«Il diritto dell'economia» issn 1123-3036, anno 67, n. 106 (3 2021), pp. 49-82

Articoli e saggi

Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*

Paola Lombardi

1. *Introduzione*

Un anziano diabetico, con difficoltà di deambulazione, ha bisogno di conoscere la quantità di zuccheri presenti in un alimento. Interroga il suo assistente digitale, il quale risolve il suo problema e gli fornisce precise indicazioni terapeutiche dietro fornitura dei dati sanitari del paziente.

Una madre ricorre ad un logopedista digitale per il suo bimbo dislessico, affinché la patologia trovi un costante monitoraggio ed un tentativo di correzione.

Altri esempi si potrebbero fare[1] per dimostrare non solo come da sempre le tecnologie supportino – e quindi condizionino – i processi curativi, ma anche come il concretizzarsi di un impiego diffuso di tecnologie all'avanguardia (o

* Lo scritto costituisce rielaborazione ed ampliamento della relazione tenuta nell'ambito del Convegno di studi italo-cinese organizzato dal CREAF, Centro Universitario Interdipartimentale di Ricerca on European Affairs del Dipartimento di Giurisprudenza dell'Università degli Studi di Brescia, sul tema "*Smart living and Environment. Justice, health, political economy and sustainability in the context of Post-Neoliberism, Post-Pandemic and Post-Postmodernism*" (7 maggio 2021).

[1] Alcuni di questi si possono trovare in C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale* e in Id., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, entrambi in *BioLaw Journal*, 2019,

smart) in ambito sanitario, che ad esempio favoriscano diagnosi precoci o l'erogazione di cure in una condizione di distanza tra medico e paziente, non sembri ormai essere molto lontano dalla realtà.

E così, se nelle linee d'indirizzo nazionali in materia di telemedicina, elaborate dal Ministero della Salute, si sottolinea tra le opportunità da questa offerte l'equità di accesso all'assistenza sanitaria, quanto precede vale, a maggior ragione, all'epoca del Covid-19, nella quale il progresso tecnologico ha consentito una raccolta di dati senza precedenti, processando i quali è stato ad esempio possibile realizzare vaccini a tempo di record[2].

In questi casi, «la tecnologia è un flusso immateriale d'informazioni che si trasforma in conoscenza professionale e poi nel *prodotto* di un'organizzazione. Ha in sostanza la capacità di trasformare un'informazione *ambientale*, immateriale (un bisogno, un'emozione, una sofferenza) in un prodotto, come potrebbe essere la cura di una malattia»[3], attraverso un processo di "avatarizzazione" della funzione medica[4].

Sempre più spesso, ad usufruire delle nuove tecnologie, ai professionisti si affiancano in verità i cittadini, che vedono il progressivo intensificarsi di un'assistenza clinica fornita al proprio domicilio, o addirittura "in movimento".

Quest'ultimo è l'effetto dello sviluppo della c.d. "sanità mobile" (*mobile health* o *mHealth*), che oggi consente l'utilizzo di *software* eseguibili su dispositivi portatili per monitorare e migliorare il proprio stato di salute, anche mediante la connessione tra molteplici strumenti e sensori indossabili, con un conseguente contenimento della spesa pubblica nel settore della sanità[5]: si pensi, in particolare, ai benefici che ne derivano in materia di dipendenze e di patologie croniche o degenerative.

Lungo questa via, la conoscenza medica diviene sempre meno appannaggio di una sola categoria di soggetti, poiché la digitalizzazione permette di renderla

---

rispettivamente 179 e 716-717, nonché in S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Torino, 2020, 72 ss.

[2] G. Maira, *Intelligenza umana e intelligenza artificiale*, in *www.federalismi.it.*

[3] M. Moruzzi, *La sanità dematerializzata e il fascicolo sanitario elettronico. Il nuovo welfare a bassa burocrazia*, Roma, 2015, 18.

[4] L'espressione 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.

[5] 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, 135-135. Sulla definizione di *mHealth*, anche E. Stefanini, *Telemedicina* mHealth *e diritto*, in *Rass. dir. farm.*, 2016, 1023 ss., e, più in generale, sulle potenzialità offerte dal digitale in sanità, D. Ielo, *L'agenda digitale: dalle parole ai fatti*, Torino, 2015, 81 ss.

disponibile per larghe fasce di popolazione, «contribuendo alla sua disseminazione universale»[6].

Detto in altre parole, l'impiego dell'Intelligenza Artificiale (IA) in medicina promette una democratizzazione di questa sia sul versante della diagnosi che delle raccomandazioni di trattamento, nel suo aprire l'accesso a prestazioni altrimenti non accessibili a tutti e contraendo sensibilmente i costi di assistenza: «una IA che sostituisca ed ottimizzi l'operato professionale è replicabile virtualmente quasi senza costo»[7].

Certamente, di questi fenomeni è possibile apprezzare gli aspetti positivi, ma non vanno sottaciuti quelli negativi.

Infatti, se da una parte si trova l'opportunità di rafforzare il rapporto fiduciario tra medico e paziente, poiché il primo, affidando all'IA il compito di analizzare i dati raccolti, recupererebbe il tempo necessario per stabilire una comunicazione più efficace con il secondo[8], dall'altra vi è 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 una situazione di rinegoziazione del potere esistente nel sistema sanitario a favore del paziente[9].

E così, l'aumento delle nuove conoscenze finisce per incidere in senso critico 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»[10].

Al tempo stesso, è soprattutto sulla *mHealth* che si concentrano le principali preoccupazioni dei pazienti quanto alla sicurezza dei dati clinici, anche per la frequente assenza di consapevolezza in ordine alle modalità di trattamento dei dati o per le autorizzazioni eccessive spesso richieste dalle singole *app*[11].

Queste circostanze, con il loro lasciar emergere relazioni del tutto nuove tra uomo e macchina, sollecitano oggi lo studioso del diritto amministrativo a rivolgere rinnovata attenzione alla tutela di dati personali "sensibili" come quelli relativi alla salute, specie nei rapporti con la pubblica amministrazione.

---

[6] A. Ardissone, *La relazione medico-paziente nella sanità digitale. Possibili impatti sul professionalismo medico*, in *Rass. it. sociologia*, 2018, 78.

[7] 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.

[8] M. Savini Nicci, G. Vetrugno, *Intelligenza artificiale e responsabilità nel settore sanitario*, cit., 607.

[9] A. Ardissone, *La relazione medico-paziente nella sanità digitale*, cit., 79 ss.

[10] R. Lombardi, *Errore umano e incidenti organizzativi in medicina*, in questa *Rivista*, 2021, 218.

[11] S. Pari, M.L. Rizzo, *L'utilizzo di applicazioni di* mHealth, cit., 138 e 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.

A tal proposito, ed in via del tutto preliminare, si noti che 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 (d'ora in poi GDPR), prevede all'art. 22 che l'interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, cui va comunque riconosciuto il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

Ferma restando la preliminare necessità di comprendere il significato del concetto di decisione basata *unicamente* sul trattamento automatizzato, che differenza farà imbattersi in un medico che è contrario *a priori* a confermare una decisione algoritmica piuttosto che venire a contatto con un medico particolarmente indulgente e pronto ad assecondare il sistema scegliendo l'opzione più idonea a supportare le scelte della macchina?

Non solo. Se il GDPR, nel sancire i principi applicabili al trattamento dei dati personali, prevede che il titolare del trattamento sia competente per il loro rispetto e debba essere in grado di comprovarlo (c.d. *accountability*), tale soggetto si dovrà in primo luogo trovare nelle condizioni di comprendere il contenuto dei suoi obblighi, sia per non incorrere in responsabilità professionale, che ai dichiarati fini di tutela.

Visto quanto precede, per cercare di fornire risposte ad alcuni degli interrogativi che sorgono dall'applicazione di tecnologie *smart* nella sanità pubblica in Italia, preliminare sarà una rapida indagine sullo stato di avanzamento della riforma in senso digitale sia della pubblica amministrazione che dello specifico settore sanitario, riforma alla quale verrà conclusivamente dedicata attenzione in un'ottica *de iure condendo*.

Pur nella consapevolezza che l'IA costituisca fenomeno ben più complesso rispetto alla sola informatizzazione dei processi[12], è tuttavia innegabile che rappresenti la frontiera più avanzata della digitalizzazione. Inoltre, l'indagine sullo stato di avanzamento di quest'ultima in Italia sarà comunque utile per appurare l'attuale capacità della pubblica amministrazione di comprendere un modo adeguato potenzialità e rischi connessi all'impiego di tecnologie *smart* in sanità.

Seguirà l'approfondimento delle disposizioni del GDPR che consentiranno di riflettere su alcune criticità che da quell'impiego discendono, alla ricerca dell'origine dei problemi e di possibili soluzioni e gettando uno sguardo nella direzione verso la quale sta volgendo o dovrebbe volgere il sistema.

[12] Su questa precisazione e sugli errori più comuni ad essa connessi, G. Pasceri, *Intelligenza artificiale, algoritmo e* machine learning. *Le responsabilità del medico e dell'amministrazione sanitaria*, Milano, 2021, 3 ss.

2. *L'amministrazione digitale nella sua evoluzione normativa: cenni*

Per quanto l'art. 3 del *Codice dell'amministrazione digitale* (d.lgs. 7 marzo 2005, n. 82, d'ora in poi C.a.d.) non fosse una novità in senso assoluto, poiché già la l. 4/2004 (c.d. *Legge Stanca*) aveva posto le premesse per il riconoscimento del diritto di accesso individuale alle tecnologie come diritto sociale strumentale al godimento delle libertà fondamentali[13], esso ha comunque costituito una disposizione di vera e propria "rottura culturale" rispetto ad un'ormai inaccettabile situazione caratterizzata da consistenti barriere tecniche, economiche e giuridiche a tale accesso[14].

Il «diritto all'uso delle tecnologie», da questo articolo sancito, ha infatti inteso costituire il simbolo di una nuova generazione di diritti, tali da rendere il Codice la chiave di volta di una riforma della pubblica amministrazione in senso digitale[15]: nel suo essere anche strumento funzionale al raggiungimento di obiettivi di maggiore efficacia ed efficienza dell'azione amministrativa e di miglioramento dei rapporti col cittadino[16], sembrava anche in grado di produrre addirittura un'evoluzione di natura sostanziale del diritto amministrativo[17], implementando le potenzialità del decisore pubblico.

---

[13] Nel senso che la stessa legge del 2004, nell'intento di favorire e semplificare l'accesso agli strumenti informatici da parte degli utenti, specie delle persone con disabilità, conteneva già la definizione di applicazioni mobili, R.M. Colangelo, *App mediche e protezione dei dati personali*, cit., 284. In generale, sulle principali tappe del percorso evolutivo seguito dalla diffusione delle risorse tecnologiche e telematiche all'interno della pubblica amministrazione in Italia, G. Piperata, *Cittadini e imprese di fronte all'amministrazione digitale*, in *Diritto Mercato Tecnologia*, 2016, 169 ss. Sugli effetti benefici di questa diffusione, già A.G. Orofino, *L'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi*, in *Giornale dir. amm.*, 2004, 1371 ss.

[14] M. Pietrangelo, *Il diritto all'uso delle tecnologie nei "rapporti" con la pubblica amministrazione: luci e ombre*, in *Inf. e dir.*, 2005, 77 ss. Sull'evoluzione normativa che ha portato all'emanazione del C.a.d., S. Rodriguez, *L'amministrazione digitale e il nuovo codice: vera rivoluzione o esagerato ottimismo?*, in *Resp. civ. e prev.*, 2011, 1439 ss. Sulle sue disposizioni, G. Cassano-C. Giurdanella, *Il codice della pubblica amministrazione digitale. Commentario al D.lgs. n. 82 del 7 marzo 2005*, Milano, 2005, I. D'Elia, M. Pietrangelo, *Il codice dell'amministrazione digitale nel processo di semplificaione normativa: genesi e criticità*, in *Inf. e dir.*, 2005, 9 ss., C. Giurdanella, E. Guarnaccia, *Il diritto pubblico dell'informatica nel d.lgs. n. 82/2005: rilievi critici*, ivi, 235 ss., M. Quaranta (a cura di), *Il codice della pubblica amministrazione digitale*, Napoli, 2006, G. Duni, *L'amministrazione digitale. Il diritto amministrativo nella evoluzione della telematica*, Milano, 2008, spec. 61 ss., E. Carloni, *La riforma del Codice dell'amministrazione digitale*, in *Giornale dir. amm.*, 2011, 469 ss., Id., *Amministrazione aperta e* governance *dell'Italia digitale*, *ivi*, 2012, 1041, M. Iaselli (a cura di), *La nuova pubblica amministrazione. I principi dell'Agenda digitale*, Roma, 2014, F. Trojani, *Il nuovo codice dell'amministrazione digitale*, Rimini, 2017 e G. Pesce, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018, 49 ss.

[15] R.M. Di Giorgi, *Democrazia, federalismo e società dell'informazione nel* Codice dell'amministrazione digitale*: spunti di riflessione*, in *Inf. e dir.*, 2005, 61.

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

[17] Su questi argomenti, D. Marongiu, *Mutamenti dell'amministrazione digitale. Riflessioni* a posteriori e I. Martín Delgado, *L'amministrazione digitale come nuovo modello di amministrazione pubblica*, entrambi in D. Marongiu, I. Martín Delgado (a cura di), *Diritto amministrativo e innovazione. Scritti in ricordo di Luis Ortega*, in *Diritto e processo amministrativo. Quaderni, 23*, 2016, rispettivamente 45 e 47 ss.

A conferma di quanto si va dicendo, lo stesso art. 2 C.a.d., nel disporre che gli enti territoriali assicurino disponibilità, gestione, accesso, trasmissione, conservazione e fruibilità dell'informazione in modalità digitale, configura una vera e propria pretesa del cittadino a fruire di strumenti tecnologici in grado di facilitare la sua interazione con l'amministrazione o, in altre parole, un vero e proprio «diritto all'amministrazione digitale»[18]. Un diritto che si presenta «come sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete»[19]: non una «somma algebrica dell'amministrazione tradizionale più la nuova tecnologica elettronica, ma un fenomeno con caratteristiche inedite e dotato di portata sistemica nell'ambito dell'ordinamento giuridico complessivo»[20].

Peraltro, emerse fin da subito la preoccupazione che la portata innovativa del decreto fosse più prospettata che attuata[21].

E ciò in ragione del fatto che il C.a.d. contiene, in prevalenza rispetto a quelle precettive, enunciazioni programmatiche e di principio[22], per loro natura prive di effetti immediatamente vincolanti, e, pertanto, rimesse alla cangiante volontà attuativa delle amministrazioni[23].

La stessa storia dell'art. 3, caratterizzata da numerosi rimaneggiamenti che hanno portato il suo primo comma, 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

---

[18] P. Pesce, *I «nuovi diritti» nell'amministrazione digitale*, in *Rass. dir. pubb. europeo*, 2007, 207. Sulla configurazione di un diritto del privato ad interagire con i pubblici poteri anche in via telematica, sia altresì consentito rinviare a P. Lombardi, *Riflessioni in tema di istruttoria nel processo amministrativo: poteri del giudice e giurisdizione soggettiva "temperata"*, in *Dir. proc. amm.*, 2016, 85.

[19] Si riportano le parole di S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 13.

[20] P. Costanzo, *Avete detto "diritti digitali"?*, in *Diritto Mercato Tecnologia*, 2016, 149.

[21] P. Pesce, *I «nuovi diritti» nell'amministrazione digitale*, cit., 203.

[22] Del resto, in giurisprudenza, la sentenza del T.a.r. Basilicata, sez. I, 23 settembre 2011, n. 478 (in *Foro amm. TAR*, 2011, 12, 4098), rappresenta la prima ed isolata pronuncia del giudice amministrativo nel senso della piena effettività del diritto all'uso delle tecnologie *ex* art. 3 C.a.d., poiché ha condannato un'amministrazione regionale a porre in essere gli adempimenti necessari alla pubblicazione sulla *homepage* del suo sito istituzionale dell'indirizzo di posta elettronica certificata (PEC) a cui il cittadino possa rivolgersi, proprio perché la pubblica amministrazione era tenuta a consentire agli utenti di interloquire tramite posta elettronica certificata al fine di rendere effettivo il loro diritto a richiedere ed ottenere l'uso delle tecnologie telematiche. In tema, P. Lopriore, *L'effettività del diritto all'uso delle tecnologie nel Codice dell'Amministrazione Digitale. La sentenza del T.A.R. Basilicata n. 478/2011*, in *Ciberspazio e diritto*, 2012, 121 ss., F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2015, 257 e M.F. Maricosu, *Il diritto all'uso delle tecnologie: quale futuro?*, in D. Marongiu, I. Martín Delgado (a cura di), *Diritto amministrativo e innovazione. Scritti in ricordo di Luis Ortega*, in *Diritto e processo amministrativo. Quaderni,* 2016, 23, 249 ss.

[23] Sul punto, S. Cacace, *Codice dell'amministrazione digitale Dd.Lgs. n. 82/2005 e n. 159/2006*, in *www.giustizia-amministrativa.it*, R.M. Di Giorgi, *Democrazia, federalismo e società dell'informazione*, cit., 65, C. Leone, *Il ruolo del diritto europeo nella costituzione dell'amministrazione digitale*, in *Riv. it. dir. pubb. com.*, 2014, 867 ss. e M.F. Maricosu, *Il diritto all'uso delle tecnologie*, cit., 239 ss.

pubblici servizi statali»[24] allo 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», tradisce la fatica per la ricerca di soluzioni normative che consentissero il reale equilibrio di tutti gli interessi coinvolti.

È stata probabilmente questa circostanza, ad esempio, a portare alla delega del governo, mediante l'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 volti a modificare ed integrare il C.a.d. tramite 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*[25].

Le disposizioni attuative della Legge Madia, tra il 2016 ed il 2017, hanno cercato di seguire il cammino tracciato dalla delega, inserendo ad esempio 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 il quale «chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato», anche a testimonianza della consapevolezza che la semplicità costituisce un efficace strumento di semplificazione.

Tuttavia, non è stata fornita un'adeguata risposta all'esigenza di superamento della mera programmaticità delle disposizioni del Codice, anche per la perdurante mancanza di un adeguato apparato sanzionatorio in caso di inerzia dell'amministrazione[26] e per la grande variabilità dei soggetti incaricati di guidare il processo d'innovazione tecnologica[27].

Del resto, anche nel campo dell'uso del digitale da parte della pubblica amministrazione, l'Italia – come meglio verrà osservato nel prosieguo – si è contraddistinta per una particolare enfasi posta sull'approccio normativo, che si è poi rivelata inversamente proporzionale rispetto al decrescere del finanziamento del-

---

[24] In relazione a questa formulazione del comma, aveva manifestato stupore per il fatto che oggetto del diritto fosse non solo l'ottenere, ma anche il richiedere, che del primo resta sempre il necessario presupposto, rilevando il carattere ridondante della disposizione, N. Lugaresi, *Codice dell'amministrazione digitale e rapporti tra cittadino e pubblica amministrazione*, in *www.giustamm.it.*

[25] Sui principi posti dalla legge Madia in materia di digitalizzazione, 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., T. Tessaro, S. Piovesan, *La riforma Madia del procedimento amministrativo. La legge 241/90 dopo la legge 124/2015*, Rimini, 2015, 142 ss. e, per un commento alla normativa di riforma degli anni 2016 e 2017, B. Carotti, *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice. Il commento*, in *Giornale dir. amm.*, 2017, 7 e 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.

[26] C. Leone, *Il principio "digital first": obblighi e diritti in capo all'amministrazione e a tutela del cittadino. Note a margine dell'art. 1 della legge 124 del 2015*, in *www.giustamm.it.*

[27] G. Cammarota, P. Zuddas, *Introduzione*, in G. Cammarota, P. Zuddas (a cura di), *Amministrazione elettronica. Caratteri, finalità, limiti*, Torino, 2020, 10-11.

le relative politiche nazionali: in altre parole, la regolazione ha progressivamente caricato su di sé l'obiettivo della digitalizzazione pubblica, di fatto favorendo la frammentazione di previsioni delle quali si è persa la complessiva portata culturale e riformatrice[28].

3. *La sanità tra digitalizzazione e precisazioni terminologiche*

Tra le riforme del C.a.d. che si sono succedute nel tempo, quella che più interessa in questa sede è contenuta nel d.l. 5/2012, c.d. *Decreto Semplificazione 2012*, intitolato *Agenda digitale italiana*, resa operativa dalle misure previste dal d.l. n. 179/2012 (c.d. *Decreto Crescita 2.0*) con l'obiettivo prioritario della modernizzazione dei rapporti tra pubblica amministrazione, cittadini ed imprese[29].

Fra le macro-aree prese in considerazione dall'Agenda digitale e dal *Decreto Crescita 2.0* si trova anche la "Sanità digitale", alla quale il d.l. 179 ha espressamente dedicato la Sezione IV.

Per sanità digitale, o sanità elettronica o *eHealth*, s'intende l'utilizzo delle nuove tecnologie nel dominio sanitario allo scopo 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)[30] ed intervenire sulle diseconomie che caratterizzano la spesa sanitaria pubblica[31].

---

[28] 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.

[29] Su questi temi, R. Carpentieri, *Il decreto "crescita 2.0"*, in *Giornale dir. amm.*, 2013, 223 ss. e 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. Sui contenuti che l'Agenda deve avere affinché costituisca veramente uno strumento di programmazione d'importanza strategica nel nostro Paese nel senso dell'innovazione, G. De Michelis, *Agenda digitale: di che cosa si sta parlando?*, in *Amministrare*, 2013, 69 ss.

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

[31] Sugli aspetti benefici della *eHealth*, S. Coronato, *Il processo di digitalizzazione del S.S.N.*, in *Dir. san. mod.*, 2019, 93 ss. Sull'andamento delle varie voci che compongono la spesa sanitaria pubblica italiana in questi ultimi anni, Aa.Vv., *Le sfide di oggi per la sanità del domani. Servizio Sanitario Nazionale: destinazione futuro*, Roma, 2018, mentre, per i dati aggiornati sulla diminuzione del finanziamento pubblico della spesa sanitaria, le cui conseguenze negative sono accentuate dalla pandemia, si veda l'attenta analisi 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.

Strettamente correlata alle politiche europee in materia[32], vi rientra anche la *mHealth*[33], cui si è fatto cenno nell'introduzione di questo lavoro.

È bene sottolineare fin da subito come l'espressione "sanità digitale" abbia un duplice significato, poiché indica l'applicazione delle tecnologie non solo in ambito diagnostico, ma anche ai processi organizzativi dei sistemi sanitari[34].

Si tratta di logiche distinte, e tuttavia spesso tra loro interdipendenti, poiché coinvolgono non solo l'erogazione della prestazione sanitaria, soprattutto in termini di attendibilità clinica, ma anche la comunicazione, gestione e conservazione dell'insieme delle informazioni a questa collegate ed un numero variabile di soggetti (pubblici e privati).

Con specifico riferimento ai processi organizzativi e di gestione dei sistemi, al fine di migliorare i servizi ai cittadini ed il monitoraggio della spesa nel settore sanitario, il d.l. 5/2012 ha dato l'avvio alla «Semplificazione in materia di sanità digitale» (art. 47-*bis*), che richiede di privilegiare, nei piani di sanità nazionali e regionali, «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», prevedendo altresì che la conservazione delle cartelle cliniche avvenga anche solo in forma digitale.

Secondo il legislatore, fulcro del sistema della sanità digitale italiana sono il fascicolo sanitario elettronico (FSE: art. 12), la prescrizione medica e la cartella clinica digitali (art. 13)[35].

---

[32] «La piena attuazione dell'*e-health* è essenzialmente subordinata ad una decisione politica, e dipende dunque in larga misura dalle scelte che gli Stati membri dell'Unione vorranno adottare in tale ambito»: così F. Gaspari, *La circolazione dei dati genetici e delle biobanche: limiti e prospettive* de iure condendo, in *www.federalismi.it*. Sul percorso seguito dall'Unione Europea ai fini dell'implementazione del settore della *Digital Health* e, in particolare, dell'interoperabilità dei sistemi sanitari, 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)* e C. Ingenito, *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, entrambi in *www.federalismi.it*.

[33] R.M. Colangelo, *App mediche e protezione dei dati personali*, cit., 281.

[34] In generale, sull'impatto dell'uso delle tecnologie sia sull'organizzazione che sull'attività amministrativa, anche in relazione al disposto dell'art. 3-*bis* l. 241/1990 che richiama le amministrazioni ad incentivare l'uso della telematica nei rapporti interni, tra diverse amministrazioni e tra queste ed i privati, 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. e Id., *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?*, in *Ciberspazio e diritto*, 2018, 322 ss.

[35] M. Martoni, *Sanità digitale*, in M. Iaselli (a cura di), *La nuova pubblica amministrazione. I principi dell'Agenda digitale*, Roma, 2014, 141 ss., utile anche per la ricostruzione della progressiva attenzione che l'Unione Europea ha rivolto alla sanità digitale e delle prime politiche europee in materia, insieme a M.G. Virone, *Il fascicolo sanitario elettronico*, cit., *passim.* Per l'approfondimento di alcuni delicati profili connessi alla gestione della *privacy* in tema di cartella clinica, già 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.

È soprattutto il FSE a consentire di svolgere considerazioni utili all'economia del presente lavoro[36], come del resto conferma l'attenzione che gli ha dedicato, al tempo del Covid-19, il d.l. 19 maggio 2020, n. 34 (c.d. *Decreto Rilancio*), convertito, con modificazioni, dalla l. 17 luglio 2020, n. 77, che, nel tentativo di superare la scarsa diffusione che ha tradizionalmente caratterizzato lo strumento[37] come contenitore storico dei soli contatti che un soggetto ha avuto con il SSN, ha previsto che il fascicolo sanitario elettronico costituisca l'insieme, aggiornato in modo tempestivo e continuativo, dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici riguardanti l'assistito e riferiti anche alle prestazioni erogate al di fuori del servizio pubblico.

Si considerino in materia anche solo le disposizioni che seguono.

Se, ai sensi dell'art. 12, co. 2, d.l. 179/2012, la sua istituzione 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» (co. 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[38], in con-

[36] Sulle definizioni di fascicolo sanitario elettronico, spesso in verità riferite a strumenti di diversa natura, specie nei documenti internazionali, M.G. Virone, *Il fascicolo sanitario elettronico*, cit., 45 ss. Più in generale, sui contenuti del FSE, M. Farina, *Il cloud computing in ambito sanitario tra security e privacy*, Milano, 2019, 46 ss., S. Coronato, *Gli strumenti necessari al processo di digitalizzazione del S.S.N.*, in *Dir. san. mod.*, 2019, 169 ss., F. Castiello, V. Tenore (a cura di), *Manuale di diritto sanitario*, Milano, 2018, 678 ss., Aa.Vv., *Le sfide di oggi per la sanità di domani*, cit., 183 ss., e sulle linee guida che, nel tempo, 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. Infine, per uno sguardo alla diffusione regionale del FSE in Italia, M. Moruzzi, *La sanità dematerializzata e il fascicolo sanitario elettronico*, cit., 24 ss.

[37] Ne danno conto E. Sorrentino, A.F. Spagnuolo, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *www.federalismi.it.* Saluta con favore questa novità, per gli effetti benefici che produce in termini di protezione della salute dell'individuo, G. Crisafi, *Fascicolo sanitario elettronico: "profilazione" e programmazione sanitaria*, *ibidem*. In argomento, si legga anche l'approfondimento di F. Covino, *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, *ibidem.*

[38] Il co. 7 chiama 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 compititi 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

formità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali» (co. 6).

Il dettato normativo di cui si è appena dato conto, anche a voler tralasciare i dubbi interpretativi che suscita l'indeterminatezza di alcune sue parti (si pensi, ad esempio, alla necessità di riempire di contenuto il concetto di «casi di emergenza sanitaria secondo modalità individuate a riguardo»), costituisce significativa dimostrazione di quanto siano profondamente e delicatamente implicati, in ambito sanitario, il tema della *sicurezza* (nella formazione, conservazione, uso e circolazione del dato clinico) e quello della *privacy*, che spesso – ed in modo del tutto improprio – vengono considerati come sinonimi[39].

In particolare, evidenzia fin da subito come, nella sanità digitale, la garanzia del sistema in termini di affidabilità, ma anche di conoscibilità, dei procedimenti ad esso sottesi e dei relativi risultati, sia essenziale tanto per la concessione del consenso al trattamento dei dati personali da parte dei pazienti, che per la tranquillità del personale sanitario sul piano della responsabilità professionale.

Viste le premesse, e secondo i propositi più sopra dichiarati, per rendere ulteriormente conto delle problematiche sottese ai processi di digitalizzazione della sanità pubblica in Italia e per tentare di fornirvi possibili soluzioni, sembra opportuno rivolgere ora l'attenzione ad alcune disposizioni contenute nel già citato Regolamento europeo 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, scelte per la loro specifica attinenza al trattamento dei dati relativi alla salute.

4. *La sanità digitale sotto la lente del GDPR: la rilevanza della "sicurezza del dato" nella prospettiva dell'accountability*

È stata proprio l'incessante e frenetica evoluzione tecnologica e, in particolare, la digitalizzazione della società e dell'economia globale, a costituire uno dei fondamentali presupposti che hanno indotto la Commissione europea a mettere mano al pacchetto di misure contenute nel GDPR[40].

---

di connettività». Sulla problematica realizzazione dell'interoperabilità tra pubbliche amministrazioni in materia di FSE, 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.

[39] M.G. Virone, *Il fascicolo sanitario elettronico*, cit., 97.

[40] G. Buttarelli, Privacy*, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche* e S. Calzolaio, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, entrambi in *www.federalismi.it*. In generale, per uno sguardo d'insieme ai contenuti del GDPR, oltre ai lavori che stanno per essere citati, F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali*, Torino, 2016 e G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2020.

E questo, soprattutto, in ragione della frammentazione della disciplina sulla protezione dei dati personali che caratterizzava il territorio dell'Unione e delle conseguenti incertezze applicative, circostanze che contribuivano ad alimentare un inefficiente clima di sfiducia nei diversi settori in cui le nuove tecnologie trovavano applicazione[41].

Il provvedimento non ha rappresentato una rivoluzione, quanto piuttosto un'evoluzione nel senso dell'uniformazione normativa rispetto alla previgente Direttiva 95/46/CE, dalla quale si distingue per la scelta della forma e della natura dell'atto: un regolamento, per l'appunto, strumento suscettibile di maggior impatto nei contesti nazionali[42] e, pertanto, meglio in grado di realizzare le finalità di protezione[43] e di rafforzamento dei diritti degli interessati[44] ad esso sottese.

Nella consapevolezza dell'esistenza di una mole infinita di dati prodotta ogni giorno dalla vita digitale delle persone (c.d. *big data*), la cui corretta interrogazione può anche costituire fonte di ricchezza[45] e di un rischio che abbraccia ogni aspetto del loro utilizzo[46], il GDPR pone al centro della sua disciplina il Titolare del trattamento, chiamato a mettere in atto misure tecnico-organizzative adeguate per garantire che il loro trattamento sia effettuato in modo conforme al Regolamento (art. 24)[47], anche integrando la protezione dei dati fin dalla sua progettazione (art. 25: *privacy by design*) e per tutta la sua durata.

---

[41] G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove Leggi Civ. Comm.*, 2017, 1 e C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *www.federalismi.it*.

[42] S. Fanni, R. Marilotti, *Ricerca genetica e tutela dei dati personali nel diritto dell'Unione Europea e nel diritto italiano: è possibile un bilanciamento?*, in *www.federalismi.it*.

[43] Nel senso che il rispetto dei requisiti previsti dal Regolamento costituisce essenziale condizione preliminare alla tutela dei diritti degli interessati, F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali*, cit., 45.

[44] L. Chieffi, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *www.federalismi.it.*

[45] Efficace è in questa sede il riferimento ad una nuova specie di capitalismo, denominato "capitalismo di sorveglianza" dall'economista Shoshana Zuboff, per indicare quella forma di "monetizzazione dei dati personali" che origina dalla cessione – spesso inconsapevole –, mediante l'uso di servizi come quelli riconducibili a Google, di informazioni personali attraverso cui è possibile dedurre – e quindi orientare – comportamenti piuttosto che preferenze, in una condizione di "squilibrio nella conoscenza" tra osservatori ed osservati: ne dà notizia C. Sartoretti, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *www.federalismi.it.* Evocativo, per gli stessi scopi, è il richiamo fatto da S. Amato, *Biodiritto 4.0*, cit., 84 ss., al romanzo di Ismail Kadarè, *Il palazzo dei sogni*, Milano, 1991, dove viene immaginata una provincia dell'impero ottomano in cui un'istituzione ha il compito di raccogliere i sogni fatti dai sudditi per ordinarli, analizzarli e filtrarli allo scopo di individuare aspirazioni nascoste ed intenti sovversivi.

[46] S. Calzolaio, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, cit.

[47] Nel senso che il riferimento al Titolare del trattamento quale sorta di "catalizzatore" di tutte le responsabilità sembri rivelare, in verità, la scarsa capacità del legislatore europeo di intercettare gli sviluppi della tecnologia connessa proprio ai *big data*, nel suo coinvolgere veri e propri trattamenti "a cascata" e, pertanto, numerosi attori che spesso non è facile controllare, G. Simeone, *Machine Learning e tutela della Privacy alla luce del GDPR*, in Aa.Vv., *Diritto e intelligenza artificiale*, Pisa, 2020, 278-279.

Già solo da queste disposizioni emerge la consapevolezza che occorre guardare alla protezione dei dati personali seguendo un innovativo approccio "dinamico", non più solo legato alla logica tradizionale di una *privacy* intesa come *right to be alone*, bensì coinvolgente anche i flussi di dati che si muovono "dall'esterno verso l'interno" dei soggetti[48], grazie all'uso di una tecnologia ormai divenuta pervasiva ed in grado di cambiare lo stesso modo con cui ci relazioniamo nel mondo[49], secondo quanto è stato in precedenza osservato.

Non a caso, del resto, il concetto di *privacy*, la cui centralità era sottesa alla Direttiva del 1995, nel 2016 cede il passo al rilievo del *dato in sé* e della sua *sicurezza.*

Disposizione-chiave per l'economia di questo ragionamento è l'art. 5 GDPR che, nell'affermare i principi applicabili al trattamento dei dati personali, e nel dirigere le competenze per il loro rispetto verso il Titolare del trattamento, che deve essere anche «in grado di comprovarlo» (principio di *responsabilizzazione*: par. 2), stabilisce che i dati sono «trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali».

È questo il principio di *integrità e riservatezza* (par. 1, lett. f), anche conosciuto come principio di *accountability*, che «può essere tradotto con responsabilità e, insieme, prova della responsabilità»[50] e che si pone quale vero e proprio "principio dei principi", la cui osservanza dovrebbe garantire il rispetto di tutti gli altri[51].

In primo luogo, è molto interessante sottolineare la concezione di sicurezza dei dati personali che emerge dalla disposizione citata.

La protezione dal loro trattamento non autorizzato o illecito, o dalla distruzione, ne costituisce una componente di certo importante, ma non la esaurisce, nel senso che la sicurezza dei dati personali, alla luce 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,

---

[48] La vocazione dinamica della protezione dei dati è messa in luce da C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit.

[49] G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *www.federalismi.it.*

[50] Così G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, cit., 2, che aggiunge come proprio la complessità del vocabolo, nel suo ricollegarsi a diversi significati, suggerisca di utilizzare sempre il termine originario di *accountability.* Per un approfondimento di questo principio, si segnala 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.

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

per quanto particolarmente rilevante[52]: una strategia che ruota intorno al "principio generale del trattamento"[53].

L'approccio di tutela dei dati personali che emerge dal GDPR è dunque basato sulla gestione complessiva del rischio e 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, chiamato a modulare "in concreto" l'attuazione dei principi sanciti dal Regolamento[54].

In secondo luogo, nella prospettiva dell'*accountability*, è evidente come la sicurezza dei dati personali, nel suo richiamare misure differenti, richieda una visione integrata di diverse competenze (informatiche, giuridiche e organizzative) che mobilitano a loro volta diverse professionalità, poiché la scelta della misura adeguata richiede una valutazione in via previa della natura dei dati, dei rischi che emergono dal contesto, dei danni potenziali e dei costi[55].

Se, di conseguenza, più che ragionevole si dimostra l'estensione della portata del concetto di sicurezza non solo alla protezione, ma anche alla formazione del dato personale, la disposizione lascia trasparire la preoccupazione del legislatore europeo per quei contesti nei quali l'applicazione delle tecnologie coinvolge non solo l'erogazione di una prestazione, ma anche la comunicazione, gestione e conservazione dell'insieme delle informazioni a questa collegate.

Contesti – vien qui da aggiungere – come potrebbero essere quelli di sanità digitale, dove la tecnologia può agevolare la circolazione delle informazioni utili alla prevenzione e cura della malattia ed al miglioramento dell'efficienza delle strutture sanitarie, ma può anche rendere molto concreto il rischio di un suo utilizzo per il perseguimento di *altri* interessi, di indole soprattutto economica, se non addirittura criminale[56].

---

[52] Così M. Farina, *Il cloud computing in ambito sanitario tra security e privacy*, cit., 1 ss.

[53] G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Padova, 2018, 60.

[54] G. Finocchiaro, *GDPR tra novità e discontinuità - il principio di* accountability, in *Giur. it.*, 2019, 2777 e M. Sala, *Privacy. Giuda alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del Codice Privacy italiano*, Torino, 2018, 46 ss.

[55] G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, cit., 1.

[56] La prospettiva è ben messa in luce da L. Chieffi, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, cit.

5. *Tecnologia e sicurezza del dato in ambito sanitario: considerazioni sull'art. 9 GDPR*

Tutto ciò che precede sembra confermare che solo allorquando la struttura sanitaria sia in grado di realizzare il rispetto dei principi sanciti dal Regolamento in materia di sicurezza dei dati personali è possibile realizzare anche la *sicurezza delle cure*, secondo quanto, del resto, ha sancito in Italia la l. 8 marzo 2017 n. 24 (*Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*, c.d. *Legge Gelli-Bianco*), nella parte in cui riconosce che la sicurezza delle cure, parte costitutiva del diritto alla salute (art. 1, co. 1), «si realizza anche mediante l'insieme di tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative» (art. 1, co. 2)[57].

In questo quadro, vale la pena di notare che, pur non risultando una sezione espressamente dedicata al trattamento dei dati personali in ambito sanitario, il legislatore europeo del 2016, a differenza di quanto accaduto con la precedente Direttiva del 1995, non ha mancato di rivolgere specifica attenzione ai «dati relativi alla salute» fin dalle definizioni contenute nell'art. 4 GDPR, che li descrive come i «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (definizione n. 15)[58].

La rilevanza attribuita dal Regolamento a questi dati è poi confermata dal successivo art. 9[59], che li ricomprende tra quelle «categorie particolari di dati per-

[57] D. Amram, G. Comandé, *Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla protezione dei dati personali UE/679/2016 e dalla legge n. 24/2017*, in *Rivista italiana di medicina legale*, 2018, 8.

[58] Ben più analitica di quanto non risulti dall'art. 4 è la descrizione contenuta nel 35° considerando del Regolamento, ove si legge che «nei dati personali relativi alla salute dovrebbero rientrare 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. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, 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*». Su queste definizioni, I. Gasparini, *La tutela penale della "privacy sanitaria" nell'era del GDPR*, in *Riv. it. med. legale*, 2019, par. 2.

[59] Per un approfondimento dei contenuti di questo articolo, M. Farina, *Il cloud computing in ambito sanitario tra security e privacy*, cit., 29 ss.

sonali» il cui trattamento è vietato, secondo limitazioni che gli Stati membri possono addirittura implementare (par. 4)[60].

A quest'ultimo proposito, si noti che il d.lgs. 10 agosto 2018, n. 101, emanato per l'adeguamento della normativa italiana alle disposizioni del GDPR, ha inserito nel d.lgs. 30 giugno 2003, n. 196 (*Codice della privacy*) l'art. 2-*septies*, rubricato «Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute», secondo il quale i dati relativi alla salute possono essere oggetto di trattamento in conformità alle misure di garanzia[61] disposte dal Garante per la protezione dei dati personali, da adottarsi tenendo conto non solo delle indicazioni fornite dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali, ma anche dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure (co. 1 e 2).

In particolare, esse devono riguardare le cautele da adottare relativamente ai profili organizzativi e gestionali in ambito sanitario e alle modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla sua salute (co. 4). Inoltre, devono individuare le misure di sicurezza, anche da un punto di vista tecnico, le misure di minimizzazione e le specifiche modalità per l'accesso selettivo ai dati (co. 5).

Leggendo le disposizioni che precedono, e che danno ulteriore prova della centralità della stretta correlazione tra sicurezza della formazione e sicurezza della conservazione e circolazione del dato sanitario, una domanda sorge spontanea: esiste in Italia una cultura del digitale così solida da sostenere il Garante nell'assolvimento dei compiti che la legge gli ha assegnato?

Non solo.

L'art. 9, par. 2, GDPR prevede un elenco di casi in cui il divieto di trattamento dei dati relativi alla salute non si applica, tra i quali è annoverato quello in cui l'interessato abbia prestato «il proprio consenso esplicito al trattamento» (lett. a).

Ebbene: se è fondamentale che questo consenso sia il più possibile consapevole, come ad esempio conferma, in ambito sanitario, la legge italiana 22 dicembre 2017, n. 219 sul «consenso informato», «nel quale si incontrano l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e

[60] In materia, si vedano le precisazioni contenute nei *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, forniti dal Garante per la protezione dei dati personali con provvedimento n. 55 del 7 marzo 2019, in *www.garanteprivacy.it*.

[61] Sulla configurazione delle misure di garanzia del Garante quali strumento di flessibilità della normativa legislativa e regolamentare al fine di consentirne l'adattabilità all'evoluzione tecnologica, contribuendo alla ricerca dell'equilibrio tra tutela dei diritti e spazio comune europeo della circolazione dei dati, F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Torino, 2021, 122, cui si rinvia (114 ss. e 411 ss.) per un attento approfondimento dei contenuti dell'art. 2-*septies* e delle problematiche dallo stesso scaturenti.

la responsabilità del medico», in una relazione di cura e di fiducia tra i due (art. 1, co. 2) che pare tracciare con decisione un percorso di "umanizzazione della medicina"[62], qual è l'impatto che su questa relazione produce l'applicazione di tecnologie *smart*? Quanto la struttura sanitaria complessivamente intessa è tecnicamente in grado di inverare questa consapevolezza?

5.1. Segue: *sicurezza nella formazione del dato sanitario e processo decisionale automatizzato alla luce dell'art. 22 GDPR*

Le considerazioni da ultimo svolte sull'importanza del consenso informato nel contesto sanitario portano a riflettere sulle problematiche scaturenti dalle disposizioni contenute in uno degli articoli del GDPR che ha catalizzato maggiormente l'attenzione dei commentatori: si tratta dell'art. 22.

Si è già ricordato nell'introduzione di questo lavoro che, ai sensi di tale articolo, l'interessato ha il diritto di non essere sottoposto[63] a una «decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona» (par. 1)[64].

Fa eccezione alla regola, tra l'altro, la circostanza che la decisione «si basi sul consenso esplicito dell'interessato» (par. 2, lett. a), nel qual caso «il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione» (par. 3)[65].

---

[62] C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, cit., 718.

[63] Il Comitato europeo per la protezione dei dati ha precisato che tale diritto corrisponde ad un divieto generale operante *ex ante*, non costituendo un mero diritto di opposizione *ex post* il cui esercizio sia affidato all'iniziativa dell'interessato. Sul punto, E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della* Black Box Society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* Responsible Research and Innovation, in *Nuove leggi civ. comm.*, 2018, 1209 ss. nonché Id., *Privacy, decisioni automatizzate e algoritmi*, in E. Tosi (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 429 ss.

[64] È interessante notare il riferimento più ampio agli effetti che possano essere prodotti dal trattamento automatizzato contenuto nella nuova disposizione rispetto al suo antecedente, costituito dall'art. 15, par. 1, della Direttiva del 1995: «gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.».

[65] Per l'esegesi dell'articolo, si segnalano fin da subito G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., 221 ss. e A. Masucci, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Dir. pubbl.*, 2020, spec. 953 ss. e G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019, 93 ss.

È molto interessante notare, in primo luogo la peculiarità di queste disposizioni rispetto a quelle che sono state finora esaminate: la questione centrale non è infatti la sicurezza del trattamento automatizzato dei dati personali *in* sé *considerato*: al centro dell'attenzione è piuttosto la decisione produttiva di effetti giuridici che su quel trattamento si basi, circostanza che colloca la disciplina in una prospettiva di protezione "più avanzata".

A tal proposito, vale la pena di notare come queste disposizioni intercettino uno dei grandi nodi problematici che sta attualmente animando il dibattito tra gli studiosi del diritto amministrativo: quello relativo ai limiti in cui è possibile demandare ad un *algoritmo* l'assunzione di decisioni, in particolare di natura amministrativa o processual-amministrativa[66], lungo un percorso tracciato da alcune recenti pronunce del giudice amministrativo di primo e secondo grado. Percorso, si badi, che il C.a.d. italiano, nonostante le sue ripetute modifiche e la diffusione del fenomeno, non ha ancora intercettato.

Alla vicenda non può che farsi un rapido cenno, comunque utile all'economia del presente lavoro.

È, in particolare, la giurisprudenza del Consiglio di Stato degna di nota, poiché è quella che ha sottolineato l'imprescindibilità della ricerca della regola tecnica che governa ogni algoritmo, con una motivazione focalizzata proprio sul diritto dell'Unione europea e sull'art. 22 GDPR[67].

La regola tecnica costituisce una regola giuridica «elaborata dal pensiero dell'uomo che ne è e ne resta, sempre e comunque, il *dominus*, laddove alla "macchina" ne viene rimessa la semplice applicazione sul terreno, quando pure ciò avvenga in via "esclusiva"»[68].

Poiché è sempre possibile rinvenire nel diritto amministrativo una sorta di "principio antropomorfico"[69], ne consegue che «la discrezionalità amministrativa non possa essere demandata al *software*», manifestando piuttosto la propria persistente attualità e rilevanza «nel momento alto e definitorio nel quale la rego-

[66] Su vantaggi e criticità discendenti in Italia da un'automazione dei processi decisionali amministrativi, F. Patroni Griffi, *La decisione robotica e il giudice amministrativo*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, 165 ss. Per una rassegna delle soluzioni adottate da alcuni Stati europei in ordine all'adozione di decisioni amministrative algoritmizzate, e dei profili problematici da queste discendenti, A. Masucci, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, cit., 963 ss.

[67] Evidenziano questa circostanza E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, 294 e M. Timo, *Algoritmo e potere amministrativo*, in questa *Rivista*, 2020, 773. Il primo Autore, peraltro, sottolinea come l'orientamento del Consiglio di Stato sembri caratterizzarsi per una maggiore apertura rispetto alla disciplina contenuta nell'art. 22, riferendosi all'ammissibilità di un intervento umano anche solo in termini di validazione e controllo del risultato prodotto in autonomia dalla macchina.

[68] R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Dir. amm.*, 2019, 781.

[69] Così S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 2019, 22.

la tecnica viene concretamente elaborata e messa in campo»[70]. E questo perché «la tecnica appartiene, tutta intera, nella sua genesi e nel suo sviluppo, al mondo dell'uomo» e «la decisione affidata al robot non è un fenomeno anti-umano, un miracolo o una catastrofe. È una decisione "umana", e appartiene, anch'essa, alla storia integrale dell'uomo»[71], alla cui capacità d'*intelligere* inevitabilmente lascia l'innovazione e la creatività[72].

Il percorso seguito porta, allora, ad interrogarsi sulla reale possibilità di garantire la trasparenza del funzionamento dei sistemi di Intelligenza Artificiale e delle logiche a questi sottese[73], ad esempio mediante l'introduzione di idonee pro-

[70] R. Ferrara, *Il giudice amministrativo e gli algoritmi*, cit., 781 e 785, che si riferisce, in particolare, a 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*. Per ulteriori approfondimenti di questa giurisprudenza, D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie*, cit., 2265 ss., S. Civitarese Matteucci, *Umano troppo umano*, cit., 27 ss., E. Carloni, *I principi della legalità algoritmica*, cit., 273 ss., M. Timo, *Algoritmo e potere amministrativo*, cit., 753 ss., C. Strinati, *Algoritmi e decisioni amministrative*, in *Foro amm.*, 2020, 1592 ss., G. Pesce, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in *www.giustizia-amministrativa.it* e G. Marchianò, *Intelligenza Artificiale: IA specifiche e l'amministrazione provvedimentale – IA generali e i servizi pubblici*, in *www.federalismi.it.* Sulle ragioni per le quali non vi sia radicale incompatibilità fra informatizzazione e discrezionalità amministrativa, poiché le nuove tecnologie non determinano tanto la scomparsa, quanto piuttosto la ridefinizione e riallocazione del potere discrezionale, si segnala in particolare il recente lavoro di A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, in Aa.Vv., *Scritti per Franco Gaetano Scoca*, vol. I, Napoli, 2020, 675 ss. Inoltre, sulle problematiche scaturenti dall'applicazione della logica degli algoritmi all'attività vincolata piuttosto che a quella discrezionale della pubblica amministrazione, R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021, 16 ss., R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2020, 309 ss., Id., *Atti e procedimenti amministrativi digitali*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, spec. 139 ss., D.U. Galetta, J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, P. Otranto, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo* e B. Raganelli, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenza diverse nell'assunzione di decisioni alternative*, tutti in *www.federalismi.it.* In particolare, nel senso che «c'è un aspetto che accumuna dottrina e giurisprudenza e che costituisce una sorta di vallo di Adriano o di muraglia cinese nei confronti della informatizzazione dell'attività amministrativa e cioè il suo carattere o meno "discrezionale"», E. Picozza, *Intelligenza artificiale e diritto - politica, diritto amministrativo* and artificial intelligence, in *Giur. it.*, 2019, 1657 ss. Sui temi qui trattati, anche A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giuridica dell'economia*, 2019, 47 ss.

[71] Le ultime due frasi tra virgolette nel testo sono di N. Irti, *Il tessitore di Goethe (per la decisone robotica)*, in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019, 21.

[72] R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, cit., 326. Su emozioni, intuizione intellettuale, creatività, coscienza ed interazione corpo/mente quali elementi caratterizzanti il cervello umano che le macchine non sono ancora riuscite a simulare o riprodurre, R. Cingolani, D. Andresciani, *Robot, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in Aa.Vv., *Diritto e intelligenza artificiale*, Pisa, 2020, 28 ss., P. Moro, *Macchine come noi. Natura e limiti della soggettività robotica*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 50 ss. e G. Maira, *Intelligenza umana e intelligenza artificiale*, cit.

[73] Sul problema della conoscibilità degli algoritmi, si rinvia, per tutti, agli approfondimenti di G. Avanzini, *Decisioni amministrative e algoritmi informatici*, cit., 117 ss. e D. Marongiu, *L'automazione delle decisioni amministrative: teorie, esperienze e sentenze*, in Aa.Vv., *Scritti per Franco Gaetano Scoca*, vol. IV, Napoli, 2020, 3369 ss.

cedure di certificazione e di controllo circa la loro affidabilità[74]. IA che – si badi, e quasi per un curioso caso – non è mai menzionata nel GDPR, per quanto molti dei dati processati dai meccanismi decisionali connessi all'IA siano qualificabili come *personali* e, pertanto, riconducibili sotto l'egida della disciplina europea[75].

Sotto questo punto di vista, si segnala che, nell'ambito della Strategia europea per l'Intelligenza Artificiale, la Commissione europea ha pubblicato, il 21 aprile 2021, la proposta di Regolamento sull'approccio europeo all'Intelligenza Artificiale, che si propone come primo quadro giuridico europeo sull'IA[76].

La proposta, oltre a vietare in termini praticamente assoluti una serie di possibili usi di alcuni sistemi di IA (come quelli che utilizzano tecniche subliminali o che sfruttano una vulnerabilità legata all'età o ad una disabilità di uno specifico gruppo per distorcere in maniera sostanziale il comportamento di una persona), prevede una specifica regolamentazione dei sistemi di IA qualificati "ad alto rischio", tali essendo le tecnologie che creano rischi elevati per la salute, la sicurezza o i diritti fondamentali delle persone, come i sistemi di IA destinati ad essere utilizzati quali componenti di sicurezza di prodotti soggetti a valutazione di conformità secondo una disciplina europea (ad esempio, i dispositivi medici)[77].

Esula dagli intenti del presente lavoro l'approfondimento di questi temi. Resta il fatto che quello del progressivo aumento del ruolo degli algoritmi nella nostra società è di grande interesse nel contesto sanitario.

Da una parte, perché l'IA applicata alla medicina soffre di un grave difetto di trasparenza, al punto che, molto spesso, «non è dato comprendere, nemmeno ai programmatori, il percorso attraverso cui la macchina produce il risultato della propria attività»[78].

Dall'altra, perché si ricollega al problema della crescente riduzione del ruolo del soggetto umano nell'assunzione di decisioni aventi conseguenze significative per la salute del loro destinatario, problema che – nella duplice prospettiva che qui si è scelto di privilegiare in tema di sicurezza dei dati – attiene non tanto (o non solo) alla circolazione/conservazione del dato sanitario, quanto soprattutto alla sua formazione: per meglio precisare, alla formazione di una decisione, rilevante per la salute dell'interessato, che sia il più possibile *sicura*.

---

[74] Sul punto, F. Donati, *Intelligenza artificiale e giustizia*, in Aa.Vv., *Scritti in onore di Franco Pizzetti*, vol. II, Napoli, 2020, 392-393. Sottolinea l'importanza di un algoritmo trasparente ed accessibile, soprattutto come condizione di correttezza della decisone assunta, anche G.M. Esposito, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo*, in *Dir. e proc. amm.*, 2019, 62 ss.

[75] G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova*, cit.

[76] Per alcune informazioni in proposito, si veda https://temi.camera.it.

[77] Tra le specifiche regole introdotte si segnalano, in particolare, l'obbligo di creare e mantenere attivo un sistema di *risk management*, l'obbligo di assicurarsi che i sistemi di IA possano essere sottoposti a supervisione da parte di persone fisiche, l'obbligo di garantire l'attendibilità, accuratezza e sicurezza degli stessi e specifici obblighi di trasparenza verso gli utenti sul funzionamento dei sistemi di IA.

[78] C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, cit., 717.

Punto di snodo del ragionamento focalizzato sull'art. 22 GDPR è la comprensione del significato di «decisione basata *unicamente* sul trattamento automatizzato», posto che è l'avverbio a fungere da discrimine tra decisioni ammissibili e non[79].

La riflessione svolta sull'onda della citata giurisprudenza amministrativa ha portato a ritenere che la componente umana non possa essere sostituita da una presunta oggettività degli algoritmi, come se fosse un dannoso "rumore di fondo" da eliminare[80]. Si tratta di un'importante riaffermazione della centralità del ruolo che la dimensione umana conserva anche al tempo delle tecnologie *smart* e che verrà ripresa nelle conclusioni di questo lavoro.

E in effetti, la dottrina prevalente ritiene che nella fattispecie considerata dall'art. 22 GDPR ci debba comunque essere un intervento umano realmente funzionale al riesame degli esiti del processo automatizzato[81], al punto che lo stesso articolo potrebbe essere "riletto" nel senso di configurare un diritto ad essere destinatari di decisioni che siano il risultato di un processo in cui sia presente la componente umana[82].

Se tutto questo è vero, ci sarà però differenza tra l'imbattersi in un medico che è contrario *a priori* a confermare una decisione algoritmica piuttosto che avere a che fare con un medico predisposto a scegliere l'opzione più idonea a supportare le scelte della macchina per l'assenza della disponibilità di informazioni che siano anche solo lontanamente paragonabili all'enorme massa di dati che ha costituito il presupposto per la decisione della macchina[83].

---

[79] Sottolinea come proprio questa circostanza chiarisca in modo univoco la porta della norma, che in effetti non è diretta a vietare la decisione automatizzata *tout court*, G. Finocchiaro, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 244-245. Per comprendere appieno i termini del problema, utile è l'approfondimento della distinzione tra decisioni algoritmiche di "Primo livello. Automazione completa", in cui la decisione viene generata dall'IA senza necessità d'intervento umano, di "Secondo livello. Automazione e intervento umano ridotto", dove è inevitabile l'interazione tra operatore umano e procedura automatizzata, e di "Terzo livello. Automazione più predizione", dove l'algoritmo elabora dati per stabilire modelli che vengono poi tradotti in decisione, applicando criteri statistici, operata da D.U. Galetta, J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?*, cit.

[80] C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, cit., 179. Sull'insostituibilità dell'intervento umano, anche A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 38.

[81] In questo senso, C. Napoli, *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Rivista AIC*, n. 3/2020, par. 3, cui *adde* G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., 223, F. Donati, *Intelligenza artificiale e giustizia*, cit., 390-391 ed E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della* Black Box Society, cit., 1209 ss.

[82] Così C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, cit., 180.

[83] P. Otranto, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, cit.

Dopotutto, non sembra sbagliato affermare che «il sistema automatico tende, nel tempo, a catturare la decisione stessa»[84], con due conseguenze di tutto rispetto: da una parte, la dimostrazione che una decisione lesiva sia basata *unicamente* su di un processo automatizzato diviene, di fatto, una vera e propria «*probatio diabolica*»[85]; dall'altra, l'eccesivo affidamento che il medico riponga sui risultati prodotti da macchine intelligenti porta al fenomeno definito come "*deskilling* professionale"[86], vale a dire alla progressiva riduzione delle competenze professionali del sanitario, che può diventare così poco avvezzo alla valutazione analitica delle informazioni disponibili da non essere più in grado di rilevare neppure gli errori grossolani.

E così, per tornare al punto dal quale si era partiti, se la presenza del consenso esplicito dell'interessato introduce un'eccezione alla regola enunciata dall'art. 22, par. 1, GDPR, dovendo tuttavia il titolare del trattamento attuare misure appropriate di tutela il cui livello minimo è costituito dal diritto di ottenere comunque un intervento umano, il problema diventerà quello di identificare le caratteristiche che questo intervento deve avere in termini di preparazione tecnica[87], e ciò rileverà a maggior ragione nel passaggio da tecnologie di facile comprensione (la cui applicazione implichi un mero accertamento tecnico) a tecnologie all'avanguardia o *smart* le cui logiche, complesse se non addirittura oscure, richiedano tra l'altro una vera e propria valutazione tecnica, per sua natura opinabile.

Si tratta di un problema che in Italia deve fare i conti con il fenomeno del *digital divide.*

6. *All'origine dei problemi della sanità digitale in Italia: riflessioni in tema di* digital divide

Per quanto sia possibile riconoscere come il nostro Paese sia stato tradizionalmente all'avanguardia nella gestione del sistema sanitario, oggi risulta essere in ritardo rispetto ad alcuni elementi di carattere strutturale quali la stessa sanità digitale, circostanza che diventa fattore d'implementazione del *deficit* reputazionale che sempre di più sta caratterizzando il nostro SSN[88].

---

[84] A. Simoncini, *Diritto costituzionale e decisioni algoritmiche*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 55.

[85] A. Simoncini, *Diritto costituzionale e decisioni algoritmiche*, cit., 56.

[86] G. Pasceri, *Intelligenza artificiale, algoritmo e* machine learning, cit., 120.

[87] La prospettiva è ben messa in luce da P. Guarda, L. Petrucci, *Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati*, in *BioLaw Journal*, 2020, 425 ss.

[88] Aa.Vv., *Le sfide di oggi per la sanità di domani*, cit., 133.

Evidentemente, la predisposizione di adeguati livelli di sicurezza in questi contesti è adempimento fondamentale ma, al tempo stesso e soprattutto in Italia, sconta la mancanza di una diffusa cultura digitale, la persistente debolezza della strategia d'innovazione tecnologica e la carenza di risorse per alimentarla[89].

Spesso vi è la tendenza ad una "digitalizzazione di facciata", basata sulla falsa credenza che sia sufficiente trasferire su computer modelli organizzativi o di azione in realtà sempre legati ad una dimensione cartacea[90]: è chiaro che, se nelle aziende sanitarie italiane il livello di utilizzo della tecnologia resta basso, i relativi investimenti in sicurezza non verranno conseguentemente avvertiti come una priorità[91].

Dagli elementi a disposizione emerge addirittura la scarsa consapevolezza da parte delle strutture pubbliche sanitarie dell'obbligo, in qualità di titolari del trattamento di dati personali coinvolto dall'applicazione di tecnologie all'avanguardia, di dover adottare misure di sicurezza a fini di protezione dei dati personali e di rispetto della normativa (anche) europea in materia. A tal proposito, è molto azzeccata la definizione di "cultura digitale" non solo come attitudine a privilegiare l'uso degli strumenti digitali nei rapporti con la pubblica amministrazione, ma anche come "consapevolezza" delle finalità e dei vantaggi dell'informatizzazione[92].

Non è solo il problema di comprendere *quale* misura adottare, ma prima ancora di capire *se* occorre adottarla. E questo vale a maggior ragione nei procedimenti più complessi, dove il problema diventa anche quello della *governance* dei "ruoli *privacy*" dei numerosi attori coinvolti.

Come si accennava alla fine del paragrafo precedente, l'insieme dei nodi problematici rilevati – *in primis* quello relativo al *gap* di consapevolezza – è riconducibile al *divario digitale* (*digital divide*)[93], che si riferisce al complesso delle disuguaglianze nell'accesso/fruizione delle tecnologie informatiche[94] e che, col passare del

[89] F. Merloni (a cura di), *Introduzione all'@government*, Torino, 2005, 59.

[90] Così, opportunamente, E. Carloni, *I principi della legalità algoritmica*, cit., 280. Sulla necessità di passare da un modello di informatica "documentaria" ad un modello di informatica "meta-documentaria", dove l'uso dello strumento informatico consente la riproduzione automatica di processi logici tipici della mente umana, D.U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (il procedimento amministrativo, fra diritto UE e tecnologie ICT)*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 114.

[91] E. Sorrentino, A.F. Spagnuolo, *La sanità digitale in emergenza Covid-19*, cit.

[92] G. Cammarota, P. Zuddas, *Introduzione*, cit., 13.

[93] Sulle definizioni di *digital divide*, la prima delle quali lo ha inteso come «il divario tra coloro che hanno accesso alle nuove tecnologie e coloro che non lo hanno», L. Sartori, *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Bologna, 2006, 11 e F. Ancora, *Considerazioni sul divario digitale*, in *Dir. e proc. amm.*, 2016, 113 ss.

[94] Sul *digital divide* quale limite al compiuto e diffuso esercizio dei diritti digitali e quale principale ostacolo alla realizzazione dell'innegabile funzione sociale che va riconosciuta alla digitalizzazione, F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, cit., 261 e F. Gaspari, *La* new information economy, cit., 172 ss.

tempo, presenta forme sempre nuove in quanto conseguenti alle nuove lacune che si vengono a creare per la continua evoluzione tecnologica (c.d. divario *avanzato*)[95].

Si tratta di disuguaglianze talmente variegate da portare alcuni studiosi a parlare, al plurale, di *divides*[96], soprattutto per il loro essere quasi sempre collegate a disuguaglianze sostanziali preesistenti[97] che, in quanto tali, sono idonee a compromettere la stessa realizzazione della "eguaglianza digitale"[98], ormai divenuta – a livello mondiale – una vera e propria "emergenza democratica", per la vasta presenza di "eremiti analogici"[99], segnati dall'incapacità di entrare nell'ecosistema digitale[100].

Di qui l'opportuna riflessione di quella dottrina che guarda al principio di uguaglianza sostanziale, sancito dall'art. 3 della nostra Costituzione, come fondante precisi obblighi d'intervento in capo alla Repubblica anche per la rimozione delle "disuguaglianze nei punti di partenza"[101] come quelle che qui ci occupano, obblighi che – a ben vedere – sarebbero già da soli in grado di riequilibrare l'assenza di precettività spesso rinvenibile nelle disposizioni contenute nel C.a.d., se non fosse per la concomitanza di altri e più rilevanti cause del fenomeno[102].

In effetti, il grado di sviluppo economico di un Paese non è decisivo per spiegare il *digital divide*, spesso collegato ad altri fattori (anagrafici, di contesto, politici, istituzionali) o al livello di istruzione.

Quest'ultimo, in particolare, rivela un ruolo-chiave nella comprensione del *digital divide*, confermando tra l'altro che è la considerazione del capitale umano ad avere, allo scopo, un impatto decisivo[103].

Occorre infatti non commettere l'errore di pensare che i c.d. *nativi digitali*, vale a dire coloro che sono nati e cresciuti "immersi" nelle tecnologie, siano sog-

---

[95] Ha evidenziato il fenomeno P. Piras, *Innovazione tecnologica e divario digitale*, relazione tenuta al Convegno Annuale dell'Associazione Nazionale dei Professori di Diritto Amministrativo (AIPDA) sul tema *Il diritto amministrativo per la ripresa: nuove fragilità, nuovi bisogni, nuove sfide* (Roma, 8 ottobre 2021).

[96] Ad esempio, c'è divisione non solo tra chi utilizza l'informatica e chi non, ma anche tra i diversi utenti dei diversi linguaggi informatici: sul punto, A.G. Orofino, *La semplificazione digitale*, in Aa.Vv., *L'amministrazione nell'assetto costituzionale dei pubblici. Scritti per Vincenzo Cerulli Irelli*, tomo II, Torino, 2021, 866.

[97] F. Merloni (a cura di), *Introduzione all'@government*, cit., 209 ss.

[98] E. D'Orlando, *Profili costituzionali dell'amministrazione digitale*, in *Dir. inf.*, 2011, 219.

[99] Le due espressioni tra virgolette compaiono in A. Masera, G. Scorza, *Internet, i nostri diritti*, Roma-Bari, 2016, rispettivamente 10 e 12. Nel senso che le potenzialità democratiche delle nuove tecnologie della comunicazione dipendono dalla possibilità di collocare i nuovi diritti dell'era dell'informazione (accesso, intervento, replica) in un quadro di "servizio universale", S. Rodotà, *Cittadinanza: una postfazione*, in D. Zolo (a cura di), *La cittadinanza: appartenenza, identità, diritti*, Roma-Bari, 1999, 317.

[100] Sul concetto di ecosistema digitale, A. Papa, *Il diritto dell'informazione e della comunicazione nell'era digitale*, Torino, 2021,1.

[101] Così A. Papa, *Il principio di uguaglianza (sostanziale) nell'accesso alle tecnologie*, in *www.federalismi.it*, nonché Id., *Il diritto dell'informazione e della comunicazione nell'era digitale*, cit., 10.

[102] Nel senso che le disposizioni del C.a.d. vivono e diventano effettive solo se lette con i relativi obblighi posti a carico delle amministrazioni, F. Faini, *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in *Dir. inf.*, 2019, 1103.

[103] Il profilo è ben messo in luce da L. Sartori, *Il divario digitale*, cit., 25 ss.

getti che non subiscano gli effetti del fenomeno, proprio perché sono l'istruzione e la cultura generale a condurre alla necessaria consapevolezza in ordine alle opportunità ed ai rischi derivanti dall'uso delle tecnologie[104].

Il *digital divide* è fenomeno che può essere riguardato sia sul "versante privato" (del cittadino) che sul "versante pubblico" (degli "agenti" dell'amministrazione[105])[106].

Si noti che il Codice dell'amministrazione digitale contiene disposizioni riferite ad entrambi i versanti, in articoli che nuovamente contengono mere enunciazioni di principio[107] e che sembrano costituire una vera e propria presa d'atto del fatto che l'innovazione tecnologica non si è sviluppata in Italia nel modo sperato[108]: e questo proprio per motivi di carattere culturale ed economico-finanziario che, nel 2020, hanno collocato il nostro Paese alla venticinquesima posizione nel *Digital Economy and Society Index (DESI)* sviluppato dalla Commissione Europea per misurare il grado di diffusione del digitale nei Paesi dell'Unione[109].

Quanto al primo versante, l'art. 8 C.a.d., rubricato *Alfabetizzazione informatica dei cittadini*, chiama le pubbliche amministrazioni a promuovere «iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni».

Si noti il cambio di paradigma che il d.lgs. 179/2016 ha portato rispetto alla formulazione originaria dell'articolo, secondo la quale «lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni».

Nell'attuale versione, lo sviluppo delle competenze digitali di base non costituisce più il fine precipuo della disposizione, bensì un mezzo per conseguire quella diffusione della cultura digitale di cui – evidentemente – nel 2016 si riconosce in modo espresso la mancanza.

---

[104] M. Martoni, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *www.federalismi.it.*

[105] P. Piras, *Organizzazione, tecnologie e nuovi diritti*, in *Inf. e dir.*, 2006, 95.

[106] In generale, sui vari profili che caratterizzano il *digital divide* in Italia, sia sul versante degli amministrati che sul versante della pubblica amministrazione, e sulle disposizioni contenute nel C.a.d. per porvi rimedio, P. Zuddas, *Cultura digitale e* digital divide, in G. Cammarota, P. Zuddas (a cura di), *Amministrazione elettronica. Caratteri, finalità, limiti*, Torino, 2020, 75 ss.

[107] Circostanza che apre tenui prospettive di effettivo superamento del fenomeno: sul punto, D. De Grazia, *Informatizzazione e semplificazione dell'attività amministrativa nel "nuovo" codice dell'amministrazione digitale*, in *Dir. pubbl.*, 2011, 650 e F. Martines, *La digitalizzazione della pubblica amministrazione*, *Riv. dir. media*, 2018, 152 ss.

[108] M. Quaranta (a cura di), *Il codice della pubblica amministrazione digitale*, cit., 204.

[109] Il dato risulta dal Piano nazionale di ripresa e resilienza, cui si farà cenno nelle conclusioni di questo lavoro. Sulla collocazione dell'Italia nelle classifiche europee relative alla digitalizzazione di Stato, famiglie ed imprese, anche M.G. Losano, *La lunga marcia dell'informatica nelle istituzioni italiane*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, XXIV.

Quanto poi al secondo versante, il Codice prevede un articolo dedicato alla *Formazione informatica dei dipendenti* (art. 13), ai sensi del quale «le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, attuano politiche di reclutamento e formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive», politiche rivolte altresì «allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali dei dirigenti, per la transizione alla modalità operativa digitale».

In questo caso, la mancanza di adeguate professionalità interne alle pubbliche amministrazioni, anch'essa frutto delle carenze sul piano della cultura digitale, finisce per tradursi nella stessa incapacità di ottimizzare l'uso delle risorse finanziarie in qualche modo destinate alla digitalizzazione[110].

Se l'emergenza provocata dal Covid-19 ha costituito (e costituisce tuttora) un momento di test collettivo delle potenzialità e dei limiti della digitalizzazione pubblica, specie nel settore sanitario, da tutto ciò che precede emerge che «il mondo di domani bussa alle porte di un'amministrazione impreparata ad aprirle»[111]: «mentre si dichiara baldanzosamente la rivoluzione digitale non si è ancora capaci di formarne e di reclutarne le avanguardie»[112].

È per questi motivi che possono essere salutati con favore i decreti legge emanati in Italia tra maggio e giugno 2021 per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR), su cui si tornerà nelle conclusioni, e che sembrano costituire il segnale di un'efficace svolta nei contesti descritti.

Pur nella consapevolezza che le grandi riforme non si possono realizzare a colpi di decretazione d'urgenza, si tratta comunque di provvedimenti che sembrano creare le condizioni di sistema per conseguire gli obiettivi del suddetto Piano. E la natura degli atti utilizzati testimonia la consapevolezza che, proprio in quei contesti, occorre intervenire quanto prima.

Si pensi, in particolare, all'entrata in vigore del d.l. 31 maggio 2021, n. 77, intitolato «*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», il cui potenziale, nel-

[110] E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Dir. pubbl.*, 2019, 368. Di recente, ha sottolineato l'importanza di una pubblica amministrazione adeguatamente formata e, in quanto tale portatrice di innovazione, F. Romano, *Intelligenza Artificiale e amministrazioni pubbliche: tra passato e presente*, in *Ciberspazio e diritto*, 2020, 69 ss.

[111] E. Carloni, *Le nuove tecnologie al servizio delle pubbliche amministrazioni*, in A.I.P.D.A., *Annuario 2019. Quali saperi servono alla pubblica amministrazione? Selezione, valorizzazione e tutela della professionalità pubblica. Atti del Convegno annuale, Pisa, 10-12 ottobre 2019*, Napoli, 2020, 31-32.

[112] G. Melis, *Non solo giuristi*, in A.I.P.D.A., *Annuario 2019*, cit., 28.

la direzione della maggiore effettività delle disposizioni di contrasto al divario digitale, è ancora tutto da esplorare.

L'articolo riconosce infatti all'Agenzia per l'Italia Digitale (AgID) poteri di vigilanza, verifica, controllo e 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.

Ancora, è probabilmente la consapevolezza dei rischi connessi all'implementazione del digitale che ha portato, di lì a poco, all'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.

Infine, si pensi 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).

7. *Riflessioni conclusive anche alla luce del Piano nazionale di ripresa e resilienza (PNRR)*

La diffusione di tecnologie *smart* e la trasformazione del modo di elaborare i dati, attraverso lo svolgimento automatizzato di attività tradizionalmente svolte dall'intelligenza umana, sta facendo conoscere alla pubblica amministrazione una quarta fase di evoluzione[113], avendo innescato un processo irreversibile «i cui tratti sono ritenuti caratteristici di una nuova "età"»[114].

[113] D.U. Galetta-J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?*, cit.
[114] A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, cit., 675.

Utilizzando come principale ambito d'indagine il contesto sanitario, le riflessioni che precedono hanno inteso mettere a fuoco alcune importanti conseguenze che ne discendono, specie sotto il profilo dell'innegabile centralità che oggi ha assunto il concetto dinamico di "sicurezza" dei dati relativi alla salute nel significato più sopra evidenziato.

Vale la pena di riflettere anche su di un ulteriore elemento, costituito dal fatto che l'art. 9 GDPR, nel vietare il trattamento dei dati relativi alla salute, prevede un'eccezione al divieto 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)[115].

Calata nel contesto italiano, la disposizione riporta all'annosa questione – a ben vedere rimasta sempre lungo la linea d'orizzonte della presente trattazione – della salute come fondamentale diritto dell'individuo, ma anche interesse della collettività, ai sensi dell'art. 32 Cost., per affrontare la quale l'emergenza da Covid-19 dimostra da una parte come la sanità vada considerata, oggi più che mai, quale problema di ordine pubblico interno ed internazionale e dall'altra come del diritto alla salute vada apprezzata soprattutto l'«oggettiva dimensione di situazione complessa e rilevante perché collettiva»[116].

E si noti il modo assolutamente peculiare con cui la pandemia ha colpito il nostro Paese, scaricando la sua tragicità sulle regioni anche a prescindere dal loro grado di sviluppo socio-economico e dimostrando come la risoluzione delle problematiche di tipo sanitario meriti una strategia d'intervento autonoma e mirata perché non necessariamente legata a contesti economico-produttivi più arretrati[117].

Percorrendo questa via, si giunge ad affermare come oggi la sicurezza dei dati coinvolti dall'erogazione di una prestazione sanitaria costituisca essa stessa strumento di realizzazione del diritto alla salute, sia nella sua dimensione individuale che nella sua dimensione collettiva.

Ma se tutto questo è vero, emerge altresì in tutta la sua drammaticità il problema di rimediare alle lacune ancora esistenti in ordine all'attuale capacità della pubblica amministrazione di comprendere in modo adeguato potenzialità e problemi connessi all'impiego di tecnologie *smart* in sanità, anche contribuendo a colmare quel divario digitale che ancora esiste in modo così diffuso.

---

[115] Sulle finalità di sanità pubblica quali presupposti leciti per il trattamento delle categorie particolari di dati, ai sensi dell'art. 9, par. 2, lett. i), GDPR, si veda l'approfondimento di 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.

[116] R. Ferrara, *L'ordinamento della sanità*, Torino, 2020, 9 e 34.

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

Certamente, la pandemia ha impresso un'accelerazione ai tentativi di superamento dei problemi connessi alla digitalizzazione, la soluzione dei quali può essere considerata a buon diritto come fondamentale per affrontare le stesse criticità portate dal Covid-19: è infatti palese come i *big data* siano ormai divenuti una risorsa essenziale per monitorare l'evoluzione della situazione sanitaria[118].

Ad esempio, in Italia, per cercare di rimediare ai problemi emersi nell'ambito della sanità pubblica digitale, il già citato *Decreto Rilancio* del 2020 ha introdotto misure urgenti per la salute, connesse all'emergenza da Covid-19, per sfruttare il potenziale ancora inesplorato del fascicolo sanitario elettronico ed ha istituito un Fondo per l'innovazione tecnologica e la digitalizzazione, mentre il d.l. 1° marzo 2021, n. 22, convertito con modificazioni dalla l. 22 aprile 2021, n. 55, ha introdotto disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri, istituendo tra l'altro un Comitato interministeriale per la transizione digitale.

È poi importante ricordare le iniziative assunte dall'Unione Europea per la gestione della ripresa economica e sanitaria post-pandemica[119].

Accanto ai programmi di finanziamento del digitale connessi all'approvazione del *Quadro finanziario pluriennale per il periodo 2021-2027* del dicembre 2020, tra i quali si annovera *EU4Health*, teso a rafforzare l'azione europea in campo sanitario, va richiamato il piano *Next generation EU* (NGEU), previsto dall'Unione Europea per sostenere gli Stati membri maggiormente colpiti dalla crisi provocata dal Covid-19[120].

Il piano contiene una parte specificamente dedicata a digitalizzazione e innovazione anche nel settore della pubblica amministrazione, per la cui attuazione gli ordinamenti nazionali godrebbero di risorse finalisticamente condizionate dal raggiungimento degli obiettivi suggeriti dalla Commissione UE mediante le *country-specific reccomendations* e indicati dal rispettivo *National Recovery and Resilience Plan 2021-23.*

A questo proposito, è del 29 aprile 2021 l'approvazione da parte del Governo Draghi del *Piano nazionale di ripresa e resilienza. Next generation Italia* (conosciuto con l'acronimo di PNRR)[121], presentato alla Commissione europea ai sensi degli artt. 18 ss. del Regolamento (UE) 2021/241, cui si affianca l'entrata in vigore

---

[118] S. Tranquilli, *Rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa "robotica"*, in A.I.P.D.A., *Annuario 2019*, cit., 306.

[119] Ne dà notizia R. Miccù, *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *www.federalismi.it.*

[120] Considerato come il più ingente pacchetto di misure d'incentivo mai finanziate dall'Unione, il piano NGEU ha previsto per l'Italia una dote di circa duecento miliardi di euro d'investimenti: sul punto, S. Civitarese Matteucci, *La riforma della pubblica amministrazione nel quadro del "*Recovery Fund", in *Forum AIPDA* Next Generation EU, in *www.aipda.it.* Per ulteriori approfondimenti sul NGEU, si rinvia anche agli altri contributi pubblicati nel *Forum.*

[121] Il testo del Piano è consultabile in *www.governo.it.*

del già citato d.l. 77/2021, che definisce il quadro normativo nazionale finalizzato a semplificare e agevolare la realizzazione dei traguardi e degli obiettivi stabiliti dal PNRR (art. 1), anche istituendo una Cabina di regia chiamata ad esercitare poteri d'indirizzo, impulso e coordinamento generale sull'attuazione degli interventi in raccordo con il Comitato interministeriale per la transizione digitale (art. 2).

Per tornare al Piano, esso 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, e tiene 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, la quale, nel sottolineare 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 si presentava disomogenea già prima della crisi.

Le misure previste dal Piano si articolano intorno a tre assi strategici condivisi a livello europeo: accanto alla transizione ecologica e all'inclusione sociale, vi si annoverano digitalizzazione e innovazione.

Articolato in sei Missioni, suddivise per Componenti cui corrispondono scelte d'investimento mirate[122], lo strumento prevede, tra le altre, una *Missione 1. Digitalizzazione, innovazione, competitività, cultura* ed una *Missione 6. Salute.*

Se la Missione 1 si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese, il Piano parte dal presupposto secondo il quale «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)»[123].

«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'ar-

[122] Per un approfondimento dei suoi contenuti, A. Sciortino, *PNRR e riflessi sulla forma di governo italiana. Un ritorno all'indirizzo politico «normativo»?*, in *www.federalismi.it.*

[123] PNRR, 116.

ricchimento 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»[124].

Ancora, la *Missione 6. Salute* mira a potenziare e riorientare il SSN per migliorarne l'efficacia nel rispondere ai bisogni di cura delle persone, anche alla luce delle criticità emerse nel corso dell'emergenza pandemica che «ha confermato il valore universale della salute, la sua natura di bene pubblico fondamentale e la rilevanza macro-economica dei servizi sanitari pubblici»[125].

In particolare, la Componente 1 di questa Missione mira al «rinnovamento e l'ammodernamento delle strutture tecnologiche e digitali esistenti, il completamento e la diffusione del Fascicolo Sanitario Elettronico (FSE), una migliore capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) attraverso più efficaci sistemi informativi»[126].

Una anche solo rapida lettura dei contenuti del Piano che sono stati riportati conferma – qualora ve ne fosse bisogno – il legame inscindibile che esiste tra digitalizzazione, salute e formazione del capitale umano.

Del resto, anche l'*Agenda 2030 per lo sviluppo sostenibile*, approvata dalle Nazioni Unite nel 2015, nel prevedere un *Goal 4: Fornire un'educazione di qualità, equa ed inclusiva, e opportunità di apprendimento per tutti*, ha di fatto messo in luce la funzionalità della tecnologia digitale rispetto alla realizzazione dell'obiettivo, a patto – evidentemente – di superare alcune barriere quali il *digital divide*[127].

In verità, il problema presenta ulteriori sfaccettature, perché investe anche la formazione professionale del capitale umano, della cui importanza la stessa *Agenda* si è fatta carico all'interno del suo quarto Obiettivo.

Qualora le potenzialità espresse dalle tecnologie *smart* venissero realmente incorporate nelle professionalità italiane, specie nel settore sanitario, numerosi sarebbero i benefici.

---

[124] PNRR, 118. Del resto, non si può non rilevare come la stessa Unione europea (anche in questo campo) si sia fatta carico del compito di soggetto propugnatore di riforme, assurgendo lentamente al ruolo di ente guida degli Stati membri e dirigendo il cambiamento verso la necessità di contemperare lo sviluppo tecnologico con le esigenze formative della popolazione da questo interessata (p. 877). Sulla forte caratterizzazione delle politiche dell'Unione Europea nella direzione del necessario potenziamento del sistema educativo attraverso l'utilizzo di nuovi programmi di formazione e una preventiva opera di alfabetizzazione informatica, C. Leone, *Il ruolo del diritto europeo nella costruzione dell'amministrazione digitale*, in *Riv. it. dir. pubb. comunit.*, 2014, 872.

[125] PNNR, 287.

[126] PNNR, 289.

[127] Sulla connessione dei temi qui trattati con gli obiettivi di sviluppo sostenibile dell'Agenda 2030, anche E. Sorrentino, A.F. Spagnuolo, *Alcune riflessioni in materia di trasformazione digitale come misura di semplificazione*, in *www.federalismi.it*.

I medici potrebbero svolgere in modo effettivo il ruolo che il GDPR, soprattutto mediante l'art. 22, assegna loro. In particolare, «si potrebbe ipotizzare uno scenario di un *professionalismo ibrido e tecnologico*, o *2.0*, seguendo la semantica digitale. In un simile scenario la categoria medica non subirebbe la digitalizzazione supinamente, ma, in un processo di negoziazione e conflitto con gli altri attori, contribuirebbe a trovare un proprio spazio e a co-plasmarla anche in funzione delle proprie esigenze e caratteristiche»[128].

È quindi molto importante creare le condizioni perché esperti di varie discipline riescano a lavorare tutti insieme, ed in una prospettiva interdisciplinare, sulle nuove sfide che gli algoritmi stanno creando, così come è importante riuscire a trasferire le nuove abilità ai giovani, che domani avranno la responsabilità della crescita della società, soprattutto per un Paese, come il nostro, così in ritardo nella formazione di capitale umano per la società digitale[129].

Non solo. Emerge altresì in tutta la sua evidenza la necessità di un nuovo ruolo del giurista, che deve farsi in primo luogo garante contro i rischi della digitalizzazione. La sua creatività non ne esce e non ne deve uscire mortificata[130], bensì amplificata nella ricerca della regola applicativa per il caso concreto[131]: l'avvento delle tecnologie determina semplicemente un cambiamento della sua epistemologia, del modo in cui organizza le regole[132].

Infatti, «è indubbio che la sfida tecnologica non possa fondarsi esclusivamente sul pensiero computazionale e richieda un recupero umanistico ed una chiara assunzione di responsabilità etica anche da parte del giurista»[133], le cui competenze sono state, per tradizione, erroneamente considerate impermeabili all'automazione, come del resto dimostra la ormai vasta diffusione che hanno ad esempio raggiunto le banche dati con i loro sistemi di ricerca indicizzati[134].

Professioni come quelle di "tecnico legale" o di "ingegnere del sapere giuridico" costituiscono alcuni significativi esempi di praticare in modo innovativo il diritto[135], restando al passo con i tempi, interpretando problemi e nuove esigenze della società: si tratta di svolgere "una rinnovata riflessione sul metodo giuridico,

---

[128] A. Ardissone, *La relazione medico-paziente nella sanità digitale*, cit., 87.

[129] Sul punto, G.F. Italiano, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia*, 2019, 18-19.

[130] In questo senso, 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, 405-406.

[131] P. Guarda, L. Petrucci, *Quando l'intelligenza artificiale parla*, cit., 425 ss.

[132] Così V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. media*, 2018, 37.

[133] P. Moro, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Riv. dir. media*, 2019, 21.

[134] S. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 2018, 1801-1802.

[135] Questi esempi sono tratti da più parti dell'opera di R. Susskind, *L'avvocato di domani. Il futuro della professione legale tra rivoluzione tecnologica e intelligenza artificiale*, Milano, 2019.

che si apra all'apporto conoscitivo delle nuove tecnologie di cui anche il giurista dovrebbe però comprendere i profili teorici essenziali"[136].

Probabilmente, lungo questa via si ritorna al punto di partenza, perché il problema diventa nuovamente quello della formazione del giurista e del capitale umano.

Eppure, è quasi paradossale il fatto che, al tempo della pandemia e dell'innovazione tecnologica, si avverta la necessità di un recupero della centralità dell'uomo, come ad esempio testimonia la volontà di superare la crisi pandemica anche attraverso una formazione che richiede l'acquisizione di nuove professionalità e di nuove abilità.

La stessa affermazione della necessità di superare il *digital divide* è uno strumento di riaffermazione della centralità dell'uomo nel contesto delle tecnologie *smart*[137].

Dopotutto, «la disciplina che decideremo di adottare per le macchine e i robot dotati di intelligenza artificiale indicherà allo stesso tempo, in via residuale, la disciplina che avremo riservato per noi stessi»[138].

---

[136] A. Lalli, *Intelligenza artificiale e diritto*, in Aa.Vv., *L'amministrazione nell'assetto costituzionale dei pubblici. Scritti per Vincenzo Cerulli Irelli*, tomo I, Torino, 2021, 646.

[137] Sul mantenimento della centralità dell'individuo nell'uso dell'intelligenza artificiale quale importante sfida per l'attuazione in Italia del Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino, M. Tresca, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in *Riv. dir. media*, 2018, 240 ss.

[138] Così, efficacemente, C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, cit., 181.

Paola Lombardi - Abstract

Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro

Da sempre le tecnologie supportano, e quindi condizionano, i processi curativi, così come il concretizzarsi di un diffuso impiego di tecnologie all'avanguardia in ambito sanitario, con il suo determinare relazioni del tutto nuove tra uomo e macchina, non pare ormai essere molto distante dalla realtà. Queste circostanze richiedono oggi una rinnovata attenzione verso il rispetto dei principi che regolano la tutela dei dati personali, soprattutto se "sensibili" come i dati relativi alla salute della persona. Leggendo il Regolamento (UE) 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, emergono le preoccupazioni che discendono dalla crescente riduzione del ruolo del soggetto umano nell'assunzione di decisioni aventi conseguenze significative per il loro destinatario, sostanzialmente demandate ad un algoritmo. È pur vero che, secondo il GDPR, il titolare del trattamento deve raggiungere determinati risultati in termini di tutela dei dati, ma è anche vero che il titolare deve essere innanzitutto in grado di comprendere il contenuto dei suoi obblighi, specie ai dichiarati fini di tutela. L'attenzione si sposta quindi sul "divario digitale": la predisposizione di adeguati livelli di sicurezza informatica è adempimento fondamentale, ma spesso sconta la mancanza di una diffusa cultura digitale e la carenza di risorse per alimentarla, soprattutto in Italia. Questo è certamente il nodo problematico più critico, specie se lo si rapporta al settore della sanità pubblica al tempo del Covid-19.

Health data security and technological evolution: past, present and future

Modern medicine has been strongly shaped by technological developments, and health technologies are key to promoting not only healing but also preventive care. In recent times, the increasing use of frontier digital health technologies is pushing the interaction between human health and machine to a new frontier. Nowadays, digital technologies in health are relevant not only to gather data, but also for treatment decisions through data analysis. Indeed, recent developments point to a future where health records will be fed into an algorithm that identifies the proper course of treatment for patients. It is therefore imperative to devote renewed attention towards compliance with the principles which regulate not only the handling and the protection of personal data, but also their use by algorithms to determine the course of treatments. This is clearly a major concern in the realm of health, in which data is sensitive, and treatments have important repercussions on humans.