richiesto, è il legislatore che procede direttamente al bilanciamento. È significativo, ad esempio, quanto fissato ancora dall'art. 12, 5° co., d.l. n. 179/2012, che, nel prevedere il necessario consenso per la consultazione dei dati presenti nel FSE, fa salva l'ipotesi dell'emergenza sanitaria, seppure «con modalità individuate al riguardo» (5°

[84] Cfr. V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, 2000, 271 ss., ripreso da T.E. FROSINI, *Liberté Egalité Internet*, cit., 105 s.

[85] Per la CGUE, causa C-518/07, 9 marzo 2010, par. 30, è necessario «stabilire un giusto equilibrio fra la protezione del diritto alla vita privata e la libera circolazione dei dati personali»; anche, CGUE, causa C-553/07, 7 maggio 2009, par. 70.

[86] Sul giudizio di proporzionalità in sede europea, cfr., *ex multis*, D.U. GALETTA, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione europea)*, in *Rivista italiana di diritto pubblico comunitario*, 6, 2019, 911 ss., e G. SCACCIA, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle Corti europee*, in *Rivista AIC*, 3, 2017, 5 ss.

[87] Al riguardo, si registra una ricca giurisprudenza della Corte di Giustizia, come, ad esempio, CGUE, causa C-293/12, 8 aprile 2014, c.d. sentenza *Digital Rights Ireland Ltd*, par. 52, laddove si sostiene, in riferimento al rispetto della vita privata, che la tutela di tale diritto può richiedere «deroghe e […] restrizioni […] alla tutela dei dati personali […] [ma] entro i limiti dello stretto necessario». Il medesimo indirizzo giurisprudenziale si riscontra in CGUE, causa C-473/12, 7 novembre 2013, par. 39; CGUE, cause C-92/09 e C-93/09, 9 novembre 2010, par. 77 e 86. Più recentemente, CGUE, causa C-203/15, 21 dicembre 2016, c.d. sentenza *Tele2 Sverige*, par. 116, dove si conferma che l'accesso ai dati conservati deve avvenire nei «limiti dello stretto necessario» in applicazione del «principio di proporzionalità». Ancora, sul giudizio di proporzionalità sia consentito rinviare a L. FERRARO, *La sentenza Weiss e il principio di proporzionalità secondo la Corte di Lussemburgo*, in *DPER online*, 2, 2021, 34 ss.

comma). In questo caso il decisore politico ha ritenuto che il consenso non rappresenti più il punto di ponderazione, a causa della diversità della fattispecie emergenziale. Difatti, sono state le regioni che nel completare il contenuto del proprio FSE hanno deciso, talune di non richiedere il consenso a fronte di una emergenza sanitaria o di rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica di un terzo o della collettività[88], talaltre di consentire ai sanitari di accedere unicamente, senza consenso del paziente, al suo Profilo sanitario sintetico, nel caso in cui questi versi in una condizione di imminente pericolo di vita e sia impossibilitato a prestare ogni forma di autorizzazione[89].

Tale indirizzo in caso d'emergenza è confermato anche dal GDPR, quando all'art. 9, par. 2, lett. i), stabilisce la possibilità del trattamento dei dati, senza ricorrere al consenso dell'interessato, se necessario «per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria». In questa ipotesi emergenziale[90], egualmente è stato il decisore politico europeo, escludendo il consenso, a procedere al bilanciamento tra interessi contrapposti, così come avviene nel caso dell'art. 9, par. 2, lett. h), più volte richiamato, per cui è possibile il trattamento dei dati, ancora senza il consenso, se il primo è necessario per finalità di medicina preventiva, di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali. Dal momento che il successivo par. 3 dell'art. 9 precisa che quest'ultima fattispecie normativa è possibile a condizione che il trattamento sia gestito da un sanitario obbligato al segreto professionale, ne consegue che il Reg. UE ha voluto individuare nel combinato disposto delle due proposizioni normative il bilanciamento utile ad escludere il consenso[91]. Del resto, è bene ribadire che proprio il GDPR ha mutato l'approccio della disciplina, almeno in sede UE, in quanto «più che il consenso dell'interessato vengono valorizzate le cautele nell'effettuare il trattamento e le misure di sicurezza»[92].

Invero, lo stesso Regolamento UE, in sede di principi applicabili al trattamento dei dati personali, ha richiamato il principio di finalità «come limite intrinseco al trattamento lecito dei dati», capace dunque di integrare le eventuali insufficienze del consenso[93]. Ne deriva che, ai sensi dell'art. 5, par. 1, lett. c), i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In questo modo, se gli scopi per cui si procede al trattamento integrano le possibili carenze del consenso, allora anche di essi si dovrà tenere conto in funzione del bilanciamento, così che le finalità dovranno essere palesi e, quindi, «determinate, esplicite e legittime», secondo quanto precisato – in una lettura sistematica – dallo stesso art. 5, par. 1, ma alla lett. b).

Dinanzi alla possibilità, a seguito di un'accelerazione della sanità digitale, che aumentino i conflitti tra situazioni giuridiche soggettive, è utile richiamare quanto è stato giustamente osservato in dottrina, per cui la sfida del futuro che «attende il costituzionalismo è, prevalentemente, quella riferita alla

[88] Il richiamo è alla regione Lombardia, https://bit.ly/3yRGo7o.

[89] È il caso della regione Campania, http://www.regione.campania.it/assets/documents/informativa-dati-personali-fse-120321.pdf.

[90] Cfr. E. SORRENTINO, A.F. SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *federalismi.it*, 30, 2020, 248.

[91] In modo conforme, cfr. C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, cit., 15 s.

[92] Ancora, C. COLAPIETRO, F. LAVIOLA, *ult. op. cit.*, 15.

[93] Cfr. C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., 110 s.

tecnologia, ovvero come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica»[94], di cui bisogna comunque cogliere tutti gli aspetti positivi. Quest'ultima rappresenta un'importante occasione di sviluppo delle libertà, che peraltro devono essere opportunamente tutelate anche dagli attacchi informatici, come dimostrano le recenti notizie di cronaca[95], in modo tale da separare i benefici prodotti dall'evoluzione tecnologica a fronte degli inevitabili risvolti problematici.

In questo contesto di progresso la sanità digitale rappresenta un tassello fondamentale, poiché coinvolge non solo la libertà di autodeterminazione informativa della persona, nella prospettiva dell'identità digitale, ma anche, come visto, una più efficace tutela del diritto alla salute. L'obiettivo dell'immediata circolazione delle informazioni di salute, infatti, oltre a riguardare l'importante capitolo del risparmio della spesa sanitaria, punta, com'è ovvio, a migliorare le prestazioni assistenziali a favore dei pazienti. Tuttavia, tale risultato deve essere raggiunto nel rispetto della tutela dei dati sensibili di salute. In una cornice di sviluppo informatico il giurista deve essere capace di tenere insieme la pluralità assiologica rappresentata dai diritti che eventualmente possono entrare in conflitto, come nel caso di quelli alla privacy, in tutte le sue implicazioni, e alla salute. Ciò sarebbe in sintonia con la pluralità di dimensioni della persona umana e, quindi, con il carattere personalista, innanzitutto della nostra Carta costituzionale, ma poi anche dell'ordinamento giuridico sovranazionale, che non a caso richiama la necessità in materia digitale di realizzare uno «spazio di libertà, sicurezza e giustizia» che possa favorire il «benessere delle persone fisiche» (GDPR, cons. 2)[96].

[94] Cfr. T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, cit., 466.

[95] Il riferimento è, ad esempio, al recente attacco hacker (agosto 2021) sferrato al Centro di elaborazione dati della regione Lazio, capace di danneggiare seriamente il sistema di prenotazione delle vaccinazioni anti-Covid. Tuttavia, come hanno precisato le autorità di Polizia preposte, sembrerebbe che non siano stati interessati i dati sanitari delle persone, La Stampa, 2 agosto 2021, https://www.lastampa.it/cronaca/2021/08/02/news/attacco-hacker-in-corso-alla-regione-lazio-blitz-partito-dall-estero-bloccate-tutte-le-attivita-1.40561127. Sugli attacchi informatici anche a strutture sanitarie di eccellenza, v. E. SORRENTINO, A.F. SPAGNUOLO, *op. cit.*, 244 ss.

[96] Su queste considerazioni cfr. L. CHIEFFI, *op. cit.*, 6.