dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2022
Data di pubblicazione – 16 giugno 2022

La sicurezza dei dati sanitari nelle *smart technologies* quale strumento di realizzazione del diritto alla salute tra telemedicina ed intelligenza artificiale*

di
Giuseppina Lofaro**

1. *Premessa.*

Le tecnologie[1] *smart* supportano i processi curativi, attraverso il loro impiego diffuso in ambito sanitario, a titolo esemplificativo mediante diagnosi precoci o attraverso l'erogazione di cure a distanza tra medico e paziente.

* Il presente lavoro di ricerca ha origine e sviluppo nell'ambito del Progetto *iCare*, (CUP J39J14001400007 – Azione 10.5.12), in cui Giuseppina Lofaro è risultata vincitrice dell'assegno di ricerca in Diritto Amministrativo (Settore scientifico disciplinare *IUS*-10) presso il Dipartimento DIIES dell'Università degli Studi Mediterranea di Reggio Calabria, per l'espletamento del programma di ricerca dal titolo *"Modelli procedimentali e semplificazione gestionale dei flussi informativi per la piattaforma di telemedicina iCare"*, finanziato nell'ambito del POR FESR FSE 2014/2020 della Regione Calabria con il concorso di risorse comunitarie del FESR ed FSE, dello Stato italiano e della Regione Calabria.

** Assegnista di ricerca *post-doc* in Diritto Amministrativo presso l'Università degli Studi *Mediterranea* di Reggio Calabria.

[1] La tecnologia è un flusso immateriale d'informazioni che si trasforma in conoscenza professionale ed in seguito nel prodotto di un'organizzazione. Essa ha la capacità di trasformare in concreto un'informazione ambientale, immateriale - ad es. un bisogno, una sofferenza - in un prodotto, utile per la cura di una malattia, mediante un processo di "avatarizzazione" della funzione medica. Il virgolettato è di M. SAVINI NICCI, G. VETRUGNO, *Intelligenza artificiale e responsabilità nel settore sanitario*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 602 ss.

Contributo sottoposto a referaggio

Alla luce delle linee guida nazionali[2], rispetto all'appropriatezza erogativa, tra le prestazioni di Telemedicina[3] rientrano le prestazioni che: possono essere assimilate a qualsiasi prestazione sanitaria diagnostica e/o terapeutica tradizionale, rappresentandone un'alternativa di erogazione; non possono sostituire la prestazione sanitaria tradizionale ma piuttosto la supportano rendendola più accessibile e/o aumentandone l'efficienza e l'equità distributiva; integrano in varia misura la prestazione tradizionale, aumentandone l'efficacia e la capacità di adattamento in maniera dinamica alle mutate esigenze di cura dei pazienti; risultino capaci di sostituire completamente la prestazione sanitaria tradizionale, costituendo nuovi metodi e/o tecniche diagnostiche e/o terapeutiche e realizzando nuove prassi assistenziali utili ai pazienti.

Ciò emerge *ictu oculi* ancor di più in epoca pandemica: durante il periodo di diffusione del *Covid-19*, mediante l'uso di tecnologie all'avanguardia, c.d. tecnologie intelligenti, è stata effettuata la raccolta di un'enorme quantità di dati[4].

Inoltre, i pazienti, attraverso l'intensificazione di un'assistenza clinica erogata al proprio domicilio, o anche "in movimento", hanno amplificato il proprio *empowerment*[5].

Certamente, lo sviluppo della c.d. "sanità mobile" (*mobile health* o *mHealth*)[6], permette, mediante l'uso di *software* eseguibili su dispositivi portatili, il monitoraggio dello stato di salute del paziente, anche attraverso la connessione tra plurimi strumenti e sensori indossabili. Si faccia riferimento specialmente ai benefici derivanti ai pazienti affetti da patologie croniche o degenerative. Ciò

[2] Cfr. "Indicazioni nazionali per l'erogazione di prestazioni in Telemedicina", 27 Ottobre 2020, 3, reperibile anche in *http://www.quotidianosanita.it/allegati/allegato2602365.pdf*.

[3] Ci si permette di rinviare, per un'analisi dettagliata, a G. LOFARO, *Rilievi sulla validazione della telemedicina: modelli procedimentali e semplificazione gestionale della piattaforma*, in *Osservatorio sulle fonti*, n. 1/2022, 231-270. Disponibile in: *http://www.osservatoriosullefonti.it*.

[4] G. MAIRA, *Intelligenza umana e intelligenza artificiale*, 7, 2021, *passim*, in *www.federalismi.it*.

[5] A. ARDISSONE, *La relazione medico-paziente nella sanità digitale. Possibili impatti sul professionalismo medico*, in *Rass. it. sociologia*, 2018, *passim*.

[6] S. PARI, M.L. RIZZO, *L'utilizzo di applicazioni di mHealth: rischi e responsabilità*, in C. FARALLI, R. BRIGHI, M. MARTONI (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura*, Torino, 2015, 135 ss.

produce, tra l'altro, un effetto positivo di contenimento della spesa pubblica nel settore della sanità.

La digitalizzazione consente *prima facie* una più ampia diffusione della scienza medica, rendendola disponibile per larghe fasce di cittadini.

L'uso dell'Intelligenza Artificiale (IA)[7] in medicina[8] consente una sua "democratizzazione" sia sotto l'aspetto della diagnosi che delle raccomandazioni di trattamento, permettendo l'erogazione di prestazioni altrimenti non universalmente accessibili e riducendo altresì i costi di assistenza[9].

Sussiste anche l'opportunità di rafforzare il rapporto fiduciario tra medico e paziente, poiché il primo, affidando all'IA[10] il ruolo di analisi dei dati raccolti, potrebbe altresì riuscire a dedicare più tempo ai fini di una comunicazione più efficace con il suo assistito[11].

---

[7] Cfr. la recente Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE, COM/2021/206, in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206*.

[8] A. E. TOZZI, *Il connubio tra telemedicina e intelligenza artificiale per un salto di qualità nelle cure*, in Riv. *Monitor*, n. 46, Dicembre 2021, 39-42, in https://www.agenas.gov.it/images/monitor/2021/46/art_agenas_11.pdf, si sofferma sulle potenzialità offerte dalla combinazione degli strumenti digitali per la telemedicina e delle tecniche di intelligenza artificiale, che consentirebbe una trasformazione dei percorsi di cura e dell'organizzazione dei servizi sanitari. Se opportunamente impiegata, l'integrazione di telemedicina e IA può rappresentare una risorsa a favore della sostenibilità e della partecipazione attiva dei pazienti alle cure, nonché garantire un accesso ai servizi anche da parte di segmenti della popolazione del tutto emarginati, predisponendo percorsi di cura con un livello elevato di personalizzazione. L'Autore prosegue, illustrando l'impatto benefico delle soluzioni di telemedicina non solo sul paziente, ma anche sull'economia sanitaria, sul clima e sull'ambiente, evidenziando possibili applicazioni di Intelligenza artificiale integrabili alla telemedicina, specialmente per quel che concerne la diagnostica del paziente cronico e la predizione di eventi gravi.

[9] «Una IA che sostituisca ed ottimizzi l'operato professionale è replicabile virtualmente quasi senza costo». Le parole racchiuse tra virgolette sono di G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'economia*, 2019, 175 ss.

[10] L'IA rappresenta, probabilmente, la frontiera più avanzata della digitalizzazione ed altresì costituisce fenomeno ben più complesso rispetto all'informatizzazione dei processi. Cfr. G. PASCERI, *Intelligenza artificiale, algoritmo e machine learning. Le responsabilità del medico e dell'amministrazione sanitaria*, Milano, 2021, 3 ss.

[11] Tuttavia sussiste altresì il rischio che «consumatori tecnologicamente più esperti siano indotti a ricorrere ad applicazioni di *mHealth* per escludere impropriamente dal loro percorso di cura il medico». In tal modo, l'incremento delle nuove conoscenze potrebbe incidere in senso critico

Specialmente nell'ambito della sanità mobile si concentrano i timori dei pazienti con riferimento alla sicurezza dei dati clinici[12], sovente altresì per la mancanza di adeguata consapevolezza rispetto alle modalità sostanziali di trattamento dei dati.

Tali questioni involgono una piena attenzione alla tutela di dati personali "sensibili" quali quelli relativi alla salute, specialmente nei rapporti con la Pubblica Amministrazione, in un'ottica giuspubblicistica.

Al fine di tentare di offrire soluzioni rispetto alle questioni originate dall'applicazione di tecnologie *smart* nella sanità pubblica in Italia, pare utile, preliminarmente, un cenno sullo stato dell'arte della riforma in senso digitale della Pubblica Amministrazione, con particolare attenzione al settore sanitario.

L'analisi sullo stato di avanzamento della digitalizzazione in Italia risulta necessaria per comprendere la capacità attuale della Pubblica Amministrazione di cogliere in modo adeguato potenzialità[13] e rischi derivanti dall'utilizzo di *smart technologies* in sanità.

Il presente lavoro di ricerca si soffermerà poi *funditus* su alcune disposizioni del *GDPR* - il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - in tema di sicurezza dei dati sanitari, al fine di riflettere sui profili critici emergenti nonché su possibili soluzioni tecnico-giuridiche applicative in una prospettiva *de jure condendo*.

2. *Breve excursus normativo in tema di amministrazione digitale: il diritto di accesso individuale alle tecnologie specialmente nei processi organizzativi e di gestione semplificata dei sistemi di eHealth.*

sul rapporto paziente/medico, poiché «il primo non appare più disposto, come un tempo, a consegnare incondizionatamente al secondo la risposta ai suoi problemi di salute, pretendendo nuove e legittime istanze di autonomia decisionale in riferimento alle possibili alternative di cura». Ne tratta *funditus* R. LOMBARDI, *Errore umano e incidenti organizzativi in medicina*, in *Il diritto dell'economia*, 2, 2021, 217-237.

[12] R.M. COLANGELO, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante*, in *Aut. loc. e serv. soc.*, 2019, 281 ss.

[13] A.G. OROFINO, *L'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi*, in *Giornale dir. amm.*, 2004, 1371 ss., mette in luce gli effetti positivi e le potenzialità della diffusione delle nuove tecnologie nella P.A.

Sotto un profilo storico-ricostruttivo, già la c.d. Legge Stanca, l. n. 4 del 2004, con la *ratio* di favorire e semplificare l'accesso agli strumenti informatici da parte degli utenti, aveva gettato le basi normative per il riconoscimento del "diritto di accesso individuale alle tecnologie" quale "diritto sociale strumentale al godimento delle libertà fondamentali"[14].

Il successivo art. 3 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82, c.d. C.a.d.)[15] ha rappresentato poi una vigorosa conferma di tale diritto di accesso, fino ad allora contrastato da ostacoli di natura tecnica, economica e giuridica.

Il diritto all'uso delle tecnologie costituisce l'emblema di una nuova generazione di diritti, nell'ambito di una riforma della Pubblica Amministrazione in senso digitale, attuata mediante il C.a.d., strumento funzionale al raggiungimento di obiettivi di ottimizzazione dell'efficacia e dell'efficienza dell'azione amministrativa[16] nonché dei rapporti col cittadino.

L'art. 2 C.a.d. sancisce il "diritto all'amministrazione digitale"[17], prevedendo che gli enti territoriali assicurino disponibilità, gestione, accesso, trasmissione, conservazione e fruibilità dell'informazione in modalità digitale, configurando in tal senso una pretesa *tout court* del cittadino ad usufruire di strumenti tecnologici idonei a semplificare i suoi rapporti con l'amministrazione.

[14] Le principali fasi evolutive di diffusione delle risorse tecnologiche e telematiche nella Pubblica Amministrazione in Italia sono ricostruite in maniera molto efficace da G. PIPERATA, *Cittadini e imprese di fronte all'amministrazione digitale*, in *Diritto Mercato Tecnologia*, 2016, 169 ss.

[15] G. CASSANO-C. GIURDANELLA, *Il codice della pubblica amministrazione digitale. Commentario al D.lgs. n. 82 del 7 marzo 2005*, Milano, 2005; E. CARLONI, *La riforma del Codice dell'amministrazione digitale*, in *Giornale dir. amm.*, 2011, 469 ss.; G. PESCE, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018, 49 ss.

[16] P. PIRAS, *L'amministrazione nell'era del diritto amministrativo elettronico*, in *Dir. Internet*, 2006, 550.

[17] P. PESCE, *I «nuovi diritti» nell'amministrazione digitale*, in *Rass. dir. pubb. europeo*, 2007, 207; S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 13: un diritto che si manifesta quale «sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete».

Si tratta di un diritto dotato di portata sistemica nell'ambito dell'ordinamento giuridico complessivo[18], nonostante il c.a.d. contenga molte norme programmatiche e di principio[19].

L'art. 3 C.a.d., più volte modificato[20], è, nella sua attuale versione, il risultato della ricerca di soluzioni normative di contemperamento degli interessi coinvolti[21].

Tuttavia, in generale, non è stata offerta una risposta in linea con la necessità di oltrepassare la mera programmaticità di alcune disposizioni del C.a.d., nella perdurante assenza di un adeguato apparato sanzionatorio in caso di inerzia dell'amministrazione nonché a causa dell'ampio mutamento, negli anni, dei soggetti incaricati di condurre il processo d'innovazione tecnologica.

In Italia, il legislatore ha progressivamente assunto, nella sua agenda dei lavori, l'obiettivo della digitalizzazione pubblica; tuttavia non se ne riesce a cogliere la

[18] Cfr. la sentenza del T.a.r. Basilicata, sez. I, 23 settembre 2011, n. 478, in *Foro amm. TAR*, 2011, 12, 4098, che rappresenta la prima pronuncia del giudice amministrativo a favore della piena effettività del diritto all'uso delle tecnologie ai sensi dell'art. 3 C.a.d.; in dottrina si v. F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2015, 257 ss.

[19] C. LEONE, *Il ruolo del diritto europeo nella costituzione dell'amministrazione digitale*, in *Riv. it. dir. pubb. com.*, 2014, 867 ss.

[20] Il primo comma dell'art. *de quo*, tra il 2005 e il 2017, dal prevedere che «i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali» è giunto a stabilire che «chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'art. 2, comma 2». Cfr. R. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, in *Il diritto dell'economia*, 3, 2021, 54-55.

[21] È stata probabilmente tale circostanza a portare alla delega del governo, *ex* art. 1 della legge 7 agosto 2015, n.124 (c.d. Legge Madia), rubricato "Carta della cittadinanza digitale", ad adottare uno o più decreti legislativi con la *ratio* di modificare ed innestare il C.a.d. con una disciplina che, «rimediando alle inefficienze dei precedenti interventi normativi legati ad esigenze ormai obsolete, fosse finalmente in grado di realizzare il principio *digital first*».

Le disposizioni attuative della Legge Madia, tra il 2016 ed il 2017, hanno tentato di seguire la via tracciata dalla delega, inserendo nell'art. 7 del C.a.d. una nuova rubrica, «Diritto a servizi on-line semplici e integrati», ed un comma, precedente al primo, secondo cui «chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato». Si v. R. LOMBARDI, *op. ult. cit.*; G. PIPERATA, *Semplificazione e digitalizzazione nelle recenti politiche di riforma della pubblica amministrazione italiana*, in F. MASTRAGOSTINO, G. PIPERATA, C. TUBERTINI (a cura di), *L'amministrazione che cambia. Fonti, regole e percorsi di una nuova stagione di riforme*, *Quaderni della Spisa*, Bologna, 2016, 255 ss.; M. PIETRANGELO, *Cittadinanza digitale e diritto all'uso delle tecnologie*, in G. CAMMAROTA, P. ZUDDAS (a cura di), *Amministrazione elettronica. Caratteri, finalità, limiti*, Torino, 2020, 26 ss.

complessiva portata riformatrice, a causa della frammentazione di previsioni segmentate nel tempo[22].

Ai fini della conduzione tecnico-giuridica del presente lavoro di ricerca, è utile rammentare che tra le riforme del C.a.d. susseguitesi negli anni, la più rilevante è sancita nel c.d. Decreto Semplificazione del 2012 (d.l. n. 5 del 2012), intitolato "Agenda digitale italiana", la cui operatività è avvenuta attraverso le misure attuative previste dal c.d. Decreto Crescita 2.0 (d.l. n. 179/2012)[23], con la *ratio legis* di modernizzazione dei rapporti tra pubblica amministrazione, cittadini ed imprese.

La Sanità digitale[24] è una tra le macro-aree dell'Agenda digitale e del Decreto Crescita 2.0.. Ad essa proprio il Decreto da ultimo menzionato ha dedicato *expressis verbis* la Sezione IV.

L'*eHealth*[25] concerne l'applicazione delle tecnologie sia in ambito diagnostico, sia ai processi organizzativi dei sistemi sanitari. Si tratta di aspetti tra loro interconnessi in quanto riguardanti sia l'erogazione della prestazione sanitaria, specialmente sotto il profilo dell'attendibilità clinica, sia la comunicazione, la gestione e la conservazione del complesso di informazioni connesse ai soggetti pubblici e privati di riferimento.

Con precipuo riguardo ai processi organizzativi e di gestione dei sistemi, con l'obiettivo di ottimizzare l'erogazione dei servizi ai cittadini nonché monitorare la spesa nel settore sanitario, il d.l. n. 5/2012 ha avviato la «Semplificazione in materia di sanità digitale» *ex* art. 47-*bis*, che dispone di privilegiare, nei piani di sanità

---

[22] E. CARLONI, *Digitalizzazione e riforma dell'amministrazione: la nuova agenda*, in *F. Mastragostino, G. Piperata, C. Tubertini* (a cura di), *L'amministrazione che cambia. Fonti, regole e percorsi di una nuova stagione di riforme*, *Quaderni della Spisa*, Bologna, 2016, 267 ss.

[23] F. GASPARI, *La new information economy, il problema del digital divide e il ruolo dei pubblici poteri*, in *Dir. pubb. europeo. Rassegna on line*, 2018, 154 ss.

[24] La sanità digitale (sanità elettronica, *eHealth*), consiste nell'impiego delle nuove tecnologie nel dominio sanitario al fine di migliorare l'accesso degli utenti all'assistenza medica, ridurre il rischio clinico, implementare l'efficacia e la sicurezza delle prestazioni erogate dal Servizio Sanitario Nazionale (SSN) ed intervenire sulle diseconomie della spesa sanitaria pubblica. Su tali profili si v. l'analisi dettagliata ed aggiornata di A. PIOGGIA, *La sanità italiana di fronte alla pandemia. Un banco di prova che offre una lezione per il futuro*, in *Dir. pubbl.*, 2020, 385 ss.

[25] D.U. GALETTA, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in AA.VV., *Scritti per Franco Gaetano Scoca*, vol. III, Napoli, 2020, 2265 ss.

nazionali e regionali, la gestione elettronica delle pratiche cliniche, mediante l'uso della cartella clinica elettronica, nonché i sistemi di prenotazione elettronica ai fini dell'accesso alle strutture da parte dei cittadini, con l'obiettivo di perseguire vantaggi sotto i plurimi aspetti dell'accessibilità e del contenimento dei costi, prevedendo altresì che la conservazione delle cartelle cliniche avvenga anche solo in forma digitale.

Alla luce della *ratio* del legislatore, strumenti nevralgici del sistema di sanità digitale italiana sono il fascicolo sanitario elettronico (FSE) di cui all'art. 12[26], la prescrizione medica digitale (c.d. ricetta dematerializzata) e la cartella clinica elettronica[27] (CCE) *ex* art. 13 del d.l. n. 179 /2012.

Il FSE risulta centrale nell'analisi della presente ricerca: in fase pandemica da *Covid-19*[28], la sua disciplina è stata rivisitata ed ampliata dal c.d. Decreto Rilancio (d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77), che, nel tentativo di oltrepassare la scarsa diffusione che ha contraddistinto tale strumento, tradizionalmente inteso quale mero contenitore storico dei contatti che un soggetto ha avuto con il Servizio Sanitario Nazionale, ha previsto che il fascicolo sanitario elettronico[29] costituisca il complesso aggiornato - tempestivamente e continuativamente -, dei dati e documenti digitali di tipo sanitario e sociosanitario che scaturiscono da eventi clinici riguardanti l'assistito, anche con riferimento alle prestazioni erogate al di fuori del servizio pubblico[30].

---

[26] M.G. VIRONE, *Il fascicolo sanitario elettronico. Sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Roma, 2015, 19.

[27] C. SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy*, in R. FERRARA (a cura di), *Salute e sanità*, 5° volume del Trattato di biodiritto, diretto da S. Rodotà - P. Zatti, Milano, 2010, 579 ss.; 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), 5, 2021, 1-28, in *www.federalismi.it*.

[28] E. SORRENTINO, A.F. SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, 30, 2020, 1-14, in *www.federalismi.it*.

[29] Sui contenuti del FSE, cfr. M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, Milano, 2019, 46 ss.

[30] N. POSTERARO, *Sanità digitale in Italia: il Fascicolo Sanitario Elettronico (FSE) dopo le modifiche introdotte dal decreto Rilancio*, 2021, in https://www.irpa.eu/sanita-digitale-in-italia-il-fascicolo-sanitario-elettronico-fse-dopo-le-modifiche-introdotte-dal-decreto-rilancio/, acutamente, rileva che: «la disciplina del FSE costituisce un'applicazione emblematica del delicato contemperamento tra il principio della libera circolazione dei dati, funzionale alla tutela della

Ai sensi dell'art. 12, co. 2, d.l. n. 179/2012, l'istituzione del FSE è prevista «nel rispetto della normativa vigente in materia di protezione dei dati personali, ai fini 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», la consultazione dei dati e documenti in esso contenuti, per le finalità di cui alla lett. a), «può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria secondo modalità individuate a riguardo» (comma 5), mentre le finalità di cui alle lett. b) e c) sono perseguite da Stato, Regioni e Province autonome «senza l'utilizzo dei dati identificativi degli assistiti presenti nel FSE, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti, con il decreto di cui al comma 7[31], in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali» (comma 6)[32].

Emerge *ictu oculi*, dal dato normativo appena evidenziato, lo stretto nesso, in ambito sanitario, tra la *quaestio* della sicurezza - nella formazione, conservazione, utilizzo e circolazione del dato clinico - e quella della *privacy*[33].

---

salute pubblica e alle esigenze di efficienza amministrativa, e il diritto alla riservatezza, posto a presidio della dignità dell'individuo. La dimensione collettiva del diritto alla salute *ex* art. 32 Cost. spinge la disciplina relativa al trattamento dei dati sensibili, da sempre oggetto di una speciale "blindatura giuridica", verso quelle aperture solidaristiche che, specie in epoca pandemica, sono apparse indispensabili».

[31] Nello specifico, il comma 7 prevede che sia il Ministro della salute e quello per l'innovazione tecnologica a stabilire, con proprio decreto, i contenuti del FSE ed «i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al FSE da parte dei soggetti di cui ai commi 4, 5 e 6, la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato, i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività».

[32] In merito alle linee guida che, a più riprese, il Garante per la *privacy* ha emanato per l'attuazione della sua disciplina, L. CALIFANO, *Fascicolo sanitario elettronico (Fse) e dossier sanitario. Il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in *San. pubb. e priv.*, 2015, 7 ss.

[33] V. GIARDINO, R. ZANI, *Sanità digitale, tutti i risvolti privacy: come tutelare i dati personali garantendo l'assistenza*, 2021, in *https://www.cybersecurity360.it/legal/privacy-dati-personali/sanita-digitale-tutti-i-risvolti-privacy-come-tutelare-i-dati-personali-garantendo-lassistenza/*.

Specificamente, nella sanità digitale, è fondamentale la sussistenza della garanzia del sistema sotto i profili di affidabilità e conoscibilità dei suoi procedimenti nonché dei relativi risultati. Ciò risulta necessario sia per la concessione del consenso al trattamento dei dati personali da parte dei pazienti, nonché ai fini della serenità del personale sanitario per quel che concerne l'aspetto della responsabilità professionale.

3. *Un approccio dinamico di trattamento nei flussi di dati personali ex art. 5 GDPR in un'ottica integrata di competenze.*

Al fine di analizzare *funditus* le questioni sottese ai processi di digitalizzazione della sanità pubblica in Italia, pare utile soffermarsi su alcune disposizioni contenute nel Regolamento europeo n. 679 del 2016 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali (c.d. *G.D.P.R.*, dall'inglese *General Data Protection Regulation*), specificamente concernenti il trattamento dei dati relativi alla salute[34].

La continua evoluzione tecnologica, nonché la digitalizzazione della società e dell'economia nel suo complesso[35], hanno indotto una modifica, da parte della Commissione europea, avente ad oggetto le misure normative contenute nel *GDPR*.

La frammentazione della disciplina sulla protezione dei dati personali in ambito europeo e le derivanti incertezze applicative hanno contribuito a causare un inefficiente clima di sfiducia nei vari settori di applicazione delle nuove tecnologie.

Il regolamento *de quo*, strumento capace di un maggiore impatto nei contesti nazionali, ha prodotto un'informazione normativa aggiuntiva rispetto alla previgente Direttiva 95/46/CE, risultando, tra l'altro, più idoneo al perseguimento dei fini di protezione[36] e di *enforcement* dei diritti degli interessati (*id est*: assistiti).

---

[34] Per un'analisi dettagliata degli obblighi dei soggetti che effettuano trattamenti di dati in ambito sanitario, si v. le chiare note di C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, in *Riv. Diritti fondamentali*, Fascicolo 2, 2019, 1-25, in *www.dirittifondamentali.it.*

[35] G. BUTTARELLI, *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche*, 1, 2015, 1-11, in www.federalismi.it.; F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali*, Torino, 2016; G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2020.

[36] L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, 4, 2018, 1-52, in *www.federalismi.it*.

Come già rilevato, sussiste una quantità enorme di dati prodotti nella vita digitale quotidiana, i c.d. *big data*[37], la cui corretta interrogazione può costituire fonte di ricchezza ma è accompagnata dal rischio che involge ogni profilo e fase del loro impiego[38].

Il *GDPR* prevede, quale figura centrale, il Titolare del trattamento[39], deputato a mettere in atto misure tecnico-organizzative adeguate ad assicurare che il trattamento dei dati sia effettuato in modo conforme al Regolamento ai sensi del suo art. 24, altresì integrando la protezione dei dati fin dalla sua progettazione *ex* art. 25 con la c.d. *privacy by design*[40], nonché per tutta la sua durata.

Può evincersi pertanto che è indispensabile perseguire l'obiettivo della protezione dei dati personali mediante un approccio "dinamico", che involge anche i flussi di dati che si muovono "dall'esterno verso l'interno"[41] rispetto ai soggetti che utilizzano la tecnologia quale pervasiva e persistente modalità relazionale.

Pare altresì opportuno sottolineare che il concetto di *privacy* - la cui centralità era sottesa alla Direttiva del 1995 - nel 2016 lascia maggiore spazio alla rilevanza al dato in sé ed alla sua sicurezza.

A tal proposito risulta centrale l'art. 5 *GDPR* che, nell'affermare i principi applicabili al trattamento dei dati personali e nel direzionare le competenze per il loro rispetto verso il Titolare del trattamento, - che deve essere anche «in grado di

---

[37] Sotto un profilo collegato, l'applicazione della tecnologia *blockchain* al settore pubblico si interseca, anche nella prospettiva dell'automazione delle decisioni amministrative, con la tematica della gestione e sfruttamento dei *big data*, offrendo enormi potenzialità ma anche sollevando questioni di compatibilità con la disciplina giuridica europea e nazionale in tema di *data protection*. Si v. il recentissimo saggio di G. GALLONE, *Blockchain e big data nel settore pubblico: spunti in tema di G.D.P.R. compliance*, n. 14, 2022, 65-83.

[38] A. MASCOLO, *La sfida della sanità digitale nel post pandemia*, 2020, in *https://www.irpa.eu/la-sfida-della-sanita-digitale-nel-post-pandemia/.*

[39] G. SIMEONE, *Machine Learning e tutela della Privacy alla luce del GDPR*, in Aa.Vv., *Diritto e intelligenza artificiale*, Pisa, 2020, 278-279, acutamente rileva che il riferimento al Titolare del trattamento quale "catalizzatore" di tutte le responsabilità riveli la ridotta capacità del legislatore europeo di intercettare gli sviluppi della tecnologia connessa ai *big data*, nel suo coinvolgere veri e propri trattamenti "a cascata" e, pertanto, numerosi attori che sovente non è facile controllare.

[40] S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, 24, 2017, 1-21, in *www.federalismi.it*.

[41] G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, 16, 2020, 1-34, in *www.federalismi.it.*

comprovarlo» alla luce del principio di responsabilizzazione[42] di cui al par. 2 -, dispone altresì che i dati sono «trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali». E' questa l'estrinsecazione del principio di integrità e riservatezza, di cui al par. 1, lett. f), altresì noto quale principio di *accountability*[43], che si atteggia come "principio dei principi", la cui osservanza dovrebbe garantire il rispetto di tutti gli altri.

Per l'economia del presente lavoro di ricerca, la concezione di sicurezza dei dati personali che emerge dalla disposizione citata risulta molto interessante. La protezione dal loro trattamento non autorizzato o illecito, o dalla distruzione, ne costituisce una componente certamente importante, ma non la esaurisce. Difatti, la sicurezza dei dati personali, ai sensi del *GDPR*, va intesa quale «vera e propria strategia omnicomprensiva e strutturale di ogni contesto aziendale pubblico e privato, di cui la protezione del dato costituisce soltanto una parte», per quanto particolarmente rilevante; una strategia che ruota intorno al "principio generale del trattamento"[44].

Dall'analisi del *GDPR* emerge un approccio di tutela dei dati personali fondato sulla gestione complessiva del rischio che rivela un nuovo orientamento di politica del diritto in questo settore, basato non tanto sulla predeterminazione "in astratto" delle misure da adottare, quanto sulla responsabilizzazione proattiva del Titolare del trattamento[45], chiamato a modulare "in concreto" l'attuazione dei principi sanciti dal Regolamento.

E' altresì utile rilevare che, nell'ottica dell'*accountability*, la sicurezza dei dati personali, involgendo l'applicazione di misure differenti, richiede una visione

---

[42] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Ciberspazio e diritto*, 2018, 211 ss.

[43] E. FACCIOLI, M. CASSARO, *Il "gdpr" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *Dir. ind.*, 2018, 561 ss.

[44] Il virgolettato è di R. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 61-62.

[45] G. FINOCCHIARO, *GDPR tra novità e discontinuità - il principio di accountability*, in *Giur. it.*, 2019, 2777 ss.

integrata di plurime competenze, - tra cui quelle giuridiche, informatiche ed organizzative **-** che mobilitano a loro volta l'ausilio di diverse professionalità in quanto l'opzione della misura adeguata necessita di una valutazione preventiva rispetto alla natura dei dati, ai rischi emergenti dal contesto di riferimento, ai costi stimati nonché ai potenziali danni arrecabili.

Alla luce di un canone di ragionevolezza[46], certamente è apprezzabile l'ampliamento dell'applicazione del concetto di sicurezza non soltanto alla protezione, bensì altresì alla formazione del dato personale. Tuttavia, la disposizione *de qua* lascia trasparire l'allarme del legislatore comunitario rispetto a quei contesti in cui l'applicazione delle tecnologie involge non soltanto l'erogazione di una prestazione, ma anche la comunicazione, la gestione e la conservazione del complesso di informazioni a questa connesse. Di certo, tra tali ambiti vi è quello della sanità digitale, in cui, come già rilevato, le applicazioni tecnologiche possono agevolare la circolazione delle informazioni utili ai fini della prevenzione e della cura della malattia nonché all'ottimizzazione dell'efficienza delle strutture sanitarie pubbliche. Tuttavia, anche nel contesto della sanità elettronica, l'impiego massiccio della tecnologia può involgere il concretarsi del rischio sostanziale di un suo uso fraudolento, finalizzato al conseguimento di interessi ultronei e tutt'altro che ortodossi, tendenzialmente economici e cybercriminali[47].

4. *Considerazioni conclusive alla luce delle ultime novità normative*.

All'esito dell'analisi tecnico-giuridica svolta, si ritiene necessaria, in Italia, l'implementazione della diffusione della "cultura digitale", quale attitudine a privilegiare l'impiego degli strumenti digitali nei rapporti con la Pubblica

[46] AA. VV., Corte Costituzionale, Servizio Studi, *I principi di proporzionalità e ragionevolezza nella giurisprudenza costituzionale, anche in rapporto alla giurisprudenza delle Corti europee*, Quaderno predisposto in occasione dell'incontro trilaterale tra Corte costituzionale italiana, Tribunale costituzionale spagnolo e Corte costituzionale portoghese, Roma, 25-26 ottobre 2013, luglio 2013, 1-43, in *www.cortecostituzionale.it*.

[47] La consapevolezza dei rischi collegati all'implementazione del digitale è stata determinante per l'entrata in vigore del d.l. 14 giugno 2021, n. 82, recante «Disposizioni urgenti in materia di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», convertito, con modificazioni, dalla l. 4 agosto 2021, n. 109.

Amministrazione, nonché come cognizione degli obiettivi e dei benefici dell'informatizzazione. Difatti, sussiste ancora una ridotta consapevolezza da parte delle strutture pubbliche sanitarie dell'obbligo, in qualità di titolari del trattamento di dati personali utilizzati nelle applicazioni tecnologiche all'avanguardia, di adozione di misure di sicurezza a fini di protezione dei dati personali e di ossequio della normativa anche comunitaria in materia.

Specialmente nei procedimenti più complessi, emerge anche la questione critica della *governance* dei "ruoli *privacy*"[48] dei diversi attori coinvolti. Tali aspetti problematici sono certamente riconducibili al c.d. *digital divide* (divario digitale)[49].

L'emergenza provocata dal *Covid-19* ha rappresentato e costituisce tuttora una fase contraddistinta da un *test* collettivo rispetto alle potenzialità nonché ai limiti della digitalizzazione pubblica, specialmente nel settore sanitario.

I decreti-legge emanati in Italia tra maggio e giugno 2021 per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) rappresentano comunque una spinta positiva nell'avanzamento digitale[50].

---

[48] Con provvedimento n. 75 del 24 febbraio 2022, il Garante della *Privacy* ha reso parere favorevole sullo schema di decreto del Presidente del Consiglio dei Ministri - da adottare, su proposta del Ministro della salute e del Ministro dell'economia e delle finanze previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano - sull'Anagrafe nazionale degli assistiti (ANA): «In ragione della manifestata esigenza di dare attuazione alle disposizioni che hanno previsto l'istituzione dell'ANA anche in relazione alla necessità di facilitare il completamento e la diffusione del Fascicolo Sanitario Elettronico indicato come obiettivo nella missione 6 del Piano nazionale di ripresa e resilienza" l'Autorità, preso atto del complesso delle misure di garanzia contenute nello schema del decreto, le ha ritenute appropriate per tutelare i diritti fondamentali e gli interessi delle persone fisiche e prive di criticità sotto il profilo della protezione dei dati personali». Cfr. Parere sullo schema di decreto del Presidente del Consiglio dei Ministri da adottare, su proposta del Ministro della salute e del Ministro dell'economia e delle finanze previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano sull'Anagrafe nazionale degli assistiti (ANA), 24 febbraio 2022, in *Osservatorio di diritto sanitario*, in *www.federalismi.it*.

[49] Cfr. l'approfondita analisi di R. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 70-75; ci si permette di rinviare alla dottrina ivi richiamata.

[50] Si fa riferimento, in particolare, all'entrata in vigore del d.l. 31 maggio 2021, n. 77, «*Governance* del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure» (c.d. Decreto semplificazioni *bis*, convertito, con modificazioni, dalla l. 29 luglio 2021, n. 108), il cui art. 41 ha aggiunto al C.a.d. un art. 18-*bis*, rubricato «Violazione degli obblighi di transizione digitale»: l'articolo *de quo* riconosce all'Agenzia per l'Italia Digitale (AgID) poteri di vigilanza, verifica, controllo e

La diffusione delle *smart technologies* e la trasformazione del *modus lavorandi* dei dati, mediante l'espletamento automatizzato di attività tradizionalmente svolte dall'intelligenza umana, rappresentano i tratti sintomatici dell'evoluzione attuale della Pubblica Amministrazione.

Nell'ambito sanitario, da ciò discendono rilevanti conseguenze specialmente sotto l'aspetto del particolare rilievo acquisito dal concetto dinamico di "sicurezza" dei dati relativi alla salute.

Inoltre, l'art. 9 *GDPR*[51], nel vietare il trattamento dei dati relativi alla salute, prevede un'eccezione al divieto[52] se «il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria […]» (par. 2, lett. i).

In Italia, la disposizione *de qua* risulta collegata all'annosa *quaestio* della salute quale fondamentale diritto dell'individuo, bensì altresì interesse della collettività ai sensi

monitoraggio sul rispetto delle disposizioni del Codice e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione e, soprattutto, il potere di irrogare una sanzione amministrativa pecuniaria di un minimo di 10.000 e di un massimo di 100.000 euro in caso di accertamento della violazione delle suddette disposizioni.

Si rifletta altresì sull'entrata in vigore del già citato d.l. 14 giugno 2021, n. 82, recante «Disposizioni urgenti in materia di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», convertito, con modificazioni, dalla l. 4 agosto 2021, n. 109.

Si pensi ancora al d.l. 9 giugno 2021, n. 80, recante «Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia», convertito, con modificazioni, dalla l. 6 agosto 2021, n. 113, il cui art. 10, ha previsto che «al fine di attuare gli interventi di digitalizzazione, innovazione e sicurezza nella pubblica amministrazione previsti nell'ambito del PNRR, fornendo adeguato supporto alla trasformazione digitale delle amministrazioni centrali e locali, presso la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, opera, fino al 31 dicembre 2026, un apposito contingente massimo di trecentotrentotto unità […] composto da esperti in possesso di specifica ed elevata competenza almeno triennale nello sviluppo e gestione di processi complessi di trasformazione tecnologica e digitale, nonché di significativa esperienza almeno triennale in tali materie […]» (co. 1).

[51] Il testo dell'articolo *de quo*, rubricato "Trattamento di categorie particolari di dati personali" è consultabile sul sito *https://www.privacy-regulation.eu/it/9.htm*.

[52] L. GRECO, *Sanità e protezione dei dati personali*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 244 ss..

dell'art. 32 Cost.[53]. L'emergenza da *Covid-19* ha dimostrato *ad abundantiam* che la sanità vada intesa quale questione di ordine pubblico interno ed internazionale ed inoltre che il diritto alla salute debba esser analizzato nella sua «oggettiva dimensione di situazione complessa»[54], rilevante poiché collettiva.

La pandemia ha colpito l'Italia in maniera assai particolare, gravando sulle Regioni anche indipendentemente dal loro livello di sviluppo socio-economico. Pertanto, la soluzione delle questioni sanitarie necessita di una strategia d'intervento ancorata ai territori di riferimento[55], in quanto non necessariamente connessa a contesti economico-produttivi sottosviluppati.

Oggigiorno la sicurezza dei dati personali e sensibili impiegati nell'erogazione di una prestazione sanitaria rappresenta strumento di realizzazione del diritto alla salute, sia nella sua dimensione individuale che in quella collettiva.

Emerge perciò nettamente l'esigenza improcrastinabile di colmare le lacune ancora sussistenti in ordine all'attuale capacità della Pubblica Amministrazione di cogliere appieno potenzialità e problemi legati all'utilizzo di *smart technologies* in sanità, contribuendo altresì per tale via a ridurre il fenomeno del c.d. *digital divide*.

La pandemia ha determinato un'accelerazione ai tentativi di superamento delle questioni connesse alla digitalizzazione, in quanto la loro risoluzione risulta essenziale per gestire le criticità emergenti dal *Covid-19*. Difatti, i *big data* hanno assunto il ruolo di risorsa fondamentale ai fini del monitoraggio dell'evoluzione della situazione sanitaria.

In Italia, per tentare di porre rimedio ai problemi emersi nel contesto della sanità pubblica digitale, il già citato Decreto Rilancio del 2020 ha introdotto misure urgenti per la salute, connesse all'emergenza da *Covid-19*, al fine di sfruttare il potenziale ancora inesplorato del fascicolo sanitario elettronico ed ha altresì istituito un Fondo per l'innovazione tecnologica e la digitalizzazione.

---

[53] C. COLAPIETRO, F. LAVIOLA, *I trattamenti di dati personali in ambito sanitario*, cit., *passim*, in *www.dirittifondamentali.it*.

[54] R. FERRARA, *L'ordinamento della sanità*, Torino, 2020, 9 ss..

[55] G. MELONE, *La crisi pandemica da Coronavirus: prove di tenuta non solo per il SSN*, in *San. pubbl. e priv.*, 3, 2020, 13 ss..

Ancora, in tema di novità normative, il d.l. 1° marzo 2021, n. 22, convertito con modificazioni dalla l. 22 aprile 2021, n. 55, ha previsto disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri, istituendo tra l'altro un Comitato interministeriale per la transizione digitale.

Nell'ambito delle iniziative assunte dall'Unione Europea per la gestione della ripresa economica e sanitaria *post*-pandemica, si menzionano i programmi di finanziamento del digitale connessi all'approvazione del Quadro finanziario pluriennale per il periodo 2021-2027 del dicembre 2020, tra cui rientra *EU4Health*[56], orientato a fornire un *enforcement* dell'azione europea nel settore sanitario[57].

Il piano *Next generation EU* (NGEU)[58], previsto dall'Unione Europea per sostenere gli Stati membri maggiormente colpiti dalla crisi provocata dal *Covid-19*, contiene una parte specificamente dedicata a digitalizzazione ed innovazione anche nel settore della P.A., ai fini della cui attuazione gli ordinamenti nazionali avrebbero a disposizione risorse finalisticamente condizionate al raggiungimento degli obiettivi indicati dalla Commissione Europea attraverso le *country-specific reccomendations*, enucleati altresì dal rispettivo *National Recovery and Resilience Plan* 2021-23.

In Italia, il Governo Draghi ha approvato il 29 aprile 2021 il Piano nazionale di ripresa e resilienza (PNRR) [59], c.d. *Next generation Italia*, presentato alla Commissione europea *ex* artt. 18 ss. del Regolamento (UE) 2021/241. Inoltre, il d.l. n. 77/2021, delinea il quadro normativo nazionale orientato a semplificare ed

[56] Regolamento (UE) 2021/522 del Parlamento Europeo e del Consiglio del 24 marzo 2021 che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 («programma UE per la salute») (*EU4Health*) e che abroga il regolamento (UE) n. 282/2014.

[57] R. MICCÙ, *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, 2021, 1-15, in *www.federalismi.it*.

[58] S. CIVITARESE MATTEUCCI, *La riforma della pubblica amministrazione nel quadro del "Recovery Fund"*, in *Forum AIPDA Next Generation EU*, in *www.aipda.it*.

[59] Il testo del PNRR è consultabile in www.governo.it. Il PNRR è stato definitivamente approvato il 13 luglio 2021 con Decisione di esecuzione del Consiglio UE (doc. 10160/21), che ha recepito la proposta della Commissione europea, tenendo conto della Raccomandazione della stessa Commissione del 20 maggio 2020 sul programma nazionale di riforma 2020 dell'Italia e che ha formulato un parere del Consiglio sul programma di stabilità 2020 che, nell'evidenziare la decisività di un'amministrazione pubblica efficace per garantire che le misure adottate per affrontare l'emergenza e sostenere la ripresa economica non siano rallentate nella loro attuazione (considerando 24), ha riscontrato, tra le carenze, il basso livello di una digitalizzazione che risultava disomogenea già prima della crisi.

agevolare il perseguimento degli obiettivi fissati dal PNRR *ex* art. 1 del d.l. *de quo*, anche istituendo una Cabina di regia deputata a svolgere compiti d'indirizzo, impulso e coordinamento generale sull'attuazione degli interventi in raccordo con il Comitato interministeriale per la transizione digitale ai sensi dell'art. 2 del citato d.l..

Le misure previste dal PNRR[60] si articolano intorno a tre assi strategici condivisi a livello europeo: accanto alla transizione ecologica e all'inclusione sociale, vi sono digitalizzazione e innovazione. Il Piano è suddiviso in sei Missioni, articolate per Componenti cui corrispondono scelte d'investimento mirate. Nello specifico, sono previste, tra le altre, la Missione 1. Digitalizzazione, innovazione, competitività, cultura e la Missione 6. Salute.

La digitalizzazione viene inquadrata quale necessità trasversale nell'ambito del PNRR[61].

Nello specifico, la Missione 6. Salute è diretta a potenziare e riorientare il SSN al fine di implementarne l'efficacia nel rispondere ai bisogni di cura delle persone,

[60] Sempre nell'ambito del PNRR, sono state previste le c.d. Case della Comunità: nel complesso rapporto tra organizzazione sanitaria e Comuni, l'evoluzione dei concetti di salute e di città favorisce un riposizionamento degli assetti raggiunti. Le Case della Comunità sono orientate a favorire una piena integrazione tra servizi sociali e prestazioni sanitarie, rappresentando uno strumento per ridefinire il ruolo dei Comuni nell'organizzazione sanitaria. Su tali aspetti, si v. il recentissimo saggio di F. PIZZOLATO, *Le Case della Comunità e il rapporto tra città e salute*, in *Riv. Diritti fondamentali*, Fascicolo 1, 2022, 1-26.

[61] Si v. PNRR, 116. La Missione 1 ha come obiettivo di conferire un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese. Ad ogni modo il Piano parte dal presupposto secondo cui «lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre. La digitalizzazione è infatti una necessità trasversale, in quanto riguarda il continuo e necessario aggiornamento tecnologico nei processi produttivi; le infrastrutture nel loro complesso, da quelle energetiche a quelle dei trasporti, dove i sistemi di monitoraggio con sensori e piattaforme dati rappresentano un archetipo innovativo di gestione in qualità e sicurezza degli *asset* (Missioni 2 e 3); la scuola, nei programmi didattici, nelle competenze di docenti e studenti, nelle funzioni amministrative, della qualità degli edifici (Missione 4); la sanità, nelle infrastrutture ospedaliere, nei dispositivi medici, nelle competenze e nell'aggiornamento del personale, al fine di garantire il miglior livello di assistenza sanitaria a tutti i cittadini (Missioni 5 e 6)». Ancora, cfr. PNRR, 118: «Questo sforzo sul lato dell'offerta, da parte della PA, di un servizio digitale performante è accompagnato da interventi di supporto per l'acquisizione e l'arricchimento delle competenze digitali (in particolare quelle di base), realizzati in coordinamento con le altre Missioni […]. Infine, a complemento degli interventi di digitalizzazione e concorrendo ai medesimi obiettivi di produttività, competitività ed equità del sistema economico-sociale, la Componente 1 si prefigge il rafforzamento delle competenze del capitale umano nella PA e una drastica semplificazione burocratica».

altresì in considerazione delle criticità emerse nel corso dell'emergenza pandemica[62] che ha confermato «il valore universale della salute, la sua natura di bene pubblico fondamentale e la rilevanza macro-economica dei servizi sanitari pubblici»[63].

In particolare, la Componente 1 della Missione Salute[64] è orientata al rinnovamento ed all'ammodernamento delle strutture tecnologiche e digitali esistenti, al completamento e alla diffusione del Fascicolo Sanitario Elettronico (FSE), nonché diretta a raggiungere una migliore capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) mediante l'ausilio di sistemi informativi più efficaci[65].

Tutto ciò esplicita il legame inscindibile sussistente tra digitalizzazione e salute.

---

[62] V. BALDINI, *La gestione dell'emergenza sanitaria tra ripristino della legalità costituzionale perduta e realizzazione di un nuovo ordine costituzionale. Aspetti problematici della tutela della salute pubblica in tempo di pandemia*, in Riv. *Diritti fondamentali*, 3, 2021, 290-304, in *www.dirittifondamentali.it*.

[63] Il virgolettato è tratto da PNRR, 287.

[64] La Commissione Europea ha annunciato, nella *Comunicazione sulla strategia europea per i dati*, la sua intenzione di fornire risultati concreti nel settore dei dati sanitari e di sfruttare il potenziale creato nelle tecnologie digitali per introdurre innovazione nella salute e nell'assistenza, aumentando l'accessibilità e la disponibilità di un'assistenza sanitaria di alta qualità.
In linea con tali indicazioni, anche con la consapevolezza del valore che rappresenta per il Paese il c.d. "uso secondario dei dati sanitari" (per la ricerca scientifica e l'innovazione, per le attività di definizione delle politiche e di regolamentazione), è stata inserito nella Missione 6 un requisito di digitalizzazione e di interoperabilità per assicurare lo scambio dei dati e, all'interno dell'Investimento 1.3 "Rafforzamento dell'infrastruttura tecnologica e degli strumenti per la raccolta, l'elaborazione, l'analisi dei dati e la simulazione", una specifica linea di finanziamento per il progetto di potenziamento ed ampliamento a livello centrale del Sistema informativo sanitario nazionale. Si intende quindi procedere in termini di evoluzione ed ammodernamento dell'infrastruttura centrale, dei sistemi di costruzione, raccolta, elaborazione, validazione e analisi dai dati sanitari, con particolare riferimento: al completamento del percorso in atto di costruzione di strumenti simulativi e predittivi del fabbisogno di salute della popolazione, anche con l'integrazione di dati non sanitari; alla valorizzazione dei dati già raccolti attraverso la definizione di meccanismi che consentano di velocizzarne la costruzione e la raccolta ai fini del monitoraggio dei LEA; all'integrazione della raccolta di dati per gli ambiti non ancora caratterizzati da rilevazioni sistematiche; all'adozione dell'approccio *One Health*; a supportare l'innovazione avanzata nella gestione dei dati sanitari attraverso strumenti di AI, *Big Data* e *Machine Learning*. Cfr. *https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it "Strategia europea in materia di dati - Fare in modo che l'UE assuma il ruolo di modello e di guida per una società più autonoma grazie ai dati"; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Dati-e-servizi-sanitari-digitali-lo-spazio-europeo-dei-dati-sanitari_it "Dati e servizi sanitari digitali - lo spazio europeo dei dati sanitari".*

[65] Si v. PNRR, 289.

È fondamentale creare le condizioni affinché esperti di varie discipline riescano a lavorare in rete, con un metodo interdisciplinare integrato, sulle nuove sfide che gli algoritmi stanno creando[66].

Emerge altresì *ictu oculi* la necessità dell'espletamento di un nuovo ruolo da parte del giurista[67], che deve farsi in primo luogo garante contro i rischi della digitalizzazione. La sua creatività risulta amplificata nella ricerca della regola applicativa per il caso concreto. La sfida tecnologica non può fondarsi esclusivamente sull'aspetto computazionale, involgendo un profilo umanistico ed una netta assunzione di responsabilità etica anche da parte del giurista, le cui competenze sono state, per tradizione, erroneamente considerate impermeabili all'automazione[68].

Professioni come quelle di "tecnico legale" o di "ingegnere del sapere giuridico" rappresentano esempi significativi di praticare il diritto in maniera innovativa, interpretando problemi e nuove esigenze della società. Perciò, è necessario effettuare una rinnovata riflessione sul metodo giuridico, che si apra all'apporto conoscitivo delle tecnologie intelligenti di cui anche il giurista dovrebbe però comprendere i profili teorici essenziali[69].

Perseguendo tale via virtuosa, si ritorna *ab origine* alla questione della formazione del giurista e delle risorse umane.

Conclusivamente, può perciò ritenersi che, in fase di tentativo di superamento della crisi pandemica, contraddistinta da un'intensa innovazione tecnologica, si avverte comunque la necessità di un recupero della centralità della persona umana, mediante una formazione che involge l'acquisizione di nuove professionalità e di nuove abilità.

---

[66] E' altresì fondamentale riuscire a trasferire le nuove abilità ai giovani, che domani avranno la responsabilità della crescita della società, soprattutto per l'Italia in ritardo nella formazione di capitale umano per la società digitale. Sul punto, si v. G.F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia*, 2019, 18-19.

[67] G. CORASANITI, *Intelligenza artificiale e diritto: il nuovo ruolo del giurista*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 405 ss.

[68] P. MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Riv. dir. media*, 2019, 21 ss.; S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 2018, 1801 ss.

[69] A. LALLI, *Intelligenza artificiale e diritto*, in AA.VV., *L'amministrazione nell'assetto costituzionale dei pubblici. Scritti per Vincenzo Cerulli Irelli*, I, Torino, 2021, 646 ss.

La stessa assunzione della necessità di superare il *digital divide*[70] rappresenta uno strumento di riaffermazione della centralità dell'uomo nell'ambito delle tecnologie *smart*[71], in cui la predisposizione ed attuazione normativa di adeguati livelli di sicurezza informatica[72] diviene adempimento fondamentale, specialmente nel settore della sanità pubblica in perdurante fase di emergenza da *Covid-19*.

In una prospettiva *de iure condendo*, altresì con l'ausilio della giurisprudenza[73], sarebbe doveroso un efficace contemperamento sostanziale tra diritto del paziente alla riservatezza ed utilità della condivisione del dato sanitario. Ciò consentirebbe quantomeno di allentare la tensione che caratterizza i dati sanitari, meritevoli da un lato della massima protezione e riservatezza e, dall'altro, di una sia pur calibrata circolazione per esigenze di sanità pubblica.

I dati sanitari necessitano altresì di protezione anche in termini di esattezza e qualità che il loro trattamento deve garantire per ridurre il rischio clinico. Difatti, qualora in sede diagnostica siano utilizzati dati inesatti, le probabilità di errori aumentano notevolmente, esponendo il paziente a rilevanti pericoli. Ciò si evince specificamente in relazione all'uso di strumenti diagnostici incentrati sull'Intelligenza artificiale.

La novellata disciplina del *GDPR* può perciò rappresentare il fulcro attorno a cui possa orientarsi "un governo lungimirante delle informazioni sanitarie"[74] e, dunque, un progetto di politiche pubbliche idoneo a valorizzare la salute quale "diritto fondamentale dell'individuo" ma altresì "interesse della collettività", con le garanzie necessarie per assicurare il rispetto della persona umana sancito dall'art.

[70] G. CAVALCANTI, *Dalla riduzione del digital divide alla semplificazione dei servizi online: le nuove misure del decreto di attuazione del PNRR, 2022*, in *https://www.irpa.eu/dalla-riduzione-del-digital-divide-alla-semplificazione-dei-servizi-online-le-nuove-misure-del-decreto-di-attuazione-del-pnrr/*.

[71] R. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 80-81.

[72] AA. VV., *e-Health Data Sharing. Best practices e soluzioni per la condivisione del dato, l'anonimizzazione e la creazione di data lake con dati sanitari*, 2021, 1-45, in *www.datawalley.it*.

[73] Cons. Stato, sez. VI, 8 aprile 2019, n. 2270 e T.a.r. Lazio, sez. III-bis, 27 maggio 2019, n. 6606, entrambe in www.giustizia-amministrativa.it. La giurisprudenza del Consiglio di Stato ha sottolineato l'imprescindibilità della ricerca della regola tecnica che governa ogni algoritmo, con una motivazione incentrata sul diritto dell'Unione europea e sull'art. 22 *GDPR*.

[74] Cfr. P. STANZIONE, *Sicurezza del dato sanitario e condivisione*, Intervento di Pasquale Stanzione, Presidente del Garante per la protezione dei dati personali, 18 febbraio 2022, in *www.garanteprivacy.it*.

32 Cost.. Tali garanzie assumono un grande rilievo poiché sulla sinergia tra salute, innovazione e *privacy* è in corso una sfida sempre più determinante per il progresso della società, che va opportunamente orientato nel segno della centralità della dignità della persona umana.

La sicurezza dei dati sanitari nelle smart technologies quale strumento di realizzazione del diritto alla salute tra telemedicina ed intelligenza artificiale

La sicurezza dei dati personali e sensibili impiegati nell'erogazione di una prestazione sanitaria costituisce strumento di realizzazione del diritto alla salute, sia nella sua dimensione individuale che in quella collettiva.

Sussiste un nesso funzionale, in ambito sanitario, tra la *quaestio* della sicurezza – nella formazione, conservazione, utilizzo e circolazione del dato clinico – e quella della *privacy*. E' indispensabile perseguire l'obiettivo della protezione dei dati personali mediante un approccio "dinamico", che involge anche i flussi di dati.

Ai sensi del *GDPR*, la strategia per la sicurezza dei dati personali è incentrata sul "principio generale del trattamento". Emerge un approccio di tutela dei dati personali fondato sulla gestione complessiva del rischio nonché sulla responsabilizzazione proattiva del Titolare del trattamento, chiamato a modulare "in concreto" l'attuazione dei principi sanciti dal Regolamento.

Nell'ottica dell'*accountability*, la sicurezza dei dati personali, involgendo l'applicazione di misure differenti, richiede una visione integrata di plurime competenze, – tra cui quelle giuridiche, informatiche ed organizzative.

La digitalizzazione viene inquadrata quale necessità trasversale nell'ambito del PNRR. Il contributo offre un'analisi tecnico-giuridica aggiornata, alla luce del recente dato normativo (anche comunitario), dottrinale e giurisprudenziale, nella più ampia prospettiva di un'integrazione equilibrata tra dimensione umana ed avanzamento tecnologico in sanità.

The security of personal and sensitive data used in the provision of a health service is a tool to realize the right to health, both in its individual and collective dimension.

There is a functional link, in the health sector, between the issue of safety – in the training, conservation, use and circulation of clinical data – and that of privacy. Data is essential to protect personal data through a "dynamic" approach, which also involves data flows.

Under the GDPR, the strategy for the security of personal data is focused on the "general principle of processing". A personal data protection approach emerges based on overall risk management as well as on the proactive accountability of the Data Controller, called to modulate "concretely" the implementation of the principles enshrined in the Regulation.

With a view to accountability, the security of personal data, involving the application of different measures, requires an integrated vision of multiple competences, – including legal, IT and organizational ones.

Digitization is seen as a transversal need within the PNRR. The essay offers an updated technical-juridical analysis, in the wider perspective of the recent wide legislative (including european), doctrinal and jurisprudential data, in the more than a balanced integration dimension between human and technological advancement in health.

G. Lofaro – La sicurezza dei dati sanitari nelle smart technologies quale strumento di realizzazione del diritto alla salute tra telemedicina ed intelligenza artificiale Scarica

Categorie: Fascicoli, Numero 2-2022, Senza categoria | - Giuseppina Lofaro

Post correlati

Procreazione medicalmente assistita e status detentionis:
2 Ottobre 2024

La salvaguardia dell'ambiente, dal punto di vista della teoria
30 Settembre 2024

Lo Stato culturale. Prime riflessioni sul tema
30 Settembre 2024

Ricerca in corso...

Newsletter

Name*

Email*

Submit

Comunicati della Rivista

Statement by the European Commission on the situation in the Central Mediterranean

Il Prof. Vincenzo Baldini ricorda e onora la memoria del Prof. Dr. Hans Meyer

La rivista "Diritti Fondamentali" ricorda e onora la memoria del Prof. Paolo Grossi

tutti i comunicati >>

Documenti di attualità

Esistenza di un evidente rischio di violazione grave da parte dell'Ungheria dei valori su cui si…

Notification of 12 applications concerning abortion rights in Poland

Commissione europea – Decisioni sui casi d'infrazione

tutti i documenti >>

dirittifondamentali.it - ISSN 2240-9823.

Direttore scientifico e responsabile:
Prof. Vincenzo Baldini

Condirettori:
Prof. Stelio Mangiameli, Prof. Fabrizio Politi, Prof. Vincenzo Tondi della Mura, Prof.ssa Agata Cecilia Amato Mangiameli

Contatti: info@dirittifondamentali.it

La Rivista Dirittifondamentali.it è registrata presso il Tribunale di Cassino n. 830 del 14.6.2017. Rivista quadrimestrale inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche