LUISS

Dipartimento di Giurisprudenza

Cattedra di Informatica Giuridica

DIGITAL HEALTH E FASCICOLO SANITARIO ELETTRONICO: LA TUTELA DEI DATI PERSONALI IN AMBITO SANITARIO

RELATORE

Chiar.mo Prof. Stefano Russo

CANDIDATO

Paola Calabrese

Matr. 143873

CORRELATORE

Chiar.mo Prof. Gianluigi Ciacci

ANNO ACCADEMICO 2020/2021

INDICE

INTRODUZIONE

Progresso, innovazione, lo sguardo fiducioso verso il futuro che l'uomo ha rivolto da sempre. Il *προκοπὴ* dell'età ellenistica e il *progressus* di Cicerone. La ruota nel 2000 a.c. e il primo progetto di computer negli anni '30. Epoche, uomini e strumenti lontanissimi ma che condividono con il nostro presente il mito di un'età dell'oro, una ricerca che però mai si arresta.

Interessante quindi soffermarsi a riflettere su come l'uomo ha da sempre compiuto un passo in avanti, a volte anche sbagliando, ma senza interrompere mai ciò che doveva evolvere.

Dagli anni 2000 infatti si può parlare dell'era della tecnologia, della terza rivoluzione industriale come affermano gli scienziati, che ha come cardine l'informatica. Infatti, nel corso dei secoli si è assistito a un progressivo affermarsi delle tecnologie all'interno delle nostre vite, a volte rendendo più difficile, ma a volte facilitando le nostre azioni quotidiane.

Oggi di ogni nostro atto vi è l'equivalente elettronico. Basti pensare alla comunicazione via web, al mondo del lavoro dove tramite la Posta Elettronica Certificata (PEC) è possibile inviare documenti estremamente importanti e in tutta sicurezza. Grazie a un computer oggi si è in grado di acquistare un prodotto situato dall'altra parte del mondo comodamente da casa.

La giurisprudenza e il legislatore hanno dovuto tener conto di questa continua evoluzione che ha comportato in vari ambiti notevoli sviluppi e complicazioni, meritevoli di essere disciplinati.

Oggetto del presente elaborato è osservare come la volontà di progresso ha dato vita al concetto di *Digital Health*[1] in ambito medico e studiare la recente disciplina della tutela dei dati personali, rapportandola a strumenti innovativi come il Fascicolo Sanitario Elettronico, risultato del presente mondo digitalizzato.

L'elaborato si articola in tre capitoli.

Nel primo capitolo si effettua uno studio del Diritto alla salute sia in ambito nazionale che europeo, affrontando la nascita della *Digital Health* e la sua evoluzione, effettuando un'attenta analisi delle nuove tecnologie adoperate con lo scopo di monitorare, prevenire o assistere nella cura delle patologie. Dimostrando quindi come queste si siano rivelate idonee a migliorare i

[1] La World Health Organization ha proposto un uso ancora più ampio del termine digital health, a cui ha fatto eco l'ITU:"*a broad umbrella term encompassing eHealth as well as developing areas such as the use of advanced computing sciences (in the fields of "big data", genomics and artificial intelligence, for example)*"ossia "*un termine molto generico che include l'e-health oltre che aree in fase di sviluppo come l'uso delle scienze informatiche avanzate (ad esempio nel campo dei "big data", della genomica e dell'intelligenza artificiale)*".

servizi sanitari per pazienti e medici. Ponendo l'accento sul concetto di "personalità del paziente" si definirà il Diritto spettante a questi.

I Governi hanno la responsabilità della sanità dei loro popoli[2] perchè il diritto alla salute è uno dei diritti fondamentali e inviolabili della persona e quindi ogni Stato ha l'obbligo positivo di garantirne a tutti i soggetti la giusta tutela e l'accesso.

L'affermarsi della Quarta rivoluzione industriale 4.0[3] ha quindi inevitabilmente influenzato il *modus operandi* in ambito medico inteso sia come esecuzione della prestazione sanitaria sia come il trattamento di dati personali del paziente.

Si discorrerà di un'assistenza sanitaria del futuro più tecnologica e incentrata sul paziente, che però prevede la riprogettazione delle infrastrutture e dei sistemi sanitari già esistenti, rendendo quindi anche inevitabile l'evoluzione del ruolo dei professionisti ma anche del rapporto medico-paziente.

Di fatto si è assistito a un forte mutamento del dialogo tra medico e assistito: alla base del successo di qualsiasi terapia vi è sempre la *compliance terapeutica*, ovvero il grado di acquiescenza dimostrata dal paziente nei confronti della terapia proposta dal medico; quindi, spetterebbe a quest'ultimo assicurarsi che il paziente segua assiduamente le prescrizioni.

Le piattaforme di salute digitali sono un valido strumento per ottimizzare il dialogo tra medico e paziente, favorendo anche il monitoraggio del trattamento e quindi anche l'esito positivo della terapia, rispettando sempre un altro tipo di trattamento, quello dei dati personali, garantito sempre e comunque[4] secondo i 3 pilastri fondamentali: riservatezza, integrità e disponibilità[5].

L'uso sempre più frequente della salute digitalizzata è dettato da vari fattori poichè riduce le inefficienze e garantisce un accesso molto più rapido alle informazioni, riduce i costi e permette

[2] La Conferenza Internazionale della Sanità (New York, 1946) e l'Organizzazione Mondiale della Sanità (OMS) definiscono la salute come "*uno stato di completo benessere fisico, mentale, sociale e non consiste soltanto nell'assenza di malattie o infermità. Il possesso del migliore stato di sanità che si possa raggiungere costituisce uno dei diritti fondamentali di ciascun essere umano, qualunque sia la sua razza, la sua religione, le sue opinioni politiche, la sua condizione economica e sociale. I Governi hanno la responsabilità della sanità dei loro popoli: essi per farvi parte devono prendere le misure sanitarie e sociali appropriate*."

[3] detta anche 4IR o Industria 4.0

[4] Garante della Privacy, schede di sintesi redatte dal Garante a mero scopo divulgativo: "*Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679 […] Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" o anche di "accountability" che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento."*

[5] Guida alla privacy e alla sicurezza delle informazioni sanitarie. L'ufficio del coordinatore nazionale per la tecnologia dell'informazione sanitaria. Dipartimento di Salute e Servizi Umani, USA.

di rendere la terapia più personalizzata in base al paziente, migliorando quindi la qualità del servizio offerto.

Nel corso degli anni è stato quindi necessario cercare di coniugare la garanzia del diritto alla salute alle nuove procedure sanitarie che, da un lato rappresentano un risultato mai raggiunto prima, ma che dall'altro implicano l'utilizzo e la circolazione di dati personali in modo molto più celere e facile.

Il diritto alla privacy, di cui affronteremo storia e applicazione nel quarto paragrafo del capitolo primo, è uno dei limiti a queste forme di progresso, infatti qualsiasi tipo di strumento innovativo può minare il "diritto a esser lasciato solo"[6]. Una struttura sanitaria che in qualche modo leda la privacy del paziente può incorrere in sanzioni amministrative di migliaia di euro, ma non solo, in questo modo essa sarà la diretta responsabile del rapporto con il paziente che, prima di essere tale, è una persona, un individuo. Basti pensare, ad esempio, al motore di ricerca Google che con tutti i dati che tratta, potrebbe avere più potere di una dittatura, essendo oggi considerati i dati personali come il nuovo petrolio[7].

La legge infatti prevede obblighi a carico di tutti gli operatori sanitari e del personale amministrativo analoghi agli oneri di condotta dettati dal segreto professionale. Ad esempio, l'unica persona in grado di ritirare la documentazione clinica è solo il paziente stesso.

L'accesso alle informazioni circa la salute personale della persona deve essere regolamentato ed essere conforme sia alle prescrizioni legali ma anche alle norme etiche, come affermava già Ippocrate nel suo Giuramento e come è enunciato dall'art 11[8] del Codice di Deontologia Medica che contiene principi e regole che, i medici iscritti agli albi professionali, sono tenuti a osservare nell'esercizio della professione.

Nel secondo capitolo si vedrà come il legislatore e la giurisprudenza, sia a livello europeo che a livello nazionale, sono stati costretti negli ultimi decenni a intervenire, cercando di tutelare e

[6]Assiteca Consultative Broker, Privacy: "cos'è il diritto alla privacy e perché è bene tutelarlo"*: "L'istituto nasce negli Stati Uniti nel 1890 come diritto "a essere lasciato solo" (to be let alone) e viene elaborato in Italia dagli anni '60-'70 come generico diritto alla libera determinazione nello svolgimento della propria personalità.",* 22 agosto 2019

[7] Antonello Soro: "Con i suoi dati Google ha più potere delle dittature". Intervista al Garante della Privacy (Intervista ad Antonello Soro, Presidente del garante per la protezione dei dati personali - "Huffington Post" del 29 agosto 2013 - di Klaus Davi)

[8] Art. 11 – Riservatezza dei dati personali. "*Il medico acquisisce la titolarità del trattamento dei dati personali previo consenso informato dell'assistito o del suo rappresentante legale ed è tenuto al rispetto della riservatezza, in particolare dei dati inerenti alla salute e alla vita sessuale. Il medico assicura la non identificabilità dei soggetti coinvolti nelle pubblicazioni o divulgazioni scientifiche di dati e studi clinici. Il medico non collabora alla costituzione, alla gestione o all'utilizzo di banche di dati relativi a persone assistite in assenza di garanzie sulla preliminare acquisizione del loro consenso informato e sulla tutela della riservatezza e della sicurezza dei dati stessi".* Codice di Deontologia Medica

regolamentare quei diritti inviolabili della persona che possono in un certo senso, essere violati dalla nascita di fattispecie che nel passato non erano neanche immaginabili, una situazione dovuta anche dalla creazione di un mercato unico digitale, completo e coerente.

Essendo la protezione dei dati, una parte fondamentale del rispetto dell'identità della persona, il legislatore è stato chiamato inevitabilmente a stabilire regole, trovando non poche difficoltà, tenendo conto della delicatezza dei profili che entrano in gioco e che sono simboli di interessi diversi.

Nel secondo paragrafo del capitolo secondo si analizzerà il ruolo dell'Unione Europea e si noterà come si è dimostrata all'avanguardia per quanto riguarda il trattamento dei dati personali: le norme introdotte si basano sulla Convenzione 108 del Consiglio d'Europa, sugli strumenti, tra i quali il Regolamento Generale sulla Protezione dei Dati e la Direttiva sulla protezione dei dati destinata alla polizia e alle autorità giudiziarie penali, ma anche sulla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea.

Un sostanziale rinnovamento della disciplina italiana, inoltre, è dovuto all'introduzione del Regolamento generale per la protezione dei dati di cui si parlerà nel terzo paragrafo. Il *GDPR* entrò in vigore nel 24 maggio 2016, abrogando la direttiva 95/46/CE, ma la sua applicazione diretta venne rinviata al 25 maggio 2018: ciò per fare in modo che gli Stati membri potessero uniformare la propria normativa nazionale in materia alle disposizioni del Regolamento, nonché alle aziende di adeguare i propri processi.

La legge n. 675/96 ha subìto numerose modifiche ed il suo contenuto è stato in gran parte immesso nel d.lgs. 30 giugno 2003, n. 196, ossia nel Codice in materia di protezione dei dati personali, anche detto *Codice della privacy:* un Codice molto vasto e diviso in tre parti, nelle quali sono contenute le disposizioni generali, le disposizioni specifiche, le forme di tutela e la funzione del Garante per la protezione dei dati personali e dalla vastità di questa opera si evince la forte importanza del diritto alla riservatezza recepita all'interno del nostro ordinamento, colmando una lacuna legislativa pluridecennale.

Di rilevante importanza, inoltre, è stata l'introduzione dello strumento del Fascicolo Sanitario Elettronico ad opera del D.P.C.M. del 29 settembre 2015, n.178, di cui si parlerà nel terzo e ultimo capitolo.

Il Fascicolo Sanitario Elettronico è "*uno degli strumenti in cui si esprime la Sanità Digitale*", che insieme alle ricette elettroniche, alla telemedicina e a tutti le tecnologie ICT in ambito sanitario, riorganizza, potenzia i servizi e coordina l'attività degli operatori. Garantisce una migliore e più semplice comunicazione tra aziende e utenti potenzialmente coinvolte come

fornitori a livello centrale, regionale e locale. Uno strumento attraverso il quale il cittadino può aggiornare e consultare in ogni momento le informazioni circa la sua anamnesi remota, sempre previo suo consenso, rendendo i dati dell'assistito interoperabili, garantendo quindi l'accesso ai soggetti autorizzati su tutto il territorio nazionale e non solo nella regione di appartenenza.

L'idea è quella di cercare di costruire un'unica piattaforma di condivisione e aggregazione delle informazioni rilevanti e di tutti i documenti sanitari e socio-sanitari relativi alla persona, generati dai vari attori del SSN e dai servizi socio-sanitari regionali.

Anche se il legislatore italiano è stato in grado di fornire adeguate norme di settore, bisogna tener conto della difficoltà nell'archiviazione e nella conservazione dei documenti informatici causata dalla loro fragilità intrinseca, potendo essere oggetto di attacchi e manomissioni informatiche.

Ciò che viene richiesto quindi, è un'assistenza istituzionale di competenze idonee in ogni fase di creazione del documento (formazione, gestione, conservazione)[9], per cercare di trovare una soluzione consona al problema della *Digital Preservation*[10].Le strutture sanitarie, infatti, per adeguarsi alla normativa in materia di FSE, devono dotarsi di sistemi di conservazione efficaci: si tratterà delle problematiche che sono emerse relative all'argomento.

Si vedrà che nella quasi totalità dei casi presi in esame, si è riscontrato una mancanza di recepimento delle responsabilità proprie delle singole strutture sanitarie che hanno l'obbligo di gestire il corretto ciclo di vita del documento, tutelando il patrimonio documentale tramite un sistema *in house outsourcing* conforme alla normativa.

Il problema è che la maggior parte dei sistemi adoperati utilizzano un set di metadati minimi (informazioni relative al produttore, l'identificazione del paziente con il codice fiscale). Questi dovrebbero essere arricchiti da una serie di metadati contenenti informazioni aggiuntive relative al ciclo di vita del documento, alla sua creazione, alla possibile combinazione con altri documenti ma anche alla possibilità che questo possa essere collegato ad altri contesti archivistici.

Si menzionerà inoltre il ruolo dell'Agenzia per l'Italia Digitale, affrontando la sua storia e i suoi compiti. Di fatto l'AGID negli ultimi anni ha emanato delle linee guida che indirettamente hanno

[9] G. Bonfiglio Dosio, S. Pigliapoco "L'archivio digitale: specificità ed esigenze formative degli archivisti" "Formazione, gestione e conservazione degli archivi digitali". Il Master FGCAD dell'Università de-gli studi di Macerata", EUM Edizioni Università di Macerata,2016, p. 19

[10]Conservazione digitale, Prof. Stefano Allegrezza "*il trasferimento su supporti analogici (output to analogue media); la conservazione tecnologica (technology preservation); il riversamento diretto (refreshing) e sostitutivo (migration); l'emulazione (emulation); l'archeologia digitale (digital archaelogy)",* 23 marzo 2021

avuto un impatto sul Fascicolo Sanitario Elettronico poiché miranti a disciplinare l'inserimento e il riuso di programmi informatici[11].

Negli ultimi paragrafi del terzo capitolo si volgerà lo sguardo alle esperienze estere di Francia, Inghilterra e Stati Uniti con i rispettivi *Dossier Médical Personnel* (DMP), *NHS Care Record Service* (NHS CRS) e gli *Electronic Health Record*, studiando i diversi sistemi sanitari e capendo perché i vari progetti di sanità elettronica si siano sviluppati in modo così complesso.

[11] In Rete https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_accessibilita_versione_rettifica_del_23_luglio_2020_002.pdf

CAPITOLO 1

IL DIRITTO ALLA SALUTE, IL DIRITTO ALLA PRIVACY E IL DIRITTO DEL PAZIENTE.

Sommario: 1.1 introduzione - 1.2 Il Diritto alla salute in ambito nazionale ed europeo - 1.3 Il concetto di *Digital Health* - 1.4 La Privacy e la protezione dei dati personali in materia sanitaria - 1.5 Il Diritto di accesso e il Diritto del paziente: Legge 22 Dicembre 2017, n. 219

Introduzione

Il diritto alla salute, soprattutto negli ultimi anni, ha posto delle esigenze che sia il legislatore nazionale che quello europeo hanno dovuto assecondare, intervenendo là dove fosse necessario, col fine di permettere una tutela effettiva e satisfattiva del diritto in questione, sancito dalla Costituzione italiana all'art 32.

In questo capitolo verranno esaminati il diritto alla salute, tutte le norme italiane, gli strumenti e gli attori internazionali che si sono susseguiti nel tempo, facendo una particolare menzione della Riforma del Titolo V della nostra Costituzione. Le esigenze poste e l'evoluzione tecnologica concomitante degli ultimi anni hanno posto in essere le basi del concetto di *Digital Health,* un tipo di sanità 2.0 assolutamente in linea con il nostro mondo digitale e digitalizzato, considerandolo come uno specchio sul piano normativo di quello che è il risultato temporaneo del progresso medico.

Ovviamente anche il diritto di accesso e il diritto alla privacy hanno dovuto adeguarsi a queste nuove creazioni: infatti l'oggetto di questo elaborato nasce proprio dalla a volte difficile convivenza tra interessi personalissimi e digitalizzazioni di un sistema, che prima era solo materiale.

Nell'ultima parte del capitolo si parlerà inoltre di un diritto del paziente facendo riferimento alla Legge n. 219 del 2017, considerando quindi l'elemento fondamentale, ovvero quello della persona, destinataria di norme e di cure mediche.

1.2 Il diritto alla salute in ambito nazionale e internazionale.

Possiamo affermare che la salute costituisce lo stato di benessere fisico, mentale e sociale[12] ed è oggetto di specifica tutela da parte dell'ordinamento, infatti consente all'individuo di integrarsi nel suo ambiente naturale e sociale. Quindi è una situazione soggettiva che deve essere assolutamente tutelata contro tutti gli elementi nocivi ambientali e da qualsiasi attacco da terzi che possa, in qualche modo comprometterlo.

La Costituzione italiana, a differenza dello Statuto Albertino che non conteneva alcun riferimento, determina la salute come un diritto fondamentale dell'individuo e come interesse primario della collettività. Essa è stata la prima costituzione europea a riconoscere, e quindi a tutelare, un diritto alla salute, sancito come un valore costituzionale primario per la sua stretta relazione con il concetto di persona e per la sua valenza come diritto sociale. Infatti, né la costituzione francese del 1958, né la costituzione tedesca del 1949, fanno alcuna menzione di tale diritto.

Secondo l'articolo 32 della Costituzione che recita "*La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti",* l'elemento fondamentale della tutela della salute è l'individuo inteso come persona[13], non facendo riferimento quindi al cittadino e quindi al suo status di cittadinanza. Infatti, compito della nostra Repubblica è quello di garantire l'accesso alle cure mediche a tutti coloro che sono presenti sul territorio italiano. Tutti siamo tutelati e tutti dobbiamo tutelare.

Lo Stato italiano ha quindi il compito di prevenire e limitare tutte quelle situazioni di non-benessere che possono ostacolare l'esercizio completo del diritto in questione. Quindi il diritto alla salute costituisce uno dei diritti fondamentali della persona e che deve essere salvaguardato anche tramite l'azione dei pubblici poteri, lo Stato sociale ha la competenza di garantire a tutti

[12] Definizione adottata nel 1948 dall' Organizzazione Mondiale della Sanità (OMS) che ha proposto che ha proposto come definizione di "salute" "*uno stato di completo benessere fisico, mentale, sociale e non consiste soltanto nell'assenza di malattie o infermità. Il possesso del migliore stato di sanità che si possa raggiungere costituisce uno dei diritti fondamentali di ciascun essere umano, qualunque sia la sua razza, la sua religione, le sue opinioni politiche, la sua condizione economica e sociale. I Governi hanno la responsabilità della sanità dei loro popoli: essi per farvi parte devono prendere le misure sanitarie e sociali appropriate*."

[13] C. Costituzionale sentenza del 26.07.1979 n.88 "*non solo come interesse della collettività, ma anche e soprattutto come diritto fondamentale dell'individuo, sicché si configura come un diritto primario ed assoluto, pienamente operante anche nei rapporti tra privati. Esso certamente é da ricomprendere tra le posizioni soggettive direttamente tutelate dalla Costituzione e non sembra dubbia la sussistenza dell'illecito, con conseguente obbligo della riparazione, in caso di violazione del diritto stesso*"

gli individui l'accesso ai diritti fondamentali, disponendo condizioni favorevoli al raggiungimento della tutela anche ai soggetti deboli e marginali.

Oltre ad essere un diritto soggettivo e individuale, la tutela della salute costituisce anche un interesse per la collettività, proprio perché assolve al compito di elevazione della dignità individuale e lo Stato, specularmente, ha un obbligo negativo di astenersi da azioni che possono comportare una lezione dei relativi diritti.

Negli ultimi anni, la coesistenza tra diritto alla salute e sanità pubblica è diventata progressivamente più complessa a causa soprattutto della mancanza dei fondi a disposizione del Governo centrale: la salute deve essere assicurata in maniera gratuita a tutti coloro che ne hanno bisogno, ma è necessario anche fare quadrare i conti dello Stato. Infatti, lo Stato stesso ha dovuto predisporre specifiche normative per affrontare questo tipo di situazione, dando vita al diritto sanitario. Esso si occupa di stabilire e fare rispettare gli aspetti organizzativi della sanità pubblica, esistono, infatti, diversi enti con lo scopo di gestire al meglio tutte le attività connesse alla salute dei cittadini

Significativa è stata la riforma sanitaria con la Legge 28-12-1978, n. 833 che istituendo il servizio sanitario nazionale ha esteso l'obbligo dello Stato di assicurare le prestazioni sanitarie e farmaceutiche, non solo a tutta la popolazione, ma anche agli indigenti, in maniera assolutamente gratuita o semigratuita tramite il pagamento di una cifra con il cd. *ticket.* Si è passati così da un sistema di previdenza sociale, che prevede l'assistenza per i cittadini solo previo versamento di un contributo, a un sistema di sicurezza sociale generalizzato, garantito dal servizio sanitario nazionale. Vedremo inoltre che la protezione della salute come diritto di accedere alla prevenzione sanitaria, e quindi di ottenere cure mediche è stata anche oggetto di una norma specifica della Carta dei diritti fondamentali dell'Unione europea all'articolo 35, garantendo quindi una tutela molto più ampia poiché si impone alle strutture sanitarie nazionali un livello notevole di protezione.

La salute costituisce l'unico diritto che la Costituzione definisce come "fondamentale" a differenza di altri che invece sono definiti come "inviolabili" e ciò è stato anche confermato dalla sessa giurisprudenza[14] che ha definito la salute come diritto primario e fondamentale, infatti questo è alla base di tutti gli altri diritti costituzionali, ed è il presupposto irrinunciabile per la piena realizzazione della persona umana.

[14] Sent. Cort. Cost. 26-9-1990 n. 455 "*i quali garantiscono, da un lato, la tutela della salute come fondamentale diritto dell'individuo e, dall'altro, la parità nei livelli delle prestazioni sanitarie. garantite a tutti i cittadini da parte delle Unità sanitarie locali."*

Il comma terzo dell'articolo 32 recita "*Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana*". Nessun trattamento sanitario può essere obbligatorio ma fanno eccezione i casi esplicitamente indicati e tassativi, in cui sia la stessa legge a prevederlo per il singolo e per la comunità: infatti solo la tutela dell'interesse alla salute collettiva può giustificare un'esigenza del genere e quindi, in un certo senso, una compressione del diritto all'autodeterminazione dell'individuo.[15]

In assenza di una tutela richiesta dall'interesse alla salute della collettività, nessun trattamento sanitario può essere oggetto di imposizione in base al diritto che spetta a tutti gli individui all'autodeterminazione terapeutica: in questo modo la Costituzione, sancisce il diritto di rifiutare le terapie, classico esempio di diritto oppositivo, secondo cui tra tutela della vita e autodeterminazione individuale prevale questa, poiché nel nostro ordinamento non vi è un obbligo generico di dovere costituzionale alla salute.

Secondo quanto disposto, il rifiuto di atti diagnostici o terapeutici deve essere esplicitamente dichiarato dalla persona in questione solo quando è nel pieno possesso delle sue facoltà mentali ed è quindi giuridicamente capace: qualora il paziente non sia più cosciente o in grado di manifestare la sua volontà, l'eventuale consenso o dissenso informato esplicitato da esso, sarà riconosciuto nelle cosiddette dichiarazioni di volontà anticipate, sottoscritte però al momento del pieno possesso delle proprie facoltà, così si è espressa anche la Corte di Cassazione che ha considerato rilevante per l'interruzione del trattamento sanitario, la volontà presunta del paziente[16].

---

[15] Sent. Cort. Cost. 307/1990: "*Osserva peraltro il giudice a quo che l'art. 32 della Costituzione tutela la salute non solo come interesse della collettività, ma anche e soprattutto come diritto primario ed assoluto del singolo (Corte cost. n. 88/1979), e che siffatta tutela si realizza nella duplice direzione di apprestare misure di prevenzione e di assicurare cure gratuite agli indigenti, anche mediante intervento solidaristico (Corte cost. n. 202/1981). Laddove, quindi, manchino del tutto provvidenze del genere, né sia dato ricorrere a forme risarcitorie alternative, la garanzia costituzionale di tutela dell'integrità fisica della persona risulta vanificata. Ed in particolare ciò avviene nel caso in esame, nel quale tale fondamentale diritto dell'individuo può essere sacrificato in conseguenza dell'esercizio da parte dello Stato di attività legittima a favore della collettività (trattamento vaccinale obbligatorio), senza previsione di un compenso equivalente, od altro equipollente proporzionato al sacrificio eventualmente occorso al singolo nell'adempimento di un obbligo imposto nell'interesse della sanità pubblica*."

[16] Sent. Della Cort. Cost. n. 21748/2007«*Ove il malato giaccia da moltissimi anni (nella specie, oltre quindici) in stato vegetativo permanente, con conseguente radicale incapacità di rapportarsi al mondo esterno, e sia tenuto artificialmente in vita mediante un sondino nasogastrico che provvede alla sua nutrizione ed idratazione, su richiesta del tutore che lo rappresenta, e nel contraddittorio con il curatore speciale, il giudice può autorizzare la disattivazione di tale presidio sanitario (fatta salva l'applicazione delle misure suggerite dalla scienza e dalla pratica medica nell'interesse del paziente),* unicamente *in presenza dei seguenti presupposti: (a) quando la condizione di stato vegetativo sia, in base ad un rigoroso apprezzamento clinico, irreversibile e non vi sia alcun fondamento medico, secondo gli standard scientifici riconosciuti a livello internazionale, che lasci supporre la benché minima possibilità di un qualche, sia pure flebile, recupero della coscienza e di ritorno ad una percezione del mondo esterno; e (b) sempre che tale istanza sia realmente espressiva, in base ad elementi di prova chiari, univoci e convincenti, della voce del paziente medesimo, tratta dalle sue precedenti dichiarazioni ovvero dalla sua personalità, dal suo stile di vita e dai suoi convincimenti, corrispondendo al suo modo di concepire, prima di cadere*

La riserva di legge prevista in questo comma, è stata variamente interpretata: alcuni autori affermano che si tratta di una riserva assoluta, ritenendo che la legge dovesse disciplinare in dettaglio casi, tipologie e procedure di ricorso ai trattamenti sanitari obbligatori, altri autori invece hanno ritenuto che la riserva di legge fosse relativa, sostenendo quindi che spetta alla legge fissare le linee essenziali della materia, rinviando a fonti di rango subordinato per le disposizioni più specifiche per l'attuazione della disciplina.

Possiamo affermare quindi che in realtà si tratta di una riserva rinforzata, poiché la legge non potrà mai violare i limiti imposti dal rispetto della persona umana in quanto tale e della sua dignità. Inoltre, si tratta di una riserva di legge statale: dev'essere garantita l'uguaglianza di trattamento di tutti i cittadini a prescindere dalla Regione di residenza.

La prima ragione di quanto disposto è facilmente rinvenibile: l'obiettivo è quello di mantenere un elevato grado di benessere fisico e psichico della popolazione che è utile a tutti noi, all'economia ma più in generale all'armonia della nostra comunità di persone. L'interesse collettivo alla salute può talvolta giustificare trattamenti sanitari obbligatori, come per esempio, soltanto nei casi previsti dalla legge (*vedi supra*), alcuni vaccini.

Lo ha riconosciuto di recente la Corte costituzionale[17], respingendo un ricorso della Regione Veneto, dove si lamentava dell'obbligatorietà di alcuni vaccini. Ovviamente la legittimità di queste misure estreme è sempre subordinata a una serie di condizioni come, ad esempio, la presenza di circostanze idonee che richiedono un patto di solidarietà tra cittadino e stato, l'assenza di conseguenze negative per il soggetto obbligato, la presenza di un indennizzo nei casi di conseguenze più rilevanti e da ultimo gioca un ruolo fondamentale anche la ragionevolezza scientifica.

Quando vengono presi in considerazione nel caso specifico più diritti costituzionali, bisogna bilanciare gli interessi: per quanto riguarda il tema dei vaccini obbligatori, ad esempio, si propone la situazione del diritto all'istruzione dei bambini non vaccinati e dei bambini che per motivi medici personali non possono ricevere la somministrazione di vaccino. In questo caso il

in stato di incoscienza, l'idea stessa di dignità della persona. Ove l'uno o l'altro presupposto non sussista, il giudice deve negare l'autorizzazione, dovendo allora essere data incondizionata prevalenza al diritto alla vita, indipendentemente dal grado di salute, di autonomia e di capacità di intendere e di volere del soggetto interessato e dalla percezione, che altri possano avere, della qualità della vita stessa».

[17] Sentenza della Corte Costituzionale n. 5/2018: "*Nell'ambito della propria competenza legislativa, pertanto, il legislatore, anche in considerazione di una flessione preoccupante delle coperture e di un mutamento nella percezione collettiva circa la necessità dei vaccini, ha ragionevolmente bilanciato i molteplici valori costituzionali coinvolti (libertà di autodeterminazione individuale, tutela della salute individuale e collettiva, tutela dell'interesse del minore), esercitando la propria discrezionalità nella scelta della modalità - l'obbligatorietà vaccinale - con la quale assicurare una prevenzione efficace delle malattie infettive*." Pr. Paolo Grossi, Rel. Est. M. Cartabia – Regione Veneto (Avv.ti Luca Antonini e Andrea Manzi) ed altri c. Presidenza del Consiglio dei ministri (Avv.ti dello Stato Enrico De Giovanni e Leonello Mariani).

legislatore italiano ha pensato di raggirare il problema impedendo la presenza della scuola dell'infanzia ai bambini non vaccinati minori di anni sei, invece, per i bambini non vaccinati maggiori di anni sei, sono state previste solo delle multe a carico dei genitori.

In risposta alla diffusione del virus *Covid-19*, nel mese di dicembre 2020, gli Stati hanno cercato di rispondere all'emergenza mondiale, ponendo sul mercato vari vaccini di case farmaceutiche diverse: infatti il tema della presunta libertà di non vaccinarsi è stato oggetto di un dibattito pubblico incapace di comprendere i dettati delle norme e delle pronunce della Consulta. Ma il disposto dell'articolo in esame va inteso nel senso che un determinato trattamento sanitario può essere imposto a ciascun cittadino solo dalla legge e che l'imposizione per legge di un trattamento sanitario non deve però comportare pregiudizio alla persona umana, la cura medica quindi, non può essere imposta a rischio e pericolo della persona, senza una previsione esaustiva di cautele ed eventuali risarcimenti, nel caso di danno da profilassi.

Le ultime parole del comma quinto dell'articolo corrente "*rispetto della persona umana*", fanno riferimento a una caratteristica della tutela della salute che come vedremo nel diritto europeo, è stata anche inserita nella Carta dei diritti fondamentali dell'Union europea che all'articolo 3 dispone "*1. Ogni individuo ha diritto alla propria integrità fisica e psichica. 2. Nell'ambito della medicina e della biologia devono essere in particolare rispettati: il consenso libero e informato della persona interessata, secondo le modalità definite dalla legge, il divieto delle pratiche eugenetiche, in particolare di quelle aventi come scopo la selezione delle persone, il divieto di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro, il divieto della clonazione riproduttiva degli esseri umani."*

La nostra Costituzione non usa parole a caso, infatti l'espressione "*in nessun caso*" è stata valorizzata dalla Corte di Cassazione nella nota vicenda di Eluana Englaro, per consentirle dopo anni la sospensione di alimentazione e idratazione forzata, avvenuto sulla base del concetto di "*dignità della persona*" che era stato assunto dalla ragazza in questione durante la sua vita. "*La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana*", uno o dei massimi principi del nostro ordinamento.

Dopo aver esaminato l'esplicazione del diritto alla salute nello Stato italiano, ora bisogna volgere lo sguardo a come il diritto alla salute viene tutelato nel diritto internazionale.

Il diritto alla salute viene garantito dalle Nazioni Unite, nel senso che viene tutelato il diritto all'assistenza sanitaria. Devono essere menzionati l'articolo 25 della Dichiarazione Universale dei Diritti dell'Uomo che al primo comma dispone "*Ogni individuo ha diritto ad un tenore di vita sufficiente a garantire la salute e il benessere proprio e della sua famiglia, con particolare*

riguardo all'alimentazione, al vestiario, all'abitazione, e alle cure mediche e ai servizi sociali necessari; e ha diritto alla sicurezza in caso di disoccupazione, malattia, invalidità, vedovanza, vecchiaia o in altro caso di perdita di mezzi di sussistenza per circostanze indipendenti dalla sua volontà" e l'articolo 12 del Patto internazionale relativo ai diritto economici sociali e culturali che al primo comma recita "*Gli Stati Parti del presente Patto riconoscono il diritto di ogni individuo a godere delle migliori condizioni di salute fisica e mentale che sia in grado di conseguire."*

Il diritto di accesso alle cure mediche però viene anche menzionato in vari strumenti specifici internazionali: come nella Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale del 1965, nella Convenzione sull'eliminazione di tutte le forme di discriminazione nei confronti della donna del 1979, nella Convenzione sui diritti del fanciullo del 1989 e nella Convenzione sui diritti delle persone con disabilità del 2006. Inoltre, il carattere universale delle prestazioni sanitarie e il diritto di accesso di ogni persona alle cure mediche sono espressamente previsti dall'Agenda 2030 per lo Sviluppo Sostenibile[18].

Anche l'Organizzazione Mondiale della Sanità (OMS) svolge un ruolo importante per quanto riguarda la tutela della salute, essa infatti essendo un'agenzia specializzata delle Nazioni Unite promuovere standard di prevenzione e cura tramite l'elaborazione di indicatori e norme attinenti alla qualità delle prestazioni mediche, per fare in modo di orientare gli Stati membri nelle loro scelte circa l'organizzazione e la gestione del proprio sistema sanitario. Tra gli obiettivi principali che gli Stati si prefiggono vi è la *essential primary health care*, riguardante il trattamento delle malattie più comuni e meno gravi da parte di medici o di personale sanitario in generale con costi modesti. Se dovessimo riferirci alla sola assistenza sanitaria primaria, dovremmo escludere l'assistenza secondaria, ovvero quella relativa alla cura di malattie più complesse che ovviamente richiedono competenze maggiori, l'uso di attrezzature specializzate o il ricovero in ospedale, e l'assistenza terziaria, ovvero il trattamento di malattie gravi e complesse presso strutture specializzate con personale e attrezzature idonee, comportando però così elevati. Ma l'Organizzazione Mondiale della Sanità ha precisato che non esiste una definizione univoca di *primary health care*[19], quindi il livello di tutela sarà tipico di quel determinato Paese preso in considerazione, e ovviamente lo *standard* applicabile sarà proporzionale al progresso economico

[18] È un programma di azione a tutela delle persone e del pianeta e mira a promuovere la prosperità. È stato firmato nel settembre 2015 da 193 paesi dell'ONU. <www.unric.org/it/agenda-2030>

[19] Definizione di primary health care sul sito dell'OMS "*PHC is a whole-of-society approach to health that aims at ensuring the highest possible level of health and well-being and their equitable distribution by focusing on people's needs and as early as possible along the continuum from health promotion and disease prevention to treatment, rehabilitation and palliative care, and as close as feasible to people's everyday environment." www.who.int/news-room/fact-sheets/detail/primary-health-care 1 aprile 2021*

e al miglioramento delle condizioni di vita. Per questo, elemento essenziale è la cooperazione tra gli Stati: infatti è necessario raccogliere informazioni ed elaborare degli *standard* che consentono di valutare celermente l'attività del singolo Stato[20]. Inoltre occorre individuare delle linee prioritarie di azione, una serie di raccolte di informazioni utili, poiché l'Ufficio Regionale per l'Europa dell'Organizzazione Mondiale della Sanità, rende evidente la necessità di sviluppare reti di prestatori pubblici e privati che siano assolutamente in grado di rispondere alle esigenze del paziente in questione, investendo così sulla formazione del personale sanitario e quindi di evitare il pagamento da parte dei cittadini, infatti, ad esempio coloro che appartengono alle minoranze, sarebbero scoraggiati ad accedere alle cure mediche per evitare un indebitamento. Inoltre, è anche necessario che le scelte riguardo l'accesso all'assistenza sanitaria siano dettate da un procedimento caratterizzato da trasparenza, assicurando quindi un'effettiva tutela dei singoli tramite meccanismi di valutazione *ex ante* definiti *impact assessment* e strumenti invece di controllo ex post di carattere amministrativo e giurisdizionale.

Il risultato di tutte queste caratteristiche è lo sviluppo di politiche volte a una giustizia sociale, creando un equilibrio tra l'intervento dello Stato e le logiche dello Stato, tutelando quindi anche i gruppi più vulnerabili di individui come gli anziani, le donne giovani o soggetti che appartengono a minoranze, garantendo a tutti l'accesso alle cure mediche.

Questo tema viene anche affrontato dall'Organizzazione Mondiale del Commercio (OMC), di cui fanno parte l'Unione e gli Stati membri e l'Accordo generale sugli scambi e servizi (GATS), che pone come principio quello della libera circolazione di servizi che non sono governativi o che non siamo menzionati da deroghe.

L'applicazione dell'Accordo ricomprende quindi anche le professioni sanitarie e i servizi di ambulanza, ospedalieri e residenziali, e restano esclusi i sistemi sanitari che operano in regime di monopolio. La libera prestazione di servizi sanitari prevista dal GATS pone quattro ipotesi, delineate dall'articolo 2 al secondo paragrafo: "*a) fornitura di un servizio dal territorio di un Membro al territorio di un altro Membro, b) nel territorio di un Membro ad un consumatore di servizi di un altro Membro; c)da parte di un prestatore di servizi di un Membro, attraverso la presenza commerciale nel territorio di un qualsiasi altro Membro e d) da parte di un prestatore di servizi di un membro, attraverso la presenza di persone fisiche di un Membro nel territorio di*

[20] L'Ufficio Regionale per l'Europa dell'Organizzazione Mondiale della Salute ha adottato un piano di azione denominato *European Action Plan for Strenghtening Public Health Capacities and Servicies* a Malta nel settembre 2012 in cui vengono individuate una serie di elementi essenziali per definire una giusta programmazione dell'assistenza sanitaria.

qualsiasi altro Membro" e quindi rientrano nel paragrafo "a" la telemedicina e le diagnosi con consulenza online (e-health) e nel paragrafo "b" rientrano le cure programmate all'estero.

In base all'enunciato dell'articolo 4 del GATS "*ciascun membro è tenuto ad accordare ai servizi e ai prestatori di servizi di un qualsiasi altro Membro, in via immediata e incondizionata, un trattamento non meno favorevole di quello accordato ad analoghi servizi e prestatori di servizi di qualsiasi altro paese*" si definisce la "clausola della nazione più favorita", ma la regola non si applica ai servizi che sono indicati nella lista allegata all'accordo, quindi vi può essere una deroga qualora vi sia una forma di integrazione regionale come le aeree di libero scambio e le unioni doganali, caso tipico dell'Unione Europea. Il trattamento riservato ai cittadini di un altro Stato contraente necessita di essere identico o diverso rispetto a quello accordato ad analoghi servizi e stabilire se si stratta di servizi simili o in concorrenza è un tipo di valutazione che deve essere compiuta tenendo conto degli standard di sicurezza e di qualità (vedi *supra*). Quindi la decisione di non rimborsare le cure mediche ricevute in un altro Stato dell'Organizzazione Mondiale del Commercio sarebbe possibile solo in presenza di condizioni uguali di garanzia per il paziente.

Merita di essere menzionato inoltre l'interesse all'assistenza sanitaria proprio del Consiglio d'Europa: bisogna infatti far riferimento, anzitutto, alla Convenzione europea di assistenza sociale e medica[21], con cui le parti firmatarie si impegnano a garantire ai cittadini delle altre parti, la stessa assistenza sociale e medica di cui godono questi nel loro Stato, purchè ovviamente siano in possesso di un permesso di soggiorno. Poi deve essere citata anche la Carta sociale europea, che in base al suo articolo 13 prescrive che "*Per assicurare l'effettivo esercizio del diritto all'assistenza sociale e medica, le Parti s'impegnano: 1)[…]possa ottenere un'assistenza adeguata e, in caso di malattia, le cure di cui necessita in considerazione delle sue condizioni; 2) […] ad accertarsi che le persone che beneficiano di tale assistenza non subiscano in ragione di ciò, una diminuzione dei loro diritti politici o sociali; 3)[…] ogni tipo di consulenza e di aiuto personale necessario per prevenire, eliminare o alleviare lo stato di bisogno personale e familiare; 4)[…] ad applicare, a parità con i loro concittadini, le disposizioni di cui ai paragrafi 1, 2 e 3 del presente articolo ai cittadini delle altre Parti che si trovano legalmente sul loro territorio in conformità con gli obblighi assunti ai sensi della Convenzione europea di assistenza sociale e medica firmata a Parigi l'11 dicembre 1953."*

[21] La Convenzione venne firmata a Parigi l'11 dicembre del 1953 ed entrò in vigore il 1 luglio del 1954, è stata ratificata da 18 Stati membri del Consiglio d'Europa tra cui il Belgio, la Danimarca, l'Estonia, la Francia, la Germania, la Gran Bretagna, la Grecia, l'Irlanda, l'Italia, il Lussemburgo, Malta, i Paesi Bassi, il Portogallo, la Spagna, e la Svezia.

Inoltre, bisogna ricordare anche la Convenzione sui diritti dell'uomo e la biomedicina di Oviedo del 1997, della quale l'articolo 3 "*Le Parti prendono, tenuto conto dei bisogni della salute e delle risorse disponibili, le misure appropriate in vista di assicurare, ciascuna nella propria sfera di giurisdizione, un accesso equo a cure della salute di qualità appropriata*."

Così il Consiglio d'Europa vuole puntualizzare che la protezione della salute copre anche il diritto a ottenere diagnosi o interventi di prevenzione, terapeutici o riabilitativi, volti a incidere sullo stato di salute della persona, senza alcuna discriminazione. Quindi non si tratta solo di un diritto proprio della persona, ma si tratta di "una serie di misure di politica sociale generale indispensabili per garantire l'applicazione della Convenzione".

Gli Stati devono quindi garantire il funzionamento del sistema sanitario, prevedendo delle misure ad hoc per i pazienti ricoverati presso strutture pubbliche o cliniche private e linee guida per l'accertamento di decessi e per la responsabilità personale dei prestatori di servizi sanitari[22]. Tutto questo ha richiesto l'intervento della giurisprudenza in molteplici casi come, ad esempio, le sentenze rese in materia di aborto[23], in caso di astensione terapeutica ed eutanasia, la regolamentazione degli ospedali psichiatrici e l'accesso all'interruzione volontaria di gravidanza[24].

Si può affermare che compito dell'Unione europea è quello di promuovere al massimo l'accesso alle cure mediche in modo non discriminatorio, garantendone anche la qualità e la loro uniformità agli *standard* di sicurezza, col fine di raggiungere dei sistemi sanitari sostenibili e validi. L'Organizzazione si fonda sul rispetto della dignità umana e dei diritti fondamentali, come sancito dall'articolo 2 del Trattato dell'Unione europea "*L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non*

[22] Calvelli e Ciglio (Calvelli e Ciglio c. Italia [GC], n. 32967/96, Corte EDU 2002 "… *I), il Governo rammenta che la Corte ha già concluso che il sistema italiano offre alle persone sottoposte alla sua giurisdizione dei mezzi, che sul piano teorico rispondono alle esigenze dell'articolo 2. Nel caso di specie, i ricorrenti hanno promosso un procedimento civile, che ha condotto all'individuazione delle cause e delle responsabilità, nonché al risarcimento degli interessati. Questi ultimi non sono quindi più vittime di una violazione della Convenzione."*

[23] Open Door and Dublin Well Woman v Ireland, (14234/88) [1992] ECHR 68 (29 October 1992) *" […] the injunction interfered with the right of the applicants by preventing them to provide information about pregnancy-related options, and with the ability of women to receive information*." <http://www.hrcr.org/safrica/life/OpenDoor>

[24] R.R. v. Polonia, ric.n.27617/04, sentenza del 26 Maggio 2011, Corte EDU. Nel caso di specie la donna già informata del rischio che il feto fosse affetto da malformazioni, le vennero consigliati ulteriori indagini genetiche, tra cui l'amniocentesi che però fu effettuata soltanto alla ventitreesima settimana di gravidanza ma il feto era affetto dalla sindrome di Turner. Quindi alla sua richiesta di sottoporsi all'interruzione di gravidanza, l'ospedale oppose un diniego fondato sul fatto che ormai erano scaduti i termini previsti dalla legge. Quindi la donna agì in giudizio, in seguito alla nascita della bambina, affetta dalla sindrome di Turner, per far accertare la responsabilità penale del personale sanitario che aveva omesso di tutelare i suoi diritti e interessi garantiti dalla legge.

discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini" e quindi il loro rispetto è garantito dalla Corte di giustizia. Ma per garantire il rispetto di detti principi, l'unione deve "*agire esclusivamente secondo le sue competenze che le sono attribuite dagli Stati membri*"[25].

Le norme di diritto primario che regolano l'intervento dell'Unione europea nel diritto alla salute sono: l'articolo 4 paragrafo 2 lett. K), dove il Trattato sul funzionamento dell'Unione europea cita i problemi di sicurezza in materia di sanità pubblica tra le materie di competenza concorrenti, e l'articolo 6 lett. A) nel quale vengono inclusi anche la tutela e il miglioramento della salute in generale tra quelle che sono definite le competenze parallele dell'Unione, in questo caso infatti le istituzioni possono svolgere azioni di vario tipo per coordinare gli Stati membri. Si può affermare che gli obiettivi principali che l'Unione europea vuole raggiungere sono: la prevenzione delle malattie e affezioni, cercando anche di adottare una politica contro l'uso di tabacco, alcol e stupefacenti, ma anche il miglioramento dei servizi sanitari disponibili nelle regioni di frontiera. Ma le istituzioni, anche in base a quanto disposto dall'articolo 168 del TFUE al paragrafo 7[26] devono comunque esercitare i loro poteri tenendo conto del fatto che saranno gli Stati membri ad essere responsabili per la loro politica sanitaria adottata, poiché mantengono una competenza esclusiva in determinati ambiti. Quindi opera una riserva statale poiché ogni individuo ha il diritto espressamente riconosciuto di accedere alle cure mediche ma solo se sussistono le condizioni stabilite dalle legislazioni nazionali e dalle norme sulla libera circolazione delle merci, delle persone e dei servizi che in certi casi ammettono una restrizione all'esercizio di detto diritto.

Con il trattato di Maastricht si ebbe una disposizione specifica in materia di salute pubblica nel diritto primario favorendo così un controllo per quanto riguarda le politiche sanitarie adottate da ogni Stato membro: infatti l'assistenza sanitaria è così notevole da essere considerata come uno dei quattro pilastri della protezione sociale e come fattore di crescita economica. Le condizioni per consentire un intervento in materia sono: innanzitutto, è necessario condividere valori sanitari generali, va ricordato che nel giugno 2006 il Consiglio ha proclamato dei principi comuni di universalità, accesso e cure di buona qualità, equità e solidarietà, sottolineando che all'interno

[25] Articolo 5 TUE sulla ripartizione e l'esercizio delle competenze a seguito del Trattato di Lisbona

[26] Versione consolidata del trattato sul funzionamento dell'Unione europea - PARTE TERZA: POLITICHE DELL'UNIONE E AZIONI INTERNE - TITOLO XIV: SANITÀ PUBBLICA - Articolo 168 (ex articolo 152 del TCE) *Gazzetta ufficiale n. 115 del 09/05/2008 pag. 0122 – 0124*" *L'azione dell'Unione rispetta le responsabilità degli Stati membri per la definizione della loro politica sanitaria e per l'organizzazione e la fornitura di servizi sanitari e di assistenza medica. Le responsabilità degli Stati membri includono la gestione dei servizi sanitari e dell'assistenza medica e l'assegnazione delle risorse loro destinate. Le misure di cui al paragrafo 4, lettera a) non pregiudicano le disposizioni nazionali sulla donazione e l'impiego medico di organi e sangue*." <www./eur lex.europa.eu/legal-content>

dell'Unione "*tutti i sistemi sanitari mirano a mettere al centro il paziente e a rispondere ai bisogni individuali*"[27].

In secondo luogo, è essenziale la sostenibilità finanziaria dei sistemi sanitari nazionali: il Consiglio e la Commissione sono intervenuti infatti per permettere varie riforme che potessero intervenire sui sistemi sanitari, a seguito della crisi economica, così che questi riuscissero a fronteggiare i contesti in evoluzione pur non disponendo di risorse economiche elevate. Dal 2012 opera un coordinamento tra gli Stati in materia sanitaria nel semestre europeo, ponendo tra gli obiettivi principali della politica di bilancio, proprio l'accesso alle cure mediche. Le forme di intervento sono varie, possono essere adottate misure di armonizzazione o programmi di finanziamento pluriennali in materia di salute, oppure possono essere prefissate delle linee guida o degli *standard* qualitativi specifici, tenendo però conto di alcuni elementi prioritari come la sicurezza del paziente, la digitalizzazione delle prestazioni mediche[28], la formazione di personale sanitario e quindi la valutazione della *performance* generale dei sistemi sanitari nazionali e delle tecnologie utilizzate. Dette predisposizioni costituiscono la politica sanitaria per il miglioramento della salute volta a consentire l'accesso ottimale alle cure mediche.

Il diritto internazionale pone dei doveri in capo agli Stati per quanto riguarda l'equità dell'accesso all'assistenza sanitaria e il Patto internazionale relativo ai diritti economici sociale e culturali menzionato prima, annovera questo dovere tra le cosiddette *core obligations* ovvero un presupposto essenziale per assicurare un'assistenza medica produttiva e per garantire il pieno rispetto della dignità umana.

[27] Conclusioni del Consiglio sui valori e principi comuni dei sistemi sanitari dell'Unione europea (2006/C 146/01): "*I valori generali di universalità, accesso a cure di buona qualità, equità e solidarietà sono valori ampiamente accettati nei lavori delle varie istituzioni dell'UE. Insieme, essi costituiscono un pacchetto di valori condivisi in tutta Europa. Universalità significa che a nessuno è precluso l'accesso all'assistenza sanitaria; la solidarietà è intimamente connessa al regime finanziario applicato al sistema sanitario nazionale e alla necessità di garantirne l'accessibilità per tutti; l'equità implica la parità di accesso in funzione del bisogno, senza distinzioni in base all'appartenenza etnica, al genere, all'età, al ceto o al censo. I sistemi sanitari dell'UE mirano inoltre a colmare il divario che produce quelle ineguaglianze nella salute che costituiscono una preoccupazione per gli Stati membri dell'UE e che sono intimamente connesse all'opera di prevenzione delle malattie che i sistemi degli Stati membri portano avanti, tra l'altro promuovendo stili di vita sani*" Testo disponibile su <www.op.europa.eu>

[28] "COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica" "*La sanità elettronica rappresenta un'importante innovazione, in grado di migliorare l'accesso all'assistenza sanitaria e di rafforzare la qualità e l'efficacia dei servizi offerti. Per sanità elettronica si intende l'applicazione delle tecnologie dell'informazione e della comunicazione all'intera gamma di funzioni che investono il settore sanitario*" Bruxelles, 30.4.2004 COM (2004) 356 www.eur-lex.europa.eu

Come è stato affermato dal Comitato europeo dei diritti sociali nel 1999[29], la tutela della salute "[…] *deve essere effettiva e non teorica […]"* perché il ricorso a strumenti legislativi è a volte necessario[30].

Inoltre, in capo agli Stati sussiste un obbligo di tipo negativo di astenersi da misure che possono pregiudicare il godimento della salute in altri Stati e di adottare invece misure per aiutare un altro Stato qualora questo non possa garantire la realizzazione del diritto alla salute[31]: gli Stati concludendo tra loro accordi bilaterali o multilaterali o partecipando ad organizzazioni internazionali, pongono un obbligo di collaborazione che deve essere rispettato qualora la situazione lo richiedesse.

È stato inoltre affermato dal Relatore Speciale sul diritto alla salute fisica e mentale[32] nel 2015, che il diritto alla salute presenta anche il carattere della progressività, nel senso che "l'obiettivo da raggiungere non è quello di raggiungere un livello prefissato, bensì il continuo miglioramento dell'accessibilità alle cure mediche". Il carattere progressivo, quindi, conferisce agli Stati una sorta di obbligazione di mezzo poiché in capi ad essi sorge l'onere di dimostrare l'idoneità degli strumenti che sono stati utilizzati per raggiungere gli obiettivi. La verifica finale sull'osservanza da parte degli Stati degli impegni assunti previamente, avviene tramite degli indicatori e *benchmark* che valutano le prestazioni dei sistemi sanitari nazionali: tutto questo ovviamente necessita di una primaria raccolta di dati che comporta però costi notevoli in capo alle autorità nazionali e inoltre, la loro tipologia varia da Stato a Stato, non potendo ottenere un sistema omogeneo.

Gli Stati devono quindi elaborare dei programmi di politica sanitaria, devono garantire che le strutture sanitarie siano disposte equamente su tutto il territorio nazionale e devono permettere

[29] Comitato europeo dei diritti sociali, Commission internationale des juristes C. Portogallo, 9 settembre del 1999 con reclamo 1/1998.

[30]PIDESC articolo 1.2. "*Per il raggiungimento dei suoi fini, tutti i popoli possono disporre liberamente delle proprie ricchezze e risorse naturali, fermi restando gli obblighi che derivano dalla cooperazione economica internazionale fondata sul principio del reciproco vantaggio, nonché dal diritto internazionale. In nessun caso un popolo può essere privato dei propri mezzi di sussistenza.*" <www.ohchr.org>

[31] PIDESC articolo 2 *"1. Ciascuno degli Stati Parti del presente Patto si impegna ad adottare misure, sia separatamente che mediante l'assistenza e la cooperazione internazionali, soprattutto economiche e tecniche, al massimo delle risorse di cui dispone, al fine di conseguire progressivamente, con tutti i mezzi, tra cui in particolare l'adozione di provvedimenti legislativi, la piena realizzazione dei diritti qui riconosciuti. 2. Gli Stati Parti del presente Patto si impegnano a garantire l'esercizio dei diritti in esso previsti, senza alcuna discriminazione di razza, colore, sesso, lingua, religione, opinione politica o di altra natura, origine nazionale o stato sociale, posizione, nascita o qualsiasi altra condizione sociali.3. I paesi in via di sviluppo, nel rispetto dei diritti umani e della loro economia nazionale, possono determinare in quale misura garantiranno i diritti economici riconosciuti in questo Patto a persone che non sono loro cittadini*." <www.ohchr.org>

[32] Il mandato del Relatore speciale sul diritto alla salute fisica e mentale è stato stabilito dalla Commissione sui diritti umani con la risoluzione 2002/31 nell'aprile 2002. Il Consiglio per i diritti umani ha approvato e ampliato il mandato con le risoluzioni 6/29 del 14 dicembre del 2007, e poi lo ha rinnovato per l'ultima volta con delibera 42/16 il 7 ottobre 2019. <www.ohchr.org>

che i servizi siano accessibili a tutti senza discriminazione, ovviamente rispettando sempre il diritto alla riservatezza e alla dignità, tema principale di questo elaborato. I beni e i servizi disposti devono essere però anche in regola con le norme etiche applicabili all'ambito medico, tenendo conto anche di diversità di modi come nelle minoranze culturali. Un limite a tutte queste disposizioni è costituito dalle risorse finanziarie e dall'impatto della crisi economica sui sistemi sanitari, ma per far fronte a queste situazioni è possibile il reperimento di finanziamenti tramite la cooperazione internazionale e il Comitato dei diritti economici, sociali e culturali dell'ONU. L'obbligo di cooperazione finanziaria può essere desunto anche dal disposto dell'articolo 1 della Carta dell'ONU[33] e viene richiamato anche in varie raccomandazioni e obblighi di *soft law*.

Alcuni autori sostengono che si tratti di responsabilità extraterritoriale, altri invece sostengono che si tratti di responsabilità condivisa, un'istituzione di fondi di finanziamento gestito dagli Stati come simbolo di solidarietà.

Dopo aver esaminato quali sono gli attori internazionali del diritto alla salute, ora si deve fare un cenno a quelli che sono i valori comuni tra gli Stati.

Ovviamente vi sono dei fattori, come la crisi economia citata prima, che hanno inciso profondamente su più fronti: l'Organizzazione mondiale della Sanità ha emanato delle linee di azione per raggiungere gli obiettivi posti. Il piano mira a raggiungere un forte potenziamento degli investimenti in assistenza primaria, concedere ad esempio una prevenzione ottimale delle malattie, intervenire direttamente sulla formazione del personale qualificato per migliorare il livello dei servizi offerti e garantendo eccellenti servizi di assistenza pubblica e privata sia intramoenia che extramoenia. Non è pensabile, però, poter adottare gli stessi strumenti di politica sanitaria in tutti gli ordinamenti: vi sono elementi come, ad esempio, il tasso di natalità o mortalità, la stabilità economica o il numero delle minoranze etniche, che caratterizzano un Paese e le sue scelte per quanto riguarda le modalità di finanziamento dei sistemi sanitari nazionali.

A livello idealistico, sono stati posti due ideali di modelli gestionali: il "modello Bismarck", un sistema mutualistico caratterizzato da un finanziamento mediante contributi obbligatori dei lavoratori e datori di lavoro sullo stipendio, con risorse gestite da imprese o fondi; e il "modello Beveridge", dove il servizio sanitario nazionale è basato sulla fiscalità generale e in questo caso è lo stesso Stato che amministra i fondi. Questi due modelli ideali si sono contaminati a vicenda

[33] Carta delle Nazioni Unite articolo 1, paragrafo 3"*Conseguire la cooperazione internazionale nella soluzione dei problemi internazionali di carattere economico, sociale culturale od umanitario, e nel promuovere ed incoraggiare il rispetto dei diritti dell'uomo e delle libertà fondamentali per tutti senza distinzioni di razza, di sesso, di lingua o di religione*" <www.difesa.it>

e quindi oggi è impossibile tentare di definire in modo specifico il sistema di quel determinato Paese[34].

La scelta del modello di sistema sanitario da adottare, ovviamente produce delle conseguenze sociali all'interno di uno Stato, ma per essere accettabile, il sistema scelto deve soddisfare quei caratteri di solidarietà, democraticità e trasparenza in modo tale che il singolo cittadino sia pienamente consapevole del diritto che gli spetta.

[34] Libro "Unione Europea e Salute" di Giacomo di Federico e Stefania Negri, capitolo 2, pagina 65.

1.3 Il concetto di *Digital Health.*

In questo paragrafo si esporrà il concetto di *Digital Health*, la sua nascita e il suo sviluppo nel tempo, parlando di una sanità del futuro, il nostro presente. È importante conoscere più da vicino questo fenomeno affermatosi degli ultimi anni, perché costituisce il punto di partenza per la valutazione del trattamento dei dati personali di fronte a metodi di comunicazione e gestione di questi, in un modo del tutto innovativo.

La *Digital Health* è l'uso delle tecnologie dell'informazione e della comunicazione nei campi della salute, dell'assistenza sanitaria, dello stile di vita e della società, con l'obiettivo di migliorare l'efficienza dell'erogazione delle cure sanitarie e rendere le terapie prescritte più personalizzate e precise. Ma la *World Health Organization* preferisce proporre un uso ancora più ampio del termine: essa intende "*un concetto molto generico che include l'e-health oltre che aree in fase di sviluppo come l'uso delle scienze informatiche avanzate (ad esempio nel campo dei "big data", della genomica e dell'intelligenza artificiale)*", ponendo l'attenzione non solo sull'uso di strumenti informatici nell'ambito sanitario ma ricomprendendo anche le scienze informatiche avanzate. Definizione è stata anche condivisa dall'International Telecommunication Union (ITU)[35]**.** Inoltre, la 58ª Assemblea mondiale della sanità[36] nel 2005 a Ginevra, ha ufficialmente definito l'eHealth come un mezzo per rafforzare i sistemi sanitari e per migliorare la qualità, la sicurezza e la possibilità di accesso alle cure, infatti ha incoraggiato tutti i suoi Paesi membri ad adottarla nei loro sistemi sanitari nazionali. Definizione è stata anche condivisa dall'International Telecommunication Union (ITU)**.**

Anche la *US Food & Drug Administration* (FDA)[37] ha proposto una sua definizione di *digital health*:*"The broad scope of digital health includes categories such as mobile health (mHealth),*

[35]La International Telecommunication Union (ITU) è l'agenzia specializzata delle Nazioni Unite nelle tecnologie per l'informazione e la comunicazione. "*Founded in 1865 to facilitate international connectivity in communications networks, we allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. Every time you make a phonecall via the mobile, access the Internet or send an email, you are benefitting from the work of ITU. ITU is committed to connecting all the world's people – wherever they live and whatever their means. Through our work, we protect and support everyone's right to communicate*." Sito uffciale www.itu.int 28 marzo 2021

[36] L'organo legislativo dell'Organizzazione Mondiale della Sanità.

[37] La Food & Drug Administration è un'agenzia federale statunitense all'interno del Department of Health and Human Services. "*The Food and Drug Administration (FDA) is responsible for protecting the public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation. The FDA also provides accurate, science-based health information to the public*". www.usa.gov28 marzo 2021

health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine."

Descrivendo anche quali sono gli obiettivi che si possono raggiungere in questo modo: ridurre le inefficienze, facilitare l'accesso alle cure mediche, ridurre i costi, innalzare la qualità dei servizi e rendere le terapie farmacologiche da seguire più personalizzate in base al paziente. La definizione proposta dalla Food & Drug Administration, quindi, intende includere categorie come la salute mobile (mHealth), la tecnologia dell'informazione sanitaria, i dispositivi che possono essere indossati, la tele-salute e la telemedicina e la medicina personalizzata, parlando quindi anche di *digital care.*

Per quanto riguarda la storia della salute digitale, si può affermare che essa è nata negli anni 90 dello scorso secolo, più precisamente poco prima del 1999 nell'ambito del marketing di alcune aziende tecnologiche[38], accostato al termine *e-Commerce* che indica il commercio elettronico e altri "*e-termini*" molto popolari. L'intento era quello di distinguere con un nome appropriato il sistema sanitario con Internet, e la connessione degli strumenti sanitari con Internet ha portato alla nascita anche del termine "*Connected Health*"[39] l'equivalente inglese del "salute in rete" italiano, per indicare tutti quei processi improntati sulla connessione alla rete. E termine analogo a questo è "*Connected Care*" che indica "*la presa in carico globale del paziente, realizzata grazie alla condivisione di informazioni, dati clinici e strategie tra tutti i soggetti coinvolti (medici e infermieri ospedalieri, operatori sanitari sul territorio e a domicilio, pazienti, assicuratori, referenti istituzionali, ecc.). In pratica si agevola la creazione di un piano di cura condiviso e integrato, includendo prestazioni sanitarie, sociosanitarie e sociali*."[40] Un modello che prevede al centro dell'esperienza digitale il cittadino e permette di considerare tutti i punti di contatto digitali tra paziente e sistema sanitario articolando questi punti di contatto in quattro fasi: la prima fase prevede la prevenzione, studiando lo stile di vita del paziente e ricercando quindi informazioni sulla sua salute, raccogliendo e gestendo dati; la seconda fase prevede l'accesso al sistema sanitario tramite la ricerca di strutture, la prenotazione di visite e il

[38] "*L'azienda Intel Corporation ne fa uso: è un'azienda multinazionale statunitense fondata nel 18 luglio 1968 con sede a Santa Clara in California. Produce dispositivi a semiconduttore, microprocessori, componenti di rete, chipset per motherboard (scheda madre), chip per schede video e molti altri circuiti integrati ed è considerata una delle più importanti nel settore*". www.ilsoftware.it visto il 29 marzo 2021

[39] Termine che viene spesso usato in un contesto socio-tecnologico in cui "*si sottolinea l'aspetto di interconnettività/ interconnessione dei dispositivi, dei servizi e delle soluzioni legate alla sanità, i cui ambiti si ampliano per includere anche l'assistenza remota (come l'assistenza a casa o in viaggio).In pratica, connected health viene usato come termine "ombrello" per includere e rimpiazzare una serie di altri termini come telemedicina (telemedicine), telehealth, mHealth, medical IoT, IoMT (Internet of Medical Things), healthcare IoT, ecc*" < it.quora.com> 9 agosto 2019

[40] Definizione rilasciata da Michela Stentella Content Manager di Forum PA nell'intervista a Claudio Carlo Franzoni, Senior Advisor P4I-Digital360, considerato uno degli esperti internazionali per quanto riguarda i Servizi ICT per gli Ospedali di nuova concezione. < www.forumpa.it/> visto il 30 marzo 2021

pagamento del servizio ; la fase tre che comprende la diagnosi e cura all'interno del settore ospedaliero usufruendo dei servizi proposti; da ultima la quarta fase di *follow up* caratterizzata dal monitoraggio della continuità ed effettività della cura[41], infatti è stato dimostrato che circa il 34% dei cittadini ha ritirato un referto online, un servizio che dovrebbe essere offerto dal Fascicolo Sanitario Elettronico, di cui parleremo dell'ultimo capitolo, ma di cui solo il 21% ne ha sentito parlare e solo il 7% ne ha effettivamente usufruito.

Quindi la Digital Health è il prodotto di tutta la rivoluzione tecnologica avvenuta prima degli anni 2000 con l'affermazione di Internet, correlata anche alla diffusione dei dispositivi elettronici di ultima generazione, denominati come *Internet of Things* come, ad esempio, i sensori indossabili come quelli che misurano il battito cardiaco.

Le caratteristiche proprie della sanità 2.0 sono varie: in primo luogo si deve fare riferimento al suo potere di connettività con la rete vocale, le reti aziendali e con l'Internet in generale; la garanzia di accessibilità per tutte le fasce della popolazione come nel caso di app per smartphone, che costituisce un nodo fondamentale per il diritto di accesso alle cure mediche che deve essere garantito a chiunque senza alcuna discriminazione; l'uso di nuove tecnologie di comunicazione come la messagistica testuale, voce e video per comunicare con gli operatori sanitari e per inviare in modo più semplice e istantaneo referti e analisi; l'indossabilità, come riferito sopra, di dispositivi che si possono portare a contatto con il proprio corpo per un determinato periodo di tempo, permettendo quindi di monitorare in modo continuativo ad esempio la frequenza cardiaca; lo scambio di dati che rappresenta la facilità di trasmissione ad esempio di prescrizioni mediche elettroniche non solo tra medico e paziente ma anche tra enti diversi; ma la trasmissione di dati è uno strumento tanto potente quanto possibilmente lesivo del diritto alla privacy, che come vedremo nel prossimo paragrafo, è stato oggetto di interventi da parte dei legislatori e che per essere rispettato necessita anche di norme stringenti come quelle dettate dal GDPR in Europa e di standard specifici per l'eHealth, come l'Health Insuranche Portability and Accountability Act[42] negli Stati Uniti d'America; la sicurezza informatica o cyber security che deve essere

[41] Informazioni prese dal Webinar del 20/05/2020 a cura di Paolo Locatelli ed Emanuele Lettieri rinvenibile su "Innovazione digitale nella sanità: dalla gestione dell'emergenza a una reale connected care" Politecnico di Milano Graduate School of Business.

[42] "*L'HIPAA (Health Insurance Portability and Accountability Act) ha reso la protezione delle informazioni sanitarie una responsabilità legale negli Stati Uniti dal 1996, infatti nell'ambito di questa legislazione sono state stabilite Norme sulla sicurezza e sulla privacy che specificano le misure di tutela che devono essere adottate con il fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette (Protected Health Information (PHI)) presenti online*". Le principali disposizioni dell'Health Insurance Portability and Accountability Act, sono composte da tre regole principali: le Norme relative a Privacy, Sicurezza, e Notifica delle Violazioni, che sono tutte pianificate per proteggere la privacy e la sicurezza delle informazioni sanitarie protette. "*La Norma relativa alla Privacy definisce gli standard per la protezione delle informazioni sanitarie e offre ai pazienti diritti importanti per quanto riguarda le loro informazioni di salute. La Norma relativa alla Sicurezza stabilisce garanzie che le entità coperte e gli associati devono implementare per proteggere la riservatezza,*

offerta agli utenti in base alle linee guida (anche denominate "best practices"); da ultimo bisogna menzionare l'uso di tecnologie di ultima generazione come sofisticati software e altre tecnologie di intelligenza artificiale o i cosiddetti micro-electromechanical systems (MEMS)[43] o tecnologie robotiche.

Per quanto riguarda le tecnologie adoperate, esistono diversi modelli per classificare l'eHealth[44], e sono: innanzitutto la telemedicina, riferendoci più nello specifico negli strumenti di tele-diagnostica, tele-chirurgia e teleassistenza; l'Informazione sanitaria online come ad esempio può avvenire tramite web o sui social media o su chat dirette con i medici; la dematerializzazione delle cartelle cliniche, rendendole online è più facile la loro trasmissione, basti pensare *all'electronic health record* o *l'e-prescription*; l'importanza del telesoccorso in caso di situazioni di emergenza che richiedono un intervento il più tempestivo possibile; ma anche le tecnologie digitale improntate sul benessere personale e la prevenzione, si parla infatti di *digital wellbeing*[45], o i dispositivi di *m-health* menzionati prima; il cosiddetto *e-Patient*, ovvero al partecipazione informata del paziente che indica la gestione in capo a questo delle proprie condizioni di salute, tramite l'informazione offerta da internet; inoltre negli ultimi anni si è assistiti a un forte miglioramento nell'ambito della robotica medica e protesica, e quindi ottimizzando la diagnostica avanzata fondata su algoritmi di intelligenza artificiale. Da ultimo bisogna considerare inoltre anche le medicine digitali come, ad esempio, quelle assunte tramite micro-sensori incorporati e quindi le terapie digitali[46] in generale, non escludendo assolutamente che

l'integrità e la sicurezza delle informazioni sanitarie elettroniche. La Norma relativa alla Notifica delle Violazioni richiede che le entità coperte informino gli individui affetti, il governo federale, e, in alcuni casi, i media di una violazione di informazioni sanitarie non garantita. Il Department of Health and Human Services, Office for Civil Rights degli Stati Uniti, fa rispettare queste tre regole e fornisce indicazioni sulla conformità delle norme." Charles Sabatino , JD, American Bar Association "Riservatezza e Health Insurance Portability and Accountability Act (HIPAA)" www.msdmanuals.com Agosto 2018

[43] I Sistemi Micro-Elettro-Meccanici, o MEMS, sono una tecnologia che può essere definita come "*elementi meccanici ed elettromeccanici miniaturizzati (cioè dispositivi e strutture) che vengono realizzati utilizzando le tecniche della microfabbricazione*". Le loro dimensioni fisiche critiche dei dispositivi MEMS possono variare da "*meno di un micron all'estremità inferiore dello spettro dimensionale, fino a diversi millimetri.*" Negli ultimi decenni i ricercatori e gli sviluppatori MEMS hanno presentati diversi microsensori per quasi tutte le possibili modalità di rilevamento, come temperatura, la pressione, le forze inerziali, i campi magnetici, e le radiazioni. Articolo "Cos'è la tecnologia MEMS?" su < www.mems-exchange.org> visto in giugno 2021

[44] "*Esistono diversi modi per classificare l'eHealth che forniscono una visione complessiva dell'eHealth, ad esempio in base ad una certa categoria di dispositivi, in base al mezzo che la tecnologia utilizza (web-based, app mobili, ecc.), in base al contesto di cura (eCare, eTherapy, eAppointment, ePrevention, ecc.) o in base agli attori (ossia in base all'interazione tra gli attori di tale sistema).*" Come affermato con l'articolo "The Grid, Classification of eHealth Applications Towards a Better (re)Design and Evaluation" da Saskia Marjan Akkersdijk. 2016

[45]Definita dal'UNESCO come "The enhancement and improvement of human well-being, in the intermediate and long term, through the use of digital media" <www.digitalwellbeing.org>Dr Paul Marsden, Chartered psychologist specialising in consumer behaviour, wellbeing and technology. University lecturer at UAL and consultant consumer psychologist with Brand Genetics.

[46] "*Le terapie digitali (DTx) sono un elemento innovativo della digital health, si tratta di software, come le App per Smartphone, validati clinicamente che possono integrare o sostituire le terapie tradizionali (software come principio attivo)*". Come affermato da Roberto Ascione CEO di Healthware Group "*Le Digital Therapeutics rappresentano una grande opportunità per le imprese che si occupano di innovazione in campo sanitario. Si contano circa 170 startup e si stima che il mercato delle DTx crescerà del 20,5% annuo fino al 2025. Le specificità*

presto, nuove tecnologie si aggiungeranno all'elenco, essendo un settore di fortissimo interesse per i sistemi sanitari nazionali, come la Enterprise Imaging, ambito consolidato in radiologia ma ancora in via di diffusione ma con benefici ormai riconosciuti.

Soprattutto nel corso del 2020 con la diffusione del virus Covid-19, la sanità digitale è diventata un elemento strategico. La pandemia, infatti, è stata una spinta senza precedenti alla medicina digitale: basti pensare alle visite mediche effettuate con videochiamata, alle terapie digitali, alle app e ai software per riconoscere in anticipo i sintomi delle malattie, ma non solo, anche il monitoraggio domiciliare e i siti per trovare un medico disponibile o richiedere informazioni utili su una malattia del tutto sconosciuta. Di questo si è discusso durante l'evento virtuale "*ConnAction* - Insieme per soluzioni innovative nella salute"[47], promosso da Pfizer Healthcare Hub e organizzato da Healthware Group con l'obiettivo di informare, educare e offrire soluzioni ai medici che durante l'emergenza sanitaria non hanno potuto instaurare il tradizionale rapporto diretto con i pazienti.

È stato osservato che ancor prima dell'epidemia da Covid-19 i cittadini erano in un certo senso già pronti a una supporto digitale poiché infatti circa il 41% dei cittadini sani utilizza un'*App* di *coaching* o un *wearable*, il 25% dei cittadini ha comunicato al proprio medico di base i dati raccolti da questi dispositivi e il 30% dei cittadini sarebbe interessato a interagire con un coach virtuale per migliorare il loro stile di vita, agendo in via preventiva con un forte interesse per l'Home Assistant di circa il 60%. La pandemia ha rappresentato un momento di forte discontinuità, ma è stata anche un "acceleratore di *macro-trend*" che erano già in atto come l'innovazione digitale, la trasformazione digitale, l'*engagement* del paziente e la sua volontà di essere sempre più attivo ma anche la decisione di riflettere sulla relazione tra aziende ospedaliere, territorio ed ecosistemi sanitari, quindi possiamo affermare che l'emergenza sanitaria li ha solo reso più espliciti, richiedendo delle soluzioni.

---

delle terapie digitali favoriscono, inoltre, la nascita di sinergie tra imprese farmaceutiche e startup." Articolo del 10/06/2019 di Adriano Fontanari rinvenibile su <www.digitalhealthitalia.com>

[47] All'incontro hanno partecipato medici, esperti di salute digitale, rappresentanti dei cittadini e delle istituzioni, e 4 tra le aziende più innovative nel settore (Empatica, Hassist, Pagine Mediche e Zana), presentando delle loro idee e soluzioni digitali per il sistema sanitario e la gestione a distanza dei pazienti. *"Il progetto nasce proprio dalla trasformazione digitale della Salute e la necessità di dare vita a un ecosistema sanitario connesso. Pfizer ha deciso di evolversi in una prospettiva beyond the pill, creando Healthcare Hub, e posizionandosi così come connettore tra l'innovazione e la classe medica.*
ConnAction, dunque, ha l'obiettivo di informare, educare e offrire soluzioni concrete ai medici che stanno fronteggiando la necessità di relazionarsi con i propri pazienti in maniera virtuale.E lo fa attraverso una serie di eventi virtuali, organizzati con Healthware Group, durante i quali si affrontano tematiche legate alla Digital Health, grazie anche alla presenza di startup e innovatori del mondo healthtech." Intervista a Laura Guerra Head of Innovation & Multichannel Marketing in Pfizer, articolo di Redazione Digital Health Italia rinvenibile su www.digitalhealthitalia.com 12 maggio 2021

La classe medica ha compreso che pazienti e i loro *caregivers*[48] preferiscano di più una "*at home care*", essendo più sicura, celere e presentando vantaggi ragguardevoli, perciò la pandemia ha accelerato la trasformazione della sanità.

Complici la pandemia e lo sviluppo notevole delle tecnologie, si prevede inoltre che, entro il 2023, grazie alla forte domanda di servizi sanitari da remoto come la telemedicina, il telemonitoraggio o i *clinical trial* virtuali, gli investimenti in questo tipo di tecnologie aumenteranno del 70%[49]. I servizi medico digitali garantiscono la loro continuità in sicurezza e arricchiscono l'esperienza per i pazienti, e tenendo conto di quanti investimenti ultimamente si riferiscano a questo ambito, i modelli di lavoro del personale medico diventeranno presto più integrativi, collaborativi e soprattutto più efficienti, conducendo una ricerca continua condotta anche dal personale medico.

Abbiamo assistito negli ultimi mesi a quanto la pratica clinica sia diventata sempre più virtuale: l'Osservatorio Innovazione Digitale in Sanità della School of Management del Politecnico di Milano ha riportato dei dati significati, infatti si stima che più del 50% dei medici di medicina generale ha svolto la propria attività da remoto, migliorando i tempi di risposta ai pazienti del 63% e la condivisione delle informazioni del 63%, mutando così anche il rapporto medico-assistito, creando una comunicazione molto più rapida e diretta e quindi garantendo, in un modo mai visto prima, il diritto alla salute. Infatti, scopo di questo elaborato è anche dimostrare come la Digital Health abbia sì comportato un rischio a una minor tutela dei dati personali, ma è anche quello di affermare come la nuova veste della sanità rappresenti una modalità di accesso alle cure estremamente innovativo e funzionale.

Durante l'emergenza Covid, inoltre, le soluzioni che sono state predisposte dai medici per i pazienti sono state ad esempio quelle di Paginemediche[50], ovvero una piattaforma di

[48] Il caregiver familiare è quella persona che a titolo gratuito e fuori dall'ambito professionale si occupa dell'assistenza di un figlio, genitore o altro familiare disabile o che comunque non sia autosufficiente.

[49] Sostenuto da International Data Corporation (IDC) che è "*la prima società mondiale specializzata in ricerche di mercato, servizi di consulenza e organizzazione di eventi nei settori ICT (tecnologie dell'informazione e della comunicazione) e dell'innovazione digitale. Vanta oltre 1.000 analisti in 50 Paesi del mondo che mettono a disposizione a livello globale, regionale e locale la loro esperienza e capacità per assistere il mercato della domanda e dell'offerta nella definizione delle proprie strategie tecnologiche e di business a supporto della competitività e della crescita aziendale*". Silvia Piai, Mirko Spinelli, Orientina di Giovanni, Maurizio Percopo. In rete: https://blogs.idc.com/ visto il 23 maggio 2021

[50] Il CEO di Paginemediche Graziella Bilotta parla della medicina digitale e del suo ruolo in questo periodo. "*Siamo entrati nell'era della medicina digitale e tornare indietro non è più possibile, anzi: ogni giorno compiamo un passo in avanti lungo questa strada. La rivoluzione digitale nella sanità italiana è ancora all'inizio, ma presto le attività cliniche erogate in televisita e teleconsulto entreranno a pieno titolo nei livelli essenziali di assistenza a livello nazionale. La digitalizzazione in ambito sanitario è un'opportunità che tutti insieme dobbiamo cogliere, perché può aiutarci a stare meglio, a curarci in maniera più efficace, a prevenire molte malattie, specie quelle legate alle cattive abitudini, e a vivere più a lungo e in maniera qualitativamente migliore*". www.paginemediche.it visto il 23 maggio 2021

telemedicina e servizi di digital health che ha saputo fronteggiare la crisi del sistema sanitario creatasi, ancor prima che la World Health Organization dichiarasse lo stato di pandemia. Paginemediche ha infatti messo a disposizione di tutto il personale sanitario e dei cittadini uno strumento specifico di identificazione precoce dei possibili contagiati, permettendo un supporto al triage, tramite un chatbot, sui sintomi rispondendo con un'*app* dedicata al telemonitoraggio domiciliare dei pazienti contagiati sintomatici o paucisintomatici: tutto questo ha permesso quindi delle video visite di controllo e quindi un'assistenza da remoto e, se ci pensiamo, si è evitato il congestionamento dei pronto soccorso. La piattaforma offre alle persone la possibilità di essere seguite e supportate nella prevenzione, diagnosi, cura e trattamento, a distanza e raccogliendo dati condividendoli in modo diretto e privato con il medico personale del paziente.

L'importante ruolo della telemedicina è stato riconosciuto anche nel nostro Paese: infatti tra il 2011 e il 2014 vi è stato un lungo iter procedurale a seguito del quale, la Conferenza Stato-Regioni e Provincie Autonome di Trento e Bolzano ha emanato le "Linee Guida Nazionali sulla Telemedicina[51]", definendo in modo chiaro le loro priorità e le modalità di servizio, integrandole con le modalità di Televisita, Teleconsulto e Telecooperazione. Il problema delle Linee Guida Nazionali però è la loro poco chiarezza su come determinati requisiti debbano essere garantiti non vengono però forniti: ad esempio, mancano indicazioni precise per quanto riguarda la gestione dei dati e quindi la loro raccolta, il loro trasferimento e la loro archiviazione, mancando inoltre anche specifici standard di qualità per quanto riguarda l'infrastruttura informatica, mancanze che non possono essere tollerate poiché comportano una disomogeneità delle prestazioni offerte da ogni Regione e da ogni struttura sanitaria. Vi è il bisogno di ulteriori regole per definire in modo chiaro e preciso gli standard di qualità da seguire per questi strumenti di comunicazione, rendendoli omogenei in tutto il territorio nazionale. Nell'ultimo capitolo di questo elaborato si parlerà del ruolo dell'Agenzia per l'Italia Digitale[52] (AGID) ma ora dobbiamo menzionare il suo percorso di qualificazione per i fornitori di *Software as a Service* (SAAS) della

[51] Le nuove Linee Guida predisposte dal Ministero della Salute e approvate dalla Conferenza Stato Regioni nel dicembre 2020 sono un punto di svolta per l'ingresso della telemedicina all'interno del Servizio Sanitario Nazionale (SSN). "*Le Linee Guida sottolineano come, per garantire l'effettivo svolgimento di una prestazione a distanza, siano necessari strumenti tecnologici che consentano al medico e al paziente di comunicare in modo sicuro ed efficace. È pertanto richiesta, ad esempio, una rete di collegamento funzionante tra medici e pazienti, un portale web a cui accedono i medici con il proprio account per la gestione dei pazienti e strumenti digitali quali computer, tablet o smartphone. Inoltre, le Linee Guida sottolineano come sia essenziale che tutti i trasferimenti di dati (sotto forma di video, immagini, files etc.) siano crittografati e in linea con le normative in materia di privacy e sicurezza. Tale requisito è posto tra le condizioni di autorizzazione, accreditamento e contrattualizzazione per l'erogazione delle prestazioni di telemedicina a carico del SSN.*" Elisa Stefanini Counsel di Portolano Cavallo, articolo rinvenibile su: https://www.agendadigitale.eu/sanita/nuove-linee-guida-nazionali-sulla-telemedicina-i-nodi-critici-per-la-piena-attuazione/ Legal Health "Nuove Linee Guida nazionali sulla telemedicina: i nodi critici per la piena attuazione" 1 febbraio 2021

[52] L'Agenzia per l'Italia Digitale (Agid) è l'agenzia tecnica della Presidenza del Consiglio con il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana. <www.agendadigitale.eu>

pubblica amministrazione, per fare in modo che le pubbliche amministrazioni possano servirsi di servizi *cloud* ottimali prescritti seguendo criteri minimi di qualità e sicurezza.

Strumenti come la Videovisita rappresentano una delle principali innovazioni che, in modo abbastanza semplice, permettono ai pazienti cronici e con particolari disabilità, di poter accedere a un tipo di cura continuativo e senza alcuna interruzione, garantendo visite di controllo e non comportando lo spostamento fisico dei pazienti. Il medico di famiglia utilizzando dati e piattaforme di telemedicina ha modo di gestire i pazienti in modo molto più semplice, personalizzando le terapie e orientandoli tempestivamente su eventuali esami da sostenere e cure specialistiche che avverranno successivamente sempre da remoto.

Attorno all'individuo-paziente ruotano l'ospedale e il territorio, che devono coordinarsi: ma ora il digitale permette al paziente di scegliere e connettersi in modo diretto ai servizi da remoto, e mostrare ed eventualmente condividere i propri dati in rete, e tutto ciò inciderà sulla geografia sanitaria.

Se mentre prima il medico e l'Ospedale erano al primo posto per quanto riguarda l'accesso alle informazioni, adesso il paziente può accedere a competenze e servizi da remoto grazie a una tecnologia molto più orientata alla condivisione e alla interoperabilità, passando da una "cura" del problema al "prendersi cura" del paziente[53], tramite un sistema completamente innovativo.

Quello a cui stiamo assistendo, quindi, è un'assistenza alla persona completamente diversa che ha caratterizzato anche il Sistema Sanitario Nazionale, potenziando il rapporto medico-paziente e quindi migliorando le pratiche assistenziali da remoto e garantendo un notevole risparmio di risorse: si devono prendere in considerazione il fascicolo sanitario elettronico, di cui parleremo in modo approfondito nell'ultimo capitolo dell'elaborato, ma del quale dobbiamo anticipare la sua primaria funzione, ovvero quella di raccogliere dati sull'anamnesi remota di ogni persona. Anche le app medicali, i big data e l'intelligenza artificiale, sono affiancati all'assistenza tradizionale per migliorare i servizi essenziali e per dematerializzare il sistema informativo della sanità, realizzando così una cartella clinica unica, virtuale e interattiva condivisa internamente tra paziente, specialista e medico di famiglia. L'obiettivo attuale è quello di portare il sistema della Digital Health oltre l'emergenza da Covid-19 e quindi considerando anche esigenze di salute in generale in modo molto più esteso.

[53] Ciò viene affermato da Roberto Ascione, imprenditore e opinion leader internazionale in ambito Digital Health in un articolo rilasciato per Regione Lombardia intitolato "L'accelerazione della sanità digitale: il futuro è già qui". "*Si passerà, quindi, dalla logica della "cura" del problema al "prendersi cura" del cittadino-paziente, attraverso un Sistema finalmente proattivo e predittivo*." In rete: https://www.openinnovation.regione.lombardia.it/it/b/633/l-accelerazione-della-sanit-digitale-il-futuro-gi-qui 8 aprile 2021

Si ricerca una sanità che deve essere di valore, ovvero una sanità focalizzata sul valore che garantisca un accesso diretto ed equo poiché molti cittadini, spesso, sono tagliati fuori dai servizi digitali per mancanza sia di capacità che di mezzi. Questo sistema deve essere inoltre di qualità, ovvero essere efficace e sicuro da un lato, ma dall'altro deve garantire l'efficienza e la produttività, tenendo conto anche delle sue notevoli risorse. Gli esperti internazionali, infatti, ribadiscono quattro pilastri fondamentali, noti anche come "Le quattro P della medicina del futuro"[54] ovvero un equilibrio tra innovazioni organizzative e innovazioni tecnologiche e digitali con una sanità che deve essere partecipata e personalizzata. Il machine learning d'intelligenza artificiale evidenza tutti i possibili scenari evolutivi e ci permette di avere una sanità basata sulle evidenze e sul valore. Tutto questo non può avvenire in mancanza di una sanità digitalmente connessa e in mancanza di specifiche competenze non solo da parte degli operatori sanitari ma anche da parte dei cittadini, come la leadership, la capacità di project manager e la capacità di saper innovare in un contesto digitale.

Avendo valutato la forte trasformazione digitale della sanità, si è discusso se questa possa in qualche modo incidere sulla professione del medico: alcuni autori sostengono che la figura del medico è destinata a scomparire perché ciò che un operatore sanitario fa, sarà sostituito dall'attività dei software o dai processi che saranno attivati dai pazienti. Altri autori[55] sostengono quindi che si arriverà ovviamente a una netta trasformazione della professione, senza prevedere la scomparsa del medico: la sua attività prevede una raccolta di informazioni in modo retrospettivo, tiene conto dell'anamnesi propria del paziente, sulla quale esso effettua delle interpretazioni e pone delle ipotesi di percorsi diagnostici da seguire, prescrivendo esami da compiere e cure da seguire. Questo tipo di attività, che possiamo definire come tradizionale, ovviamente subirà un forte mutamento: la salute digitale si baserà, anziché su dati o sensazioni passate come avviene nella medicina presente, su un tipo di metodo anticipatorio e predittivo. Il medico, quindi chiederà il consenso al paziente per accedere ai dati personali di quest'ultimo, dati raccolti da *devices* e da *app* che saranno condivisibili su più piattaforme. In questo modo, servendosi dell'aiuto di *software* e algoritmi, il medico effettuerà un tipo di diagnosi molto più

[54]Nel *paper* pubblicato nel 2012 sul Journal of Internal Medicine, i ricercatori hanno introdotto "La medicina delle 4P (P4 Medicine)" ovvero la medicina Preventiva, Partecipativa, Personalizzata e Predittiva e la sua prima formulazione si deve all'Institute for System Biology di Seattle, diretto da Leroy Hood. E' un tipo di medicina sistemica che, come descritto anche da Hood, scienziato esperto di biotecnologia "*permette di fornire approfondimenti sui meccanismi delle malattie, stratificare malattie complesse in sottotipi distinti con maggiore efficacia dei farmaci, fornire nuovi approcci alla targetizzazione degli stessi farmaci, generare metriche per la valutazione del benessere."* Articolo rinvenibile su "*Medicina delle 4P: un modello di medicina per il futuro. La Medicina Preventiva, Partecipativa, Personalizzata e Predittiva è legata a doppio filo allo sviluppo del data mining e dell'IoT Health: perché? Di che si tratta? Applicazioni e scenari*" a cura di Josephine Condemi www.internet4things.it Sez: smart health. 15 febbraio 2021

[55] Roberto Ascione esprime la sua teoria nel libro "*Il futuro della salute: come la tecnologia digitale sta rivoluzionando la medicina*" pp. 187

specifica in base ai dati raccolti propri del paziente in questione, prescrivendo un tipo di terapia che non andrà a curare una malattia già esistente, ma una terapia anticipatoria e basata sulla prevenzione, con lo scopo di evitare l'insorgenza o la prosecuzione della patologia. Il fatto che i dati del paziente siano rinvenibile su più piattaforme contemporaneamente, sempre previo suo consenso, renderà possibile un lavoro simultaneo e multidisciplinare di più medici contemporaneamente creando un *care team*. Tutto questo comporterà delle conseguenze: bisogna considerare la quantità di tempo risparmiata da ogni singolo medico nella raccolta dei dati dei pazienti e nella formulazione di ipotesi, tenendo conto anche del fatto che il rapporto tra paziente e personale infermieristico muterà, poiché quest'ultimo svolgerà un ruolo molto più ampio, creandosi così un rapporto, paradossalmente, più umano essendo il paziente libero da tutti gli oneri burocratici e amministrativi cui deve adempiere.

Come abbiamo anticipato prima, essenziale per una vincente digitalizzazione della sanità, è necessaria la formazione del personale medico: ad oggi non esistono ancora né percorsi universitari né post universitari specifici e idonei a fornire le competenze necessarie per la professione del medico digitalizzato. L'interpretazione dell'esame per immagini richiede una grande esperienza del medico, ovvero aver visionato un elevato numero di immagini e allo stesso tempo saper riconoscere subito la patologia presente, ma un software di *image recognition*[56] è studiato per poter memorizzare milioni di immagini e informazioni annesse, un compito che la mente umana non riuscirebbe a svolgere. Si stima quindi che in futuro ci saranno meno specializzazioni di questo tipo e più specializzazioni per conseguire le conoscenze necessarie per guidare i pazienti nel corso dei vari processi digitali.

Recentemente è stata avviata una startup che prevede un sistema di messagistica istantaneo direttamente con i medici, in questo modo il sistema comunicherà in modo sicuro e veloce quel dato specifico della persona soltanto a determinati medici specializzati in quella patologia.

In questo modo l'*empowerment* della professione medica sarà un ovvio risultato, dando vita alla Smart Health[57], un'interazione medico-paziente immediata e costante. L'Osservatorio

[56]Questo tipo di tecnologia innovativa consente a sistemi di intelligenza artificiale di simulare il comportamento del cervello umano per quanto riguarda la vista, grazie alle cosiddette reti neurali convolutive "*artificial neural network* (ANN)" ovvero "*un modello computazionale parallelo, costituito da numerose unità elaborative omogenee fortemente interconnesse da collegamenti di varia intensità. Vi sono delle unità di input che recepiscono i dati del problema da risolvere e poi il processo di elaborazione che si propaga in parallelo nella rete fino alle unità di output, che forniscono il risultato"*. Quindi grazie alle reti neurali convolutive si riesce a imitare tutta la componente umana propria dell'apprendimento per ottenere un risultato,il riconoscimento di immagini. Articolo "*Image Recognition: cos'è, come funziona e quali sono i vantaggi per le aziendeLa consapevolezza del valore dei dati sta portando a una trasformazione dei processi aziendali. L'impiego dell'AI trova così sempre più spazio nei progetti di business, con l'Image Recognition e l'Image Detection tra le declinazioni a maggior tasso di crescita*" di Loris Frezzato rinvenibile su < www.internet4things.it> 30 settembre 2020

[57] È una nuova modalità di comunicazione medico-paziente, sempre più utilizzata nell'ambito sanitario per condividere documenti come ad esempio i referti, trasmettere informazioni di tipo organizzativo come l'orario e il

Innovazione Digitale in Sanità[58] della *School of Management* del Politecnico di Milano ha dimostra che i modi più utilizzati dai pazienti per comunicare con i medici, sono le e-mail al primo posto, seguite dalla piattaforma WhatsApp utilizzata dal 52% dei Medici Specialisti e dal 63% dai Medici Generali, solo il 4% di questi dichiara di non farne uso, e da ultimo gli sms. In questo modo vengono condivisi documenti come ad esempio i referti, vengono trasmessi informazioni per quanto riguarda gli orari e i luoghi degli appuntamenti presi e informazioni più specifiche riguardo il quadro clinico del paziente. L'ultimo report Global Digital del 2019[59], la piattaforma WhatsApp riconferma il suo primo post tra le app più utilizzate, quindi possiamo affermare che il suo utilizzo anche in ambito sanitario, sia avvenuto in modo progressivo e naturale.

Ma le opportunità legate alla facilità d'utilizzo e al fatto che la piattaforma è ormai presente sui *devices* di tutti, implicano dei rischi nel settore sanitario: l'utilizzo di questi strumenti potrebbe costituire nel tempo un pericolo alla protezione dei dati del paziente, essendo queste modalità non completamente regolamentate, essendo assolutamente estranee alle policies aziendali e alle regole di deontologia della professione medica, implicando anche problematiche relative alla privacy e alla sicurezza dei dati del paziente, di cui tratteremo nel prossimo paragrafo. È necessario quindi che le strutture ospedaliere adottino soluzioni uguali a tutti gli ambiti sanitari, in modo che i costi e gli sprechi della sanità pubblica siano minimizzati.

Il continuo sviluppo della tecnologia e il suo uso in molteplici ambiti del nostro quotidiano non si fermerà, le aziende farmaceutiche tradizionali saranno adiuvate dalle aziende digitali produttrici di software e dalle startup del settore, dando vita a un'evoluzione dei nostri comportamenti. Già da ora dati di milioni di persone sono raccolti in tutto il mondo creando un'immagine dello stato di salute in tempo reale quindi sempre aggiornato.

---

luogo degli appuntamenti o di tipo clinico come i sintomi, tra pazienti e altri operatori sanitari. "*Anche i pazienti approfittano di questa piattaforma per scambiare facilmente con il proprio medico informazioni, dubbi, domande o foto di documenti, al principale scopo di evitare visite superflue*". "La comunicazione medico-paziente ai tempi di WhatsApp" autore sconosciuto www.sinesy.it 13 marzo 2019

[58] "*Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano nascono nel 1999 e svolgono la funzione di diffondere le ultime ricerche negli ambiti della Innovazione Digitale, fornendo dati specifici per quanto riguarda l'impatto delle tecnologie sulle imprese, pubbliche amministrazioni e cittadini*". "*La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese*." <www.osservatori.net> visto il 10 giugno 2021

[59] Indagine condotta da We are Sociale e Hootsuite, piattaforma leader nel settore del social media manager. Con il report Digital 2019 hanno voluto dimostrare lo scenario digitale dell'anno 2019, quindi valutando come l'utilizzo di internet e delle piattaforme social sono entrati sempre di più nel nostro quotidiano, andando a ricoprire ruoli fondamentali per quanto riguarda il nostro benessere. Articolo " *Digital 2019: tre italiani su cinque attivi sui sociale per quasi due ore al giorno*" di Matteo Starri www.wearesocial.com 31 gennaio 2019

Ma il fatto che i medici non sono ancora pienamente formati a questa rivoluzione digitale, rappresenta un problema diretto sia per i medici stessi perché non essendo pienamente competenti potrebbero perdere l'autorevolezza della loro figura, sia per i pazienti stessi che si potrebbero ritrovare senza un supporto idoneo ed essenziale. Ma la posizione precaria del medico rappresenta la più debole delle due poiché esso non saprà adeguarsi in modo automatico al nuovo assetto, coinvolgendo anche le istituzioni come le università, i servizi sanitari nazionali e le aziende ospedaliere. In quest'ottica aziende e università dovranno collaborare per cercare di minimizzare questi *gap*, sempre sotto il controllo dell'autorità statale, una sfida alquanto ardua considerando che si dovrà intervenire non solo sulle conoscenze di chi sarà medico domani, ma dovranno essere perfezionate le capacità digitali di chi è medico oggi.

Ciò che caratterizza maggiormente questa rivoluzione digitale sanitaria è la quantità di dati di ogni singola persona che dovranno essere trattati per essere disponibili per evitare controversie legali ed etiche. Come prima cosa bisogna affermare che colui che inizierà a raccogliere i dati sarà il paziente stesso, e solo dopo la sua volontà esplicita di condividerli li trasmetterà al suo medico di base e a eventuali medici specialisti. In questo modo, come stavamo accennando prima, vi sarà un *care team* attorno a ogni paziente che avrà accesso ai suoi dati in tempo reale così da prescrivere passo dopo passo la terapia più adeguata alle esigenze dell'assistito, basti pensare ad esempio all'assunzione di farmaci prescritti da due medici diversi per due diverse patologie che possono non essere compatibili tra loro. Rimarranno immutati il rapporto di fiducia necessario tra paziente e medico e la necessità di privacy dei dati personali: infatti, vi saranno delle problematiche etiche, totalmente estranee al nostro mondo presente, ad esempio la gestione delle urgenze, ma non solo, anche controversie legali su situazioni sempre nuove, come ad esempio i dati ambientali interpolati ai dati genetici, che permetteranno di prevedere l'insorgenza e il decorso delle malattie, e che quindi dovranno essere gestite, costituendo delicate tematiche legali e di amministrazione politica.

Nell'ultimo capitolo di questo elaborato, osserveremo l'esperienza americana, dovendo qui anticipare come il modello statunitense di digitalizzazione e di fruizione dei dati sanitari, risulti oggi al primo posto, avendo dato via a un dibattito interessante: infatti, ci si chiede se effettivamente sia giusto che il paziente possa accedere in modo semplice ai suoi dati, anche a quelli che di solito vengono custoditi dai *care provider*[60], e se la cartella clinica sia effettivamente

[60] Secondo le normative federali, un "operatore sanitario" è definito come "*un medico in medicina o osteopatia, podologo, dentista, chiropratico, psicologo clinico, optometrista, infermiere, infermiere-ostetrica o un assistente sociale clinico autorizzato ad esercitare dallo Stato e che svolgono nell'ambito della loro pratica come definito dalla legge dello Stato, o un professionista della Scienza Cristiana. Un fornitore di assistenza sanitaria è anche qualsiasi fornitore dal quale l'Università o il piano sanitario di gruppo del dipendente accetterà la certificazione*

accessibile a tutti coloro che ne richiedono l'accesso al paziente o se alcuni dati siano più privati di altri, e quindi non consultabili anche nel caso di un esplicito consenso del titolare. Sono tutti interrogativi che in futuro dovranno essere risolti, materie che dovranno essere regolamentate e tutelate, garantendo l'accesso ai dati che risultano più importanti. Bisognerà anche verificare l'impatto psicologico di un accesso facilitato ai dati sanitari sulla popolazione: un'informazione più diretta ma non offerta da un medico in sede di visita, potrebbe generare preoccupazioni in chi le riceve ad esempio con una notifica sul proprio smartphone. Ma sarà anche possibile al contempo, prenotare una visita specialistica per il giorno stesso in modo semplice, essendo ottimizzati i tempi e i servizi, o magari effettuare subito un test, approvato scientificamente, e ottenere in tempo reale il risultato, e quindi già discutere con il proprio medico la terapia da seguire, quindi i benefici saranno proporzionati a quelle che saranno le situazioni spiacevoli che si potrebbero creare.

Oltre a questi aspetti bisogna considerare anche il valore importante dell'economia sanitaria che da sempre ha rappresentato una concentrazione di interessi economici, un mercato che ad oggi vale trilioni di dollari. Il fatto che negli anni la capacità di cura è migliorata, basti pensare agli antibiotici e ai vaccini, è stato l'effetto di un aumento della popolazione mondiale, secondo i dati dei demografi si è arrivati a 7,2 miliardi di persone nel 2015, e per il 2030 è previsto un aumento di 1,2 miliardi arrivando quindi a 8,4 miliardi di persone presenti sulla Terra. La salute, cosa che interessa tutti indistintamente, ovviamente avrà un fortissimo impatto sia sull'economia ma anche sulla politica e sull'industria. Un farmaco o un vaccino innovativo avrà mercato non solo nello Stato in cui è stato prodotto ma nell'intero mercato mondiale, poiché una stessa patologia è uguale in tutto il mondo, e stessa cosa vale anche per i servizi offerti da un'azienda sanitaria. Quindi si può comprendere come una forte digitalizzazione della sanità, possa comportare un domani un guadagno non indifferente. Infatti, se prima il valore economico in ambito sanitario, cresceva in modo incrementale, essendo assolutamente analogo ad altri settori, con la rivoluzione digitale, si avrà una crescita economica esponenziale dettata dal mutamento delle tecnologie digitali che stravolgerà la vita di tutti noi. Il 2017 ha costituito un anno da record per la Digital Health, poiché si è assistito a un incremento dei finanziamenti del 35% in più rispetto al 2016 con 794 contratti firmati, ma solo nel 2018 si è avuta l'affermazione completa di questo settore, considerato dagli investitori uno dei mercati principali, arrivando nel 2024 a un valore di ben 400 miliardi di dollari[61]. Possiamo prendere come esempio il caso del Giappone, l'Asia è il

medica per corroborare una richiesta di benefici." Sito ufficiale Berkeley University of California www.hr.berkeley.edu visto il 10 giugno 2021

[61] Dati rinvenibili sull'articolo "Record di investimenti per la Digital Health" di Francesco Marino su <www.digitalic.it>: "*In questo scenario generale spicca la performance del settore digital health che si avvia verso la cifra record di 24,14 miliardi di dollari investiti nel corso di tutto il 2020 (in netto aumento rispetto ai 19,3*

secondo Paese al mondo dopo il Nord America, che avendo adottato tecnologie sanitarie innovative, vedrà i costi dell'assistenza sanitaria crescere del 29% entro il 2024, superando i 20 miliardi di dollari, in reazione anche all'ondata di pandemia.

Il 26% degli investimenti a livello globale, sono stati destinati a dieci aziende giganti, qui faremo un particolare riferimento alle prime tre ovvero Grail e Guardant Health che si occupano di ricerca della *healthcare*, e Peloton che invece si occupa di *wellness*. L'America e la Cina sono i due Paesi che muovono più flussi di investimenti poiché il primo vanta un'esperienza senza precedenti nelle innovazioni digitali, basti pensare alle aziende *tech* presenti della Silicon Valley in California, e il secondo dimostra una forte capacità per quanto riguarda il riconoscimento dei *trend* finanziari, ad esempio Tencent[62] conta 500 miliardi di dollari di capitalizzazione che tramite investimenti e acquisizioni sta operando nel settore della *healthcare*.

Nel nostro Paese invece, il settore sanitario vale 190 miliardi di euro, e secondo uno studio dell'Osservatorio Innovazione Digitale in Sanità della School of Management del Politecnico di Milano, nel 2016 sono stati spesi 1,27 miliardi di euro per digitalizzare la sanità, di cui 870 milioni di euro sono stati spesi nelle strutture sanitarie, 300 milioni sono stati impiegati dalle regioni, 72 milioni dai medici generali e 16 milioni dal Ministero della Salute[63]. Ma il dato più significativo è che la maggior parte del denaro è stato impiegato per la digitalizzazione delle cartelle cliniche con un ammontare di 65 milioni di euro. Questo succedeva cinque anni fa, il risultato oggi è che la maggior parte delle strutture sanitarie consente al paziente di poter scaricare il proprio referto online e di poter prenotare tramite il loro portale internet una visita. Inoltre, le regioni stanno adottando e regolamentando sempre di più il Fascicolo Sanitario Elettronico, di cui parleremo nell'ultimo capitolo dell'elaborato. Quindi la necessità e la volontà di digitalizzazione, negli ultimi anni, è aumentata esponenzialmente, essendosi riconosciuti gli enormi vantaggi di questo modo di fare sanità soprattutto da parte dei medici.

---

miliardi del 2018 e ai 18,6 miliardi del 2019). Sulla scia di quanto accade nel complesso del settore, si osserva un rialzo degli investimenti a partire dal secondo trimestre, ma è il terzo trimestre a segnare i numeri più alti degli ultimi anni con 8,4 miliardi di investimenti; tra ottobre e dicembre la curva scende nuovamente attestandosi attorno ai 5,5 miliardi. Per quanto riguarda il numero delle transazioni, il trend si è mantenuto sostanzialmente stabile nel corso dell'anno: il dato più consistente, 505 transazioni, è stato registrato nel terzo trimestre, ma non si tratta di un record assoluto, visto che nel Q2 2018 erano state messe a segno ben 538 transazioni (operazioni però decisamente meno "ricche" che hanno totalizzato "solo" 4,9 miliardi di dollari di investimenti)." 21 aprile 2021

[62]Tencent Holdings Limited è una società per azioni d'investimento fondata nel 1998 e presieduta da Ma Huateng, e fornisce servizi per intrattenimento, internet e mass media. Ha sede a Shenzen, nel distretto di Nansha e offre servizi come reti sociali via web, portali web e servizi di commercio elettronico. "*Tencent is an Internet company using technology to enrich the lives of Internet users and assist the digital upgrade of enterprises.Our mission is "Value for Users, Tech for Good"*." Sito ufficiale <www.tencent.com> articolo del 7 agosto 2020 su "What is Tencent?" di Zoe Kleinman Technology reporter, BBC News su <www.bbc.com>

[63] Dati rinvenibili sul libro "Il futuro della Il futuro della salute. Come la tecnologia digitale sta rivoluzionando la medicina (e la nostra vita) di Roberto Ascione a pagina 223 del capitolo 14.

Ciò che ci aspetta quindi è una rivoluzione che nasce dal digitale, ma che sarà più che altro una rivoluzione culturale, etica, legale, mentale e soprattutto umano e nessuno di noi potrà rimanerne indifferente.

La medicina di oggi viene definita come "acuta", nel senso che è un tipo di medicina di emergenza, essendo quindi un tipo di intervento a posteriori rispetto al verificarsi dell'evento-patologia: il medico tramite l'anamnesi e la ricostruzione di quanto accaduto, formula la terapia da seguire. La medicina del futuro invece sarà un tipo di intervento predittivo, nel senso che tramite la raccolta di tutti i dati della persona, relativi alla sua anamnesi remota, al suo stato di salute attuale e alla familiarità con determinate patologie, sarà possibile prevenire il manifestarsi della patologia. Un tipo di controllo medico del nostro presente, comporta un'osservazione diretta del paziente, il professionista infatti, esamina la persona che ha di fronte, valuta le analisi, in futuro invece, oggetto di valutazione saranno i dati che il paziente collezionerà in modo assolutamente automatico, così che il medico possa visionarli in tempo reale, eliminando le pratiche burocratiche che di solito bisogna seguire e che purtroppo richiedono tempo, e quindi garantendo un rapporto molto più diretto e umano con l'assistito. Inoltre, sarà anche possibile comparare la situazione della persona in questione, con situazioni analoghe di altre persone, effettuando così una valutazione più completa. Con l'avanzamento dello studio della genomica, inoltre, sarà possibile risalire alle predisposizioni alle malattie di cui, a volte, non si può essere a conoscenza, garantendo così una prevenzione ottimale e ricevendo consigli e prescrizioni per condurre uno stile di vita più adatto alle proprie esigenze.

Si sostiene che la prognosi di una patologia sia influenzata da vari fattori come, ad esempio, il reddito della persona, la conoscenza della struttura sanitaria giusta o del medico giusto, la disponibilità di quel determinato farmaco e la possibilità di acquistarlo, troppe variabili. La medicina del futuro permetterà di raccogliere in tempo reale dati circa la salute, sintomi, farmaci che si stanno assumendo, in modo tale da garantire un'informazione istantanea in caso di complicanze e nello stesso tempo la possibilità di prenotare una visita con il medico più appropriato tramite un sistema di *capacity management*[64], ma non solo, in questo modo si avrà quasi la certezza dei rischi che si corrono o delle terapie da seguire, potendo accedere anche

[64]Il capacity management è un processo che "*fornisce una precisa base di analisi dei costi raffrontata all'utilizzo delle risorse, permettendo di individuare le aree di maggior spesa e quelle in cui si possono realizzare dei risparmi salvando la qualità del servizio erogato. […] Partendo invece dal capacity management si affronta certamente un processo complesso e anche oneroso, ma si ha una base di analisi, e quindi di attribuzione, dei costi più precisa e soprattutto si realizza un processo che serve all'It. Per capire dove si stanno spendendo i soldi e quindi come si potrebbero spendere meglio*. […]" Intervista a Pietro Ferraro, Practice Manager IT Intelligence di Sas su "Ottimizzare i costi IT con il capacity management" di Giampiero Carli Ballola in rete: https://www.zerounoweb.it/techtarget/searchdatacenter/ottimizzare-i-costi-it-con-il-capacity-management/ 7 giugno 2010

all’esperienza di tutte le altre persone. Solo allora potremo affermare che si avrà un’ottima offerta di sanità, ma si potrà invece affermare che il diritto alla salute sarà garantito a chiunque?

1.4 La Privacy e la protezione dei dati personali in materia sanitaria.

Fra i diritti che rientrano nella sfera privata della persona, vi è il diritto alla protezione dei dati personali, affermatosi soprattutto in seguito allo sviluppo delle nuove tecnologie dell'informazione e di natura informatica, protetto a livello internazionale dalla Convenzione del 28 gennaio del 1981 del Consiglio d'Europa. Questo diritto richiede che i dati della persona possano essere acquisiti, raccolti e utilizzati solo ed esclusivamente dopo il consenso della stessa, o in base alla legge, solo se questa risulti soddisfare i requisiti di chiarezza e prevedibilità e assicuri un bilanciamento degli interessi generali[65]. Il diritto ad essere lasciato solo "*right to be let alone*" costituisce l'inizio dell'esigenza del diritto alla privacy alla fine del 1800, dove due avvocati di Boston diedero vita a questo diritto in risposta all'intromissione della stampa nella vita privata della moglie di uno dei due.

Ad oggi i dati privati di ogni persona, costituiscono un elevato valore, sia morale perché ci garantiscono la libertà alla vita privata con l'esclusione di terze persone, ma anche economico, basti pensare che nel Dark Web i dati relativi alla nostra identificazione, quelli dei conti bancari o le informazioni circa gli account Paypal[66], hanno un costo che reca profitto a qualcuno.

In questo paragrafo, parleremo però del valore dei dati e del loro trattamento in ambito sanitario, secondo tema principale di questo elaborato.

La raccolta e l'archiviazione in formato digitale dei dati sanitari consentono considerevoli benefici per quanto riguarda la maggior efficienza e il risparmio di risorse, garantendo un potenziamento della ricerca e della medicina predittiva, ovvero la Digital Health, di cui abbiamo discusso nel precedente paragrafo. Abbiamo anche analizzato i vantaggi offerti dall'era digitale in contrapposizione a quanto le nuove tecnologie possano risultare invasive e possibilmente lesive dei nostri dati. La c.d. "Direttiva Madre" n. 95/46/CE, che per la prima volta tutelò la circolazione dei dati, riguardava la tutela non del dato in sé, ma delle persone fisiche, quindi si richiede un bilanciamento tra la protezione della persona fisica e la libera circolazione dei dati all'interno dell'Unione europea. Tutto ciò era finalizzato a ottenere un controllo dei dati

[65] Diritto alla vita privata e familiare, protezione dei dati personali e diritto all'oblio. Capitolo V, pagina 160 del libro "Lezioni di tutela internazionale dei diritti umani" del Professore Pietro Pustorino.

[66] Account Paypal da 42 a 418 euro, dettagli delle carte di credito da 5 a 16 euro, dati identificativi come nome, cognome, e-mail e numero di telefono da 0,40 a 8 euro. Dati specifici forniti dall'Avvocato Luisa Di Giacomo, DPO e consulente GDPR.

personali delle persone fisiche qualora fossero stati utilizzati da autorità pubbliche o imprese private, per permettere lo svolgimento di tutte le attività necessarie.

Per raggiungere obiettivi importanti in materia di privacy, sono stati necessari degli interventi normativi per cercare di uniformare la disciplina a livello comunitario: il Regolamento UE 679/2016 General Data Protection Regulation, di cui parleremo in modo approfondito nel secondo paragrafo del secondo capitolo, è intervenuto proprio con lo scopo di regolare il diritto alla protezione dei dati personali in ragione della sua finalità sociale, ed essendo un regolamento, si previde la diretta applicabilità di quanto prescritto sul territorio europeo. A fronte del Regolamento, vi è l'obbligo per ogni Stato di adeguarvisi, ma vi è anche l'onere di dettare una disciplina nelle materie specifiche come la sanità, infatti in Italia, l'effetto dell'adeguamento alla normativa comunitaria è rappresentato dal c.d. Codice della Privacy emanato con il d.lgs. 101/2018. Per quanto riguarda la protezione dei dati personali in ambito sanitario, si sono susseguiti nel tempo pareri e linee guida del Garante Europeo per la protezione dei dati[67] e del Comitato Europeo per la protezione dei dati[68] e le linee guida dettate dall'Autorità Garante per la protezione dei dati personali. Nel secondo capitolo dell'elaborato, affronteremo in modo molto dettagliato questi strumenti normativi, concentrandoci ora sugli aspetti più generali.

È necessario fornire una definizione di "dato sanitario", ma prima dobbiamo volgere lo sguardo alla comprensione di altri termini che sono indicati nel Regolamento: un "dato personale" consiste "*in qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, tramite il nome, un numero di identificazione, un identificativo online, o tramite uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica o economica*"; il "dato genetico" è "*relativo alle caratteristiche genetiche ereditarie o acquisite della persona fisica che forniscono informazioni circa la fisiologia o la salute di questa, risultanti dalle analisi di un campione biologico*"; per "dati biometrici" si intendono "*i dati personali ottenuti da un trattamento relativi alle caratteristiche fisiche, fisiologiche e comportamentali di una persona che permettono la sua identificazione univoca come ad esempio*

[67] "*Il Garante Europeo per la protezione dei dati (European Data Protection Supervisor- EDPS) controlla il trattamento dei dati personali da parte dell'amministrazione dell'Unione Europea per assicurare il rispetto delle norme sulla privacy; inoltre riveste il ruolo di consulente per le istituzioni e gli organi nell'applicazione del trattamento dei dati personali, gestisce le denunce e conduce eventuali indagini necessarie, collabora con le amministrazioni nazionali dei paesi per assicurare l'uniformità nell'ambito della protezione dei dati e controlla le nuove tecnologie che possono influire e nuocere sulla protezione dei dati*." Sito ufficiale dell'Unione Europea, v. Garante Europeo per la protezione dei dati <www.europa.eu>

[68] "*Il comitato europeo per la protezione dei dati (European Data Protection Board- EDPB) è un organo europeo indipendente il cui compito è contribuire all'applicazione coerente delle norme sulla protezione dei dati in tutta Europa e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE, ha quindi l'obiettivo di garantire l'applicazione coerente nell'Unione europea del regolamento generale sulla protezione dei dati e della direttiva sulla protezione dei dati personali nelle attività di polizia e giudiziarie*". Sito ufficiale del Comitato Europeo per la protezione dei dati <www.edpb.europa.eu>

l'immagine del suo volto"; i "dati relativi alla salute", sono "*relativi alla salute fisica o mentale della persona fisica e quindi rivelano lo stato di salute della persona*"[69]. Il fatto che il legislatore europeo, abbia voluto fornire più definizioni necessarie per raggiungere quella definitiva di dato sanitario, dimostra l'importanza e la consapevolezza della possibile pericolosità della gestione di tutti i dati personali circolanti all'interno delle strutture sanitarie. Dobbiamo poi tener conto delle definizioni offerte dai considerando del Regolamento 2016/679 che al 34 menziona i dati genetici "*È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti*". Il considerando 35 tratta dei dati relativi alla salute "*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*." E da ultimo il considerando 51 definisce i dati biometrici e sostiene che "[…] *il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio , di pubblici poteri di cui*

[69] Definizioni fornite dal libro "La privacy nella sanità" di Giuseppe Carro, Sarah Masato, Massimiliano Domenico Parla da pagina 13 a pagina 16.

è investito il titolare del trattamento. […]", quindi se le fotografie non sono trattate tramite un dispositivo che consente l'identificazione della persona, costituiscono dati personali comuni, in caso contrario, sono da qualificare come dato biometrico. Tutto questo evidenza la necessità, di cui il legislatore si è fatto carico, secondo cui i dati personali che devono essere trattati per finalità di salute, devono ricevere una maggiore protezione.

Si può affermare che i dati relativi alla salute sono quelli presenti nelle cartelle mediche ad esempio diagnosi, risultati di esami, pareri di medici curanti o terapie seguite o interventi. E un dato sanitario, genetico o biometrico, troverà applicazione nella sanità pubblica "*l'insieme di tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità, e disabilità incluse i determinanti aventi un effetto su tale stato di salute, la necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e la cause di mortalità*"[70], inoltre, il dato sanitario merita tutela anche in caso di ricerca scientifica, opereranno infatti delle norme specifiche bilanciatrici di diritti e progresso scientifico, come esposto dal considerando 159 del Regolamento "*Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. […] Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. […]*"

In base alle distinzioni sopra esposte, vi sono delle differenze anche per quanto riguarda le modalità di trattamento: il Codice della Privacy, di cui parleremo nel prossimo capitolo, distingue tra dati personali, sensibili e sensibilissimi, associando loro una diversa regolamentazione. I primi, ad esempio nome e cognome del paziente, sono definiti come "*qualunque informazione relativa alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione*", secondo l'articolo 4, comma 1, lett.b. I secondi, sono i dati sensibili ovvero *" dati personali idonei a rivelare l'origine razziali ed etnica, le convinzioni religiose, filosofiche e di altro genere, le opinioni politiche, le adesioni ai partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"* menzionati dalla lett. C). Ma all'interno di quest'ultimi, il legislatore ha inteso ricondurre un'altra categoria, definita dei diritti sensibilissimi, ovvero "*quelli idonei a rivelare lo stato di salute e la vita sessuale*" e all'interno di questi sono ricompresi ance i dati sanitari, oggetto del nostro studio, che richiedono quindi

[70] Riferimento all'articolo 2 lett. C) Reg. CE n. 1338/2008

una tutela particolarmente rigida, infatti sono dati che devono essere oggetto di una protezione rafforzata, utilizzabili solo previo consenso dell'interessato, in base all'articolo 26 comma 5 del Codice Privacy.

Avendo spiegato cosa si intende per dati sanitari e quindi avendo esposto l'oggetto del trattamento, ora devono essere menzionati i vari ruoli che ci possono essere.

Come primo ruolo bisogna considerare quello del Titolare del trattamento[71], che ai sensi dell'articolo 4, punto 7) del GDPR è definito come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente, o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.",* quindi Titolare del trattamento è colui che determina le finalità o le modalità del trattamento dei dati personali. Quindi saper determinare chi effettivamente sia il Titolare dei dati trattati, è di fondamentale importanza, poiché su questi incomberanno non solo diritti ma anche obblighi, e analogamente, saranno individuati anche coloro cui il soggetto potrà rivolgersi qualora subisca un danno.

Il titolare del trattamento può essere sia una persona fisica che una persona giuridica, e per quanto riguarda la prima, non riguarda coloro che rappresentano la persona giuridica, ma solo ed esclusivamente coloro che effettuano un trattamento dei dati a titolo strettamente personale. Tutto ciò avviene all'interno del settore privato, in quello pubblico, invece, il Titolare del trattamento è l'entità nel suo complesso, basti pensare all'ASL[72] o al Ministero della Salute, e non quindi la persona fisica che la rappresenta, assumendo questi solo incarichi di responsabilità e colui che è responsabile di non attribuire i giusti ruoli, può essere sanzionato[73].

Vi sono dei concetti da cui partire per stabilire se un soggetto è Titolare o meno del trattamento: intanto bisogna tener conto della definizione offerta dal GDPR, e poi bisogna anche far riferimento ai concetti di "*controller*" cioè il titolare e "*processor*" è il responsabile, che sono

[71] La prima definizione di titolare del trattamento è stata : "*d) per "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza*" definizione di titolare di trattamento articolo 2 lett. D) L. n. 675 del 31 dicembre 1996, rubricata Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

[72] Con l'acronimo ASL, Azienda Sanitaria Locale, si intende "*un ente pubblico appartenente alla pubblica amministrazione italiana, che ha lo scopo di erogare servizi sanitari. L'ASL adempie ai compiti del SSN (Servizio Sanitario Nazionale) in un determinato ambito territoriale, che può essere un comune, una provincia o un insieme di città, e l'acronimo ASL viene usato solo in 5 regioni del nostro Stato. Ogni cittadino ha un ASL di appartenenza a cui rivolgersi per determinati servizi di genere sanitario, veterinario ecc*."

[73] Noto caso che riguardava un gruppo di società che utilizzavano degli agenti come titolari autonomi del trattamento ma che in realtà risultavano come responsabili del trattamento "[…]*Le risultanze istruttorie hanno dimostrato, tuttavia, che in tutti i casi oggetto di indagine gli outsourcer agiscono in carenza degli imprescindibili presupposti perché possa essere loro riconosciuta autonoma titolarità nel trattamento di dati personali, come risulta alla stregua delle seguenti, numerose considerazioni* […]"Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali - 15 giugno 2011,Pubblicato sulla Gazzetta Ufficiale n. 153 del 4 luglio 2011,Registro dei provvedimenti n. 230 del 15 giugno 2011

stati introdotti ad opera del Gruppo di Lavoro Art. 29[74]. Si sostiene che il concetto di titolare, sia un concetto di tipo funzionale, poiché è finalizzato a individuare chi abbia la responsabilità e quindi un'influenza effettiva sul trattamento: da qui possiamo affermare che la vera distinzione si avrà in ordine all'indipendenza di ciascuna parte di determinare il suo controllo sui dati personali, quindi il Titolare sarà "colui che determina". Sarà colui che potrà assumere determinate decisioni, un potere attribuitogli dalla legge, come ad esempio le strutture sanitarie pubbliche, appartenenti al Servizio Sanitario Nazionale, che hanno l'obbligo imposto dalla legge di trattare i dati dei pazienti, i Titolari. Ma non solo, la facoltà può essere conseguente a regole giuridiche, in questo caso si parla di "competenza implicita", come ad esempio la facoltà dell'editore per quanto riguarda i dati dei suoi abbonati. La facoltà di determinare il trattamento spetta anche a colui che assume il ruolo di Titolare per l'influenza che esso esercita: si parla infatti di un approccio sostanziale poiché il titolare del trattamento è effettivamente colui che ne può influenzare la modalità, anche se in questo caso, rilevare chi effettivamente detenga questa qualifica, risulta spesso piuttosto difficile.

La seconda figura che merita attenzione è quella dei contitolari, prevista dall'articolo 26 paragrafo 1 del Regolamento 2016/679 "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*."

Ma il Gruppo di Lavoro Art. 29 ha affermato che non vi è una classificazione specifica di tutte le possibili contitolarità e corresponsabilità, da ciò infatti vi è l'onere di porsi alcuni interrogativi in sede di qualificazione: ci si deve chiedere se siano entrambi i soggetti a definire le modalità e le finalità del trattamento, e in quale modo entrambi influiscono, ad esempio, sulla tipologia dei dati che deve essere raccolta. Provvedimento illuminante in materia è stato quello del Garante per la protezione dei dati personali[75], nel quale l'autorità è intervenuta per qualificare il

[74] "*Il Gruppo di lavoro ex Articolo 29 è un organismo consultivo e indipendente, istituito dall'art. 29 della Direttiva 95/46 del Parlamento europeo e del Consiglio sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, e alla libera circolazione di tali dati*". "Cosa è il gruppo di lavoro ex art. 29?" Avv. Gianluca Lanciano 5 Novembre 2017 - Aggiornato il 5 Agosto 2018

[75] Garante per la protezione dei dati personali, Trattamento di dati personali per finalità di marketing - 15 giugno 2017 [6629169] Registro dei provvedimenti n. 268 del 15 giugno 2017. "[…] *7.2. A questo proposito, deve infatti rilevarsi, in prima battuta, che, con riguardo ai trattamenti di dati personali effettuati per finalità di marketing, deve ritenersi che le due Società abbiano operato come co-titolari del trattamento ai sensi dell´art. 4, comma 1,*

particolare rapporto tra due società di telemarketing e si chiarisce che affinché i due soggetti possano ritenersi contitolari, le decisioni sul trattamento dei dati utilizzati devono essere adottate da entrambi, e che, in questo caso entrambe le società avevano l'accesso agli stessi dati personali. Ma nel rapporto di contitolarità vi è per forza una differenza in termini di responsabilità: sarebbe impossibile, infatti, un tipo di responsabilità cumulativa, è quindi necessaria una ripartizione. Una responsabilità congiunta non implica una responsabilità equivalente, poiché i due soggetti possono intervenire nel trattamento dei dati in modi e tempi del tutto differenti, creandosi così gradi di responsabilità diversi, implicando degli adempimenti, derivanti dalla normativa privacy, proporzionati al grado di influenza del soggetto[76].

Il GDPR richiede infatti la redazione di un contratto di contitolarità, nel quale devono essere presenti dei contenuti fondamentali che sono stati messi a disposizione dal Garante tedesco, prevedendo un modello.

La prima cosa da stabilire è l'ambito del trattamento dei dati personali e il grado di partecipazione di ogni soggetto, dal quale deriverà, come abbiamo detto prima, la responsabilità tipica di ognuno. Sarà poi necessario effettuare una ripartizione per quanto riguarda la raccolta dei dati personali, la fornitura dell'informativa agli interessati, la notifica al Garante per quanto riguarda un'eventuale violazione, la valutazione di impatto ecc. Ma non solo, dovranno essere presenti anche il motivo del rapporto di contitolarità, dovranno essere specificate le fasi del processo in cui sussiste la contitolarità e cosa implica per gli interessati.

Soggetti ulteriori del trattamento dei dati personali sono i cosiddetti responsabili del trattamento, menzionati all'articolo 4, comma 1 punto 8 del GDPR come coloro che "*trattano dati personali per conto del titolare del trattamento*" e il disposto dell'articolo 28 sancisce che "*il responsabile del trattamento sarà colui che effettuerà il trattamento qualora il Titolare non possa, purché il responsabile ne garantisca la tutela dei diritti*". Per instaurare questo rapporto, vi sarà un previo

lett. f), del Codice. In tal senso depongono una pluralità di indici, ed in particolare le circostanze accertate nel corso delle verifiche e sopra menzionate secondo cui: a. le decisioni concernenti il trattamento dei dati trattati utilizzati nelle varie campagne di marketing sono adottate congiuntamente dalle Società (aventi peraltro identico amministratore) (punto 6.2); b. entrambe le Società sono risultate avere accesso, mediante la rete locale, ai medesimi dati personali (originariamente raccolti da Idea Sorriso e quindi) utilizzati per l´effettuazione dell´attività di marketing (cfr. punti 6.1 e 5.2); c.le risorse tecno-organizzative di entrambe le società (che peraltro condividono la medesima sede) sono state utilizzate in modo promiscuo per lo svolgimento dell´attività di telemarketing (punto 5.4). […]"

[76] Questo quanto affermato dalla Corte di Giustizia Europea nella sentenza del 29 luglio 2019, nella causa C-40/17 ECLI:EU:C:2019:629 Nella causa C-40/17, una domanda di pronuncia pregiudiziale proposta alla Corte, "*ai sensi dell'articolo 267 TFUE, dall'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf, Germania), con decisione del 19 gennaio 2017, pervenuta in cancelleria il 26 gennaio 2017, nel procedimento Fashion ID GmbH & Co. KG contro Verbraucherzentrale NRW eV,con l'intervento di: Facebook Ireland Ltd,Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*"

contratto con cui il Titolare affida e prescrive istruzioni al responsabile che dovrà quindi essere inevitabilmente una persona giuridica distinta dal primo e dovrà elaborare i dati per conto di questi, quindi effettuerà la gestione sempre sotto l'autorità del titolare. Il responsabile però, potrà prendere alcune decisioni in totale autonomia: ad esempio quale sistema IT adottare per la raccolta dei dati, in che modo conservarli, i dettagli delle misure di sicurezza o i modi per garantire i termini di conservazione dei dati personali, ma tutto questo potrà essere fatto sempre sotto una sorveglianza del Titolare che dovrà garantire il giusto rispetto di quanto disposto dalla disciplina dei dati personali. Il responsabile ha inoltre la facoltà di poter nominare un sub-responsabile, figura del tutto analoga alla sua, ma che richiede puntualizzazioni offerte dal GDPR: infatti si prescrive che il Responsabile deve prontamente informare il Titolare, e raggiungere un accordo con questi, sul fatto che vuole avvalersi di un terzo per l'esecuzione di alcune attività, ma non solo, dovrà anche stipulare un accordo scritto con chi ricoprirà il ruolo di subappaltatore e inviarne copia al Titolare[77]. Più precisamente il GDPR disciplina la figura del sub responsabile all'articolo 28, paragrafo 2 ". *Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche*." Quindi la cosa fondamentale è che gli obblighi assunti dal Responsabile, dovranno essere rispettati inevitabilmente anche dal Sub-responsabile, e a questi dovranno essere impartite le istruzioni necessarie affinché l'attività sia svolta nel modo conforme alla disciplina e alla tutela dei dati.

Si contempla un'altra figura, quella dei "destinatari dei dati", ovvero persone fisiche o giuridiche esterne o interne al titolare o al responsabile che riceve la comunicazione dei dati personali. Rispettivamente, all'articolo 4, paragrafi 9 e 10 del GDPR si prescrive "[…] *"destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;10) "terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare*

[77] Trattamento dei dati personali attraverso un sistema "Rfid" di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Verifica preliminare richiesta da Azienda Ospedaliera e Sas - 29 novembre 2012 [2276103] Registro dei provvedimenti n. 370 del 29 novembre 2012

del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile; […]" la differenza tra la figura del destinatario e quella del terzo è che il primo ha un'accezione più ampia, e può essere sia un soggetto interno all'organizzazione, sia un soggetto esterno, ricoprendo in quest'ultimo caso il ruolo di terzo. Vi è però il problema quando si tratta di stabilire se un terzo è o meno responsabile del trattamento: se un soggetto esterno ha la capacità legale di decidere gli obiettivi del trattamento o ad esempio sceglie le informazioni di cui ha bisogno per compiere la propria attività, in questo caso sarà titolare autonomo dei dati, come succede all'interno di enti o istituzioni pubbliche dove i titolari del trattamento hanno l'obbligo di comunicare i dati personali. In caso contrario, se un terzo svolge la sua attività di trattamento in autonomia ma è sempre subordinato alle istruzioni del titolare, in questo caso sarà responsabile esterno.

La distinzione tra le due figure è di rilevante importanza, poiché un soggetto interno all'organizzazione del titolare è autorizzato a trattare i dati, nel caso in cui invece, il soggetto dovesse rivestire un ruolo del tutto esterno, non sarà in alcun modo autorizzato a trattare i dati e quindi vi sarà la necessità di identificare su che basi giuridiche vi può sussistere la comunicazione dei dati.

Ultima figura da dover analizzare è quella degli "autorizzati al trattamento", prevista dall'articolo 29 del GDPR "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*." Le persone fisiche che operano sotto l'autorità del Titolare devono essere autorizzate da quest'ultimo al trattamento dei dati personali. Nell'ambito sanitario, le persone private che possono ricoprire il ruolo di autorizzati sono i dipendenti, non tutti, delle strutture pubbliche e private, ma non solo, anche i liberi professionisti possono ricevere esplicita autorizzazione operando sempre e comunque sotto la sorveglianza del Titolare. Ad esempio. Se un medico lavora all'interno di una struttura sanitaria pubblica, sarà autorizzato poiché svolgerà le sue attività seguendo i protocolli predisposti, al contrario, se lo stesso medico operasse all'interno della struttura sanitaria pubblica in modo non continuativo, utilizzando come banca dati un proprio computer, non seguendo i protocolli predisposti, in questo caso, potrà rivestire solo il ruolo di responsabile del trattamento. Per quanto riguarda chi dovrà nominare gli autorizzati, si rinvia al rapporto tipo di rapporto di lavoro instaurato al di là di schemi fissi.

L'individuazione di questi ruoli risulta piuttosto problematica quando si parla di medici e di pediatri convenzionati, poiché il Garante non ha mai preso una posizione chiara. In base al

disposto legislativo[78], si stabilisce che il rapporto tra il Servizio Sanitario Nazionale e i medici convenzionati, sia un tipo di rapporto c.d. parasubordinato, che comporta quindi una connessione funzionale diretta a tutelare la salute pubblica, che presuppone un'inevitabile ingerenza da parte del committente. Quindi il medico convenzionato sarebbe un ausiliario della ASL e il rapporto non sarà assolutamente analogo a quello di un libero professionista che sceglie di svolgere la professione in favore di un soggetto: il paziente sceglierà un medico convenzionato che esercita nel comune della propria residenza. Infatti, in questo caso il medico scelto non è parte di un rapporto giuridico obbligatorio come quello tra Servizio Sanitario Nazionale e paziente, ma interviene soltanto in una seconda fase, quella relativa allo svolgimento, che sarà sempre soggetto al controllo della ASL. Ai sensi dell'articolo 1228 del codice civile, sorgerà la responsabilità civile in capo alla ASL qualora il medico convenzionato ponga in essere un fatto illecito, invece, qualora si tratti di un libero professionista, vi sarà un contatto sociale tra questi e l'assistito[79].

Per quanto riguarda i ruoli che ogni soggetto ricopre nella la materia che stiamo trattando, il Codice privacy non chiarisce alcunché, ma si limita a menzionare solo l'obbligo di informare i pazienti circa il trattamento dei loro dati personali, sussistente in capo ai medici generali e ai pediatri[80]. Il rapporto tra ASL e medici convenzionati prevede che il Servizio Sanitario Nazionale ha l'obbligo di garantire la salute di tutti i cittadini tramite i suoi dipendenti o tramite soggetti esterni, che sia il medico curante il diretto responsabile per le prestazioni sanitarie che pone, e che le ASL, inseriscano i medici all'interno del loro piano organizzativo-amministrativo. In questo modo, secondo le disposizioni del GDPR viste prima, l'ASL assumerebbe il ruolo del Titolare, i medici sarebbero i Responsabili esterni, oppure sarebbe possibile che sia che l'ASL che i medici diventino Titolari autonomi dei dati. Nel primo caso l'ASL eserciterebbe un tipo di controllo globale, essendo solidalmente responsabile con il medico qualora vi dovesse essere un fatto illecito e potrebbe ordinare al medico, in caso di cessazione del rapporto parasubordinato,

[78] D. lgs. Del 30 dicembre 1992, n.502 Riordino della disciplina in materia sanitaria.

[79] Quanto disposto dalla Cass. civ. Sez. III, Sent., 27-03-2015, n. 6243 "*In particolare, il rapporto di convenzionamento, come detto, assume natura di rapporto di lavoro autonomo, ma con i caratteri della "parasubordinazione", ossia - come affermato costantemente da questa Corte (tra le tante, Cass., 19 aprile 2002, n. 5698) - in presenza della continuità della prestazione, della sua personalità e, in particolare, della coordinazione, "intesa come connessione funzionale derivante da un protratto inserimento nell'organizzazione aziendale o, più in generale, nelle finalità perseguite dal committente e caratterizzata dall'ingerenza di quest'ultimo nell'attività del prestatore". E tali caratteri sono stati da sempre riconosciuti dalla giurisprudenza di questa Corte (come in precedenza evidenziato) nel rapporto di convenzionamento tra medici generici e ASL, operando i primi per il soddisfare gli scopi istituzionali della seconda*." Testo della sentenza rinvenibile tramite l'articolo "L'ASL è responsabile per l'errore del medico convenzionato" martedì 07 aprile 2015 di Gribaudi Maria Nefeli - Avvocato in Milano su <www.quotidianogiuridico.it>

[80] Articolo 78 del Codice della Privacy "1. *Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento.* […]"

la cancellazione immediata di tutti i dati da lui tenuti. Ma è più logico affermare che il medico convenzionato risulti come titolare del trattamento dei dati personali poiché li raccoglie con finalità di cura: l'erogazione della prestazione sanitaria, è sì il compito primario, ma non l'unico, poiché sussistono anche la promozione della salute tramite campagne di prevenzione, la realizzazione di un equilibrio perfetto tra strutture sanitarie e territori, garantire la continuità dell'assistenza. In tutti questi casi il medico opera per conto del Servizio Sanitario Nazionale e in questi casi, si vedrà la figura del Responsabile esterno del trattamento, ovvero il medico convenzionato.

Quando un soggetto accede a una prestazione sanitaria, si sviluppa un processo erogativo che coinvolge una serie di soggetti diversi, basti pensare a una singola struttura e a medici di base o anche a soggetti privati che offrono supporto sanitario, come i *care giver:* in questi casi, bisogna effettuare uno studio più attento di come i dati vengono trattati, essendoci una moltitudine di soggetti. Le figure che presenzieranno saranno le stesse illustrate sopra: si avrà una contitolarità dove più soggetti decidono i mezzi da adottare, è il caso ad esempio di un Percorso Diagnostico Terapeutico Assistenziale (PDTA)[81] che condivide con gli ospedali o altre strutture i dati presenti su un unico software, in questo caso sarà necessaria la stipulazione di un contratto tra le parti, richiesta dall'articolo 26 del GDPR *"[…] Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, […]*" .Qualora invece fossimo in presenza di un ospedale che invia dati e analisi a un altro soggetto che effettua attività di studio e indagine, si avrà un tipo di rapporto tra Titolare e Responsabile, poiché un soggetto decidere i mezzi da adottare, l'altro agirà in nome e per conto del primo, essendo richiesto anche in questo caso un contratto ex articolo 28, paragrafo 4 del GDPR *"[…] 4.Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti*

[81] "*I PDTA (Percorsi Diagnostici Terapeutici Assistenziali) insieme al PTI (Piano Terapeutico Individuale) e al PAI (Piano Assistenziale Individualizzato) rappresentano gli strumenti di pianificazione efficaci in grado di raccordare le fasi di diagnosi, cura, assistenza e riabilitazione. Nello specifico i PDTA sono uno strumento utilizzato in tutto il mondo che ha lo scopo di uniformare l'approccio clinico a determinate categorie di pazienti, dando vita al cosiddetto clinical pathway o integrated care pathway, termini creati dalla National Library of Medicine inglese. Questi inoltre prevedono l'assistenza di un gruppo specifico di paziente durante un periodo di tempo prefissato*." "STANDARD IN SANITA' PDTA, Percorsi Diagnostico Terapeutici Assistenziali" Articolo pubblicato il 30.11.18 di Davide Mori <www.nurse24.it>

per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. […]"

Infine, qualora un soggetto potesse decidere finalità e mezzi del trattamento, in questo caso, saremo in presenza di un Titolare autonomo. Quindi si dovrà consegnare all'interessato l'informativa, contenente anche la base giuridica che legittima il trattamento e trasferimento dei dati.

Avendo effettuato l'analisi dei soggetti del trattamento, ora meritano attenzione gli adempimenti per una corretta gestione dei dati.

Prima di tutto, bisogna parlare del Registro delle attività di trattamento, introdotto dal Regolamento UE 679/2016, che "*ha l'obiettivo di tracciare e mantenere controllati i processi di trattamento dati e garantire la conformità alla normativa*"[82]. Opera innanzitutto il principio di "*accountability*", ovvero una forma di responsabilità molto più ampia che comprende anche competenza e capacità di dimostrare l'adeguatezza dell'attività svolta, infatti il soggetto per dimostrare che la sua attività sia conforme al disposto normativo, deve detenere il registro: per garantire un'adeguata tutela e liceità, infatti, il Garante per la Protezione dei dati personali potrebbe richiedere un'attività ispettiva sul Registro regolarmente tenuto[83]. È previsto inoltre che vi siano situazioni in cui il Registro non sia obbligatorio, come nel caso delle imprese o le organizzazioni sotto i 250 dipendenti, difficilmente quindi si è esonerati. Per quanto riguarda l'area sanitaria, il provvedimento del 7 marzo 2019 del Garante Privacy ha previsto l'obbligo del Registro ai singoli professionisti sanitari in libera professione, gli ospedali privati, le case di cura, le aziende sanitarie del Servizio Sanitario Nazionale, le farmacie e parafarmacie e i medici di medicina generale e i pediatri. In nessuno di questi casi vi può essere ipotesi di esclusione.

In ogni documento dovranno essere presenti elementi essenziali: dovranno essere descritte le finalità, le categorie degli interessati, le categorie dei dati personali, le categorie di destinatari a cui sanno comunicati i dati, se opportuno dovranno essere indicati eventuali trasferimenti di dati verso un terzo paese o un'organizzazione internazionale, i termini previsti per la cancellazione, e se previste, le misure di sicurezza da adottare. Oltre a questi elementi che sono definiti come essenziali, sarà a discrezione del Titolare aggiungere eventuali voci, poiché il Registro rappresenta, oltre alla sua funzione primaria, uno strumento di gestione e controllo dei dati.

[82] Libro "la tutela dei dati personali in ambito sanitario", nello specifico, capitolo 4 "i principali adempimenti" a cura di Fabio Marinello, Alessandra Delle Ponti e Vittoria Piretti, pagina 75.
[83] Articolo 30, paragrafo 4 del GDPR "4. *Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo*."

La chiave del corretto trattamento dei dati, anche in materia sanitaria, è data da una scelta perfetta dei fornitori poiché, una scelta errata di *software*, servizi sanitari in outsourcing e medici, costituirebbe un rischio elevato per il trattamento. Basti pensare a un noto caso[84] in cui il servizio di manutenzione delle macchine di diagnostica per immagini, caratterizzato da un controllo in remoto, aveva trasmesso sui server degli Stati Uniti i dati dei pazienti contenuti nei macchinari. Complici di questo illecito sono stati una scorretta gestione della fornitura e i relativi accordi per la manutenzione di questi apparecchi, vedendo come responsabile il fornitore del trattamento, che aveva deciso gli elementi fondamentali del trattamento in totale autonomia dalla struttura sanitaria, con la quale aveva concluso l'accordo. Quindi si è assistito all'importanza di una corretta scelta del fornitore, che dovrebbe tradursi in un vero e proprio processo di selezione da parte del Titolare. Infatti, la scelta del Responsabile esterno risulta determinante, qualora dovesse risultare scorretta implicherebbe una c.d. *culpa in eligendo.* La scelta corretta del fornitore significa garantire un livello di tutela dei pazienti adeguato. Le attività che comportano un trattamento di dati personali sensibili, come ad esempio la conservazione del dossier sanitario o della cartella clinica, sono parti integranti della prestazione sanitaria, non meri strumenti, e quindi un trattamento non corretto implicherebbe una scorretta gestione dei pazienti. Scelto il fornitore, seguirà l'accordo, un atto scritto *ex* articolo 28, paragrafo 3 del GDPR, che porrà tutte le attività attribuite. Per quanto riguarda i contenuti del contratto, varie autorità hanno presentato i loro modelli, tutti accomunati dalla presenza dell'oggetto, ovvero la nomina del fornitore come responsabile del trattamento dei dati, e il contenuto, ossia l'insieme delle clausole che compongono il contratto, definito come capitolato: si farà riferimento alla durata del trattamento, alla natura e finalità dello stesso, alla tipologia dei dati trattati, alla categoria degli interessati, agli obblighi e ai diritti spettanti al titolare e al responsabile[85],e tutti gli adempimenti richiesti dall'articolo 28, paragrafo 3 dalla lettera a) alla lettera h) del GDPR. Oltre a questi elementi definiti essenziali, potranno aggiungersi, a discrezione delle parti in questione, ulteriori aspetti accidentali, costituendo integrazioni contrattuali: il documento tecnico ad opera del fornitore, contiene la descrizione dettagliata del servizio offerto e costituisce una forma di garanzia per il

[84] Trattamento non consentito di dati sanitari raccolti tramite apparecchiature diagnostiche - 10 aprile 2014 [3152119], Registro dei provvedimenti n. 186 del 10 aprile 2014. "*La XY S.p.a. (di seguito XY), è una società appartenente al Gruppo XX (di seguito Gruppo XX) che cura la produzione e la distribuzione di apparecchiature medicali e di diagnostica di precisione (quali macchine ecografiche, TAC; vascolari, ecc.). XY fornisce alle strutture sanitarie proprie clienti (principalmente ospedali e laboratori di diagnostica) anche servizi di manutenzione e di assistenza per apparecchiature di diagnostica per immagini. In tale quadro, la società, nel marzo del 2012, ha avviato contatti preliminari con questa Autorità e ha contestualmente comunicato alle strutture sanitarie coinvolte di aver riscontrato, a seguito di un´inchiesta interna, che, attraverso i canali di connessione utilizzati per il controllo in remoto dei predetti dispositivi, erano stati automaticamente trasferiti e registrati, su server del Gruppo XX situati negli Stati Uniti, dati personali "eccedenti le normali finalità di diagnostica e manutenzione" riferiti ai pazienti interessati, insieme ad altre informazioni relative alle prestazioni delle macchine*."

[85] Elenco specifico tratto dal Libro "la tutela dei dati personali in ambito sanitario", nello specifico, capitolo 4 "i principali adempimenti" a cura di Fabio Marinello, Alessandra Delle Ponti e Vittoria Piretti, pagina 87

responsabile per quanto riguarda il suo livello di sicurezza; in caso di stipulazione di contratto con fornitori con sede in Paesi extra-europei, dovranno essere inoltre aggiunti i cosiddetti *model law* dettati dalla Commissione UE; in caso di gestione del contenzioso, è necessario identificare il foro competente o prevedere un previo ricordo a un organismo di mediazione; in caso di inadempimento del fornitore di quanto contenuto nell'accordo, è utile l'inserimento di una clausola risolutiva espressa; da ultimo merita particolare attenzione, la "clausola di manleva" in caso di inadempimento nella fornitura di servizi, qualora dovesse risultare complessa.

La tutela dei dati personali presuppone anche una sicurezza informatica che sia in grado di salvaguardare, in questo caso, i pazienti, poiché se le informazioni, contenute nei sistemi, venissero minacciate, la qualità delle cure prescritte verrebbe meno. Gli obiettivi principali sono la riservatezza delle informazioni, poiché queste devono essere accessibili solo a chi è stato autorizzato dal titolare, l'integrità dei dati archiviati, essendo questi modificabili solo da chi autorizzato, e la disponibilità, poiché le informazioni devono essere reperibili qualora sia necessario. Quindi la sicurezza informatica assolve a tutti questi compiti, cercando a volte anche di prevedere quelle che potrebbero essere le possibili minacce ai sistemi adoperati che possono essere sia di tipo accidentale, basti pensare alle calamità naturali, oppure di tipo intenzionale, caratterizzati da dolo, ad esempio coloro che vogliono recare un danno all'azienda in questione.

L'integrità e la disponibilità dei dati, soprattutto nella materia di cui stiamo trattando, sono di vitale importanza, poiché un evento lesivo di questi, metterebbero in pericolo temi personalissimi, comportando un danno estremamente lesivo nei confronti degli interessati. I *ramsomware*[86], ad esempio, sono stati causa di gravi danni ad ospedali e ad aziende sanitarie, accedendo a e-mail, cartelle cliniche elettroniche e sistemi, per criptare e rendere inaccessibili i dati presenti nei computer.

[86] "*Con la parola ransomware viene indicata una classe di malware che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese ransom, per ripristinarli. Tecnicamente sono trojan horse crittografici e hanno come unico scopo l'estorsione di denaro, attraverso un "sequestro di file", attraverso la cifratura che, in pratica, li rende inutilizzabili.*
Al posto del classico sfondo vedremo comparire un avviso che sembra provenire dalla polizia o da un'altra organizzazione di sicurezza e propone un'offerta. In cambio di una password in grado di sbloccare tutti i contenuti, intima di versare una somma di denaro abbastanza elevata (in genere erano sotto i 1.000 dollari fino a qualche anno fa, ma negli ultimi anni sono saliti anche fino a milioni di dollari): in genere il riscatto viene richiesto in criptovaluta (Bitcoin, ma non solo).
Per questo motivo i ransomware rappresentano un attacco che si rivela pressoché immediatamente, perché l'obiettivo dei cyber criminali è quello di batter cassa. In questo senso si differenzia dai più sofisticati attacchi APT (Advanced Persistent Threat), il cui scopo è quello di persistere nel sistema attaccato il più a lungo possibile". Articolo disponibile su "Guida al ransomware: cos'è, come si prende e come rimuoverlo" di Giorgio Sbaraglia, Consulente aziendale Cyber Security, membro del Comitato Scientifico CLUSIT, del 20 aprile 2021: https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/

Per far fronte a questo tipo di problematiche, adottare un approccio basato sul rischio, e quindi conoscere l'eventuale danno, risulta essere una strategia vincente, infatti il GDPR adotta un sistema basato sul rischio, prevedendo quindi un approccio caratterizzato dalla prevenzione, adottando tutte le misure messe a disposizione per prevenire l'eventuale evento dannoso. Soltanto studiando i possibili elementi di minaccia e adottando misure idonee a tutelare i diritti degli interessati da possibili attacchi, si può nettamente ridurre la possibilità che si verifichino violazioni. Ad esempio, si potrà migliorare la *governance* dei dati, aumentando gli obiettivi raggiunti dall'impresa, sviluppando così anche la fiducia degli interessati. Le misure che devono essere adottate, sono a discrezione del titolare del trattamento, ma il "Disciplinare tecnico in materia di misure minime di sicurezza"[87] prevedeva dei criteri minimi e indispensabili per una gestione sicura. I più importanti erano: "l'utilizzo di un sistema di autenticazione informatica tramite codici, parole chiave e dispostivi di autenticazione; l'utilizzo di programmi antivirus come i programmi *antimalware*; misure di sicurezza e di sorveglianza fisiche per gli uffici, i locali e gli archivi; sistemi di *disaster recovery* che permettono il recupero integrale dei dati in caso di danneggiamento; sistemi di cifratura dei dati personali per separare automaticamente i dati più sensibili dagli altri". Anche se questo tipo di misure non è più prescritto, vengono comunque adoperate poiché mantengono una buona efficacia e rappresentano un ottimo punto di partenza per una tutela piena ed effettiva.

Qui bisogna menzionare l'eccellente lavoro effettuato dall'Agenzia per l'Italia Digitale[88], agenzia di cui parleremo nell'ultimo capitolo di questo elaborato, ovvero l'emanazione di linee guida di per la gestione del rischio informatico, contando l'aderenza di oltre cento amministrazioni tra Pubbliche Amministrazioni locali e centrali[89]. Queste misure consistono in una serie di controlli tecnologici, procedurali e organizzativi e, tenendo conto del livello di sicurezza di base del sistema in questione, queste possono essere integrate tramite tre modelli di attuazione, minimo, standard e avanzato. Quindi la fase primaria prevederà uno studio minuzioso

[87] ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA - D.LGS. 196/03 (Artt. da 33 a 36 del codice) Trattamenti con strumenti elettronici Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici. Abrogato dal d.lgs. 101/2018

[88] "*L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese. AgID sostiene l'innovazione digitale e promuove la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali*." Definizione rinvenibile sul sito ufficiale dell'Agenzia <www.agid.gov.it>

[89] Stima fornita dall'articolo "Sicurezza informatica: dalla consapevolezza alla gestione del rischio, Il supporto di AgID sul risk management alle PA italiane e l'esperienza del Consorzio dei Comuni Trentini" del 18/10/2019, rinvenibile sul sito ufficiale dell'Agenzia. In rete: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/10/18/sicurezza-informatica-consapevolezza-gestione-del-rischio

del contesto di lavoro seguito dalla considerazione degli aspetti critici e quindi dalla vulnerabilità dei sistemi adoperati, ovvero la valutazione dei rischi e delle minacce future, effettuata tramite un giudizio prognostico, utili a tal fine è il Registro delle attività di trattamento redatto ai sensi dell'articolo 30 del GDPR.

L'articolo 32 del GDPR, disciplina l'evento minaccioso, ovvero "*la distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale*"[90]. Come si stava anticipando prima, gli elementi da considerare sono la tipologia di attività di trattamento che sono svolte, i terzi coinvolti, la diversità delle sedi di trattamento poiché alcune potrebbero essere più esposte, e le fonti di rischio possibili distinguendole in cartacee e digitali. Gli eventi che possono costituire minaccia per i dati trattati sono molteplici. I fenomeni naturali come gli incendi o i terremoti sono eventi rari ma che devono essere tenuti conto per il loro grado elevato di possibilità di danno. La perdita di energia dovuta a un blackout del fornitore, com'è facilmente intuibile, comporta gravi conseguenze ai macchinari. Bisogna anche considerare, purtroppo, la mancanza di un controllo adeguato degli accessi, che dovrebbero essere sottoposti a rigorose procedure di controllo: infatti l'utilizzo di dispositivi come il *Bring Your Own Device* (BYOD)[91] espone al rischio di malware, permettendo attività illecite di furto di dispositivi personali. Anche gli errori effettuati dai medici e dal personale sanitario o dai pazienti possono comportare rischi come diagnosi errate, comportando anche danni all'immagine della struttura sanitaria in questione. Ormai è assodato che la posta elettronica, usata da 3,8 miliardi di utenti, è il principale vettore di attacco dominante per quanto riguarda i *malware* e il reato di *phishing*[92], che permettono al reo di reperire i contatti. Le norme standardizzate permettono di individuare ulteriori forme di minacce, tra queste ricordiamo l'allegato A dell'ISO 27001 che contiene tutti i controlli necessari per la valutazione del rischio informatico, la norma ISO 27799 relativa all'area medica, e la British Standards BS 10012 per la gestione e protezione dei dati personali. Inoltre, bisogna menzionare la ISO/DTR 22696 per quando riguarda l'identificazione e

[90]Libro "la tutela dei dati personali in ambito sanitario", nello specifico, capitolo 4 "i principali adempimenti" a cura di Fabio Marinello, Alessandra Delle Ponti e Vittoria Piretti, pagina 98

[91] "*L'acronimo BYOD sta per Bring Your Own Device, che in inglese significa "porta il tuo dispositivo". […] È un approccio all'incorporazione delle tecnologie e dei dispositivi personali in ambiti pubblici o privati di carattere aziendale. Ad esempio, con una politica di BYOD, un'azienda può permettere ai dipendenti di svolgere il lavoro sui propri computer e smartphone, in ufficio e al di fuori di esso*." Articolo "BYOD: futuro o già passato?" Pubblicato il 17 ottobre del 2019 <www.pandasecurity.com>

[92] *"E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Può avvenire tramite messaggi di posta elettronica ingannevoli, tramite e-mail, solo apparentemente proveniente da istituti finanziari, ad esempio le banche o da siti web che richiedono l'accesso previa registrazione. Di solito nel messaggio è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati ma in realtà il sito a cui ci si collega è falso, in questo modo, i dati immessi diventeranno di disponibilità del reo*". "Phishing. Phishing che cos'è?" Polizia Postale e delle Comunicazioni Polo Anticrimine della Polizia di Stato. In rete: https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html visto in giugno 2021

l'autenticazione dei dispositivi sanitari personali e la ISO/DTR 21332 per il *cloud computing*[93] e la ISO/AWI 22697 per le informazioni sanitarie personali. La fase seguente è la valutazione del rischio seguendo criteri quali la probabilità e la gravità, calcolato sulla base del prodotto dei due fattori.

L'ENISA[94], ha emanato delle linee guida di sicurezza informatica proprie dei sistemi sanitari: prevede infatti degli elementi che dovrebbero essere posti alla base della sicurezza informatica. Si fa riferimento all'amministrazione del sistema, fondamentale per garantire la responsabilità per la tutela dei dati, poiché gli amministratori possono applicare molte misure di sicurezza come il piano di *disaster recovery*. Dovrà essere posta una politica di sicurezza informatica, contenente le regole relative al modo in cui i dati devono essere gestiti, ed elencando le attrezzature elettromedicali. Visto che qualsiasi sistema informatico potrebbe subire degli attacchi, è necessario prevedere adeguati *log* per la registrazione che permettono di risalire ad eventuali aggressori. Il GDPR ritiene che il sistema di crittografia o cifratura rientri tra le tecniche più efficaci e consigliate per una protezione effettiva dei dati, requisito che ricade sul Titolare stesso. Per quanto riguarda il monitoraggio, l'identificazione e la gestione delle vulnerabilità, sono previsti dei processi specifici come il *Vulnerability Assesment* che ha lo scopo di classificare i possibili rischi e vulnerabilità del sistema utilizzato e che quindi rappresenta un indice di rischio, comportando l'adozione delle dovute misure. Il *Penetration test* prevede, invece, un'analisi più minuziosa che prevede la simulazione di un cyber attacco per andare a rafforzare il sistema laddove sia più attaccabile. Da ultima la segmentazione della rete permette la protezione di compartimenti separati quando determinati dispositivi non possono essere aggiornati come altri perché potrebbero risultare poi incompatibili.

---

[93] "*Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security*." Definizione disponibile in rete "Cloud Computing" By Jake Frankelfield modificato da Julius Mansa del 28 Luglio 2020 https://www.investopedia.com/terms/c/cloud-computing.asp

[94] *"L'Agenzia dell'Unione europea per la sicurezza informatica, ENISA, è l'agenzia dell'Unione dedicata al raggiungimento di un elevato livello comune di sicurezza informatica in tutta Europa. Istituita nel 2004 e rafforzata dalla legge sulla cyber sicurezza dell'UE, l'Agenzia dell'Unione europea per la cyber sicurezza contribuisce alla politica informatica dell'UE, migliora l'affidabilità dei prodotti, servizi e processi TIC con sistemi di certificazione della cyber sicurezza, collabora con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso la condivisione delle conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza dell'infrastruttura dell'Unione e, in ultima analisi, mantenere la società e i cittadini europei al sicuro dal punto di vista digitale."* Sito ufficiale dell'Agenzia https://www.enisa.europa.eu/about-enisa

Dopo aver esaminato gli elementi essenziali del trattamento e le possibili misure di sicurezza da adottare, ora bisogna volgere lo sguardo a quella che è definita come "*una violazione di dati che può essere accidentale, come una perdita accidentale di un computer, o intenzionale, ovvero un hacker che viola un sistema informatico, e comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" ovvero il *Data Breach.* In caso di violazione di dati, la prima cosa da fare, come statuito dagli articoli 33 e 34 del GDPR, è quella di notificare l'accaduto all'Autorità Garante per la protezione dei dati personali entro 72 ore. La notifica dovrà contenere la natura della violazione, ovvero, dovrà essere indicato se la violazione è stata accidentale o intenzionale, i dati oggetto di violazione, il numero specifico degli interessati, ed eventualmente, se in seguito al danno vi sono pericoli riguardanti diritti e libertà fondamentali degli interessati, quindi le loro conseguenze, inoltre, dovranno essere descritte le misure da adottare per minimizzare la violazione. Il Titolare, quindi, sarà obbligato a comunicarlo agli interessati, tranne in due casi, qualora abbia preventivamente posto in essere tutte le misure tecniche e organizzative necessarie per scongiurare rischi per i diritti e le libertà fondamentali di questi, e se il titolare ha adottato, dopo l'evento, misure adeguate a impedire che i dati illecitamente diffusi abbiano conseguenze negative.

Per prevenire un *Data Breach* è necessario avere protocolli di risposta, effettuare test periodici per verificare che le misure adottate siano adeguate, stipulare una polizza assicurativa che protegga dal rischio di *data breach* e tenere regolarmente un registro degli incidenti. Si ricorda che tutto questo non potrà avvenire in assenza di un'adeguata struttura informatica. Inoltre, appare essenziale, l'adeguata formazione e sensibilizzazione del personale, poiché ricordiamo che sia il principio di *accountability* che il principio della *privacy by design*[95], si basano sull'importanza della prevenzione di questi eventi dannosi.

Ultimamente i casi di *Data Breach* nel settore sanitario sono andati via via aumentando, come i crimini informatici: ad esempio nell'aprile 2020 il Sistema di informazione per la sicurezza della repubblica ha comunicato l'apertura di un'indagine poiché vi erano stati numerosi attacchi informatici a diverse strutture sanitarie italiane. Ma soprattutto nel settore sanitario sono molti i

[95] È stata introdotta dal Regolamento Europeo sulla Protezione dei Dati Personali, e letteralmente significa privacy fin dalla progettazione ex articolo 25 GDPR. Quando parliamo di trattamento dei dati personali e quindi tutela dei diritti e libertà, il titolare deve adottare tutte le misure tecniche e organizzative, non solo nel momento della progettazione, ma durante tutta la durata del trattamento. Devono essere procedure adeguate sia in astratto che in concreto, ovvero devono servire per lo scopo per il quale sono state progettate. Questo principio si incardina nel principio di accountability, prevendo un approccio ex ante. Viene integrato qualora siano rispettati la natura del trattamento, il concetto di stato dell'arte e siano valutati i costi dell'attuazione delle misure sia in termini di tempi che di risorse. "*Privacy by design, cos'è e come attuarla*". Avvocato Luisa di Giacomo DPO, disponibile in rete: https://www.youtube.com/watch?v=ANPEVkrnP1o visto in giugno 2021

casi di *ransomware*, com'è successo nel 2019 per l'Ospedale Sacra Famiglia di Erba[96], cui sono stati rubati 35 mila radiografie, rovinando l'immagine della struttura sanitaria.

La gestione della documentazione medica, quindi, è volta non solo al miglioramento dell'efficienza delle strutture sanitarie, ma è anche funzionale alla prevenzione dei rischi sulla sicurezza dei dati. Quindi alla luce del progresso medico digitale vi è l'esigenza di creare e gestire un tipo di procedura interna ad ogni struttura, che sia in grado di consentire una comunicazione immediata al paziente dei relativi risultati clinici, ma che allo stesso tempo sia in grado di garantire la massima tutela dei dati sanitari del paziente e il rispetto del diritto alla privacy di ognuno, garantendo la libertà di ogni paziente.

Questo obiettivo è perseguito tramite il "Sistema di Refertazione Online", introdotto con il D.P.C.M. del 2013, prevedendo un domicilio digitale dei cittadini. Il paziente può accedere ai referti con una modalità digitale, che ormai è offerta dalla gran parte delle strutture sanitarie. Fondamentali sono state le Linee Guida approvate nel 2009 dal Garante della Privacy: prevedono che l'assistito debba rilasciare il suo consenso alla ricezione del referto tramite la sottoscrizione di un modulo di informativa in cui sono specificati tutti i caratteri del servizio offerto. Presentano inoltre misure di sicurezza idonee alla natura dei dati trattati, ad esempio sono previste modalità di crittografia, sistemi di autenticazione forte e l'uso di *password*, di solito il codice fiscale, per l'apertura del *file*. L'informativa, quindi, è volta a consentire all'assistito di effettuare una scelta libera e pienamente consapevole e sarà onere del Titolare del trattamento fornire in modo esaustivo le caratteristiche del servizio di refertazione. Il paziente presterà il suo libero consenso, in modo assolutamente autonomo e qualora questi volesse ritirare il suo consenso, dovrà avere la possibilità di revocarlo, in questo modo sarà soddisfatto il principio di *accountability*. Per quanto riguarda le misure di sicurezza, dovranno essere assicurati standard minimi di sicurezza ma esse saranno diverse a seconda della consultazione che può avvenire tramite servizi Web accessibile da internet, o tramite posta elettronica certificate o altra modalità. Tutte queste attività saranno poi inserite all'interno del Registro delle attività di trattamento ex articolo 30 GDPR.

[96]"*Inoltre, visto che la violazione ha ad oggetto le immagini radiografiche relative a circa 35mila persone, occorre considerare la nozione di "dato biometrico", ovvero un dato ottenuto "da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca". Altrettanto importante è la descrizione di che cosa il Regolamento consideri come una violazione (c.d. data breach), ossia una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". È importante sapere che una violazione può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali*." Articolo "Attacchi informatici in aumento: il Data Breach dell'ospedale di Erba" disponibile in rete: https://www.frareg.com/it/legge-sulla-privacy/attacchi-informatici-in-aumento-il-data-breach-dellospedale-di-erba/ visto in giugno 2021

Ulteriore strumento è la cartella clinica, ovvero "*l'insieme di documenti nei quali sono registrate molteplici informazioni di un paziente ad opera di medici e infermieri*". Saranno presenti quindi le informazioni anagrafiche, sanitarie, sociali e giuridiche, nonché il percorso terapeutico. La cartella clinica rappresenta notizie riguardanti la storia sanitaria del paziente, ma ha natura di atto pubblico di fede privilegiata poiché rilasciata da un Pubblico Ufficiale: i fatti in essa contenuti quindi avranno rilevanza giuridica poiché pongono in essere il diritto del paziente di ricevere le cure necessarie e l'obbligo in capo allo Stato di fornire le cure adeguate. La sua digitalizzazione, avvenuta nel gennaio del 2006 con il Codice dell'Amministrazione Digitale, poneva l'esigenza della *privacy* dei pazienti. Si ebbero interventi successivi, come il Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 che stabilì le "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" e poi il Decreto del dicembre 2013 che fissò le "Regole tecniche in materia di sistema di conservazione sostitutiva" e le "Regole tecniche in materia di sistema di documento informatico, gestione documentale e conservazione di documenti informatici", e da ultimo il Regolamento electronic IDentification Authentication and Signature (eIDAS), il Regolamento UE n. 910/2014 sull'identità digitale: si dimostrarono particolarmente efficaci perché per la prima volta vennero stabilite le regole e le procedure tecnologiche necessarie per garantire l'autenticità del documento.

L'enorme vantaggio offerto da questi strumenti risiede nel fatto che i dati e le informazioni contenute possono essere trasmessi in modo celere tra diverse strutture sanitarie. A fronte di ciò, la Commissione Europea, dopo aver approvato le linee guida del 2018, ha posto degli obblighi a carico degli Stati membri: utilizzare i dati sensibili sulla salute solo per scopi sanitari, rispettando gli obblighi di privacy del paziente; garantire a ogni soggetto la possibilità di poter accedere alla sua area personale; rendere possibile l'accesso alla cartella solo al personale sanitario necessario; adottare sistemi di sicurezza per garantire l'accesso solo alle persone che ne hanno la dovuta autorizzazione; garantire la trasparenza nei confronti dell'assistito.

Inoltre, è fondamentale garantire l'accesso ai dati solo agli interessati, diritto di cui si parlerà nel prossimo paragrafo. Legittimato a richiedere l'accesso ai dati sarà il paziente stesso o un soggetto definito incapace o deceduto o terzi non coinvolti nella situazione giuridica di chi è interessato. La struttura sanitaria dovrà quindi effettuerà una valutazione della richiesta di accesso e di chi propone la richiesta. In caso di violazioni e illegittimità di accesso, la responsabilità civile sarà dell'ente detentore dei dati, basti pensare al noto caso dell'Azienda Ospedaliero Universitaria

Integrata di Verona[97], che è stata sanzionata per aver permesso a persone non autorizzate all'accesso, in particolare un tirocinante e un radiologo, di poter visionare i dati sanitari dei loro colleghi medici. Il motivo è stato ricondotto a delle misure tecniche adottate estremamente inefficaci, determinando un trattamento del tutto illecito.

[97] "*Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria - e considerato che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante" - si rappresenta che gli elementi forniti dal titolare del trattamento nelle memorie difensive non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dall'Azienda Ospedaliero Universitaria Integrata di Verona, nei termini di cui in motivazione, in particolare, per aver trattato dati personali in violazione dell'art. 5, par. 1, lett. f), del Regolamento*." [doc. web n. 9269629] Provvedimento correttivo e sanzionatorio nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona - 23 gennaio 2020 Registro dei provvedimenti n. 18 del 23 gennaio 2020 In rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9269629

1.5 Il Diritto di accesso e il Diritto del paziente: Legge 22 Dicembre 2017, n. 219.

Tema principale del diritto alla riservatezza nel trattamento dei dati, in questo caso sanitari, è il diritto dell'interessato, poiché tutta la disciplina sopra esposta e tutte le considerazioni venture, ruotano attorno alla sua tutela.

Il diritto di accesso, di cui all'articolo 15[98] del GDPR, è un diritto fondamentale dell'individuo, tutelato anche dal Codice della Privacy come "diritto dell'interessato", ed è oggetto di una tutela a carattere generale, nel senso che i diritti del soggetto sono automaticamente riconosciuti, anche quando non vige la regola del consenso. In questo modo, il paziente che si rivolge a una struttura sanitaria, pubblica o privata, per un determinato servizio, vede riconosciuto il suo diritto alla riservatezza per quanto riguarda i dati personali e sanitari poiché sensibili e, in linea alla disciplina affrontata prima, si può affermare che la tutela di detto diritto sarà una tutela rafforzata, poiché sono previste specifiche regole disciplinanti il trattamento da porre in essere.

Titolare del diritto è l'interessato (*data subject*), la persona fisica a cui si riferiscono i dati personali, concetto che è mutato nel tempo, complici le nuove tecnologie, che hanno permesso di definire come "interessato" tutta la società, assumendo una veste dinamica[99]. Le persone giuridiche, come gli enti o le associazioni, come espressamente disposto dall'articolo 14 del GDPR, non possono assumere il ruolo di interessato, anche se possono subire danni a seguito di

[98] *"1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.*
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. 4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui." Articolo 15 del GDPR, in rete: https://www.privacy-regulation.eu/it/15.htm

[99] Articolo "Interessato al trattamento" Scritto da Bruno Saetta Categoria: Soggetti Pubblicato: Novembre 14, 2018 Ultima modifica: Marzo 01, 2021. In rete: https://protezionedatipersonali.it/interessato-del-trattamento

un trattamento di dati illecito, in questo caso, sarà esperibile un'azione di risarcimento danni ai sensi dell'articolo 2043 del codice civile.

Il Codice della Privacy all'articolo 76, Titolo V, menziona il "Trattamento dei dati personali in ambito sanitario" "*1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute: a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato; b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività. 2. Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II. 3. Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.*" Si può notare come il Codice si rivolge a tutti coloro che esercitano la professione sanitaria e a tutti gli organismi sanitari, definendo quindi l'ambito soggettivo di applicazione di tale diritto.

Da ciò derivano due figure distinte di consenso informato, poiché un consenso farà riferimento al trattamento sanitario, l'altro tipo di consenso, invece, riguarderà il trattamento dei dati personali del paziente[100]. Quindi, gli esercenti le professioni sanitarie e gli organismi sanitari, dovranno adottare una procedura di raccolta dati assolutamente in regola con quanto disposto dalla legge, anche tramite l'ausilio del *Data Protection Officer* (DPO)[101]. L'interessato ha il diritto di "*ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intellegibile*" questo è quanto disposto dall'articolo 7, comma1 del Codice della Privacy, che ha il fine di tutelare il diritto degli individui, ma non solo, l'interessato da quanto disposto al comma 2, ha diritto di essere destinatario di un determinato trattamento "*2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi*

[100] Libro "Privacy, protezione e trattamento dei dati" di Marco Soffientini Editore: Ipsoa

[101] Il Data Protection officer è il responsabile per la protezione dei dati, figura introdotta dal Regolamento in Italia, distinto dal consulente privacy che invece è un soggetto che effettua una semplice consulenza presso l'azienda. Il DPO invece è una sorta di organismo di vigilanza che deve affiancare e tutelare l'azienda e che deve prestare aiuto qualora ci sia un *data breach*, ha inoltre il compito di fungere da tramite tra titolare del trattamento e interessati o tra azienda a Garante Privacy. Assiste nella redazione della valutazione sul trattamento dei dati e in caso, fornisce i pareri. Per capire se un'azienda ha l'obbligo di nominare un DPO, vi sono 3 casi menzionati dell'articoloR37 del regolamento: qualora il titolare sia un ente pubblico, qualora il titolare effettui trattamenti su larga scala su categorie definite particolari (dati sensibili), qualora il titolare effettui un'attività in cui vi è il monitoraggio di dati interessati su larga scala. Informazioni rese dall'Avvocato Luisa di Giacomo "IL DPO: LA TUA AZIENDA NE HA BISOGNO?", in rete: https://www.youtube.com/watch?v=olmoWuWrips visto in giugno 2021

identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2: e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati." Il soggetto interessato, inoltre, ha anche il potere, come disposto dal comma 3 dell'articolo corrente, di rettificare o aggiornare i propri dati, per garantirne l'attendibilità, e di cancellare o trasformare gli stessi. Sarà a cura del titolare garantire la facoltà dell'interessato di porre in essere le attività elencate.

Inoltre, vi è il diritto di opporsi al trattamento dei dati offerto dal titolare per motivi di legittimità, ad esempio qualora dovessero essere riscontrate finalità di invio di materiale pubblicitario o di comunicazioni commerciali.

Per quanto riguarda la disciplina del diritto di accesso secondo il Regolamento UE, definitivamente efficace dal maggio 2018, si pone l'interessato nella facoltà di ottenere dal titolare del trattamento la conferma o meno che i suoi dati sono trattati, ottenendo così l'accesso ad essi, come disposto dall'articolo 15 "1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:* […]" anche a livello europeo sono posti come essenziali delle condizioni che mirano ad ottenere una procedura di informazione legittima. Ma ciò che ancora di più rilevante, è la possibilità di rettifica e cancellazione, il diritto di opposizione e il processo decisionale automatizzato relativo alle persone fisiche, menzionati rispettivamente nella sezione 3 e nella sezione 4.

Si parla infatti anche di diritto all'oblio, ovvero la cancellazione dei dati personali di una persona, e qualora siano rispettate le condizioni di cui all'articolo 17, il titolare del trattamento dovrà dare piena attuazione della cancellazione, eccezion fatta per i dati che sono oggetto di trattamento per motivi di interesse pubblico, definite come "categorie particolari di dati personali"[102], limiti però calmierati da una serie di deroghe che vedono come finalità la medicina preventiva. Sulla base di questo, gli Stati membri possono e devono adottare tutte le misure idonee per tutelare la libertà e la volontà dell'interessato, come il segreto professionale. Basti pensare all'importanza e alla delicatezza di tipi di trattamenti che hanno come oggetto dati referenti epidemie transfrontaliere, vaccinazioni obbligatorie.

[102] GDPR - Regolamento generale sulla protezione dei dati (UE/2016/679) Articolo 9 Trattamento di categorie particolari di dati personali "1. *È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*. […]" in rete: https://www.altalex.com/documents/news/2018/04/12/articolo-9-gdpr-trattamento-di-categorie-particolari-di-dati 24.01.2021

Alternativo al diritto all'oblio è il diritto di oscuramento dei dati, ovvero la volontà del soggetto, revocabile nel tempo, di oscurare determinati nati o documenti sanitari, in questo modo i soggetti che sono abilitati ad accedere all'area privata del paziente, non vedranno i dati e i documenti oggetti dell'oscuramento. Ad esempio, nel Fascicolo Sanitario Elettronico, vi è una "busta elettronica sigillata"[103], cui è possibile accedervi solo con l'esplicito consenso e la collaborazione dell'interessato. In questo caso, il titolare del trattamento, dovrà informare coloro che intendono accedere ai dati, che questi non sono completi, essendoci un'area resa privata dall'interessato.

Per esercitare il diritto di accesso, il Codice della Privacy, all'articolo 8, comma 1, prevede una richiesta informale da parte dell'interessato al titolare o al responsabile del trattamento entro un periodo di tempo limitato "1. *I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo*." E le modalità per esercitare il diritto sono rispettivamente tramite raccomandata, telefax, posta elettronica ecc.

In ambito sanitario, deve essere fornita all'interessato al trattamento l'informativa relativa all'utilizzo futuro di dati, sempre per finalità sanitarie. Dopo seguiranno la raccolta, redatta in modo estremamente preciso per garantire la verità dei dati contenuti, la registrazione che può avvenire tramite molteplici *devices,* la conservazione dei dati in appositi archivi, l'utilizzo riservato al solo interessato e la comunicazione a soggetti diversi dall'interessato ma da esso individuati, solo quando sia la legge a prevederlo, sempre in conformità con quanto disposto dal Garante.

L'informativa e il consenso rappresentano i due elementi fondamentali affinché il diritto al consenso da parte dell'interessato, sia garantito[104]: il Codice Privacy e il Regolamento UE sono le fonti di questo istituto. Nello specifico, il legislatore, individua nell'articolo 13 del Codice Privacy, tutte le informazioni necessarie che devono essere fornite all'interessato, elemento fondamentale e indispensabile affinché il trattamento sia legittimo. Bisogna tener presente, che in ambito sanitario, gli esercenti la professione, devono trattare i dati che sono realmente idonei a rilevare lo stato di salute della persona in questione, ma oltre al consenso dell'interessato, se

[103] Libro "La privacy nella sanità"- Giuseppe Carro, Sarah Masato, Massimiliano Domenico Parla, pagina 159.

[104] "3. *Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato*." Articolo 12, capo 3, Diritti dell'Interessato, Sezione 1, Trasparenza e modalità del Regolamento UE in rete: https://consulenzaprivacyregolamentoue679.it/testo-del-regolamento-ue-2016679/capo-iii-diritti-dellinteressato/#toggle-id-1

sono presenti dati sensibili, è necessario anche il consenso del Garante. Questa procedura dovrà essere completata dall'adozione delle opportune misure di sicurezza che rappresentano un obbligo per il titolare. Nel Regolamento UE, di rilevante importanza è l'articolo 12[105], in cui si fa riferimento all'obbligo di trasparenza delle informazioni, comunicazioni e modalità finalizzate all'esercizio del diritto da parte del paziente. Quindi qualora vi siano ulteriori informazioni rilevanti, il titolare deve darne pronta notifica all'interessato, rispettando la correttezza e la trasparenza richiesti, qualora questi non dovesse informare in modo integrale l'interessato, si avrebbe un consenso incompleto dettato da un'informativa imparziale, soggetto quindi a invalidità. Solo la legge può dettare deroghe a quanto statuito, qualora ad esempio siano individuate modalità diverse di informativa o quando sia in rilievo il pubblico interesse. Anche il Regolamento richiede cognizione e responsabilità da parte del titolare, ma cosa lo distingue dalle nostre leggi nazionali, è la volontà di rendere attivi nel rapporto tutti i soggetti, per garantire l'effettiva tutela dei dati, prescrivendo agli articoli 13 e 14[106] del Regolamento le informazioni da fornire. L'informativa non è posta come un mero obbligo burocratico dove l'interessato agisce in modo passivo, ma è costituita da una pluralità di atti informativi, quindi adempimenti gestiti dai soggetti del trattamento in modo attivo e dinamico. Il risultato sarà la gestione di atti in modo molto più celere, condividendo i dati sensibili con tutti i soggetti abilitati, ne è un esempio il Fascicolo Sanitario Elettronico. Gli articoli 12,13 e 14 del Regolamento UE hanno quindi lo scopo di controllare l'attività posta dal titolare del trattamento, che può essere un'azienda sanitaria pubblica o privata, in modo che sia imposto l'obbligo per queste di rivedere i propri atti informativi forniti ai pazienti, integrandoli, laddove fosse necessario, con un nuovo consenso.

Il consenso ha la finalità di delimitare e predisporre l'ambito di applicazione del trattamento, limitando quelli che sono i poteri concessi al titolare. In ambito sanitario, è necessario però distinguere il "consenso al trattamento sanitario" e il "consenso al trattamento dei dati personali", poiché i dati sanitari sono dati sensibili che riguardano la sfera più intima della persona. Nel caso del consenso al trattamento sanitario, il paziente rende legittimo l'intervento clinico sanitario, quindi si farà riferimento a tutte le informazioni riguardanti la diagnosi e la terapia da seguire. In caso, invece, di consenso al trattamento di dati personali, il consenso riguarderà il trattamento

[105] Trasparenza nella gestione dei trattamenti "*Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).*" Art. 12 GDPR - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato-Regolamento UE 2016/679, art. 12 di Redazione Altalex in rete: https://www.altalex.com/documents/news/2018/04/12/articolo-12-gdpr-informazioni-modalita-trasparenti-interessato

[106] Si rimanda al testo del Regolamento UE 2016/679, consultabile presso il sito ufficiale del Regolamento Generale per la Protezione dei Dati Personali. in rete: https://gdpr-info.eu/art-13-gdpr/

delle informazioni sullo stato di salute del paziente. È possibile, quindi, che al momento della sottoscrizione del consenso da parte del paziente, lui dia l'approvazione per entrambi i tipi di trattamenti, ed essendo un atto fondamentale, dovrebbe contenere tutte le informazioni necessarie affinché il paziente possa prendere una decisione ed esercitare il suo consenso in modo assolutamente libero e consapevole[107].

Nell'ottica del Codice della Privacy, rispettivamente all'articolo 76[108], si pongono le basi dell'esercizio del consenso in ambito sanitario, dettando nello specifico la non necessarietà dell'autorizzazione del Garante qualora il trattamento riguardi dati e operazioni indispensabili per fine di tutela di salute o dell'incolumità della persona. Quindi il consenso viene posto come una sorta di epilogo delle finalità dell'informativa che lo precede e può essere espressamente dichiarato dall'interessato stesso o da un prossimo congiunto o da un familiare.

Mettendo sempre a confronto le figure del Codice della Privacy, con quelle proprie del Regolamento UE, si nota che qualora il consenso sia già stato espresso dall'interessato o da chi per lui, e qualora vi siano nuove disposizioni, basterò che il vecchio atto di consenso sia conforme alla nuova situazione di fatto, per evitare sanzioni. Quindi, se dopo un attento esame, l'azienda sanitaria dovesse constatare la non uniformità dei loro consensi alla disciplina del 25 maggio 2018, saranno necessari interventi. Per quanto riguarda la forma del consenso, troverà applicazione sia la modalità telematica sia la modalità orale, anche se al considerando 42[109] si

---

[107] Libro "La privacy nella sanità"- Giuseppe Carro, Sarah Masato, Massimiliano Domenico Parla, pagina 172

[108] Testo dell'articolo 76 del Codice della Privacy "[1. *Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute: a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato; b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività. 2. Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II. 3. Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.*]" Rinvenibile in rete: https://www.brocardi.it/codice-della-privacy/parte-ii/titolo-v/capo-i/art76.html

[109] 42) "*Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di prestare un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio (10) è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio*". Testo del Considerando 42 relativo all'onere della prova rinvenibile su "REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 Arricchito con riferimenti ai Considerando Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018" in rete: https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

prevede che è necessario dimostrare il consenso espresso, quindi l'atto di consenso scritto assumerebbe valore probatorio, quindi anziché essere richiesta una forma *ad substantiam* si richiede la forma *ad probationem*. Qualora per esprimere il consenso, si dovesse usare un mezzo telematico, in questo modo, dichiarare il proprio consenso sarà più semplice e immediato, dovendo cliccare su un'apposita casella. L'articolo 7 del Regolamento UE menziona invece, le condizioni che devono essere poste per avere il consenso e l'onere della prova, richiamando il considerando 42. Al paragrafo 3 che recita "3. *L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato*. ([1])" fa riferimento al potere dell'interessato di revocare in qualunque momento il proprio consenso, ponendo in capo al titolare del trattamento, un obbligo positivo di rendere la modalità di revoca chiara e semplice, esattamente come l'accordo.

Avendo analizzato le modalità secondo le quali deve essere predisposto un trattamento legittimo e avendo fatto riferimento al diritto di accesso, esercitabile da ogni individuo che accede a qualsiasi servizio sanitario, ora è necessario commentare la Legge 22 dicembre 2017, n. 219, entrata in vigore il 31 gennaio 2018, contenente "Norme in materia di consenso informato e di disposizioni anticipate di trattamento", approvata a conclusione di un acceso dibattito. Una Legge del tutto innovativa che trova le sue radici nella storia della nostra cultura, essenziali da citare la Convenzione sui diritti umani e la biomedicina (Convenzione di Oviedo), la Carta dei diritti fondamentali dell'Unione Europea e i codici deontologici dei medici e delle professioni sanitarie, che fino al 2017 non avevano trovato esplicita regolamentazione.

Scopo della presente legge era quello di porre un esplicito Diritto del Paziente, e di disciplinare le modalità di espressione e di revoca del consenso informato, ponendo le basi della legittimazione ad esprimerlo e a riceverlo, le condizioni, regolamentando inoltre anche le cosiddette disposizioni anticipate di trattamento, tramite le quali il soggetto in questione è in grado di esprimere le proprie volontà riguardo il "fine vita", qualora per motivi di salute si possa ritrovare in uno stato irreversibile di incapacità di intendere e di volere. Nodo centrale della legge è la relazione di fiducia e di cura che deve sussistere tra paziente e medico, creata sulla base del consenso informato.

Il provvedimento, entrato in vigore il 31 gennaio del 2018, è composto da 8 articoli, riferenti rispettivamente al consenso informato, alla terapia del dolore, ovvero il divieto di ostinazione irragionevole nelle cure e dignità nella fase finale della vita, al diritto dei minori e degli incapaci di poter esprimere la loro volontà, alle disposizioni anticipate di trattamento (DAT), alla

pianificazione condivisa delle cure, alle norme transitorie, alla clausola di invarianza finanziaria e alla relazione delle camere. Statuendo in quest'ultimo articolo che il Ministro della salute deve trasmettere alle Camere, entro il termine del 30 aprile di ogni anno, una relazione sull'applicazione della Legge e le regioni hanno l'onere di fornire le informazioni necessarie seguendo degli appositi questionari predisposti dal Ministero della salute, entro il mese di febbraio di ogni anno[110]. In questa legge vengono richiamati principi fondamentali di cui agli articoli 2, 13 e 32 della nostra Costituzione, gli articoli 1, 2 e 3 della Carta dei diritti fondamentali dell'Unione Europea ed è posto con particolare evidenza il tanto desiderato dalla medicina 2.0 rapporto fiduciario tra medico e paziente, con il coinvolgimento anche dei familiari di quest'ultimo, il convivente o altre persone di fiducia in caso di minori o incapaci. Ciò che si intende valorizzare è una nuova e moderna forma di relazione di cura, costituita dall'autonomia di decisione propria dell'assistito, facendo nascere in capo ad esso un vero e proprio diritto, e sulla competenza e responsabilità del medico.

Si parla formalmente di *living will* ovvero il testamento biologico[111], come previsto dal Codice di deontologia medica, tramite il quale la persona è legittimata ad esprimere anticipatamente e in un momento di capacità mentale e legale, la sua volontà riguardo a future opzioni di cura.

Il testo della Legge intende inoltre disciplinare le modalità secondo cui il consenso informato può essere espresso: o tramite un atto scritto o attraverso una videoregistrazione o dispositivi specifici qualora le condizioni fisiche del paziente richiedano una modalità *ad hoc*, come sancito al primo articolo, comma 4 "*il consenso informato, acquisito nei modi e con gli strumenti più consoni alle condizioni del paziente, è documentato in forma scritta o attraverso videoregistrazioni o, per la persona con disabilità, attraverso dispositivi che le consentano di comunicare. Il consenso informato, in qualunque forma espresso, è inserito nella cartella clinica e nel fascicolo sanitario elettronico*".

In ogni momento la persona può rivedere le sue decisioni, ed eventualmente, può rifiutare fin dall'inizio o rinunciare nel tempo a tutti i trattamenti sanitari, inclusi anche quelli relativi

[110] Informazioni fornite dal sito ufficiale della Camera dei Deputati: Speciale Provvedimenti- Sanità e affari sociali COMMISSIONE: XII AFFARI SOCIALI Welfare Consenso informato e disposizioni anticipate di trattamento informazioni aggiornate a mercoledì, 17 gennaio 2018, in rete: https://www.camera.it/leg17/522?tema=consenso_informato_e_dichiarazioni_anticipate_di_trattamento#disposizioni_anticipate_di_trattamento visto in giugno 2021

[111] Articolo "*La legge sul consenso informato e sulle disposizioni anticipate di trattamento" di Fabio Cembrani (Direttore U.O. di Medicina Legale, Azienda provinciale per i Servizi sanitari di Trento) "L'Autore affronta alcune delicate questioni poste, sul piano applicativo, dalla Legge 22 dicembre 2017, n. 219 soprattutto riguardo alle persone non più capaci di esprimere le proprie volontà in merito alle scelte di cura. Ed auspica che la figura dell'amministratore di sostegno e quella del fiduciario possano rappresentare un valido strumento per correggere le molte derive che scaturiscono dal considerarle aprioristicamente incapaci*."
28 Febbraio 2020, in rete: https://www.luoghicura.it/sistema/programmazione-e-governance/2020/02/la-legge-sul-consenso-informato-e-sulle-disposizioni-anticipate-di-trattamento/

all'idratazione e nutrizione artificiali. Al comma 5 e 6 dell'articolo 1 sono prospettati dei doveri in capo al medico "*Qualora il paziente esprima la rinuncia o il rifiuto di trattamenti sanitari necessari alla propria sopravvivenza, il medico prospetta al paziente e, se questi acconsente, ai suoi familiari, le conseguenze di tale decisione e le possibili alternative e promuove ogni azione di sostegno al paziente medesimo, anche avvalendosi dei servizi di assistenza psicologica. Ferma restando la possibilità per il paziente di modificare la propria volontà, l'accettazione, la revoca e il rifiuto sono annotati nella cartella clinica e nel fascicolo sanitario elettronico*". "*Il medico è tenuto a rispettare la volontà espressa dal paziente di rifiutare il trattamento sanitario o di rinunciare al medesimo e, in conseguenza di ciò, è esente da responsabilità civile o penale. Il paziente non può esigere trattamenti sanitari contrari a norme di legge, alla deontologia professionale o alle buone pratiche clinico-assistenziali; a fronte di tali richieste, il medico non ha obblighi professionali*". E nelle situazioni di emergenza o di urgenza "*il medico e i componenti dell'équipe sanitaria assicurano le cure necessarie, nel rispetto della volontà del paziente ove le sue condizioni cliniche e le circostanze consentano di recepirla*".

Ciò che intende fare questa Legge è una forte propaganda della necessità di comunicazione tra le due parti del rapporto, esplicitandolo al comma 8 dell'articolo 1 "*il tempo della comunicazione tra medico e paziente costituisce tempo di cura*", e cercando di promuovere l'idea di una relazione medica empatica, tenendo conto della dimensione soggettiva del rapporto. Una comunicazione così tanto significativa da aver trovato risconto successivamente nell'articolo 4, comma 1 della Legge, secondo cui le disposizioni anticipate di trattamento possono essere espresse solo «*dopo aver acquisito adeguate informazioni mediche*»[112].

Si può dedurre dal testo di Legge che le principali tematiche regolamentate sono il consenso informato, la pianificazione condivisa delle cure e la terapia del dolore e le cure palliative, vietando l'ostinazione irragionevole nelle cure e il non rispetto della dignità della persona nella fase finale della vita.

Affrontando il tema del Consenso informato, in base all'articolo 1, comma 1 "*La presente Legge tutela il diritto alla vita, alla salute, alla dignità e all'autodeterminazione della persona e stabilisce che nessun trattamento sanitario può essere iniziato o proseguito se privo del consenso libero e informato della persona interessata, tranne che nei casi espressamente previsti dalla Legge*" e in base al comma 3 "*Ogni persona ha il diritto di conoscere le proprie condizioni di salute e di essere informata in modo completo, aggiornato e a lei comprensibile riguardo alla*

[112] "Il tempo della comunicazione costituisce tempo di cura": l'approccio narrativo nella Legge 219/2017 21 Gennaio 2019 Caterina Iagnemma in Giurisprudenza Penale Web, 2019, 1-bis – ISSN 2499-846X, in rete: https://www.giurisprudenzapenale.com/2019/01/21/tempo-della-comunicazione-costituisce-tempo-cura-lapproccio-narrativo-nella-legge-219-2017/

diagnosi, prognosi, ai benefici e ai rischi degli accertamenti diagnostici e dei trattamenti sanitari indicati, nonché riguardo alle possibili alternative e alle conseguenze dell'eventuale rifiuto del trattamento sanitario e dell'accertamento diagnostico o della rinuncia ai medesimi" si evince come il consenso informato non costituisca un mero atto prodromico di accesso alle cure, bensì sia espressione di un diritto fondamentale proprio della persona assistita. Infatti, essenziale nel nostro ordinamento è il riconoscimento dell'autodeterminazione del paziente nella sua adesione ai trattamenti medici proposti dal personale medico in totale autonomia, vi è quindi un principio consensualistico nei trattamenti sanitari. Si deve porre il paziente della condizione di poter scegliere in modo consapevole e autonomo la cura da adottare o addirittura se astenersi o meno da questa. Nella celebre sentenza della Corte Costituzionale n.438/2008[113] si è statuito che "*il consenso informato, inteso quale espressione della consapevole adesione al trattamento sanitario proposto dal medico, si configura quale vero e proprio diritto della persona e trova fondamento nei principi espressi nell'art. 2 della Costituzione, che ne tutela e promuove i diritti fondamentali, e negli artt. 13 e 32 della Costituzione, i quali stabiliscono, rispettivamente, che «la libertà personale è inviolabile», e che «nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge*».

In base a queste disposizioni, nasce il dovere di cura, correlato però al riconoscimento della libertà di autodeterminazione, ovvero la possibilità per il paziente di non ricevere il trattamento terapeutico qualora esso non dia un esplicito consenso (comma 5): in questo caso, infatti, l'intervento non è considerato legittimato e le terapie già iniziate diventano illegittime.

La libertà del paziente di poter scegliere circa le terapie da seguire, è così ampia e protetta che ha dato vita al diritto alla desistenza terapeutica, ovvero permettere al paziente di accettare che la malattia faccia il suo corso, nonostante le conseguenze che ne derivano. La persona ha il diritto di scegliere autonomamente come vivere la propria vita e come affrontare le ultime fasi, rispettando la sua dignità. Ovviamente, basilare è la pronta informazione del paziente circa la sua diagnosi, prognosi e trattamento terapeutico, effettuando anche un giudizio prognostico:

[113] Caso che prevedeva la prescrizione di farmaci "L'impugnato art. 3, comma 1, stabilisce che: «*Nella Regione il trattamento con sostanze psicotrope, e nello specifico farmaci psicostimolanti, antipsicotici, psicoanalettici, antidepressivi e ipnotici su bambini e adolescenti fino a 18 anni può essere praticato solo quando i genitori o tutori nominati esprimono un consenso scritto, libero, consapevole, attuale e manifesto». Il successivo comma 2 affida alla Giunta regionale il compito di predisporre un modulo per il consenso informato, attraverso il quale il medico di medicina generale, il pediatra, lo psichiatra o il neuropsichiatra infantile forniscono le informazioni relative ai vantaggi presunti della terapia, agli effetti collaterali del farmaco consigliato, ai possibili trattamenti alternativi ed alle modalità di somministrazione*." Testo rinvenibile: Sentenza 438/2008 (ECLI:IT:COST:2008:438) Udienza Pubblica del 18/11/2008; Decisione del 15/12/2008 Deposito del 23/12/2008; Pubblicazione in G. U. 31/12/2008 n. 54
Norme impugnate: Art. 3 della legge della Regione Piemonte 06/11/2007, n. 21. In rete: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2008&numero=438#:~:text=dichiara%20l'illegittimit%C3%A0%20costituzionale%20dell,Consulta%2C%20il%2015%20dicembre%202008.

l'assistito ha la possibilità di poter autorizzare la cura, di comunicarlo ai parenti e scegliere addirittura di non ricevere alcuna informazione sul decorso della malattia, superando il vecchio modello di cura di impronta paternalistica[114]. In questo modo, è concessa la revoca di alimentazione e idratazione artificiali e non vi sarà alcuna responsabilità di tipo civile o penale in capo al medico e alla sua *équipe*. Fondamentale risulta la capacità di comunicazione dei professionisti sanitari, abilità raggiungibile tramite dei percorsi formativi appositamente predisposti. La collaborazione simultanea tra personale medico e assistito seguirà la procedura della pianificazione condivisa delle cure secondo l'articolo 5, comma 4 "*La pianificazione delle cure può essere aggiornata al progressivo evolversi della malattia, su richiesta del paziente o su suggerimento del medico*" e sarà documentata dall'équipe sanitaria nelle cartelle o nel fascicolo sanitario elettronico, seguendo la disciplina disposta prima. In questo modo la cura sarà legittima.

L'articolo 4 parla in maniera esplicita delle Disposizioni Anticipate di Trattamento (DAT**)**, al comma 1 "*Ogni persona maggiorenne e capace di intendere e di volere, in previsione di un'eventuale futura incapacità di autodeterminarsi e dopo avere acquisito adeguate informazioni mediche sulle conseguenze delle sue scelte, può attraverso le DAT, esprimere le proprie volontà in materia di trattamenti sanitari, nonché il consenso o il rifiuto rispetto ad accertamenti diagnostici o scelte terapeutiche e a singoli trattamenti sanitari. Viene indicata altresì una persona di sua fiducia, denominata fiduciario che ne faccia le veci e la rappresenti nelle relazioni con il medico e con le strutture sanitarie*" e al comma 5 "*Il medico è tenuto al rispetto delle DAT, le quali possono essere disattese, in tutto o in parte, dal medico stesso, in accordo con il fiduciario, qualora esse appaiano palesemente incongrue o non corrispondenti alla condizione clinica attuale del paziente ovvero sussistano terapie non prevedibili all'atto della sottoscrizione, capaci di offrire concrete possibilità di miglioramento delle condizioni di vita*". Si tratta quindi di uno strumento assolutamente innovativo per quanto riguarda la libera espressione dell'assistito circa la sua volontà di aderire alle terapie a lui presentate e il suo diritto di accesso alle cure, così da tutelare la sua libertà e risolvere *ex ante* possibili controversie. Nei commi successivi si fa riferimento alla precisa procedura da seguire per disporre correttamente

[114] "*Il rapporto medico – paziente è stato caratterizzato fin dal giuramento di Ippocrate da un'etica medica paternalistica, vale a dire da una concezione etica che prescrive di agire, o di omettere di agire, per il bene di una persona senza che sia necessario chiedere il suo assenso, in quanto si ritiene che colui che esercita la condotta paternalistica (nel caso specifico il medico) abbia la competenza tecnica necessaria per decidere in favore e per conto del beneficiario (il paziente). Da questa prospettiva, il medico è impegnato a ripristinare una oggettiva condizione di salute (indipendente dalle preferenze del paziente) e la relazione è fortemente asimmetrica poiché il paziente viene considerato non solo privo della conoscenza tecnica ma anche incapace di decidere moralmente. I principi etici che sono alla base del paternalismo sono il principio di beneficenza – che prescrive l'obbligo di agire per il bene del paziente – ed il principio di non maleficenza – che esprime l'obbligo di non arrecare danno al paziente*" Articolo "Rapporto medico-paziente" in rete: https://www.consultadibioetica.org/rapporto-medico-paziente/, visto in giugno 2021

le DAT: devono essere redatte per atto pubblico o per scrittura privata autenticata o consegnata personalmente dal disponente e possono essere revocate anche verbalmente, in presenza però del medico e di almeno due testimoni. Sono disposizioni che vendono predisposte dal titolare in un momento della vita in cui si è pienamente coscienti delle proprie scelte e che trovano applicazione qualora dovesse sopraggiungere uno stato di incoscienza o quando vi è una situazione di conflitto tra fiduciario e medico e spetta al giudice tutelare decidere. Tutte le DAT consegnate presso i notai, i Comuni, le strutture sanitarie competenti e i consolati italiani all'estero sono inserite nella Banca Dati Nazionale delle DAT presso il Ministero della salute, come previsto dalla legge di bilancio 2018[115].

La novità di questa Legge è stata quella di disciplinare l'esercizio del diritto di accesso e del diritto autodeterminazione che sorgono in capo a ogni paziente, garantendo la libertà di poter accedere alla propria cartella clinica, di concedere o revocare il proprio consenso. Sono presenti varie locuzioni piuttosto diverse e confuse tra di loro come capacità di agire, maggiore età, incapacità e capacità di decisione, volte però alla volontà di stabilire chi effettivamente detenga il potere di scegliere e di far scegliere, chi possa accedere a quell'area estremamente privata come una cartella clinica e chi invece veda negato l'accesso. Tutto questo tenendo conto anche dei possibili rischi legali in capo al secondo soggetto del rapporto, il personale medico, che oltre a dover affrontare situazioni particolarmente delicate dal punto di vista umano, possa ritrovarsi a ledere il diritto della persona a condurre la vita con dignità, risultando colpevole civilmente e penalmente, situazioni in cui il consenso alle cure non può essere comparato a una scelta morale.

[115] *"La Banca dati DAT, regolamentata dal DM 10 dicembre 2019, pubblicato sulla Gazzetta Ufficiale n.13 del 17 gennaio 2020, è stata attivata a partire dal 1 febbraio 2020*". DAT in rete: https://www.salute.gov.it/portale/dat/dettaglioContenutiDat.jsp?lingua=italiano&id=4954&area=dat&menu=vuoto

CAPITOLO 2

LA TUTELA DEI DATI PERSONALI IN AMBITO SANITARIO.

Sommario: 2.1 Introduzione - 2.2 Il Regolamento generale per la protezione dei dati personali n. 2016/679 nella tutela dei dati sanitari - 2.3 L'evoluzione italiana in risposta alla normativa europea - 2.4 Il Garante per la protezione dei dati personali e la sua attività nell'ambito dei dati sanitari.

2.1 Introduzione

Nello scorso capitolo si è visto come la necessità di garantire la salute, lo sviluppo costante delle tecnologie e il diritto alla riservatezza dei propri dati, abbiano costituito sia un *trend*, non solo europeo ma anche mondiale, sia una grossa sfida che il legislatore ha dovuto fronteggiare.

Nel primo paragrafo si effettuerà l'analisi dell'avvento del Regolamento 679/2016 e la sua disciplina circa l'oggetto di studio, i dati sanitari, recependo l'importanza degli stessi attribuita dal legislatore europeo. Sarà inevitabile, successivamente, notare come anche la nostra disciplina italiana sia inevitabilmente mutata, poiché destinataria della norma comunitaria. Nell'ultima parte del capitolo corrente, si vedrà come nel concreto sia importante l'ausilio e l'intervento del Garante per la protezione dei dati personali, in tutti quei casi, come successo in epoca di Covid-19, in cui la disciplina europea possa risultare a volte piuttosto frammentaria o poco chiara, vista la moltitudine di interessi e di fattispecie sempre nuove che sarebbero impossibili da prevedere.

Infatti, si può definire la privacy come un sistema *in progress*, costituito da normative e strumenti sempre nuovi per cercare di contenere le varie azioni: sarebbe infatti impossibile immaginare un codice della privacy assunto in un determinato momento storico che resti immutato per anni e che sia sufficiente a regolare la materia, bensì è necessario un lavoro di adeguamento e adesione, descritto in questo capitolo, a ciò che succede nel presente. La tutela dei propri dati è un valore irrinunciabile, un valore alla riservatezza che costituisce l'ultimo baluardo della nostra tradizione europea, diventando uno dei pilastri fondamentali della civiltà occidentale, che è assolutamente contro al tentativo odierno, da parte della tecnologia contemporanea, di spersonalizzazione e massificazione. Al contrario, il lavoro sinergico del legislatore e dell'Autorità è volto a difendere e a tutelare quell'originalità indistruttibile propria dell'individuo.

2.2 Il Regolamento generale per la protezione dei dati personali n. 2016/679 nella tutela dei dati sanitari.

Lo sviluppo delle nuove tecnologie costituisce il *leitmotiv*, non solo del progresso tecnologico in ambito sanitario, ma anche della grande opera effettuata dal legislatore comunitario. Infatti, si è osservato nello scorso capitolo, come nell'attuale scenario storico le imprese private e le autorità pubbliche siano oggi in grado di utilizzare dati personali nello svolgimento della loro attività: le persone fisiche rendono disponibili al pubblico una quantità notevole di informazioni personali che le riguardano. Nel capitolo precedente si è notato, inoltre, come vi fosse una esigenza di apportare al trattamento dei dati personali una protezione più significativa, infatti il legislatore sovranazionale ha cercato di bilanciare la libera circolazione dei dati personali all'interno dell'Unione Europea con la doverosa protezione degli stessi. Si sono susseguiti nel tempo vari atti e interventi normativi volti a raggiungere questo intento: è doveroso menzionare il punto di partenza della tutela, ovvero la Direttiva 95/46 CE, adottata il 24 ottobre del 1995, con lo scopo di armonizzare le norme in materia di protezione dei dati personali per consentire un "*free flow of data*"[116], ovvero un flusso libero di dati, cercando di promuovere un livello notevole di tutela. La situazione precedente, infatti, era caratterizzata da una preoccupante frammentazione della materia in questione nei diversi paesi europei, per cui risultò indispensabile un'armonizzazione delle normative nazionali che però garantisse una piena tutela. La direttiva però non riuscì a garantire la piena tutela e la non frammentarietà della protezione offerta in quel tempo, presentando varie lacune dettate dalla natura giuridica della direttiva stessa, poiché com'è noto, un atto comunitario non è direttamente applicabile negli Stati ma deve essere preceduto da apposite misure nazionali, in questo modo si formò una situazione ancora più variegata e complicata, totalmente contrastante con l'intento iniziale. Ad esempio, l'articolo 4[117] della direttiva prevedeva che ogni Stato membro dovesse applicare la sua legge nazionale di recepimento della stessa in relazione ai trattamenti dei dati personali effettuati nell'attività di un

[116] Direttive europee Scritto da Bruno Saetta Categoria: Normativa Pubblicato il 22 Luglio del 2018 "Direttiva 95/46/CE". In rete: https://protezionedatipersonali.it/direttive-europee

[117] "*Diritto nazionale applicabile 1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali: a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile; b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico; […]*" Testo della Direttiva 95/46/CE rinvenibile in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31995L0046&from=EL

responsabile presente nel territorio dello Stato in questione, qualora il soggetto fosse stato presente nel territorio di più Stati, avrebbe dovuto applicare gli obblighi stabiliti da ciascun diritto nazionale. Da qui l'esigenza di un mutuo riconoscimento tra le normative nazionali di tutti gli Stati europei. La Direttiva, definita anche come la "Direttiva madre", era lo specchio di un dibattito culturale e di un pensiero dottrinale ormai passati, devolvendo un tipo di trattamento dei dati personali fin troppo statico rispetto alla velocità dello sviluppo delle tecnologie negli anni '90: prima, infatti, non esistevano *smartphone* o *social network,* quindi era prevista una tutela elementare di un semplice rapporto tra interessato e titolare del trattamento. Con l'avvento dei social network e soprattutto con i motori di ricerca, in grado di fornire informazioni su qualsiasi persona, vi fu l'esigenza di disciplinare un rapporto non più tra due individui, bensì un mondo intero digitalmente connesso, rendendo la primaria circolazione unilaterale, una circolazione di tipo globale.

In Italia il diritto alla protezione dei dati personali è stato formalmente introdotto con la L. 31 dicembre del 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", trovando poi esplicito riscontro nell'articolo 1 del d.lgs. 30 giugno del 2003 disponendo che "*chiunque ha diritto alla protezione dei dati personali che lo riguardano*".

Il legislatore, quindi, optò per uno strumento normativo diverso, ovvero il regolamento, essendo un atto comunitario dotato di maggior incisività, essendo obbligatoriamente e direttamente applicabile negli Stati, avendo loro margini di autonomia piuttosto ridotti, l'unico idoneo a poter disciplinare e tutelare il settore delicato della privacy. La Direttiva 95/46 venne abrogata ufficialmente dal Regolamento 679/2016, adottato dal Parlamento europeo e dal Consiglio, il quale disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione. Denominato successivamente come General Data Protection Regulation (GDPR), entrato in vigora il 24 maggio 2017 ma che ha trovato piena applicazione dal 25 maggio 2018.

L'obiettivo del regolatore europeo è stato quello di creare un mercato digitale dei dati, nel pieno rispetto dei valori condivisi. L'articolo 1[118] del Regolamento, infatti, prevede un doppio oggetto, ovvero la protezione delle persone fisiche nel trattamento dei dati personali e la libera circolazione degli stessi, due interessi totalmente in antitesi, ricercando quella "circolazione sicura"[119], conforme al Regolamento. Il modello prospettato dal Regolamento prevede la forte

[118] GDPR - Regolamento generale sulla protezione dei dati (UE/2016/679) Articolo 1, Oggetto e finalità "*1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. […]*" in rete: https://www.altalex.com/documents/news/2018/04/12/articolo-1-gdpr-oggetto-finalita

[119] Libro "La protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n.101" di Giusella Finocchiaro capitolo 1 pagina 2.

centralità del titolare del trattamento, che, come abbiamo visto nel precedente capitolo, effettua la valutazione dei rischi e decide le misure da adottare. La differenza con la Direttiva precedente è l'approccio sostanziale adottato, non la forma: ad esempio quanto previsto sull'informativa e sul consenso è stato ampiamento confermato, introducendo però un contesto normativo innovativo basato sul principio di *accountability*[120].

Oggetto dell'elaborato è la valutazione del trattamento dei dati in ambito sanitario, ma solo dopo una valutazione generale delle novità apportate dal Regolamento è possibile tracciare con chiarezza quelle che sono state le rilevanti modifiche all'interno della materia della tutela dei dati sanitari. Infatti, è inevitabile considerare detta disciplina alla luce dell'approccio adottato dal Regolamento, basato, come si è visto nel primo capitolo, sulla *governance* del rischio e sul principio di *accountability*[121]. In questo modo è stato inevitabile il cambiamento dell'organizzazione *privacy* delle strutture sanitarie.

Il Regolamento prevede degli aspetti caratteristici, come ad esempio la puntualizzazione dell'informativa, la specificazione delle modalità di attuazione di alcuni adempimenti, delle sanzioni molto più aspre (v. consenso del minore), ponendo come denominatori comuni un nuovo approccio alla sicurezza dei dati personali, l'introduzione del principio di *accountability* e l'affermazione del diritto europeo come diritto direttamente applicabile.

Sono state così introdotte delle tematiche che hanno dato vita a un dibattito giuridico che non si esaurirà in breve tempo: basti pensare alla duplice natura dell'informazione, considerata sia come un bene economico ma anche come un diritto fondamentale dall'altro; oppure la concezione del diritto alla protezione dei dati personali come diverso dal diritto alla riservatezza. Nel tempo bisognerà constatare se il modello europeo, nel contesto delle comunicazioni globali, diventerà un modello a cui tutto il mondo farà riferimento, o se il diritto comunitario risulterò incompatibile con la prassi mondiale. Il Regolamento costituì quindi uno strumento di uniformazione del diritto, eliminando le molteplici differenze e le lacune presenti in quel periodo, recependo la diffusione delle transazioni elettroniche nel mercato interno e aumentando così l'efficacia dei servizi offerti.

Per quanto riguarda il contenuto del Regolamento, si piò affermare che alcune disposizioni, come quelle sul consenso, non hanno carattere innovativo, essendo semplicemente il risultato dell'esperienza europea. Importanti definizioni come quelle relative ai dati biometrici o alla

[120] v. Capitolo 1, paragrafo 4.
[121] Si veda il paragrafo 4 del capitolo 1

"pseudonimizzazione"[122], sono invece state introdotte con successo. È stata introdotta inoltre un'esplicita previsione sul consenso dei minori, e come si è osservato nel capitolo precedente, di rilevante importanza è stata anche l'introduzione del diritto all'oblio, la possibilità dell'interessato di cancellare per sempre i link collegati ai suoi dati personali. Proprio perché la circolazione dei dati è diventata globale, si è prevista una specifica disciplina del trasferimento dei dati all'estero, prevedendo il c.d. "meccanismo di coerenza"[123] per attuare un'applicazione uniforme del Regolamento europeo. Venne inoltre introdotto il regime della responsabilità civile, ovvero la previsione del danno cagionato dal titolare per il trattamento posto in essere da lui.

Fra le novità principali della disciplina sostanziale rientrano il principio di accountability, esaminato nello scorso capitolo, ovvero la previsione della responsabilità del titolare del trattamento, e il criterio di ragionevolezza. Quest'ultimo sintomo dell'influenza della cultura di *common law*, riscontrando nel testo del Regolamento i termini "ragionevole" e "ragionevolmente", come ad esempio nel considerando n. 26[124].

È interessante, inoltre, notare come il Regolamento abbia fornito delle definizioni di dato personale e dato sanitario, essendo doveroso specificarne la differenza per comprendere la disciplina seguente. Il GDPR non prevede una disciplina specifica per il trattamento dei dati personali effettuato in ambito sanitario al di là di riferimenti specifici relativi all'applicazione di alcune norme o istituti.

---

[122] La pseudonimizzazione è quel procedimento con il quale si impedisce di identificare un individuo tramite i suoi dati e l'impossibilità di risalire all'identità del proprietario dei dati deve essere assoluta. "*Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*". Articolo 4 del Regolamento, "Pseudonimizzazione e anonimizzazione dei dati: differenze tecniche e applicative" articolo di Edoardo Limone Cyber Security Expert, rinvenibile in rete: https://www.cybersecurity360.it/legal/privacy-dati-personali/pseudonimizzazione-e-anonimizzazione-dei-dati-differenze-tecniche-e-applicative/, 17 ottobre 2019

[123] *"Meccanismo di coerenza. Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione*." Articolo 63 del GDPR rinvenibile in rete: https://www.cyberlaws.it/en/2017/articolo-63-gdpr-regolamento-generale-sulla-protezione-dei-dati-ue2016679/

[124] "*È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la* ***ragionevole*** *probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca*." Testo rinvenibile in rete: https://www.utopiathesoftware.com/gdpr-recital/rec-026, visto in luglio 2021

Il Regolamento definisce il dato personale come "*1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*" ex articolo 4, comma 1, definizione del tutto in linea con quanto veniva disposto dalla Direttiva madre all'articolo 2, lettera a) "*a) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;*". Da queste norme si potrebbe pensare che il concetto di dato e il concetto di informazione, siano la stessa cosa, ma sono del tutto differenti tra loro. Il dato infatti costituisce la fonte dell'informazione, e dal dato o dai dati l'informazione può essere ricavata, quindi "*l'informazione è elaborazione del dato*"[125]. Nei dati personali sono ricompresi i dati sensibili, i dati giudiziari e i dati genetici. Quest'ultimi sono una specificazione dei dati sanitari, infatti come disposto dal considerando 35 del Regolamento *"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 (9); 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.*" Anche all'articolo 4, numero 15 del Regolamento si trova una definizione di dato relativo alla salute *"«dati relativi alla salute»: 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;*" Il GDPR qualifica, quindi, i dati sanitari come dati sensibili, alla stregua di quanto si

[125] Affermazione presente nel libro "La protezione dei dati personali in Italia" a cura di Finocchiaro, nel capitolo 2 scritto da Caterina del Federico e Anna Rita Popoli, pagina 66.

disponeva della Direttiva madre, e per loro natura meritevoli di una tutela rafforzata, integrando diritti e libertà fondamentali. A differenza però della Direttiva madre, il GDPR assimila nei dati sensibili anche i dati genetici e i dati biometrici, soggetti a condizioni di trattamento ulteriori e diverse, di volta in volta introdotte dagli Stati. Secondo la Corte di Cassazione italiana, come statuito in svariate sentenze[126], i dati che riguardando la salute e il sesso della persona in questione, devono essere definiti come "supersensibili", poiché attengono alla sfera più intima della persona sia nel corpo che nella psiche. Significativo è anche il disposto dell'articolo 9 del Regolamento, "*1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*." con il quale si sancisce il generale divieto di trattamento di dati personali rivelanti le informazioni sancite, ma ciò che nella trattazione corrente occorre puntualizzare, è che nell'ambito sanitario tale divieto non opera in qualora debbano essere poste in essere prestazioni sanitarie intese complessivamente. Infatti, il Regolamento adotta un approccio più dinamico e flessibile, ampliando di molto le ipotesi di legittimazione di trattamento dei dati sanitari[127]. Ma la nozione di dato sanitario, data la moltitudine di affermazioni diverse, costituisce uno degli ambiti più ostici poiché gli Stati membri risultano avere discipline estremamente diverse e incerte. Soprattutto con l'avvento della health-care, la nozione di dato sanitario ha via via assunto un arricchimento costante, basti pensare anche a quanto disposto dal Gruppo di Lavoro ex Art. 29 che sostiene che esista una categoria di dati diversa risultanti dall'attività di App sullo stile di vita che non possono essere considerati come "*dati sulla salute*" ma costituirebbe solo "*informazioni sanitarie grezze*" da cui non è assolutamente possibile ottenere delle informazioni precise sullo stato di salute della persona cui riferiscono.

È possibile che vi siano fattispecie riguardanti diversi interessi personalissimi in gioco, in questo caso opera il "bilanciamento degli interessi", e così è quanto espressamente previsto dal considerando n. 4 del Regolamento "*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e*

[126] Si veda la sentenza Cass. civ., sez. VI, sent. del 11 gennaio 2016, n. 222, in rete: https://renatodisa.com/corte-di-cassazione-sezione-vi-ordinanza-11-gennaio-2016-n-222-il-semplice-smarrimento-di-documenti-con-dati-supersensibili-da-parte-del-ministero-non-da-diritto-al-risarcimento-del-danno-se-manc/

[127] Si veda la nozione di medicina preventiva nel paragrafo 4 del capitolo 1 e la nozione di medicina del lavoro nel capitolo corrente.

familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica." Vi sono susseguiti vari casi esaminati dalla Corte di Giustizia, tra cui il caso "Volker und Markus Schecke e Eifert"[128], in cui erano presenti due cause riunite, che vedeva come protagonisti un'impresa agricola avente la forma di società semplice (procedimento C-92/09) e un agricoltore a tempo pieno (procedimento C-93/09). Essi avevano presentato una domanda di finanziamento al Fondo Europeo Agricolo di Garanzia (FEAGA) e Fondo europeo agricolo per lo sviluppo rurale (FEASR), accolte correttamente. Dopodiché, il sito Internet della Bundesanstalt, pubblicò i nomi di coloro che avevano ottenuto i finanziamenti, con indicazione della località delle sedi delle società e degli importi annuali rilasciati, e il sito era dotato di un apposito motore di ricerca. I ricorrenti, quindi, lamentarono la violazione della loro riservatezza ai dati personali, poiché le informazioni pubblicata *online* riferivano a informazioni personali. In questo caso possiamo notare come la Corte di Giustizia ha effettuato un doveroso bilanciamento tra interessi personalissimi della persona, arrivando a una peculiare conclusione, ovvero la dichiarazione di invalidità "*degli articoli 42, punto 8 ter e 44 bis del regolamento (CE) del Consiglio 21 giugno 2005, n. 1290, relativo al finanziamento della politica agricola comune, ed il regolamento (CE) della Commissione 18 marzo 2008, n. 259, recante modalità di applicazione del regolamento (CE) n. 1290/2005*" nella parte in cui è prevista la pubblicazione delle informazioni dei beneficiari dei finanziamenti provenienti dai fondi.

Analogo risultato si riscontra nella nostra esperienza italiana della Corte di Cassazione, illuminante a proposito la sentenza n. 10280 della sezione III, con la quale si affermò che il diritto alla protezione dei dati della persona, pur essendo un diritto personalissimo, potrà essere sacrificato, qualora in gioco ci siano altri diritti personalissimi che richiedano una tutela più

[128] *"[…]48 Il diritto alla protezione dei dati personali non appare tuttavia come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale (v., in tal senso, sentenza 12 giugno 2003, causa C-112/00, Schmidberger, Racc. pag. I-5659, punto 80 e giurisprudenza ivi citata). 49 L'art. 8, n. 2, della Carta autorizza quindi, a determinate condizioni, il trattamento dei dati personali. A tale riguardo la suddetta disposizione prevede che i dati personali «devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge […]1) Gli artt. 42, punto 8 ter, e 44 bis del regolamento (CE) del Consiglio 21 giugno 2005, n. 1290, relativo al finanziamento della politica agricola comune, come modificato dal regolamento (CE) del Consiglio 26 novembre 2007, n. 1437, ed il regolamento (CE) della Commissione 18 marzo 2008, n. 259, recante modalità di applicazione del regolamento (CE) n. 1290/2005 per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR), sono invalidi nella parte in cui, con riguardo a persone fisiche beneficiarie di aiuti del FEAGA e del FEASR, tali disposizioni impongono la pubblicazione di dati personali relativi ad ogni beneficiario, senza operare distinzioni sulla base di criteri pertinenti come i periodi durante i quali esse hanno percepito simili aiuti, la frequenza o ancora il tipo e l'entità di questi ultimi*.». Cause riunite C-92/09 e C-93/09 Volker und Markus Schecke GbR e Hartmut Eifert contro Land Hessen, rinvenibile in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62009CJ0092&from=EN

ampia. La disciplina in questione troverà limiti nelle norme regolanti altri diritti e nelle norme civilistiche, poiché il diritto alla protezione dei dati richiede una doverosa tutela, ma pur sempre limitata dalla preponderanza di altri beni meritevoli di piena attuazione.

È necessario volgere lo sguardo al ruolo della Corte di Giustizia, essendo doveroso ricordare che i lavori preparatori per l'emanazione di questo strumento giuridico si sviluppati in concomitanza all'attività della Corte di Giustizia. Vi sono state infatti varie pronunce che sono state inevitabilmente anticipatorie di quella che sarebbe stata la disciplina del 2016. La sentenza *Digital right Irland* dell'8 aprile 2014[129], riguardava la conservazione dei dati generati o trattati nella fornitura di servizi di comunicazione elettronica accessibili al pubblico, poiché era ritenuta troppo lesiva dei diritti fondamentali. L'attività della Corte di Giustizia ha portato all'abrogazione della Direttiva 2006/24, poiché risultante poco chiara e precisa. Qui la Corte ha effettuato un'operazione di bilanciamento degli interessi personali in gioco, di cui si è fatto cenno prima. Oppure la sentenza *Google Spain* del 13 maggio 2015[130] con cui la Corte ha tracciato in modo molto più netto la primazia dei diritti degli articoli 7 e 8 della Carta, ampliandone l'ambito di applicazione addirittura oltre i confini europei.

Da tutte le decisioni che sono state poste dalla Corte di Giustizia, si può affermare che questa ha solo anticipato la disciplina del 2016, assumendo un ruolo di "supplenza politica"[131], riconducendo la supremazia dell'Unione nell'ambito della tutela dei dati, considerando che altri modelli, come quello americano, risultano essere contraddittori e non esaustivi. Bisogna tenere conto anche del fatto che in Europa, la tutela dei dai personali è equiparata alla tutela dei diritti fondamentali, caratterizzata quindi dall'insindacabilità e dalla necessità di un'operazione di bilanciamento, che fortunatamente viene effettuato in Europa.

Ciò che viene posto dal Regolamento 679/2016 è l'importanza della disciplina del consenso in materia di protezione dei dati personali. Agli articoli 7 e 8 sono poste le condizioni generali del consenso e le condizioni applicabili al consenso dei minori. Quindi, si intende "consenso" "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento",* ex articolo 4, paragrafo 1 del Regolamento. Nell'ambito sanitario, oggetto

[129] SENTENZA DELLA CORTE (Grande Sezione) 8 aprile 2014, nelle cause riunite C-293/12 e C-594/12, in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0293&from=IT

[130] SENTENZA DELLA CORTE (Grande Sezione) 13 maggio 2014, causa C-131/12 in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&from=en

[131] Libro "La giurisprudenza della Corte di Giustizia in materia di dati personali. Da Google Spain a Schrems" di Giusella Finocchiaro, pdf rinvenibile in rete: https://romatrepress.uniroma3.it/wp-content/uploads/2019/05/5lagi-gifi.pdf

dell'esame, si può affermare che il consenso è inteso come "*l'accettazione espressa del paziente al trattamento dei propri dati, che può essere espressa solo dopo aver ricevuto adeguate informazioni circa l'utilizzo che si farà dei dati, una volta acquisiti*"[132]. È doveroso effettuare una distinzione tra consenso al trattamento dei dati e quindi il "consenso privacy" e il consenso informato al trattamento sanitario. Quindi si avrà un consenso riferito alla dichiarazione dell'interessato di accettazione che i propri dati vengano trattati secondo finalità e modalità stabilite a priori, e si avrà, inoltre, un consenso che rappresenterà la volontà del soggetto di sottoporsi al servizio sanitario, ovvero un intervento, una terapia o più in generale una prestazione medica. Quest'ultimo tipo di consenso è presente in vari strumenti normativi come la Convenzione di Oviedo del 1997[133] rispettivamente all'articolo 5 "*Un intervento nel campo della salute non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato. Questa persona riceve innanzitutto una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle sue conseguenze e i suoi rischi. La persona interessata può, in qualsiasi momento, liberamente ritirare il proprio consenso*." e viene ribadito anche nella Carta dei diritti fondamentali dell'Unione europea, rispettivamente all'articolo 3, comma 2, lettera a) *"[…] 2. Nell'ambito della medicina e della biologia devono essere in particolare rispettati: a) il consenso libero e informato della persona interessata, secondo le modalità definite dalla legge; […]*", in entrambi gli strumenti vengono però citati anche il diritto alla riservatezza e la protezione dei dati personali, ponendo quindi dei limiti al trattamento dei dati. In Italia invece, come fonti vi sono il Codice di deontologia medica che rispettivamente discorre, al Titolo IV, sul "consenso informato" e ovviamente anche sul dissenso, ponendo ovviamente l'obbligo in capo al medico professionista di informare il paziente di tutte le informazioni necessarie affinché lo stesso sia pienamente consapevole del suo stato di salute. Solo con la l. 22 dicembre del 2017, n.219, il consenso informato è diventato un requisito essenziale al fine del trattamento sanitario, di fatto all'articolo 1 viene sancito che "1. *La presente legge tutela il diritto alla vita, alla salute, alla dignità e all'autodeterminazione della persona e stabilisce che nessun trattamento sanitario può essere iniziato o proseguito se privo del consenso libero e informato della persona interessata, tranne che nei casi espressamente previsti dalla legge*."[134]

[132] Definizioni offerta dal Libro "La protezione dei dati personali in Italia" di Giusella Finocchiaro, al capitolo "Sanità e protezione dei dati sanitari" scritto da Laura Greco, pagina 260.
[133]Testo della convenzione rinvenibile in rete:
https://rm.coe.int/168007d003#:~:text=Articolo%205%20%E2%80%93%20Regola%20generale,sue%20conseguenze%20e%20i%20suoi%20rischi.
[134] Testo della Legge rinvenibile in rete: https://www.gazzettaufficiale.it/eli/id/2018/1/16/18G00006/sg

Come si vedrà successivamente, vi sono dei casi in cui il consenso espresso dell'interessato non costituisce presupposto essenziale al trattamento, e quindi lo stesso dovrà limitarsi a esternare la propria volontà delle cure mediche per poter accedere ai servizi sanitari.

Si potrebbe affermare che la manifestazione di volontà prestata dall'interessato costituisca la conclusione di un accordo di natura contrattuale con il titolare, ma questa conclusione non appare condivisibile. Innanzitutto, è bene ricordare che il diritto alla protezione dei dati è ricondotto all'interno dei diritti della persona, ma non solo, il titolare del trattamento ha la propria legittimazione a trattare dati in ragione di poteri autoritativi derivanti dalla libertà di circolazione, diversa da ogni caso, basti pensare alla libertà di impresa o alla libertà di espressione. Per coordinare un giusto consenso con il rispetto dei diritti fondamentali della persona, è necessario effettuare un bilanciamento tra gli stessi (vedi *supra)* ponendo quindi un fondamento della legittimità del trattamento. Le condizioni che rendono lecito il consenso, selezionano gli interessi in gioco ed effettuano un controllo, esplicitamente previsto dal sistema giuridico, per fare in modo da far prevalere il potere privato, ovvero l'autonomia privata e la manifestazione del pensiero, e il potere pubblico, come i poteri autoritativi degli enti pubblici. Le condizioni di liceità, quindi, eliminano i limiti che potrebbero sussistere al potere del titolare del trattamento. Alcuni autori sostengono che il consenso, abbia una natura autorizzatoria di tipo integrativo e non costitutivo: in questo modo l'autorizzazione richiede un consenso preventivo e non successivo come quello disposto dall'approvazione, riconducendola all'autorizzazione amministrativa poiché essa si riferisce a una situazione di potere preesistente. In questo tipo di autorizzazione, il privato non attribuisce al soggetto autorizzato un diritto o un potere, semplicemente rimuove un limite con un atto precedente, non avendo quindi valore costitutivo. Quindi nel trattamento di dati, si ha una manifestazione di volontà ma non vi è alcun trasferimento in capo ad altri di un potere personale, semplicemente viene rimosso un limite all'esercizio di poteri che l'ordinamento attribuisce al titolare del trattamento. Si può affermare che il consenso, in questo modo, costituisce un atto giuridico autonomo e distinto, essenziale allo svolgimento dell'attività del titolare del trattamento, e in mancanza di questi il trattamento non potrebbe essere sanato tramite una convalida, in questo caso sarebbe del tutto illecito, soggetto quindi alle sanzioni previste. Quindi la tesi prevalente è quella che prevede l'autorizzazione integrativa del consenso, potendo lo stesso essere revocato dal disponente in qualunque momento. L'interessato del trattamento ha bisogno di strumenti di protezione collegati al diritto della personalità poiché esso fa valere la propria capacità di autodeterminazione informativa, quindi necessita di tutela della propria vita privata, poiché l'autorizzazione potrebbe essere inserita all'interno di un accordo di natura contrattuale, a titolo oneroso o gratuito, avendo così due tipi di atti di esercizio dei diritti: in questo modo i due consensi sono funzionali tra di loro

poiché sono strettamente collegati. Il risultato sarà quindi un consenso di natura autorizzatoria, inquadrabile all'interno dell'articolo 9, paragrafo 2, lettera a)[135], che risponde alle esigenze di protezione dei dati personali come diritti della persona, e un consenso di natura contrattuale tramite il quale, l'interessato concorda con il titolare le modalità di trattamento nel quale la protezione dei dati è sempre garantita *in toto*. In questo modo, qualora dovesse sussistere un rapporto contrattuale, l'interessato sarà assolutamente in grado di mantenere un sano controllo dei suoi dati, potendo esercitare il suo diritto di revoca ex articolo 7, paragrafo 3 "*3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. ([1])*" la revoca del consenso, in questo modo, implicherebbe automaticamente la caducazione degli effetti dell'accordo sull'utilizzo dei dati, il titolare perderebbe così il proprio fondamento legittimo e il contratto posto in essere non avrebbe alcun effetto.

In sintesi, si può affermare che il consenso sanitario e il consenso contrattuale, sono due modalità di esercitare la propria volontà del tutto indifferenti: la manifestazione del consenso all'esecuzione del contratto non può assolutamente presupporre la volontà a sottoporsi a un determinato trattamento sanitario. Infatti, la proposta e la decisione di sottoporsi a un'operazione medica, ad esempio, potranno essere possibili solo qualora siano state eseguite un'anamnesi e una diagnosi, quindi, solo previo "contratto di assistenza e di cura."

Dopo aver esternato l'avvento del Regolamento 679/2016 e i suoi elementi essenziali, è doveroso poiché costituente l'oggetto di questo elaborato, occuparsi di come il Regolamento ha assunto efficacia, anche in ambito sanitario.

È stato posto che tutti i trattamenti di dati, ovviamente quelli previsti dalla normativa Privacy, dovranno essere conformi al Regolamento, quindi tutti i titolari del trattamento avranno l'obbligo di allineare i loro sistemi al nuovo ordinamento. Gli operatori sanitari si sono ritrovati a dover adeguare i loro standard di comportamento nei trattamenti di dati sensibili disposti da loro. Il considerando 35 del Regolamento costituisce un principio fondamentale per quanto riguarda il giusto trattamento delle informazioni circa lo stato di salute della persona, poiché capaci di rivelare lo stato di salute fisica della persona, recitando "*Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino*

[135] "*2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; […]*"

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 (9); 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." L'impatto quindi delle norme attuali sulla disciplina in questione ha dato vita a un sistema in cui un progressivo ampliamento di obblighi da seguire, sarà inevitabile, rendendo le strutture sanitarie sempre le dirette destinatarie delle norme.

In base alla procedura di bilanciamento di interessi esposta sopra, bisogna affermare che, soprattutto in ambito sanitario, possono emergere ipotesi di conflitto tra diritti di pari livello, ad esempio la protezione dei dati personali e il diritto di libertà di espressione, con la conseguente soddisfazione di un interesse ma con la compressione dell'altro. In ambito sanitario, la protezione dei dati personali del paziente appare strumentale al corretto compimento delle prestazioni sanitarie. Complice anche lo sviluppo delle tecnologie mediche, la disciplina ha assunto una crescente rilevanza, poiché in passato i dati rimanevano nel rapporto medico-paziente, ora, avendo osservato i passi avanti della *digital health*[136], il sistema sanitario è basato sul coinvolgimento di una pluralità di professionisti e una sempre più grande gestione dei dati in modo digitale.

Con il Regolamento, il legislatore europeo ha voluto ribadire dei concetti già esistenti nella abrogata Direttiva 95/46/CE, per disciplinare il precario equilibrio esistente tra il diritto alla protezione dei dati personali e il diritto alla salute, considerata la moltitudine di informazioni che circola all'interno delle strutture sanitarie ma anche tra diversi organismi, ad esempio quelli assicurativi e previdenziali.

L'approccio, quindi, è fortemente mutato rispetto al passato: prima si ricercava la libera circolazione delle informazioni, ma che a causa delle normative piuttosto stringenti, era venuta meno. Ora il disegno attuale prevede un mercato interno che garantisca l'effettiva libera circolazione delle informazioni, temperata da adeguate misure di sicurezza e da cautele. Infatti,

[136] Si veda il paragrafo 1.3 del Capitolo 1, pagina 14

volgendo lo sguardo alla disciplina dei dati sanitari, si può notare come venga privilegiata maggiormente la tutela del paziente, prevedendo l'autorizzazione al trattamento dei dati, anche in assenza del consenso dell'assistito, per il perseguimento del suo stato di salute. Infatti, all'articolo 9, comma 2, lettera h) del Regolamento che rispettivamente cita "*h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3*;" è considerato come una base giuridica per il trattamento da porre in essere, alternativo al consenso dell'interessato. Ovviamente, ciò non significa che vi dev'essere il rischio di un utilizzo abusivo di dati, anzi, proprio per queste ragioni, sono state innalzate le soglie di tutela, specificando l'oggetto del trattamento: ad esempio, i dati biometrici e genetici sono stati ricondotti nella categoria di "dati particolari"[137]. Il legislatore europeo lascia ampio margine di movimento agli Stati per quanto riguarda le condizioni e le limitazioni da adottare, poiché la particolare categoria di dati in questione coinvolge fattori culturali, sociale, etici e politici che ovviamente sono propri di ogni Stato e che a livello comunitario non potrebbero trovare piena previsione. Quindi, in capo allo Stato membro vige l'obbligo di adeguarsi alla normativa europea, in base a quelle che sono le proprie esigenze di ordinamento.

Bisogna ricordare che il trattamento dei dati in ambito sanitario non è direttamente disciplinato dal Regolamento: come si è osservato prima all'articolo 9, la norma si limita a introdurre la finalità sanitaria tra le condizioni di liceità poiché rientranti nella categoria particolare di dati. Questi ultimi, infatti, sono soggetti a una disciplina particolare, derivante proprio dalla loro particolare natura e per il loro legame con l'identità della persona, infatti un loro trattamento illecito potrebbe comportare danni rilevanti in capo alla persona in questione. Il primo limite riscontrante all'interno del Regolamento è dettato dall'articolo 9, comma 1 "1. *È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.", ovvero il divieto generale di trattare di trattare questa tipologia di dati. Un divieto però non assoluto, infatti, il legislatore pienamente cosciente delle facilità odierna di condivisione delle informazioni e della loro necessità, pone in essere una serie di condizioni di fronte alle quali, il divieto generale cede il passo alla legittimazione del trattamento. Condizioni rinvenibili al comma 2 dell'articolo 9 "2. *Il paragrafo*

[137] Si veda il paragrafo 4 del capitolo 1

1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) 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 e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del

diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato." Quindi le previsioni della normativa europea sono una legittima base giuridica per il trattamento dei dati, alternativa al consenso. Il Regolamento, quindi, pone in essere un significativo ampliamento delle condizioni di legittimità: da un lato prevede un oggetto della deroga più grande, poiché secondo le condizioni viste, non solo possono essere trattati i dati personali relativi alle proprie origini razziali ecc, ma sono trattabili anche i dati biometrici e genetici, in passato esclusi dalla definizione di categorie particolari di dati. Viene inoltre esteso anche l'ambito finalistico della deroga: infatti sono ricompresi non solo trattamenti effettuati per la semplice attività di prevenzione, diagnosi e cura ma sono anche quelli relativi alla medicina del lavoro e alla valutazione della capacità lavorativa del dipendente, o quelli relativi alla terapia sanitaria o sociale. In base anche a quanto osservato nello scorso capitolo circa i caratteri della medicina 2.0, l'obiettivo del legislatore europeo è stato quello di voler semplificare e agevolare l'esecuzione delle prestazioni sanitarie, eliminando gli adempimenti burocratici che nel tempo sono stati considerati superflui. A beneficio di tutto ciò, non è solo il sistema sanitario in sé, quanto tutti gli operatori sanitari, che nel futuro saranno sempre più esentati dallo svolgere attività, come la raccolta del consenso, del tutto estranee al loro ruolo. Eliminando questo tipo di adempimenti, inoltre, si evitano statisticamente gli errori formali che potrebbero risultare da ostacolo a ciò che è realmente importante: una prestazione sanitaria idonea ed efficace per la persona.

Un trattamento dei dati con finalità di medicina preventiva rende superfluo il consenso espresso del paziente, in questo caso, il bilanciamento tra tutela dei dati e diritto alla salute del paziente opera automaticamente poiché dettato dalla situazione di fatto in questione. In casi particolari come i soggetti interessati definiti "vulnerabili"[138], ad esempio i lavoratori, vige una tutela molto più rigida, in ragione della delicatezza del rapporto data dallo squilibrio contrattuale: infatti i lavoratori sono considerati i soggetti deboli del rapporto di lavoro rispetto al datore di lavoro. Il

[138] Definizione rinvenibile al considerando n. 75 del Regolamento "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*."

Regolamento però pone in un certo senso una tutela datoriale, poiché il datore di lavoro ha la necessità di conoscere l'idoneità lavorativa del proprio dipendente e quindi l'accesso ai dati di quest'ultimo, senza un suo previo consenso. Il legislatore europeo ha voluto quindi effettuare un bilanciamento *ex ante* a favore del datore di lavoro, considerando l'interesse dello stesso superiore rispetto a quello del lavoratore. Una posizione del genere, ovviamente, apre la strada a dibattiti di natura etica, poiché in questo caso si pone il lavoratore in una posizione di assoggettamento al datore, che vede le sue informazioni rese note senza il proprio consenso, essendo quindi destinatario di effetti pregiudizievoli. A queste problematiche, deve supplire la disciplina nazionale, che ha il dovere di intervenire con norme più dettagliate circa il trattamento di questi dati con il fine di contemperare interessi contrapposti: in questo modo, ad esempio, il datore di lavoro potrebbe conoscere circa l'idoneità o meno del lavoratore a poter svolgere determinate mansioni, ma non potrà sapere, in caso di non idoneità, la malattia specifica di quest'ultimo. Informazioni che potrebbero ledere il diritto alla riservatezza dei dati personali della persona, ma che in contesti come quello lavorativo, si rivelano di particolare rilevanza se pensiamo ai rischi che potrebbe correre una persona affetta da malattia durante lo svolgimento di determinate azioni. Quindi, qualora il trattamento debba essere effettuato a fronte di una qualsiasi delle finalità presenti nell'articolo 9, comma 2, lettera h) (vedi *supra*), anche se effettuato nei confronti di categorie particolari di soggetti, il trattamento sarà assolutamente legittimo.

Oltre a quanto finora affermato, vi è un altro requisito, dettato dall'articolo 9, comma 3 del Regolamento, ovvero il necessario segreto professionale "3. *I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti*." In questo modo viene ristretto l'ambito soggettivo di chi può effettivamente effettuare il trattamento per le finalità di tutela della salute e di gestione dei servizi e dei sistemi sanitari. In capo al professionista sanitario che non attui un trattamento legittimo con l'ulteriore segreto professionale circa le informazioni personali del paziente, sarà applicabile l'articolo

622[139] del codice penale italiano che punisce la rivelazione dei segreti professionali[140]. Questo requisito opera anche nei confronti del personale diverso da quello medico ma comunque interno alla struttura sanitaria, poiché è assolutamente in grado di venire a conoscenza dei dati. Inoltre, il requisito del segreto professionale deve trovare applicazione anche qualora non sia possibile annoverare l'attività svolta come sancito dal considerando n. 35, basti però che rimanga afferente ad un'organizzazione sanitaria.

Riguardo al segreto professionale, il Regolamento autorizza determinati organismi a dettare regole specifica in materia, riferendosi quindi agli ordini e ai collegi professionali. Basti pensare all'articolo 10[141] del Codice di deontologia medica che pone in capo al medico l'obbligo di segreto professionale.

Sempre rimanendo nel tema dei presupposti di liceità del trattamento, l'articolo 9, comma 2, lettere i) e j) disciplinano la sanità pubblica e la ricerca scientifica, sostenendo che rappresentano due adeguate basi giuridiche per il trattamento dei dati, cui il trattamento può essere anche sprovvisto del consenso dell'interessato, disciplina analoga a quella prevista per il trattamento avente finalità di tutela della salute. " […] *i) 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 e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in*

[139] "*Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società. Il delitto è punibile a querela della persona offesa*." Art 622 c.p.

[140] "*Il codice deontologico precisa che il medico non collabora nella costituzione, nella gestione o nell'utilizzo di banche dati aventi ad oggetto informazioni relative agli assistiti se mancano delle garanzie sull'acquisizione preliminare del consenso informato e sulla tutela della riservatezza e della sicurezza dei dati*". Fonte: "Il segreto professionale del medico" https://www.studiocataldi.it/articoli/33473-il-segreto-professionale-del-medico.asp#ixzz70hHdO968
(www.StudioCataldi.it) 24 luglio 2021

[141] "*Il medico deve mantenere il segreto su tutto ciò che gli è confidato o di cui venga a conoscenza nell'esercizio della professione. La morte del paziente non esime il medico dall'obbligo del segreto. Il medico deve informare i suoi collaboratori dell'obbligo del segreto professionale. L'inosservanza del segreto medico costituisce mancanza grave quando possa derivarne profitto proprio o altrui ovvero nocumento della persona assistita o di altri. La rivelazione è ammessa ove motivata da una giusta causa, rappresentata dall'adempimento di un obbligo previsto dalla legge (denuncia e referto all'Autorità Giudiziaria, denunce sanitarie, notifiche di malattie infettive, certificazioni obbligatorie) ovvero da quanto previsto dai successivi artt. 11 e 12. Il medico non deve rendere al Giudice testimonianza su fatti e circostanze inerenti il segreto professionale. La cancellazione dall'albo non esime moralmente il medico dagli obblighi del presente articolo*." Articolo 10 del Codice di deontologia medica, rinvenibile in rete: https://www.ordinemedicivenezia.it/codice-deontologico-1-10

conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. […]". Il bilanciamento richiesto ed effettuato, in questo caso, prevede il rapporto tra l'interesse collettivo all'utilizzo del dato e l'interesse individuale alla riservatezza dei propri dati personali, in questo caso però, il bilanciamento risulta ancor più difficile, poiché i dati sanitari e genetici che vengono impiegati in questi tipi di attività, oltre a riguardare la sfera intima della persona, rappresentano anche un'utilità sociale non indifferente. Prendendo il caso della sanità pubblica, ad esempio, è di fondamentale importanza rammentare ciò che è stato posto nel Regolamento CE 1338/2008 del Parlamento europeo e del Consiglio, all'articolo 3, lettera c) " *[…] «sanità pubblica» tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale ad essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità; […]*" in questa definizione si riscontra cosa debba intendersi per sanità pubblica ed è compito del legislatore nazionale di ogni Stato prevedere delle misure e sanzioni idonee per tutelare la libertà dell'interessato.

Anche nel caso di trattamento dati per finalità di ricerca scientifica, il legislatore europeo ha ritenuto preponderante l'interesse della collettività all'evoluzione scientifica, assicurando al contempo un elevato grado di sicurezza dei trattamenti, come sancito dal considerando n.159 "*Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisse motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure*."

2.3 L'evoluzione italiana in risposta alla normativa europea.

In Italia, l'esperienza circa il trattamento dei dati personali, risulta decisamente diversa rispetto a quella comunitaria: infatti, se è vero che il quadro normativo europeo non ha subìto un drastico cambiamento a seguito dell'introduzione del Regolamento nel 2016, poiché come si è visto la Direttiva 95/46/CE aveva anticipato quasi del tutto la disciplina, fino al 25 maggio del 2018, si richiedeva ancora il consenso per i trattamenti aventi finalità sanitaria, poiché non era stata recepita la disposizione della Direttiva che prevedeva la decadenza del divieto generale di trattamento delle categorie particolari per finalità di prevenzione, diagnostica medica e altri[142].

Il Codice in materia di protezione dei dati personali, noto anche come "Codice della privacy", introdotto con il Decreto legislativo 30 giugno 2003, n. 196, e in vigore dal 1º gennaio 2004, contiene le norme nazionali relative alla tutela dei dati personali: l'articolo 23, comma 4, abrogato poi dal d.lgs. 101/2018, prevedeva l'espresso consenso dell'interessato, in forma scritta, come atto necessario per ogni trattamento di dati sensibili e l'articolo 26, prevedeva inoltre un'obbligatoria autorizzazione da parte del Garante al trattamento. I soli trattamenti che non necessitavano di questa doppia volontà erano quelli indicati nell'articolo 26, comma 3, rispettivamente "3. *Il comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria; b-bis) dei dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis.*" Solo all'articolo 26, comma 4, erano previsti determinati trattamenti che non richiedevano il consenso dell'interessato ma che comunque necessitavano del consenso del Garante "4. *I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente*

[142] Si veda il paragrafo precedente.

ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111." Questo schema, ovviamente, si rifletteva nel trattamento dei dati in ambito sanitario, ed erano previste delle modalità di espressione del consenso semplificate, per consentire le pratiche degli operatori sanitari. Con l'avvento del Regolamento europeo, anche l'Italia ha dovuto adeguarsi alla nuova disciplina vigente molto più liberale di quella precedente.

Il primo risultato è stato l'ampliamento delle categorie di dati che possono essere trattate in ambito sanitario, poiché il Codice Privacy prevedeva che il trattamento fosse possibile solo nei confronti di dati idonei a rivelare lo stato di salute. Con il Regolamento, invece, si prevede che tutte le categorie particolari di dati, elencati nell'articolo 9 di cui si è discorso prima, possono essere tranquillamente oggetto del trattamento. Una seconda conseguenza è stata l'abrogazione delle norme relative al consenso, del tutto incompatibili con quanto disposto dal Regolamento.

Ma oltre, alle disposizioni circa il consenso, sono state abrogate norme sul trattamento in ambito sanitario, come quelle sull'adozione delle misure minime di cautela per garantire il rispetto dei

diritti e della dignità degli interessati; altre riguardo le modalità e le precauzioni nella prescrizione di medicinali o le comunicazioni di dati all'interessato[143]. È facilmente intuibile il perché vi sia stata l'abrogazione di dette norme: la risposta è da trovare nel principio di *accountability* proprio del Regolamento, in cui si prevede la responsabilizzazione del soggetto che effettua il trattamento anche per quanto riguarda la sua capacità di adottare delle misure specifiche per la tutela dei dati degli interessati.

Quindi, il Regolamento pose un approccio del tutto diverso rispetto a quello precedente: improntato quindi sulla responsabilizzazione del titolare, non prevedendo più standard minimi di sicurezza o liste di istruzioni da seguire, bensì spetta proprio ai titolari del trattamento compiere un'attività continua di verifica delle misure da loro adottate, dei rischi e delle finalità[144]. Quindi si è passati da un'imperativa osservanza di istruzioni analitiche alla richiesta al titolare di una condotta molto più dinamica e diretta dell'attività svolta da esso, lasciando al Codice il compito di definire in modo generale il trattamento dei dati sanitari, ma facendo riferimento alla disciplina del Garante per le regole più specifiche.

Come si è anticipato nel precedente paragrafo, il Regolamento si limita a tracciare gli aspetti essenziali della disciplina del trattamento dei dati, lasciando ampia discrezionalità agli Stati europei per quanto riguarda la tutela dei dati relativi alla salute, biometrici e genetici. Ogni Stato, per i suoi trascorsi culturali, sociali, politici ed economici, ovviamente ha una diversa esperienza rispetto agli altri, trovando quindi diverse discipline circa la stessa materia.

In Italia, ad esempio, per quanto riguarda il trattamento dei dati personali, ha trovato notevole impatto l'attività posta in essere dal Garante: attraverso provvedimenti, Linee guida, autorizzazioni e un'attività simultanea con il Ministero della Salute è riuscito nel tempo a elaborare una disciplina solida, godendo di un potere di riserva affidatogli dal legislatore nazionale. Significativo, infatti, è il disposto dell'articolo 2 septies del Codice introdotto con il d.lgs. 101/2018 rubricato "*Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*" disponente "1. *In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformita' alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.*"[145]. Non viene specificato espressamente cosa si debba intendere per "misure", infatti il legislatore italiano ha inteso promuovere la possibilità di introdurre regole diverse

[143] Si vedano gli articoli 83 ss. del Codice *ante* riforma.
[144] Si veda il paragrafo 4 del capitolo 1.
[145] Articolo rinvenibile in rete: https://www.ricercagiuridica.com/codici/vis.php?num=24909

rispetto a quanto disposto dalla normativa generale, poiché, tenendo conto della particolarità della materia in questione, è necessario e doveroso predisporre una sana disciplina *ad hoc*, idonea al tipo di contesto in questione.

Le misure di emergenza da adottare, sono però vincolate ad una serie di regole: il Garante deve effettuare lo studio dello stato dell' evoluzione scientifica e tecnologia dello Stato in questione e delle Linee guida e raccomandazioni emanate dal Comitato europeo per la protezione dei dati personali[146]; inoltre le stesse non possono risultare come troppo o troppo poco restrittive, avendo come scopo principale la libera circolazione dei dati all'interno dell'Unione "*c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.*"[147]. Tenendo conto della rilevanza del trattamento di questo tipo di dati, le misure di garanzie devono essere poste a una previa "*3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni*" ex articolo 2-septies, comma 3 e qualora le stesse riguardino attività di diagnosi, cura e prevenzione, sarà necessario il parere del Ministro della Salute e del Consiglio superiore di sanità come disposto dal comma 6 dell'articolo corrente "*6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalita' di prevenzione, diagnosi e cura nonche' quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanita'. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche.*" Le misure possono essere adottate in qualsiasi tipo di settore purchè siano coinvolti dati genetici, biometrici o relativi alla salute, ma il disposto dell'articolo 2-septies al comma 4 presenta un elenco non tassativo di settori che devono essere disciplinati dalle misure di garanzia in modo del tutto obbligatorio "*4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da*

[146] "*Il comitato europeo per la protezione dei dati è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Il comitato europeo per la protezione dei dati è composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR), senza però che i loro rappresentanti godano del diritto di voto o di essere eletti presidente o vicepresidenti. Il comitato è istituito dal regolamento generale sulla protezione dei dati e ha sede a Bruxelles. La Commissione europea e, per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto. Il comitato si avvale di un segretariato, fornito dal GEPD. Un protocollo d'intesa definisce i termini della collaborazione tra il comitato e il GEPD.*" Il Comitato europeo per la protezione dei dati ha sostituito il già citato Gruppo di Lavoro Art. 29 dal 25 maggio 2018. In rete: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_it

[147] Articolo 2 septies, comma 2, lettera c), rinvenibile in rete: https://www.ricercagiuridica.com/codici/vis.php?num=24909

adottare relativamente a: a) contrassegni sui veicoli e accessi a zone a traffico limitato; b) profili organizzativi e gestionali in ambito sanitario; c) modalita' per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute; d) prescrizioni di medicinali". Il contenuto delle misure di sicurezza si prevede che esse debbano osservare i principi generali del trattamento e gli obblighi predisposti dichiarando però che alcuni aspetti possono regolati dalle misure di garanzia "*5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalita' del trattamento e possono individuare, in conformita' a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati*". Inoltre, data la particolare natura delle misure, il legislatore ha stabilito al comma 6 che, qualora vi sia un elevato rischio nel trattamento dei dati genetici, possa essere necessario anche il consenso dell'interessato "*6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalita' di prevenzione, diagnosi e cura nonche' quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanita'. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche*", questa disposizione dimostra come il legislatore goda di ampia discrezionalità. Al comma 7, invece, è peculiare il ruolo assegnato ai dati biometrici: essi, infatti, possono essere adoperati sia in procedure di accesso fisico che logico "7. *Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo*". Il dato biometrico si riferisce a una persona fisica e quindi è in grado di rilevarne l'identità, ed è inoltre una misura di sicurezza oggetto di una tutela stringente, in ragione del suo forte rapporto con l'identità del soggetto. Qualora si intenda perseguire le finalità sopra indicate, non sarà necessario il consenso espresso dell'interessato, poiché il legislatore ha già operato un bilanciamento preventivo, disponendo la legittimità del trattamento dei dati biometrici con finalità di accesso e sicurezza.

All'articolo 2-quater dello stesso codice, troviamo il riferimento ai codici di condotta come ulteriori fonti "*Regole deontologiche. 1. Il Garante promuove, nell'osservanza del principio di*

rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto." È quindi compito degli operatori professionali e delle associazioni rappresentative delle categorie in questione regolare le varie materie col fine di emanare le "regole deontologiche" il cui rispetto costituisce un elemento fondamentale per un trattamento dei dati lecito e corretto[148].

Si può affermare che la disciplina italiana in materia di trattamento di dati sanitari, debba essere ancora completata: un ruolo importante ricoprono le misure adottate dal Garante, e in attesa di queste, gli operatori sanitari sono obbligati dall'adottare la disciplina sopra esposta, trovando spesso parecchie incertezze dovute alla troppo genericità delle norme. Opera quindi un regime transitorio individuato dallo stesso legislatore nazionale: infatti, facendo riferimento agli articoli 20 e 21 del già citato d.lgs. 101/2018 si menzionano "le norme di continuità" con quella che era la disciplina previgente alla riforma, articolo 20 "*Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto 1. Le disposizioni del codice di deontologia e di buona condotta di cui agli allegati A.5 e A.7 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti, sino alla definizione della procedura di approvazione cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni: […]*" e articolo 21 "*Autorizzazioni generali del Garante per la protezione dei dati personali 1. Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del presente decreto, individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma è adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica. 2. Le autorizzazioni generali sottoposte a verifica a norma del comma 1 che sono state ritenute incompatibili con le disposizioni del Regolamento (UE) 2016/679 cessano di produrre effetti dal momento della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana del provvedimento di cui al comma 1*." Infatti, viene disposto che le disposizioni debbano continuare a produrre effetti fino alla pubblicazione dei

[148] Si veda il comma 4 dell'articolo corrente "4. *Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali*."

provvedimenti del Garante con cui viene sancita la piena compatibilità delle stesse con il Regolamento europeo, e le disposizioni compatibili prenderanno il nome di "regole deontologiche" che saranno pubblicate dalla Gazzetta Ufficiale della Repubblica italiana e saranno aggiunte all'allegato A del Codice in materia di protezione dei dati personali da parte del Ministro della Giustizia.

Quindi finché la disciplina italiana non sarà completamente finita, gli operatori professionali dovranno applicare i codici deontologici, le Linee guida del Garante e i suoi provvedimenti e le autorizzazioni sempre richiedendo la loro compatibilità con il Regolamento europeo. È doveroso notare, infatti, come in questo regime di transizione, operi più che mai, il principio di *accountability*, ovvero la valutazione di quali regole seguire è totalmente rimessa a coloro che effettuano il trattamento.

2.4 Il Garante per la protezione dei dati personali e la sua attività nell'ambito dei dati sanitari.

Dopo aver esaminato la disciplina del Regolamento 679/2016 e aver osservato la sua influenza su quella che è la disciplina circa il trattamento dei dati personali in ambito sanitario, ora, per completezza, è necessario esprimersi sull'autorità che esercita il proprio controllo sulla materia in questione.

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente[149], autorità prevista anche dalla Convenzione di Strasburgo[150], ed istituita dalla "Legge sulla privacy" n. 675 del 31 dicembre 199, poi menzionata anche dal Codice in materia di protezione dei dati personali, introdotto con il d.lg. n.196 del 30 giugno 2003 ma modificato dal Decreto legislativo n.101 del 10 agosto 2018. Quest'ultimo strumento, inoltre, ha dichiarato che il Garante per la protezione dei dati personali è l'autorità di controllo che provvede anche all'attuazione del Regolamento generale sulla protezione dei dati personali[151]. È un organo collegiale che è formato da quattro membri, di cui metà eletti soni eletti dalla Camera dei deputati e l'altra metà dal Senato della Repubblica, tra di loro viene designato un Presidente e la durata del mandato dei membri è di sette anni, non rinnovabile. L'articolo 154 del Codice della privacy attribuisce a questa autorità una moltitudine di compiti " […] *a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico; b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalita' specifiche per la trattazione, nonche' fissando annualmente le priorita' delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di*

[149] "*Le autorità amministrative indipendenti esercitano funzioni di controllo e regolamentazione in settori considerati particolarmente sensibili o ad alto contenuto tecnico. In questi casi, è richiesta una condizione di autonomia allo scopo di garantire la neutralità nei confronti degli interessi pubblici e privati coinvolti.*
Questi organismi sono istituiti da specifiche leggi ed hanno poteri normativi, di vigilanza, sanzionatori e di risoluzione delle controversie. Nonostante non vi sia una disciplina organica a regolarne il funzionamento, un tratto comune a tutte le autorità è il ruolo di indipendenza nei confronti del potere politico, che comunque ne nomina i vertici." Definizione rinvenibile nell'articolo "Quante sono le autorità amministrative indipendenti. Sono soggetti sottratti al controllo diretto del governo chiamati a regolare settori ritenuti particolarmente delicati e ad alto contenuto tecnico." Aggiornato venerdì 19 Giugno 2020 in rete: https://www.openpolis.it/parole/quante-sono-le-autorita-amministrative-indipendenti/

[150] Convenzione n. 108 sulla protezione delle persone rispetto l trattamento automatizzato dei dati di carattere personale adottato il 28 gennaio 1981 a Strasburgo. "*"Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)"*. In rete: https://protezionedatipersonali.it/convenzione-108-consiglio-europa

[151] Si veda il paragrafo 2 del capitolo 2.

riferimento; c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-quater; d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni; e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce; f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice; g) provvedere altresi' all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento. […]". Il potere di controllo del Garante, viene esplicato nello specifico all'articolo 158, al comma 5 " […] *Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresì riguardare reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on-line. A tal fine, viene redatto apposito verbale in contradditorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento*.", esso può quindi chiedere al titolare e al responsabile del trattamento di dati l'esibizione di documenti e informazioni, effettuare delle ispezioni e delle verifiche, effettuando un'attività simultanea a quella della Guardia di finanza come sancito dall'articolo 1 del "Protocollo d'intesa relativo ai rapporti di collaborazione tra il Garante per la protezione dei dati personali e la Guardia di finanza" [152]"*In attuazione delle disposizioni richiamate nel preambolo del presente Protocollo d'intesa, il Garante, per l'accertamento delle violazioni alla normativa in materia di trattamento dei dati personali, si avvale della collaborazione della Guardia di Finanza. In particolare, la Guardia di Finanza collabora alle attività ispettive attraverso: a. il reperimento di dati e informazioni sui soggetti da controllare; b. la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento; c. l'assistenza nei rapporti con l'Autorità Giudiziaria; d. lo sviluppo di attività delegate o sub-delegate per l'accertamento delle violazioni in materia di protezione dei dati personali; e. la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate; f. la partecipazione di proprio personale, a richiesta del Garante, a ispezioni congiunte con autorità di protezione dei dati personali appartenenti ad altri Paesi*. […]".

[152] "PROTOCOLLO D'INTESA RELATIVO AI RAPPORTI DI COLLABORAZIONE TRA IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E LA GUARDIA DI FINANZA" Roma, 10 marzo 2016 per la Guardia di Finanza Gen. C.A. Saverio Capolupo per il Garante per la protezione dei dati personali Il Presidente Dott. Antonello Soro rinvenibile in rete: https://www.garanteprivacy.it/documents/10160/0/Protocollo+di+intesa+tra+Garante+per+la+protezione+dei+dati+personali+e+Guardia+di+finanza+del+10+marzo+2016.pdf/38d5e81d-0d31-9763-f78b-05f3f33ff195?version=1.1

Un ulteriore potere del Garante è il potere consultivo, infatti, il Presidente del Consiglio dei ministri e i Ministri hanno l'obbligo di interpellare il Garante qualora dovessero porre atti predisponenti norme regolamentari e atti amministrativi che possano in qualche modo incidere su quanto stabilito dal Codice sulla protezione dei dati personali. A esso spetta inoltre il compito di adottare le necessarie misure affinché i trattamenti siano conformi alle norme vigenti e può vietare e bloccare un trattamento che risulti illecito. Qualora il trattamento illecito sia comunque predisposto e attuato, si incorrerà nel reato di cui all'articolo 170 del d.lgs. 30 giugno 2003 n. 196 che prevede "*1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.*"[153], e la violazione dei provvedimenti disposti dall'Autorità, implicava l'applicazione della sanzione amministrativa prevista dall'articolo 162, comma 2-ter del d.lgs. 30 giugno 2003, n. 196 "[…] *2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro* […]."[154], articolo poi abrogato dal d.lgs. 10 agosto 2018, n. 101.

Un aspetto essenziale che garantisce al Garante la sua autorità è il fatto che il Codice della privacy ne afferma "*la piena autonomia*" e "*l'indipendenza di giudizio e di valutazione*", ponendo quindi il carattere della terzietà e imparzialità come elementi costitutivi della figura. L'indipendenza del Garante è data dall'indennità di funzione e dal divieto assoluto per i membri di ricoprire il ruolo di amministratore o di dipendente di enti pubblici o privati, di esercitare attività di consulenza o professionali o di ricoprire cariche elettive. Per quanto riguarda le spese proprie del Garante, è previsto un fondo apposito nel bilancio dello Stato, presentando un

[153] "Articolo 170 - Inosservanza di provvedimenti del Garante (Decreto legislativo n° 196, 30 giugno 2003)" Testo dell'articolo rinvenibile online: https://www.medicoeleggi.com/argomenti00/italia8/16470.htm
[154] Articolo rinvenibile in rete: https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-i/art162.htm

rendiconto circa la sua gestione finanziaria che sarà soggetto all'attività di controllo[155] esercitato dalla Corte dei conti ex articolo 100[156] della Costituzione italiana.

Dopo la riforma del 2018 però, si continua ad avere una certa libertà per quanto riguarda la redazione del rendiconto, mentre l'articolo 156, paragrafo 8 del Regolamento, dispone che i bilanci annuali del Garante debbano essere inclusi nei bilanci generali statali. "*8. Le spese di funzionamento del Garante, in adempimento all'articolo 52, paragrafo 4, del Regolamento, ivi comprese quelle necessarie ad assicurare la sua partecipazione alle procedure di cooperazione e al meccanismo di coerenza introdotti dal Regolamento, nonché quelle connesse alle risorse umane, tecniche e finanziarie, ai locali e alle infrastrutture necessarie per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposita missione e programma di spesa del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti. Il Garante può esigere dal titolare del trattamento il versamento di diritti di segreteria in relazione a particolari procedimenti*."

Il Garante per la protezione dei dati personali intende quindi, comunicare a una serie di destinatari, alle Regioni e alle autorità in materia sanitaria, e invita tutti a dare massima diffusione di quanto dispone, effettuando chiarimenti circa la disciplina in ambito sanitario adottato il 7 maro del 2019. L'articolo 57 del Regolamento pone infatti i compiti del Garante, stabilendo che esso *"[…] b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori; c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e*

---

[155] "*Si tratta di un controllo esterno e neutrale svolto in posizione di assoluta imparzialità rispetto agli interessi di volta in volta perseguiti dal governo o dall'amministrazione. Accanto a dette funzioni, individuate in modo diretto dall'art. 100 della Costituzione, ve ne sono altre, introdotte da leggi ordinarie, che trovano il loro fondamento costituzionale nell'art. 97 della Costituzione (principio del buon andamento degli uffici pubblici), nell'art. 81 (rispetto degli equilibri di bilancio) e nell'art. 119 (coordinamento della finanza pubblica). In particolare, la legge 14 gennaio 1994 n. 20 ha attuato una riforma completa delle funzioni di controllo della Corte dei conti, riducendo il numero degli atti sottoposti al controllo preventivo di legittimità ed introducendo una nuova forma di controllo successivo sulla gestione del bilancio e del patrimonio delle amministrazioni pubbliche, nonché sulle gestione fuori bilancio e sui fondi di provenienza comunitaria, improntata ai parametri di economicità ed efficacia che debbono sempre ispirare l'azione amministrativa (legge 7 agosto 1990 n. 241)*" L'attività di controllo della Corte dei Conti, rinvenibile in rete sul sito ufficiale : https://www.corteconti.it/Home/Attivita/Controllo

[156]Articolo 100 della Costituzione italiana: "*Il Consiglio di Stato è organo di consulenza giuridico-amministrativa e di tutela della giustizia nell'amministrazione.*
La Corte dei conti esercita il controllo preventivo di legittimità sugli atti del Governo, e anche quello successivo sulla gestione del bilancio dello Stato. Partecipa, nei casi e nelle forme stabiliti dalla legge, al controllo sulla gestione finanziaria degli enti a cui lo Stato contribuisce in via ordinaria. Riferisce direttamente alle Camere sul risultato del riscontro eseguito.
La legge assicura l'indipendenza dei due Istituti e dei loro componenti di fronte al Governo." Articolo rinvenibile in rete: https://www.mondadorieducation.it/media/contenuti/pagine/campus_economico_giuridico/02_discipl_giuridiche/2_biennio/10_costituzione_commentata/articoli/art100.html

istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento; […] d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;[…] " Funzione cui il Garante assolve tramite comunicazioni o convegni, quindi, non servendosi di provvedimenti di natura normativa o prescrittiva diretta, bensì esso mira a promuovere la consapevolezza di coloro che costituiscono il pubblico utente dei servizi sanitari ma anche dei titolari e dei responsabili del trattamento. Si può affermare quindi che l'attività posta in essere dal Garante rappresenta una forma di ammonimento per i soggetti del trattamento, infatti, qualora essi non seguano quanto disposto dall'Autorità, saranno destinatari di sanzioni. Il Garante, quindi, ha inteso intervenire poiché in ambito sanitario, a seguito della normativa e del d.lgs. 101 del 10 agosto 2018, la disciplina risultava piuttosto lacunosa, situazione del tutto inammissibile considerando la delicatezza della stessa, poiché riguardante il settore sanitario, il diritto personalissimo alla salute e il diritto alla protezione del dato sanitario, che la vecchia normativa definiva come "sensibile" e che invece oggi viene sancito come "dato relativo alla salute" ex articolo 9 del GDPR[157].

Meritevole di trattazione è il provvedimento del Garante del 7 marzo 2019 n. 9091942 sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario: tramite esso il Garante ha inteso chiarire la disciplina dei decreti precedenti. Infatti, nella premessa del documento è possibile rinvenire il riferimento al d.lgs. 101/2018 "[…] *Il decreto legislativo n. 101/2018, in vigore dal 19 settembre 2018, ha previsto, al riguardo, che il Garante completi l'individuazione dei presupposti di liceità dei suddetti trattamenti, adottando specifiche misure di garanzia e promuovendo l'adozione di regole deontologiche (artt. 2-septies e 2-quater del Codice).* […]". Detto decreto ha inteso introdurre un regime transitorio e le disposizioni di attuazione, e questo regime è stato attuato dal Garante tramite il provvedimento del 13 dicembre del 2018, con il quale l'Autorità ha stabilito che le prescrizioni delle vecchie autorizzazioni della normativa previgente, rimangono applicabili. Il secondo provvedimento è quello del 19 dicembre del 2018, riguardante i codici di deontologia, di rilevante importanza perché il settore sanitario è governato dai suddetti codici. "*Analogamente, con provvedimento del 19 dicembre 2018 (doc. web n.9069637), il Garante ha provveduto alla verifica della conformità delle disposizioni contenute nei Codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, statistici, scientifici al Regolamento e alla loro conversione in regole deontologiche, il cui rispetto costituisce condizione essenziale per la liceità e correttezza del*

[157] Si veda il paragrafo 2 del capitolo 2.

trattamento dei dati personali (art. 2-quater del Codice)." Nonostante gli articoli 2-quater[158] e 2-septies[159] de d.lgs. 196/2003, "*Sebbene il quadro regolatorio, come sopra evidenziato, non sia ancora definitivo, l'Autorità ritiene opportuno fornire alcuni chiarimenti sull'applicazione della disciplina di protezione dei dati in ambito sanitario*", il Garante, anche se non ha adottato le disposizioni di cui sopra, intende intervenire con questo provvedimento, inteso come uno strumento più soft e meno strutturato, per fornire indicazioni precise agli utenti e ai soggetti del trattamento.

Come è stato esposto nei capitoli precedenti, la disciplina del Regolamento 679/2016 prevede all'articolo 6 le condizioni di liceità del trattamento, pertanto si rimando alle pagine seguenti. Ciò che interessa qui puntualizzare è che in ambito sanitario, non siamo in presenza di dati generici ex articolo 6, ma occorre una disciplina diversa per i "dati extrasensibili"[160]. All'articolo 9, sono presenti i tre casi di legittimazione del trattamento al comma 2, di cui il Garante, tramite il Provvedimento del 7 marzo 2019, fa esplicito riferimento, sottolineando l'ambito applicativo nel settore sanitario "*1. Disciplina per il trattamento dei dati relativi alla salute in ambito sanitario. Le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per: a. motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice; b. motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi*

[158] Testo articolo 2- quater del d.lgs. 196/2003 "1. *Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto. 2. Lo schema di regole deontologiche e' sottoposto a consultazione pubblica per almeno sessanta giorni. 3. Conclusa la fase delle consultazioni, le regole deontologiche sono approvate dal Garante ai sensi dell'articolo 154-bis, comma 1, lettera b), pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice. 4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.*" In rete: https://www.cyberlaws.it/2018/articolo-2-quater-nuovo-codice-privacy-d-lgs-196-2003-agg-d-lgs-101-2018/

[159] Testo articolo 2-septies del d.lgs. 196/2003 "*1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformita' alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo. 2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 e' adottato con cadenza almeno biennale e tenendo conto:* ***a)*** *delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;* ***b)*** *dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;* ***c)*** *dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.*" In rete: https://www.cyberlaws.it/en/2018/art-2-septies-d-lgs-196-2003/

[160] "Privacy e sanità nel Provv. Garante n. 55 del 7 marzo 2019 (18 marzo 2019)" di Simone Chiarelli, rinvenibile in rete: https://www.youtube.com/watch?v=WqmcwaJ6g-8

minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare); c. finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza."[161] Il Garante, inoltre, dispone che il principio generale prevede che al di fuori delle cause sopracitate, da interpretare sempre in senso restrittivo, occorre impiegare un altro titolo di legittimazione del trattamento, il consenso, che dovrà necessariamente essere espresso in modo più puntuale, calcolando la delicatezza e l'importanza di questo tipo di dati, rispetto ai dati generali. Nel provvedimento, infatti, troviamo espliciti esempi "*a. trattamenti connessi all'utilizzo di App mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale (cfr. Faq CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità(1))*;" Nel caso in questione, un'App medica non ha una finalità di cura, quindi qualora un operatore sanitario volesse far scaricare al cliente un'applicazione della sua struttura, proprio perché non ha la finalità richiesta, dovrà necessariamente avere il consenso dell'assistito. Inoltre, anche "*b. trattamenti preordinati alla fidelizzazione della clientela*", "*c. trattamenti effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali*", "*d. trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali (cfr. provv. del 6 marzo 2014, doc. web n. 3013267)*" e da ultimo "*e. trattamenti effettuati attraverso il Fascicolo sanitario elettronico (d.l. 18 ottobre 2012, n. 179, art. 12, comma 5)*".

Altro elemento rilevante trattato dal Garante è quello dell'informativa. "*Con specifico riferimento all'attività posta in essere da titolari del trattamento operanti in ambito sanitario che effettuano una pluralità di operazioni connotate da particolare complessità (es. aziende sanitarie), si ritiene opportuno suggerire di fornire all'interessato le informazioni previste dal*

[161] Si rimanda al testo integrale del Provvedimento 7 marzo 2019 n. 9091942, in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942

Regolamento in modo progressivo. Ciò significa che nei confronti della generalità dei pazienti afferenti a una struttura sanitaria potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie (cfr. art. 79 del Codice). Gli elementi informativi relativi a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici on-line, finalità di ricerca) potrebbero essere resi, infatti, in un secondo momento, solo ai pazienti effettivamente interessati da tali servizi e ulteriori trattamenti. Ciò andrebbe a beneficio di una maggiore attenzione alle informazioni veramente rilevanti, fornendo la piena consapevolezza circa gli aspetti più significativi del trattamento." La stessa ricopre un ruolo fondamentale nei dati sensibili e soprattutto nel contesto di coloro che gestiscono tutto il complesso dei dati sensibili, come nel settore sanitario. Il Garante, perciò, pone dei suggerimenti di disciplina, in verità già contenuti nel d.lgs. 101/2018, ponendo però un tipo di informativa cosiddetta "*progressiva*", ovvero, il paziente, in caso di una moltitudine di prestazioni mediche eseguite nella stessa struttura sanitaria, dovrà ricevere di volta in volta un'informativa diversa, quindi ricevere istruzioni dettagliate per quella singola operazione che intende seguire (ad esempio analisi del sangue, risonanze magnetiche ecc.). Si richiama quindi, il concetto di "*consenso granulare*"[162] proprio del Regolamento 679/2016. Ovviamente nel caso di rilascio di ogni informativa, qualora un trattamento non sia tra quelli menzionati dall'articolo 9, dovrà necessariamente essere correlato al consenso dell'assistito.

Ulteriore elemento che il Garante pone come obbligatorio in caso ai soggetti che intendono svolgere attività di trattamento dati in ambito sanitario, è la nomina all'interno della struttura di un Data Protection Officer (DPO) introdotto dalla nuova normativa sui dati personali, ovvero il responsabile per la protezione dei dati personali, ovvero un organismo di vigilanza che deve affiancare il titolare dell'azienda per la corretta applicazione del GDPR. Il DPO è nominato in modo obbligatorio nei casi previsti dall'articolo 37 del Regolamento 679/2016 e, nell'ambito sanitario oggetto di trattazione, il Garante ha previsto che "*In generale, si ritiene che i trattamenti dei dati personali relativi a pazienti effettuati da un'azienda sanitaria appartenente al SSN devono essere ricondotti a quelli per i quali è prevista la designazione obbligatoria del RPD, sia in relazione alla natura giuridica di "organismo pubblico" del titolare, sia in quanto*

[162]"*Che il soggetto interessato deve poter esprimere il suo consenso al trattamento dei dati non necessariamente con riferimento a tutte le tipologie di trattamento. Deve poter accettare in riferimento a delle specifiche finalità e non ad altre. Ad esempio, può acconsentire per i cookies tecnici e riufiutare il consenso per le finalità di marketing*." Articolo "*GDPR e consenso granulare nell'European Data Protection Board (Edpb) del 4 maggio 2020 "L'Edpd chiarisce l'accettazione dei cookies da parte dell'utente in un sito web. È richiesto il consenso esplicito e l'accettazione granulare dei cookie mentre viene negata la validità dell'accettazione tramite scrolling e swipe o tramite un banner che permette l'accettazione in blocco dei cookies. Pena una sanzione salata*." In rete: https://seocrate.it/blog/gdpr-e-consenso-granulare-nell-european-data-protection-board-di-maggio-2020/

rientrano nella condizione prevista dall'art. 37, par. 1, lett. c), considerato che le attività principali del titolare consistono nel trattamento, su larga scala, di dati sulla salute. Si ritiene che anche il trattamento dei dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da una residenza sanitaria assistenziale (RSA) possa rientrare, in linea generale, nel concetto di larga scala. (Linee guida sui Responsabili della protezione dei dati, WP243, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, punto 2.1.3, doc. web n. 612048, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, cfr. Endorsement n. 1/2018)." Quindi un ospedale privato o una clinica dovranno per forza servirsi della consulenza e dell'assistenza del responsabile del trattamento dei dati, discorso diverso vale invece per i poliambulatori o per i singoli professionisti, per i quali non vige alcun obbligo di nomina.

L'ultimo elemento posto dal Garante come essenziale ai fini di un'attività uniforme a quanto disposto dalla disciplina comunitaria è l'obbligo del Registro delle attività di trattamento "*Con riferimento a questo adempimento si rappresenta, in linea generale, la sussistenza di tale obbligo in ambito sanitario. Tale posizione tiene conto del fatto che, essendo le fattispecie di esenzione di cui all'art. 30, par. 5 del Regolamento tra loro alternative (cfr. Gruppo di lavoro Art. 29 per la protezione dei dati - Position paper related to article 30(5), fatte proprie dal Comitato europeo per la protezione dei dati-Endorsement n. 1/2018), la deroga alla tenuta del registro non opera in presenza anche di uno solo degli elementi indicati dal predetto par. 5 (trattamento che presenta un rischio per i diritti e le libertà per l'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati). Ciò, in coerenza con la circostanza che il registro delle attività del trattamento costituisce uno strumento di accountability e di gestione del rischio*." Quindi, se l'attività è professionale e non occasionale, tutti i trattamenti posti dovranno essere contenuti all'interno del Registro.

L'unica circostanza in cui tale obbligo non sussiste, è quella che prevede un'attività professionale in assenza sia di dipendenti sia di fidelizzazione di clienti, poiché del tutto sfornita di trattamento dati. L'adempimento all'obbligo di Registro risulta essere autonomo, ma è uno strumento di così evidente rilevanza che costituisce il primario strumento per la soddisfazione del principio di *accountability,* poiché tramite lo stesso, il titolare del trattamento sarà in grado di dimostrare a tutti i soggetti coinvolti e soprattutto anche al Garante medesimo, di aver posto in essere un trattamento lecito e assolutamente conforme alla normativa *privacy*.

In conclusione, lo scopo di tale provvedimento, ma anche di tutti i provvedimenti che sono posti dal Garante, è quello di promuovere la consapevolezza e la giusta applicazione della normativa vigente, tramite anche convegni, riunioni e *newsletter* dell'Autorità.

Un altro esempio di intervento dell'attività del Garante, di estrema attualità, è stato il suo parere positivo sul decreto attuativo per l'attivazione della "Piattaforma nazionale-DGC"[163] che prevede il rilascio del Green Pass, introdotto dal decreto "Riaperture" firmato dal Presidente Draghi il 17 giugno 2021, a seguito della pandemia da Covid-19 e della campagna vaccinale in Italia, per consentire gli spostamenti e l'accesso ai luoghi pubblici. Inizialmente, l'Autorità aveva addirittura sanzionato il Governo italiano perché questi, nella sua prima versione di *green pass*, non aveva informato il Garante circa gli aspetti che riguardavano il trattamento dei dati. La consultazione del Garante è un obbligo di legge ogni volta che venga emesso un provvedimento che abbia ad oggetto i dati personali e quindi l'Autorità aveva emesso un ammonimento nei confronti del nostro Governo: in particolare era stato rilevato che nella prima versione del green pass non era stato rispettato il principio della minimizzazione dei dati, non erano chiare le misure di sicurezza del trattamento e non erano specificati né il titolare del trattamento né i soggetti autorizzati al controllo della certificazione. Nel mese di Luglio del 2021 il Garante ha dato il suo *placet* sulla seconda versione del green pass presentata dal Governo italiano. L'autorità, ovviamente, ha presentato al Governo italiano i punti critici del decreto, disponendo che il carattere della chiarezza delle disposizioni risultano essenziali per capire quando effettivamente possa essere richiesto alla persona di dover esibire la certificazione in questione per consentirle l'accesso. La poca chiarezza di quanto disposto all'inizio, infatti, ha fatto in modo che le Regioni e le Province autonome richiedessero l'uso della certificazione per ulteriori scopi, rendendo necessario l'intervento del Garante. Lo stesso ha sostenuto che il Regolamento europeo sul *green pass*, già prevede che gli Stati possano utilizzarlo per ulteriori scopi ma solo in presenza di una norma nazionale che lo preveda espressamente. Inoltre, il Garante esige estrema chiarezza per quanto riguarda le finalità del green pass che dovranno essere stabilite necessariamente a priori: la certificazione potrà essere rilasciata solo dalla Piattaforma nazionale-DGC e dovrà essere verificata attraverso l'App VerificaC19, poiché risulta l'unico modo idoneo per verificare l'attendibilità di quanto dichiarato dalla certificazione, garantendo allo stesso tempo la protezione dei dati personali e sanitari, poiché coloro che richiederanno di esibire il green pass potranno venire a conoscenza solo delle generalità della persona senza conoscere alcunché circa

[163] "*È una Certificazione in formato digitale e stampabile, emessa dalla piattaforma nazionale del Ministero della Salute, che contiene un QR Code per verificarne autenticità e validità*" Pagina "RIPARTIAMO IN SICUREZZA. La Certificazione verde COVID-19 permette di accedere a eventi, strutture e altri luoghi pubblici in Italia e facilita gli spostamenti in Europa. #EUCOVIDCertificate" in rete: https://www.dgc.gov.it/web/, visto in agosto 2021.

la sua anamnesi remota. La grande novità è che la certificazione avrà sia un formato analogico, sia un formato digitale poiché sarà messa a disposizione tramite strumenti digitali come "*il sito web della Piattaforma nazionale-DGC il Fascicolo sanitario elettronico la App Immuni e la App IO*", e gli interessati saranno in grado, quindi, di visualizzare la certificazione.

Nel Giungo 2021, inoltre, il Garante è intervenuto[164] sostenendo che esibire il proprio *green pass* in modo non idoneo, ad esempio attraverso la sua condizione sui social network, risulterebbe piuttosto pericoloso, poiché il "*qr code*", la veste del *green pass*, apparentemente incomprensibile, è assolutamente in grado di fornire molteplici dati circa la salute e la vaccinazione contro il Covid-19 eseguita, dati del tutto personalissimi, ma non solo, in questo modo si potrebbe dare opportunità a un terzo di poter copiare il green pass e quindi di fornirsi e divulgare certificazioni false, eludendo il disposto del decreto. Si noti quindi come l'attività del Garante sia abbastanza decisiva per quanto riguarda ogni forma di decisione o strumento che abbia ad oggetto il dato, personale o sanitario, ponendo come unico obiettivo del suo ruolo, una corretta gestione dei dati e la loro massima tutela, in linea con quanto disposto e richiesto dal Regolamento comunitario, e con quanto reso necessario dalla sempre più presente tecnologia nel quotidiano.

Il ruolo del Garante, inoltre, è stato di fondamentale importanza anche per quanto riguarda i criteri per la conservazione dei dati, ovvero i tempi e i modi che ovviamente saranno diversi a seconda della natura del dato oggetto di trattamento.

È necessario definire innanzitutto cosa si intende per *data retention*, ovvero il periodo di conservazione dei dati, posta dal Regolamento UE n.679/2016. Di fatto, il Regolamenti, non ha posto nulla di nuovo rispetto a quanto disposto dal Codice Privacy, che all'articolo 11 prevedeva " […] *b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; […] e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. […]".*

Dal testo del Regolamento, si possono desumere due principi in tema di conservazione dei dati: il primo viene definito come il "principio della limitazione della conservazione" disposto dall'articolo 5, paragrafo 1 lettera e, che prevede "*e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più*

[164] "*Pericoloso mettere sui social il Qr-Code del green pass, l'allarme del Garante Privacy*" Intervento di Guido Scorza, Componente del Garante per la protezione dei dati personali (Agenda Digitale, 24 giugno 2021), in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9673513

lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);" e il "principio di minimizzazione", desunto dal combinato degli articolo 5 e 6 del Regolamento, si pone quindi l'esigenza di condizioni di liceità e finalità idonea a raggiungere lo scopo per il quale i dati sono raccolti.

I dati, anche quelli sanitari oggetto di trattazione, possono essere conservati sia tramite supporti cartacei, sia tramite strumenti digitali, tenendo presente che in quest'ultima modalità non è propriamente corretto parlare poi di distruzione di documento, essendo un dato informatico praticamente indistruttibile. Il Garante è quindi intervenuto per regolamentare quali sono i parametri ufficiali e uniformi contenenti i tempi e le modalità di conservazione dei dati. Fondamentale per la definizione degli stessi è stato l'apporto delle Associazioni di categoria e degli Ordini professionali, che, conoscendo le esigenze del proprio settore, sono in grado di fornire gli elementi indispensabili per una corretta disciplina, conoscendo anche quelle che potrebbero costituire eventuali problematiche derivanti da una conservazione non adeguata al tipo di dato in questione, rendendo necessario spesso un bilanciamento.

Per definire il computo del periodo di conservazione dei dati bisogna volgere lo sguardo agli obblighi di legge, che possono derivare sia da obblighi nazionali sia internazionali, dalle pronunce delle autorità come il Garante ma anche delle Associazioni di categoria o le Pubbliche Amministrazioni e dell'esperienza della dottrina.

Il Garante ha effettuato una precisazione: la conservazione dei documenti sanitari è ben diversa dalla conservazione dei dati sanitari, differenza riscontrabile nel Regolamento 679/2016 tra i documenti digitali o digitalizzati e i documenti cartacei.

Per quanto riguarda la procedura è indispensabile predisporre una "politica di conservazione dei dati" anche detta "*Data Retention Policy*" e poi una "procedura di conservazione dei dati", contenente indicazioni specifiche per quanto riguarda le modalità di conservazione e le tempistiche massime della conservazione. Il contenuto della politica di conservazione dei dati prevede: la fissazione delle modalità di comunicazione della stessa da parte del Titolare del trattamento a tutti gli interessati, la predisposizione di un sistema di controllo idoneo a controllare periodicamente i dati contenuti ed eventualmente cancellarli qualora il tempo sia scaduto, la modalità di cancellazione dei dati prefissata tra il Titolare e i tecnici e le sanzioni da applicare qualora non dovessero essere rispettate le misure poste, comportando o la revoca o la sospensione

dell'accesso della persona in questione ai sistemi dell'azienda. Inoltre, l'Autorità ha posto vari chiarimenti per quanto riguarda i tempi di conservazione della documentazione sanitaria[165]. Nel nostro ordinamento, infatti, si prevede che i tempi di conservazione del materiale sanitario nei vari archivi siano del tutto differenziati rispetto ad altri settori: il tempo della documentazione sarà quindi dettato dalla natura propria del documento che implicherà l'adozione di una normativa specifica ad opera dell'operatore sanitario, sia esso pubblico o privato.

Prima di procedere con la trattazione della conservazione del documento sanitario, è doveroso effettuare una precisazione tra cartella clinica e documentazione radiologica. La prima deve essere conservata insieme ai propri referti "illimitatamente"[166], e se si dovesse definire la cartella clinica, si potrebbe affermare che essa "*un atto pubblico che esplica la funzione di diario dell'intervento medico e dei relativi fatti clinici rilevanti, sicché i fatti devono essere annotati conformemente al loro verificarsi*" ed è "*caratterizzata dalla produttività di atti costitutivi, traslativi, modificativi o estintivi rispetto a situazioni giuridiche soggettive di rilevanza pubblicistica, nonché dalla documentazione di attività compiute dal pubblico ufficiale che redige l'atto*" [167]. Inoltre, l'articolo 26 del Codice di deontologia medica prescrive "*La cartella clinica delle strutture pubbliche e private deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica e contenere, oltre ad ogni dato obiettivo relativo alla condizione patologica e al suo decorso, le attività diagnosticoterapeutiche praticate. La cartella clinica deve registrare i modi e i tempi delle informazioni nonché i termini del consenso del paziente, o di chi ne esercita la tutela, alle proposte diagnostiche e terapeutiche; deve inoltre registrare il consenso del paziente al trattamento dei dati sensibili, con particolare riguardo ai casi di arruolamento in un protocollo sperimentale*". Quindi la cartella clinica contiene l'anamnesi remota dello stato di salute del paziente, e ogni annotazione effettuata dal medico ha un suo valore documentale definitivo e qualora essa venga in qualche modo contraffatta, si veda l'applicazione delle sanzioni di cui agli articoli 476 e 479 del codice penale, poiché qualsiasi modifica effettuata sarà considerata come un falso. Questo documento infatti, ha l'efficacia probatoria propria dell'articolo 2700 del codice civile "*L'atto pubblico fa piena prova(1), fino a querela di falso, della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché delle dichiarazioni delle parti e degli altri fatti che il pubblico*

[165] Dematerializzazione della documentazione clinica - 26 novembre 2009 [1688961] del 26 novembre del 2009, in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1688961

[166] "*Le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico-sanitario*". Circolare del Ministero della Sanità del 19 dicembre 1986 n.900 2/AG454/260, in rete: https://www.omceo.me.it/sportello/professione/cartella/archivi.pdf

[167] Definizione offerta da "*La dematerializzazione dei documenti sanitari*" Autore: Perfetti Telesio In: Diritto civile e commerciale in rete: file:///C:/Users/Utente/Downloads/la-dematerializzazione-dei-documenti-sanitari.pdf, visto in agosto 2021

ufficiale attesta avvenuti in sua presenza o da lui compiuti.", quindi deve essere considerata come "*un atto pubblico certificativo e munito di fede privilegiata*", poiché firmato e attestato dall'operatore sanitario come pubblico ufficiale. Avendo posto gli elementi essenziali della cartella clinica, si può affermare che sono possibili eventuali correzioni tramite apposita rettifica o integrazione, a condizione che le stesse siano facilmente individuabili e visibili tramite il loro inserimento tra due parentesi, e successivamente sottoscrivere il documento tramite il timbro, firma e indicare la data.

L'ulteriore modo di conservazione è la documentazione radiologica che ai sensi del D.M. del 14 febbraio 1997 si pone la distinzione tra l'iconografica radiologica che deve essere conservata per un periodo non inferiore a dieci anni, e il referto radiologico che deve essere conservato illimitatamente. L'articolo 3 del D.M. 14.2.97 definisce la documentazione radiologica come "*1. La documentazione disciplinata dal presente decreto e di cui al precedente art. 1, e' cosi' stabilita: a) documenti radiologici e di medicina nucleare: consistono nella documentazione iconografica prodotta a seguito dell'indagine diagnostica utilizzata dal medico specialista nonche' in quella prodotta nell'ambito delle attivita' radiodiagnostiche complementari all'esercizio clinico; b) resoconti radiologici e di medicina nucleare: la documentazione del presente punto consiste nei referti stilati dal medico specialista radiologo o medico nucleare*." E lo stesso decreto si occupa all'articolo 5 di regolare i modi di acquisizione disponibilità e archiviazione delle rappresentazioni iconografiche "*1. Con il presente decreto viene stabilito che il riferimento di archivio che dovra' essere utilizzato per la documentazione di cui al precedente art. 3 deve coincidere con quello riportato nel decreto emanato ai sensi dell'art. 114 del decreto legislativo 17 marzo 1995, n. 230 e relativo alle prestazioni effettuate su pazienti e riportate: sia nel registro delle indagini e dei trattamenti con radiazioni ionizzanti; sia nel libretto radiologico personale. 2. Il riferimento di archivio deve essere tale che non vi siano dubbi ne' del paziente, ne' dell'esame espletato, ne' della struttura che ha erogato la prestazione*."[168]

La disciplina generale del Garante, prevede che debba essere il Titolare del trattamento a definire i tempi di conservazione dei dati sanitari a seconda della finalità, quindi le tempistiche saranno tutta la durata del trattamento in più dieci anni, considerando la prescrizione civile. Qualora ad esempio, il paziente non dovesse più recarsi presso la struttura sanitaria che detiene la sua documentazione e l'operatore sanitario debba comunque conservarla, in questo caso esso potrà conservare i dati anche oltre dieci anni, come stabilito dal Regolamento, la cui applicazione interviene ogniqualvolta la disciplina appaia poco chiara. Quindi, per garantire un'adeguata disciplina circa la conservazione e la documentazione dei dati svolgono un ruolo fondamentale

[168] Testi degli articoli rinvenibili in rete: https://www.unipd.it/rpx/Legislazione/Lex_14_2_97_doc_rad.html

le misure tecniche emanate come norme dal Regolamento, che devono necessariamente essere seguite sia dai pazienti che dal personale medico. Con il DPCM 11/2014 in G.U. del 12 gennaio 2015, si introdusse per la prima volta la definizione di "Metadati", ovvero "*insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto*."[169] In ambito radiologico, quando vi sono delle modificazioni che vengono trasferite sui sistemi Picture Archiving and Communication System (PACS)[170], la modificazione deve riferirsi in modo univoco a quel determinato paziente con quella determinata storia clinica, in questo modo, non solo il referto sarà contenuto nella giusta cartella clinica, ma saranno anche applicati i metadati al documento informatico con il fine anche di registrare tutti gli accessi alla stessa per permettere di effettuare un controllo qualora ce ne fosse bisogno e sapere chi è stato il reale autore delle modifiche.

Per la conservazione di dati esiste una procedura apposita, definita anche come "una misura organizzativa e di accountability" per garantire gli oneri posti dal Regolamento e dal Garante. Vi sono procedure sia per la gestione degli archivi cartacei sia per la gestione delle modalità digitali, nettamente più complesse. Si può affermare che entrambe le procedure prevedono disposizioni ben specifiche circa "*la creazione, consultazione, archiviazione e distruzione*": ad esempio, per quanto riguarda gli accessi agli archivi, fisici e digitali, sono richieste informazioni ben specifiche, o ad esempio in capo a chi è designato come responsabile dell'archivio vi è la responsabilità per ogni tipo di accesso non autorizzato, ma ancora vi è l'obbligo di porre delle misure necessarie per evitare un possibile danneggiamento dei documenti ivi contenuti. Le procedure, essendo ben dettagliate, sono in grado di fornire abbastanza chiarezza circa tutti gli elementi fondamentali per la conservazione di un dato, poiché disciplinano anche il momento di distruzione dello stesso.

Si è visto, quindi, come la prassi da seguire preveda l'applicazione sia delle regole poste dal Regolamento 679/2016 sia delle Linee guida di volta in volta indicate dal Garante: potrebbe sembrare una disciplina abbastanza frammentaria, ma bisogna tener conto di quanto diverse

---

[169] Testo del DPCM 11/2014 in G.U. 12 gennaio 2015 rinvenibile in rete: https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/dpcm_13_11_2014.pdf

[170] "*Il sistema applicativo RIS PACS emaging core è il punto attorno al quale ruota l'intera piattaforma emaging SUITE. Utilizzato da professionisti qualificati contribuisce a semplificare e rendere più efficiente il flusso di lavoro di tutto il personale impiegato nella Diagnostica per immagini, aumentando la Qualità e la Sicurezza dei servizi offerti al paziente. Proprio per ottenere i migliori risultati emaging core è stato progettato e sviluppato sulla base degli ultimi standard di sicurezza richiesti dalle Strutture che operano nell'ambito Radiologico e consente la gestione dell'intero flusso di lavoro in una unica soluzione*." in rete: http://eurochimica.net/prodotti/linea-emaging/core/

possono essere le singole fattispecie e gli interessi in gioco. I dati sanitari, contenenti informazioni molto dettagliate circa lo stato di salute e le eventuali terapie eseguite, necessitano di procedure estremamente minuziose e rigorose, soprattutto per quanto riguarda la loro archiviazione o distruzione, procedura diverse tra loro inevitabili se si considera la diversità di documenti, come ad esempio, l'esito di analisi del sangue e un'immagine radiografica, essendo strumenti su supporti e con finalità diverse.

A seguito di quanto visto, si può notare come il Garante, dopo vari anni di attività, continui a voler attirare l'attenzione sull'aspetto positivo della sua azione. Si è passati infatti, dalla concezione della privacy come un sistema di limite a un tipo di sistema generale di risorse[171]. Perché se è vero che la disciplina del Garante e della privacy in generale prevede divieti e prescrizioni, è anche vero che, la sinergia svolta dal legislatore e dall'Autorità, va ad aumentare il valore e la tutela dell'oggetto in questione, i dati. Esattamente come accade in ambito sanitario, prescrizioni, obblighi e divieti, non sono finalizzati a costituire solo obblighi burocratici in capo agli operatori sanitari, ma sono volti a dare in definitiva estremo valore alle informazioni circa la salute di ogni persona. Da un lato l'attività del Garante va, in un certo senso, a privare di qualcosa, ma al contempo restituisce affidabilità e chiarezza a un sistema, quello sanitario, che se fosse illogico o non regolamentato, comporterebbe danni di rilevante entità. Quindi, si è visto come il contemperamento di interessi, prassi ormai comune sia a livello comunitario sia in capo al Garante, costituisca il punto di partenza per un tipo di cultura all'ascolto e alla conoscenza, raggiungendo il fine ultimo dei recenti anni di interventi normativi sopra menzionati, ovvero un dialogo costante non solo esplicitamente consentito dal punto di vista normativo, ma assolutamente necessario e gradito dal presente digitalizzato.

[171] Intervista all' ex Vice Presidente dell'Autorità Garante per la protezione dei dati personali Giuseppe Chiaravalloti per CCTV e IPSecurity Forum, rinvenibile in rete: https://www.youtube.com/watch?v=r0m4vonWSHI

CAPITOLO 3

IL FASCICOLO SANITARIO ELETTRONICO.

Sommario: 3.1 introduzione - 3.2 Il Fascicolo Sanitario Elettronico in Italia - 3.3 Il ruolo dell'Agenzia per l'Italia Digitale - 3.4 Il Personal Health Record, il National Health System e il Dossier Médical Personnel, l'esperienza americana, inglese e francese.

Introduzione

In questo terzo e ultimo capitolo si discorrerà dell'ulteriore tema centrale dell'elaborato: il Fascicolo Sanitario Elettronico.

Nel secondo paragrafo, infatti, si tracceranno le origini di questo strumento rivoluzionario, considerandone i benefici ma anche le difficoltà di percorso, recependo il forte nesso tra il Fascicolo e la volontà dei servizi sanitari di diventare sempre più digitali. Uno strumento che non costituisce una mera cartella clinica contenente delle informazioni circa la salute, bensì rappresenta la fiducia di ogni singolo assistito in Italia riposta nel sistema sanitario e la volontà di cooperare e comunicare con l'*èquipe* medica, affidando i propri dati al presente digitalizzato conformemente a quanto disposto dalla legislazione esposta nel precedente capitolo.

Si tratterà poi circa il fondamentale ruolo dell'Agenzia per l'Italia Digitale, agenzia con lo scopo di promuovere il progresso digitale nel nostro Paese, offrendo la propria attività di coordinamento ma anche di controllo tramite le sue Linee Guida.

Da ultimo si volgerà lo sguardo a quelli che sono l'equivalente del nostro Fascicolo Sanitario Elettronico negli Stati Uniti, in Inghilterra e in Francia, analizzandone i sistemi sanitari e recependo la differenza di diritti, leggi ed usi che caratterizzano i singoli Paesi, solo accomunati, forse, dalla volontà di un mondo digitale.

3.2 Il Fascicolo Sanitario Elettronico in Italia

Si è assistito negli ultimi anni, come esaminato nel primo capitolo, a una costante ricerca di digitalizzazione della salute, dopo aver osservato e valutato i molteplici vantaggi derivanti dall'introduzione della tecnologia nel quotidiano. In ambito sanitario è stato evidente il forte progresso dettato dalle tecnologie sempre più nuove, arrivando a una digitalizzazione delle pubbliche amministrazioni.

Il Fascicolo Sanitario Elettronico costituisce il ruolo centrale di tutto quello che è l'ecosistema della sanità digitale, definito in accordo alla Missione "Tutela della salute" e con il documento "Strategia per la crescita digitale 2014 2020" in cui per "Sanità digitale" si intende una vera e propria azione. Rappresenta una vera e propria infrastruttura operativa nell'ambito del Servizio Sanitario Nazionale ed è attivo in tutto il territorio a livello regionale. All'interno del Fascicolo, sono presenti ulteriori strumenti essenziali all'attività sanitaria, come la Cartella Clinica Elettronica, il *Dossier* sanitario e i referti on-line. La famosa Legge n. 24/2017 "Gelli-Bianco"[172] ha inteso aumentare gli standard delle cure praticate, e il Fascicolo costituisce un requisito essenziale per raggiungere tale scopo. Com'è noto, infatti, tale legge ha affrontato i temi della sicurezza delle cure e della trasparenza della documentazione sanitaria: infatti sono state poste delle disposizioni specifiche in materia di sicurezza delle cure volte a promuovere migliori pratiche sanitarie con lo scopo di ridurre al massimo gli errori medici. Inoltre, per quanto riguarda la responsabilità professionale degli operatori sanitari, sono stati introdotti ulteriori requisiti di trasparenza e digitalizzazione di tutte le pratiche che quotidianamente sono seguite nelle strutture sanitarie, rendendo necessario il famoso bilanciamento di interessi posto dal Regolamento 679/2016, garantendo una protezione dei dati personali ottimale.

Quindi, negli ultimi anni soprattutto, è stato necessario trovare un punto di incontro tra la Sanità e la Privacy, raggiungendo un ottimo livello di servizio offerto coniugato alla digitalizzazione dei sistemi. Però, è necessario tenere conto del fatto che il diritto alla salute e il diritto alla protezione dei dati inerenti alla salute della persona, spesso si trovano in conflitto, essendo espressioni di due interessi opposti. E quindi, l'enorme lavoro e la sfida che il legislatore comunitario e nazionali hanno raggiunto, non si arresteranno mai, tenendo conto del fatto che vi

[172] Legge dell'8 marzo del 2017 n. 24 "Disposizioni in materia di sicurezza delle cure e della persona assistita, nonche' in materia di responsabilita' professionale degli esercenti le professioni sanitarie. (17G00041) (GU Serie Generale n.64 del 17-03-2017)" testo rinvenibile in rete: https://www.gazzettaufficiale.it/eli/id/2017/03/17/17G00041/sg

saranno fattispecie sempre nuove da dover disciplinare e tutelare. L'e-health, di cui si è trattato nel primo capitolo di questo elaborato, è da anni al centro dello studio da parte delle istituzioni, poiché è stata la causa di vari interventi normativi e di una rivoluzione sul "fare medicina" e di ricevere le cure decisamente caratteristico del presente sempre più digitale.

Il Fascicolo Sanitario Elettronico trova le sue radici normative del Decreto-legge n. 179 del 2012 che lo istituisce nell'ambito delle regioni e delle province autonome, sempre nel rispetto della normativa della protezione dei dati personali. In questo decreto è indicato, inoltre, che il fascicolo è istituito con il fine di prevenzione, cura e diagnosi, ed è indicato che può essere istituito anche con fini di studi e di ricerche scientifiche. Il progetto iniziale si ispirava a una *governance* che richiede una programmazione sanitaria che permetta la verifica della qualità delle cure e la valutazione dell'assistenza fornita dalle strutture,

Successivamente, il D.P.C.M n.278 del 2015 ha posto le regole per la regolarizzazione del fascicolo e ha indicato quelli che sono i contenuti del fascicolo sanitario, così da pervenire a una definizione di fascicolo sanitario elettronico ben precisa "*a) "FSE", il Fascicolo Sanitario Elettronico, di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221*;"[173] , potendo quindi affermare che "*il fascicolo è inteso come un insieme di dati e documenti digitali di tipo sanitario e sociosanitario che sono generati dai diversi eventi clinici che l'assistito si trova a dover subire come eventi nell'ambito sanitario*"[174]. La storia normativa di questo strumento ha inizio nel luglio del 2009 con le Linee Guida del Ministero della Salute e le Linee Guida del Garante per la protezione dei dati personali in materia di Fascicolo sanitario elettronico e *dossier* elettronico. Il progetto di questo strumento si fonda su una gestione dei dati a livello regionale ex articolo 12, comma 2 del decreto-legge sopra citato "[…] *2. Il FSE è istituito dalle regioni e province autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali, a fi ni di: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifi ca in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifi ca delle qualità delle cure e valutazione dell'assistenza sanitaria*. […]", infatti, è compito di ogni regione italiana predisporre gli strumenti necessari ai fini di una corretta gestione, ed è attivo per tutta la vita del paziente. Quest'ultimo, infatti, sarà lui stesso ad aggiornare a mano a mano le informazioni contenute all'interno del fascicolo, così da avere la storia clinica aggiornata e digitalizzata.

[173] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 29 settembre 2015, n. 178
Regolamento in materia di fascicolo sanitario elettronico. (15G00192) (GU Serie Generale n.263 del 11-11-2015), testo rinvenibile in rete: https://www.gazzettaufficiale.it/eli/id/2015/11/11/15G00192/sg

[174] Definizione offerta dalla Dott.ssa Enrica Massella (Agid) al minuto 00:05:21 "Il Ruolo del Fascicolo Sanitario Elettronico" nel Webinar sul "Fascicolo sanitario elettronico" del 13/12/2018, rinvenibile online: https://www.youtube.com/watch?v=WDGDqYaTVvI

I documenti che devono far parte del fascicolo prevedono un nucleo minimo, relativo ad esempio ai dati identificativi, ai referti e a tutto il profilo sanitario generale elencati all'articolo 2 del D.P.C.M. 178/2015 "*1. I contenuti del FSE sono rappresentati da un nucleo minimo di dati e documenti, nonche' da dati e documenti integrativi che permettono di arricchire il Fascicolo stesso. 2. Il nucleo minimo, di cui al comma 1, uguale per tutti i fascicoli istituiti da regioni e province autonome, e' costituito dai seguenti dati e documenti: a) dati identificativi e amministrativi dell'assistito di cui all'articolo 21; b) referti, inclusi quelli consegnati ai sensi del decreto del Presidente del Consiglio dei ministri 8 agosto 2013, pubblicato nella Gazzetta Ufficiale n. 243 del 16 ottobre 2013; c) verbali pronto soccorso; d) lettere di dimissione; e) profilo sanitario sintetico, di cui all'articolo 3; f) dossier farmaceutico; g) consenso o diniego alla donazione degli organi e tessuti.*" Gli altri documenti non necessari che possono comunque essere inseriti all'interno del fascicolo sono quelli previsti espressamente al comma 3 dello stesso articolo "*3. I dati e documenti integrativi, di cui al comma 1, sono ulteriori componenti del FSE, la cui alimentazione e' funzione delle scelte regionali in materia di politica sanitaria e del livello di maturazione del processo di digitalizzazione quali: a) prescrizioni (specialistiche, farmaceutiche, ecc.); b) prenotazioni (specialistiche, di ricovero, ecc.); c) cartelle cliniche; d) bilanci di salute; e) assistenza domiciliare: scheda, programma e cartella clinico-assistenziale; f) piani diagnostico-terapeutici; g) assistenza residenziale e semiresidenziale: scheda multidimensionale di valutazione; h) erogazione farmaci; i) vaccinazioni; l) prestazioni di assistenza specialistica; m) prestazioni di emergenza urgenza (118 e pronto soccorso); n) prestazioni di assistenza ospedaliera in regime di ricovero; o) certificati medici; p) taccuino personale dell'assistito di cui all'articolo 4; q) relazioni relative alle prestazioni erogate dal servizio di continuita' assistenziale; r) autocertificazioni; s) partecipazione a sperimentazioni cliniche; t) esenzioni; u) prestazioni di assistenza protesica; v) dati a supporto delle attivita' di telemonitoraggio; z) dati a supporto delle attivita' di gestione integrata dei percorsi diagnostico-terapeutici*;". Il dossier farmaceutico, che è contenuto all'interno del fascicolo, contiene invece tutti i dati necessari affinché il paziente segua una terapia idonea alla propria esigenza, contenendo informazioni circa i medicinali e i loro dosaggi, per ottimizzare l'aderenza del paziente alle prescrizioni rilasciate dai medici, e quindi garantire il successo della cura.

Cosa di fondamentale importanza, è che all'interno del fascicolo sanitario elettronico, possono essere presenti dei dati che sono già definiti come "sensibili" ma che per la loro particolare rilevanza concedono al paziente il diritto di anonimato come sancito dall'articolo 5 del D.P.C.M. "*1. I dati e i documenti sanitari e socio-sanitari disciplinati dalle disposizioni normative a tutela delle persone sieropositive, delle donne che si sottopongono a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle*

persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonche' i dati e i documenti riferiti ai servizi offerti dai consultori familiari, sono resi visibili solo previo esplicito consenso dell'assistito, fermo restando che, nel caso l'assistito scelga di ricorrere alle prestazioni in anonimato, non e' ammessa l'alimentazione del FSE da parte dei soggetti che erogano le prestazioni. 2. Nei casi di cui al comma 1, e' responsabilita' dei professionisti o degli operatori sanitari che erogano la prestazione acquisire l'esplicito consenso dell'assistito." Tali dati, quindi possono essere resi visibili solo dopo che il paziente abbia espressamente prestato il suo consenso: qualora lo stesso intenda accedere alle prestazioni in forma anonima, sarò vitato alle strutture sanitarie in questione di aggiornare il Fse, bensì spetterà all'assistito aggiornarlo.

Dal titolare del trattamento deve essere fornita un'idonea ed esaustiva informativa circa l'istituzione del fascicolo, poiché la persona deve essere messa in condizione delle giuste pratiche per attivare il fascicolo, su come può accedere e il contenuto effettivo dello stesso. Essa deve contenere tutti gli elementi richiesti dall'articolo 13[175] del Codice Privacy, con il fine di formare un fascicolo che presenti tutta la storia clinica del paziente. Inoltre, l'informativa deve informare il soggetto del fatto che qualora esso non presti il suo consenso, ciò non inciderà assolutamente sull'accesso alle cure. Saranno menzionati i soggetti diversi dal titolare che potranno accedere al Fse e sarà posta la possibilità dell'interessato di istituire coloro che potranno avere accesso al fascicolo. Inoltre, il Fse potrebbe essere consultato senza espressa autorizzazione dell'interessato ma sempre nel rispetto di quanto disposto dall'Autorità Garante, qualora vi sia la necessità di salute di una terza persona o della collettività, ex articolo 76, lettera b) del Codice Privacy "*b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività*."

Ovviamente, a garanzia di questo strumento vi sono le disposizioni del Regolamento 679/2016 che al considerando 63[176] dispone l'interessato ha il diritto di poter accedere ai suoi dati sanitari

[175] Si veda il paragrafo 3 del capitolo 2

[176] Testo art 63 del Regolamento 679/2016 "(63) *Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Garante per la protezione dei dati personali dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato,*

e indicando quali prestazioni ha ricevuto: infatti il Fse non è solo un mero documento digitale, ma molti autori lo definiscono come "*un'infrastruttura digitale*"[177] poiché non include solo la cartella clinica, ma possono essere presenti anche immagini come le risonanze magnetiche, i referti di analisi ecc., quindi, qualsiasi persona che abbia attivato il Fse deve essere capace di poterlo aggiornare. Sulla base di ciò, essenziale è una corretta identificazione della persona dell'interessato e di coloro che possono avere l'accesso, quindi il titolare del trattamento offerto dovrebbe adottare dei sistemi di identificazione *on-line* del tutto attendibili.

Infatti, l'accesso avviene attraverso le credenziali e le modalità, attualmente richieste dalla normativa vigente, richiedono al paziente o lo SPID[178], un sistema di identità digitale, o la tessera sanitaria. Avviene tramite il portale nazionale e consente di avere informazioni circa lo stato dell'approvazione del fascicolo sanitario, e il portale consente anche di accedere ai siti regionali che ogni regione mette a disposizione per il proprio territorio. Ovviamente, l'assistito deve prestare il proprio consenso all'attivazione del fascicolo e alimentarlo di volta in volta sulla base del consenso che fornisce il popolamento del fascicolo con quelli che sono i dati di diagnostica, ogni volta che esso abbia bisogno di ricevere delle cure. Quindi il fascicolo diventa il cardine per tutte quelle che possono essere le analisi dei dati della cura, la ricerca e, per il Governo, per quelle che sono le attività che sono svolte in ambito sanitario a livello nazionale. Ciò che il fascicolo si occupa di fare è anche aumentare il livello di sostenibilità del sistema sanitario poiché in questo modo è ottimizzata il livello di appropriatezza delle cure che vengono somministrate, tenendo conto anche della lieve evoluzione del rapporto tra assistito e medico fondato su una comunicazione rapida ed efficace, migliorando la qualità della vita e dei cittadini, andando in contro a quelle che sono le esigenze delle persone che presentano delle disabilità e che hanno bisogno di un percorso continuo e personalizzato in base alle loro esigenze.

Come si è accennato nello scorso capitolo, per quanto riguarda il consenso al trattamento dei dati nel Fse deve essere "un tipo di consenso autonomo e specifico" rispetto a quello prestato per il generico trattamento dei dati per fini di cura: infatti il consenso al fascicolo deve essere disciplinato da norme più specifiche e deve essere espressione della piena libertà del paziente, che come si è detto prima, è esso stesso a decidere l'attivazione o meno dello strumento e quindi

il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce."

[177] Libro "La privacy nella sanità" di Giuseppe Carro, Sarah Masato e Massimiliano Domenico Parla, pag. 187

[178] "*Con il Sistema Pubblico d'Identità Digitale - SPID puoi accedere ai servizi online della pubblica amministrazione e dei privati aderenti, con una coppia di credenziali (username e password) personali.*
Semplice e sicuro, puoi usare SPID da qualsiasi dispositivo: computer, tablet e smartphone, ogni volta che, su un sito o un'app di servizi, trovi il pulsante "Entra con SPID".
Scegli come attivarlo, gratuitamente o a pagamento, sul sito di uno dei gestori di identità abilitati. Una volta ottenuto, l'utilizzo di SPID è gratuito per il cittadino." In rete: https://www.spid.gov.it/, visto in agosto 2021

ne ha pieno controllo. Il consenso prestato ha quindi vari caratteri: deve necessariamente essere espresso inequivocabilmente, ha il compito di esprimere un carattere generale, quindi la volontà del paziente di attivare il suo fascicolo e il compito di esprimere un carattere specifico, costituente la libera scelta dell'assistito di decidere quali informazioni inserire all'interno dello stesso. Solo dopo che la persona ha effettuato tutte le scelte a essa riservate, gli operatori e le strutture sanitarie potranno accedervi e consultarne le informazioni, ex articolo 7 del D.P.C.M. " *1. Il FSE puo' essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito. 2. Per le finalita' di cui alla lettera a) del comma 2 dell'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, la consultazione dei dati e documenti presenti nel FSE puo' avvenire solo dopo che l'assistito ha preso visione dell'informativa di cui all'articolo 6 e ha espresso il consenso di cui all'articolo 6, comma 2, lettera e). […] 5. Il consenso di cui ai commi 1, 2, 3 e 4 puo' essere espresso anche per via telematica, previo accesso al FSE secondo le modalita' di cui al comma 2 dell'articolo 23.* […]". E secondo quanto disposto dai commi 6,7 e 8 "*6. L'assistito puo' in ogni momento revocare, anche per via telematica, il consenso di cui al comma 1. 7. La revoca del consenso di cui al comma 1 determina l'interruzione dell'alimentazione del FSE, senza conseguenze in ordine all'erogazione delle prestazioni del servizio sanitario e dei servizi socio-sanitari regionali. Il FSE viene comunque alimentato da eventuali correzioni dei dati e dei documenti che lo hanno composto fino alla revoca del consenso, da parte degli organismi sanitari che hanno generato tali dati e documenti e che mantengono la titolarita' su di essi. In caso di nuova e successiva prestazione del consenso di cui al comma 1, vengono resi nuovamente visibili nel FSE i dati e i documenti che lo hanno alimentato fino alla precedente operazione di revoca del consenso, ivi comprese le correzioni anche successive alla predetta revoca. 8. La revoca del consenso di cui al comma 2 determina la disabilitazione della consultazione dei dati e dei documenti presentinel FSE da parte dei professionisti sanitari e socio-sanitari precedentemente autorizzati, senza conseguenze in ordine all'erogazione delle prestazioni del servizio sanitario e dei servizi socio-sanitari regionali. L'assistito puo', successivamente, esprimere un nuovo consenso alla consultazione dei dati e dei documenti di cui al comma 2.*" Quindi il paziente ha assolutamente la libertà di interrompere il suo fascicolo in qualunque momento, essendo al contempo sicuro riguardo la non interruzione delle cure mediche, l'unica conseguenza della revoca del suo consenso sarà la "disabilitazione della consultazione dei dati" da parte di coloro che ne avevano accesso. Qualora il paziente volesse in un secondo momento riattivare quello che era il suo Fse, lo potrà fare sempre in via telematica e il fascicolo conterrà tutto ciò che era presente al momento della revoca.

L'articolo 7 del Codice Privacy e l'articolo 12 del Regolamento Ue costituiscono gli elementi fondamentali sui quali si deve basare il trattamento dati. Infatti, all'interessato è doveroso garantire una semplice modalità di accesso al suo fascicolo ed eventualmente ricevere una copia da poter consegnare a terze persone che lui ritiene necessarie: ciò avviene tramite il "riscontro" ex articolo 10, comma 3 del Codice Privacy, dove si prevede che "*3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1*." Quindi, è vero che l'interessato può ovviamente avere copia di quanto contenuto all'interno del fascicolo, ma vi sono particolari disposizioni come quelle di cui all'articolo 84[179], comma 1, in cui si prevedono eventuali disposizioni per quanto riguarda una lecita divulgazione dei dati ivi contenuti. Ad esempio, si prevede la necessaria autorizzazione da parte del titolare o del responsabile del trattamento che deve avvenire per iscritto qualora debbano rendere i dati del paziente, tutto ciò dovrà avvenire tramite "l'atto formale di incarico" per gli operatori sanitari con il fine di rispettare quanto voluto dal paziente. Qualora il responsabile o il titolare del trattamento non dovessero adempiere a quanto richiesto dall'interessato, quest'ultimo potrà adire l'autorità Garante prima di instaurare un contenzioso giudiziario.

Per quanto riguarda i soggetti che eseguono il trattamento dei dati, ovviamente, sono solo quelli operanti nel settore sanitario, quindi sono esclusi da questi "*le compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, periti e organismi amministrativi operanti in ambito sanitario e anche al personale medico nell'esercizio di attività medico-legale*"[180]. All'interno di una struttura sanitaria però vi è il personale amministrativo addetto alla prenotazione delle visite e degli esami: in questo caso esso potrà conoscere circa i dati necessari personali del paziente solo per adempiere a tali compiti. Quindi sarà onere del titolare indicare le operazioni consentite a quali soggetti, distinguendo in modo minuzioso le attività del personale sanitario e le attività del personale amministrativo, indicando anche la loro possibilità di modificare quanto contenuto nel Fascicolo sanitario.

---

[179] *"[1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.]*" testo dell'articolo 84 del Codice Privacy

[180] Libro "La privacy nella sanità" di Giuseppe Carro, pagina 192.

Come si è accennato prima, in base a quanto disposto dall'articolo 84 del Codice Privacy, l'interessato deve essere messo nella condizione di poter accedere liberamente e in qualunque momento al proprio fascicolo sanitario, quindi l'accesso sarà consentito solo a colui che lo ha attivato e ai soggetti da lui designati. In questa operazione, ovviamente, è necessario garantire la privacy di quanto contenuto all'interno del Fse, approvando di volta in volta l'identità della persona che vi sta accedendo da remoto. Come accennato prima, le persone che possono accedervi sono munite di una forma di identità digitale che ne attesti la legittimazione, vale a dire codici di accesso, smart-card rilasciate ad esempio dalla struttura sanitaria oppure delle *keys* di accesso rilasciate solo dopo aver certificato l'identità della persona in questione.

Infatti, dati i possibili attacchi informatici alle aziende sanitarie, ma non solo, anche i tentativi di furto di identità a carico di persone, sono necessarie delle misure di sicurezza applicabili ai sensi dell'articolo 31[181] del Codice Privacy, che devono essere predisposte dal titolare del trattamento, secondo il principio di *accountability*. I sistemi di memorizzazione e di archiviazione hanno particolare necessità di protezione, di fatto devono essere assicurati dei sistemi idonei di autorizzazione in base ai vari incarichi sanitari, delle procedure di verifica di identità eseguite da *identity provider*, dei criteri di cifratura e separazione dei dati per differenziare i dati relativi alla salute e quelli relativi alla vita sessuale, dei sistemi che permettono di tracciare ogni accesso e di geolocalizzarlo per rintracciare attività sospette, e dei sistemi di "*audit log*". Ovviamente, il responsabile del trattamento dovrà servirsi della consulenza di un DPO per adottare le misure necessarie e innovative, considerando ormai il rischio di danno sia sempre più elevato. Quindi, tutti coloro che vogliono attivare il proprio fascicolo sanitario, devono poter essere rassicurati sulla protezione dei loro dati. Bisogna considerare che il progetto di fascicolo viene condiviso da reti apposite delle Pubbliche Amministrazioni, ovvero il "Sistema Pubblico di Connettività" (SPC), dotato di misure di sicurezza in grado di garantire la massima riservatezza.

Per quanto riguarda la diffusione del Fascicolo sanitario dopo il D.P.C.M del 2015, si è assistiti a un fenomeno di "interoperabilità". Le strutture sanitarie si devono adeguare agli standard e devono essere in grado di produrre informazioni che possono essere lette da tutte le strutture di tutto il territorio nazionale. Per fare ciò si seguono due modelli diversi: il primo denominato "*modello a registry centrale*", ovvero il fascicolo è inteso come un documento unico rilasciato

[181] *"[1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.]*" Articolo 31 del Codice Privacy.

dalla struttura che offre il servizio: in questo caso l'informazione è unica e non ci possono essere duplicazioni, proprio per evitare il disallineamento tra regioni. Il secondo modello, "*modello a registry distribuito*", è attuato qualora la regione non sia in grado di predisporre il fascicolo e quindi viene rilasciato a livello centrale.

Negli anni siamo partiti da un tipo di "*interoperabilità federata*", dove le regioni colloquiano tra di loro, con la conseguenza che il modello presentava delle lacune di carattere tecnico: a volte le informazioni delle anagrafi regionali non corrispondevano a quelle dell'anagrafe centrale e quindi in presenza di databases diversi, il consenso non era allineato su tutto il territorio. Si è arrivati quindi a un "*modello centralizzato*" che prevede la verifica dell'identificazione dell'assistito tramite la tessera sanitaria e nello stesso tempo avviene la verifica del consenso, permettendo quindi una circolazione delle informazioni estremamente efficace. Si discorre anche di "*interoperabilità a carattere europeo*", grazie allo sviluppo di standard che sono utilizzati a livello comunitario: il "*patient summary*" ovvero del profilo sanitario sintetico e della "*prescription*" ovvero della prescrizione. Questo è ciò che l'Europa sta attuando, ovvero la produzione lo scambio di informazioni a livello europeo tramite un connettore tra diversi Stati Membri, in grado di rendere possibile un continuo dialogo tra paesi.

Nel 2016 è stato istituito il Tavolo Tecnico di monitoraggio e indirizzo per l'attuazione del FSE presso il Ministero della Salute ex articolo 26 del D.P.C.M Fse, disponendo "*Tavolo tecnico di monitoraggio e indirizzo 1. E' istituito nell'ambito della Cabina di Regia del NSIS il Tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. 2. Partecipano al Tavolo tecnico di cui al comma 1 i rappresentanti delle amministrazioni, delle regioni e delle province autonome specificatamente individuati in relazione al settore e alla materia trattata. Ai componenti del predetto Tavolo non spettano compensi, rimborsi o altri gettoni di presenza. 3. Il Tavolo tecnico di cui al comma 1: a) svolge un monitoraggio costante dello stato di attuazione e utilizzo del FSE presso le regioni e le province autonome, riportandone i risultati alla Cabina di Regia del NSIS; b) propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, gli obiettivi annuali di avanzamento per l'anno successivo, sia in termini di copertura, sia per l'alimentazione del FSE, nonche' per l'effettivo utilizzo dello stesso, anche sulla base di quanto previsto dai piani di progetto regionali; c) elabora e propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, i contenuti, i formati e gli standard degli ulteriori documenti sanitari e socio-sanitari del nucleo minimo di cui all'articolo 2, comma 2, e gli aggiornamenti degli stessi; d) elabora e propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, i contenuti, i formati e gli standard dei*

documenti sanitari e socio-sanitari di cui all'articolo 2, comma 3, lettere da a) a z), e gli aggiornamenti degli stessi; e) valuta i documenti sanitari e socio-sanitari di cui all'articolo 2, comma 3, lettera aa), nonche' elabora e propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, i contenuti, i formati e gli standard degli stessi e i relativi aggiornamenti; f) valuta, elabora e propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, le variazioni agli standard di cui all'articolo 24, comma 2; g) valuta, elabora e propone alla Cabina di Regia del NSIS, ai fini dell'approvazione, le variazioni ai servizi di cui all'articolo 25, comma 3. 4. I contenuti e i relativi aggiornamenti di cui al comma 3, lettere c), d), e), f), g), approvati dalla Cabina di Regia del NSIS, sono recepiti in appositi decreti adottati ai sensi dell'articolo 27, comma 3. 5. I formati, gli standard e i relativi aggiornamenti di cui al comma 3, lettere c), d), e), f), g), approvati dalla Cabina di Regia del NSIS, sono pubblicati in apposite sezioni dei siti web del Ministero della salute e dell'Agenzia per l'Italia digitale."[182] A questa *governance* parteciparono i rappresentanti del Ministero della Salute, del Ministero dell'Economia, dell'AgiD, dell'Autorità Garante privacy e delle Regioni. I compiti del Tavolo Tecnico sono il monitoraggio e il controllo costante della formazione dei fascicoli sanitari in ogni regione e presso le Pubbliche Amministrazioni e l'elaborazione di standard e di contenuti minimi dei documenti sanitari e sociosanitari. Nel 2017 sono stati istituiti nove gruppi di lavoro, e ognuno di questi aveva il compito di elaborare un "Data set" comune contenente tutte le informazioni e definire delle codificazioni a livello nazionale così da fare in modo che tutte le regioni siano aggiornate alla prassi corrente. Il Clinical Document Architecture è "*uno standard per i markup dei documenti per la struttura e la semantica di documenti clinici interoperabili*", quindi è un documento che viene firmato che per essere letto ha bisogno di un suo foglio di stile, solo in questo caso i pazienti o gli operatori sanitari possono prenderne visione. Il documento è diviso in due parti: la prima parte è chiamata "*header*" nella quale sono presenti tutte le informazioni e i dati specifici degli utenti, quindi sia del medico che del paziente, nella seconda parte che viene denominata "*body*" vi è tutta la parte clinica strutturata con tutti i referti. Utilizzare uno standard del genere permette di raggiungere molteplici vantaggi, come ad esempio l'elevata qualità della documentazione, è uno strumento di supporto per quanto riguarda le decisioni cliniche ed è la chiave per l'uso secondario dei dati per finalità di ricerca da parte del Governo, ma soprattutto, consente di tracciare una *roadmap* vincente con il fine di garantire quel livello di interoperabilità sia a livello nazionale che comunitario.

[182] In rete il testo del D.P.C.M.: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/dpcm_178_2015.pd

Al momento in Italia bisogna affermare che il Fascicolo Sanitario Elettronico è attivo in 21 regioni su 21 e i dati riportati[183], sono confortanti. La maggior parte delle regioni presenta un tasso di attivazione pari almeno al 99 per cento, Lombardia, Toscana, Puglia e Sicilia invece riportano un livello del 100 per cento, mentre le regioni meno attive sono la Liguria con l'86 per cento, l'Umbria con l'86 per cento e l'Abruzzo con il 36 per cento. Attualmente il numero totale a livello nazionale di fascicoli attivati è 52.783.391, numero aumentato dopo l'emergenza da Covid-19, considerando che prima della pandemia, coloro che avevano prestato il consenso al fascicolo erano oltre 13,3 milioni.

Come si è accennato prima, ogni regione gestisce il proprio servizio di fascicolo sanitario, potendo quindi riscontrare delle diversità tra i fascicoli attualmente attivi in Italia: ad esempio, in Lombardia è possibile prenotare delle visite specialistiche o avere informazioni circa le invalidità, in altre regioni invece è addirittura presente un'applicazione per il proprio cellulare. Quindi vi è una disparità notevole tra regioni. Vi sono casi, inoltre, in cui sono proprio i medici a non utilizzare questo strumento e quindi i pazienti non sono spronati ad attivarlo. Anche se il progetto di fascicolo sia a livello nazionale che europeo risulta del tutto innovativo e anche a volte necessario, vi sono delle cause che ne rallentano la diffusione: l'Osservatorio Innovazione digitale in Sanità del Politecnico di Milano, sostiene che la prima causa della mancata attivazione del fascicolo è proprio la mancata comunicazione dell'esistenza dello strumento: dovrebbero essere gli stessi medici a indirizzare i loro pazienti verso un tipo di medicina collaborativa.

È anche vero, però, che i medici specialisti e quelli di medicina generale, molto spesso, presentano una capacità di utilizzare gli strumenti digitali piuttosto bassa, poiché, come si discorreva nel primo capitolo, al momento non vi sono alcuni corsi specifici per impartire al personale sanitario idonee competenze digitali. Anche le stesse aziende sanitarie sono troppo poco digitalizzate, infatti, non tutte queste presentano dei macchinari idonei a porre in essere questo tipo di operazioni.

Attualmente, quindi, vi è il bisogno di un progetto di rilancio del Fse che ovviamente necessita di finanziamenti, prevedendo un sistema formato da un archivio centrale, garantendo l'interoperabilità, e dall'integrazione dei documenti da parte delle regioni. Il Fascicolo sanitario elettronico deve essere rilanciato poiché esso costituisce un punto di accesso per medici e pazienti, garantisce informazioni omogenee e sarà uno strumento valido per l'operato delle Asl per effettuare indagini e migliorare i propri servizi offerti.

[183] Dati sul Fascicolo Sanitario Elettronico rinvenibili sul sito ufficiale dell'AgiD, in rete: https://www.fascicolosanitario.gov.it/

3.3 Il ruolo dell'Agenzia per l'Italia Digitale.

Nei capitoli precedenti si è osservato come stia avanzando il bisogno di digitalizzazione nelle amministrazioni e nello scorso paragrafo si è notato come uno strumento innovativo come il Fascicolo Sanitario Elettronico sia straordinariamente funzionale alla medicina del futuro. Bisogna però tenere conto anche della difficile progressione verso il digitale che ancora caratterizza il nostro presente.

In questo paragrafo sarà posto in evidenza il ruolo dell'Agenzia per l'Italia Digitale e come questa riesca a fungere da guida nel *mare magnum* dell'amministrazioni digitale.

L'AgiD è l'agenzia tecnica della Presidenza del Consiglio che ha lo scopo di diffondere un uso corretto della tecnologia, favorendo così lo sviluppo economico del nostro Paese, realizzando quelli che sono gli obiettivi prefissati dall'Agenda Digitale Italiana. È un'agenzia pubblica ed è stata istituita con il Decreto-legge 22 giugno 2012, n. 83 "Misure urgenti per la crescita del Paese"[184], successivamente convertito con modificazioni dalla Legge 7 agosto 2012, n. 134 "[…] *Visti gli articoli 77 e 87 della Costituzione; Ritenuta la straordinaria necessita' ed urgenza di emanare disposizioni per favorire la crescita, lo sviluppo e la competitivita' nei settori delle infrastrutture, dell'edilizia e dei trasporti, nonche' per il riordino degli incentivi per la crescita e lo sviluppo sostenibile finalizzate ad assicurare, nell'attuale situazione di crisi internazionale ed in un'ottica di rigore finanziario e di effettivo rilancio dello sviluppo economico, un immediato e significativo sostegno e rinnovato impulso al sistema produttivo del Paese, anche al fine di garantire il rispetto degli impegni assunti in sede europea indispensabili, nell'attuale quadro di contenimento della spesa pubblica, al conseguimento dei connessi obiettivi di stabilita' e di crescita; Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 15 giugno 2012; Sulla proposta del Presidente del Consiglio dei Ministri e dei Ministri dello sviluppo economico e delle infrastrutture e dei trasporti, di concerto con i Ministri dell'economia e delle finanze, del lavoro e delle politiche sociali, della giustizia, delle politiche agricole alimentari e forestali, per la cooperazione internazionale e l'integrazione e per gli affari regionali, il turismo e lo sport*; […]"

È sottoposta al potere di vigilanza e indirizzo del Presidente del Consiglio dei ministri o da un ministro da lui delegato. Essa intende quindi, aiutare le pubbliche amministrazioni e i cittadini a

[184] "DECRETO-LEGGE 22 giugno 2012, n. 83 Misure urgenti per la crescita del Paese. (12G0109)", atto completo online: https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dl-22-giugno-2012-n.83_0.pdf

raggiungere il livello massimo di innovazione "*nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia*." Compito fondamentale è inoltre autorizzare quei soggetti sia pubblici che privati a svolgere determinate azioni digitali, come ad esempio PEC[185] e PagoPA[186].

Il compito dell'Agenzia è anche indirettamente disciplinato dall'articolo 117, comma 2 lettera r) della Costituzione disponendo "[…] *r) pesi, misure e determinazione del tempo; coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale; opere dell'ingegno*; […]".

Le norme principali regolanti l'attività e le funzioni dell'Agenzia sono rispettivamente: il Decreto-legge 18 ottobre 2012, n. 179 denominato "*Ulteriori misure urgenti per la crescita del Paese*", poi convertito con modificazioni dalla Legge 17 dicembre 2012, n. 221, la Legge 7 agosto 2012, n. 134 rubricata "*Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini*", il Decreto-legge 6 luglio 2012, n. 95 "*Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini nonché misure di rafforzamento patrimoniale delle imprese del settore bancario*", il Decreto-legge 7 maggio 2012, n. 52- "Disposizioni urgenti per la razionalizzazione della spesa pubblica" (convertito con modificazioni dalla Legge 6 luglio 2012 n. 94) e il Decreto-legge 22 giugno 2012, n. 83 "*Misure urgenti per la crescita del Paese*".

Nello specifico l'AgiD ha il compito di emanare le Linee Guida che sono sempre consultabili presso il suo sito ufficiale, deve supportare le amministrazioni secondo quanto disposto dalla legge 4/2004, deve monitorare l'accessibilità dei siti *web* dei servizi pubblici essenziali e fare in modo che ciò avvenga in maniera semplice, predispone una compilazione online riservata solo alle pubbliche amministrazioni, con cui le stesse dichiarano la l'accessibilità del proprio portale *web*[187] e da ultimo, in seguito alla direttiva europea, deve presentare una relazione ogni 3 anni alla Commissione Europea sui risultati del monitoraggio. Il "*Piano Triennale per l'informatica*

---

[185] "*La Posta Elettronica Certificata è il sistema, ormai diffuso, attraverso il quale è possibile inviare mail con valore legale equiparato a quello di una raccomandata con ricevuta di ritorno.*
La PEC è indispensabile per l'attivazione del domicilio digitale, obbligatorio per imprese e professionisti dal 1° ottobre 2020.
Con il domicilio digitale PEC sarà possibile ricevere comunicazioni dalla Pubblica Amministrazione direttamente sulla propria casella, accessibile da qualsiasi luogo e dispositivo." Sito ufficiale di Aruba: https://www.pec.it/acquista-posta-elettronica-certificata.aspx?pk_campaign=adw-src&gclid=CjwKCAjwr56IBhAvEiwA1fuqGljPeZISJ6usgFXwg8lIFm86pVplJiXvsoZl2DGbKssrg_UIKHFIdxoCpWIQAvD_BwE

[186] "*PagoPA è la piattaforma nazionale che ti permette di scegliere, secondo le tue abitudini e preferenze, come pagare tributi, imposte o rette verso la Pubblica Amministrazione e altri soggetti aderenti che forniscono servizi al cittadino*." Sito ufficiale di PagoPA: https://www.pagopa.gov.it/

[187] Informazioni del webinar "AgiD e l'accessibilità ai servizi pubblici" del 22-23 maggio 2020 Claudio Celeghin (Responsabile Servizio Sviluppo web e communities @ AgID - Agenzia per l'Italia Digitale) durante gli Accessibility Days 2020, in rete: https://www.youtube.com/watch?v=FYalesEbww0

nella Pubblica amministrazione è il documento di indirizzo strategico ed economico che nasce per guidare operativamente la trasformazione digitale del Paese e diventa riferimento per le amministrazioni centrali e locali nello sviluppo dei propri sistemi informativi".

Il Piano, quindi, definisce un modello di riferimento per la diffusione dell'informatica nell'amministrazione italiana, fissando al contempo i principi architetturali fondamentali, le regole per garantire la interoperabilità. E anche con quanto stabilito dalla Legge di stabilità del 2016[188], il Piano è adottato per permettere alle amministrazioni di adeguarsi a vicenda per quanto riguarda l'obiettivo di risparmio della spesa annuale per il settore informatico del Paese. Così AgiD ha il dovere di guidare le amministrazioni in questa fase di adeguamento, tenendo conto anche delle attività svolte a livello regionale equiparandole a quelle svolte in sede ammnistrativa, avendo come comuni denominatori il modello di governance, il monitoraggio e il coordinamento necessario tra le loro attività. Più in generale, i piani che vengono predisposti dall'Agenzia sono degli strumenti essenziali che hanno il fine di promuovere e far sviluppare la trasformazione digitale del Paese su tutti i fronti, soprattutto quello delle Pubbliche Amministrazioni. È possibile sul sito dell'Agenzia, inoltre, monitorare l'andamento dei vari Piani: l'ultimo, quello del 2020-2022 prevede la realizzazione nel concreto di quelle che sono state le scelte predisposte dai due piani precedenti, si può quindi affermare che ogni piano è strumentale all'altro. Infatti, tramite essi, si vogliono raggiungere diversi scopi, come favorire lo sviluppo di una società digitale, ovvero mettere a disposizione dei cittadini e delle imprese dei servizi digitalizzati (ad esempio il fascicolo sanitario elettronico), promuovere lo sviluppo ma tenendo conto anche del rispetto dell'ambiente e contribuire a formare dei sistemi di servizi pubblici del tutto uniformi sul territorio italiano dal punto di vista digitale. Saranno le stesse Pubbliche Amministrazioni a dover adeguarsi ai livelli di tecnologia richiesti da AgiD, infatti sono state definite circa 200 azioni sia a carico della stessa Agenzia sia a carico delle Pubbliche Amministrazioni. Sul sito ufficiale[189]

[188] "*La legge di stabilità definisce la politica di bilancio per il 2016 e gli anni successivi, che si associa strettamente al processo di attuazione delle riforme strutturali. Essa si propone di ricondurre stabilmente l'economia italiana su un sentiero di crescita sostenuta e favorire l'occupazione. Si fonda su una graduale e incisiva riduzione del carico fiscale, volta a incoraggiare l'offerta di lavoro e gli investimenti in capitale fisico e umano e a sostenere i consumi delle famiglie. Numerosi interventi sono finalizzati a sostenere strutturalmente la competitività del sistema economico del Paese.*
Nel corso dell'esame in Parlamento, la legge di stabilità si è arricchita di importanti novità che ne hanno potenziato gli effetti espansivi con l'obiettivo di accelerare la crescita, come gli ulteriori interventi per favorire gli investimenti nel Mezzogiorno. Inoltre, in considerazione dei gravi fatti di terrorismo, per rafforzare l'apparato di sicurezza nazionale è stato approvato un pacchetto di misure che si muove lungo due direttrici: contrastare il rischio che si possano verificare episodi di terrorismo attraverso l'ammodernamento delle dotazioni strumentali in uso alle forze di sicurezza e di difesa, il potenziamento delle loro capacità di sorveglianza e della sicurezza informatica, l'incremento del trattamento economico del personale dei due comparti; rafforzare ulteriormente la difesa dei valori culturali che sono i pilastri della nostra società con interventi che vanno dalla riqualificazione urbana delle periferie alle iniziative per accrescere il patrimonio culturale da parte dei giovani." Legge di stabilità del 2016, sito ufficiale del Ministero dell'Economia e delle Finanze: https://www.mef.gov.it/focus/Legge-di-Stabilita-2016/
[189] Monitoraggio del Piano triennale: https://monitoraggiopianotriennale.italia.it/, visto in agosto 2021

dell'Agenzia, inoltre, è possibile consultare in qualunque momento gli andamenti degli scopi prefissati misurati in percentuali.

Ovviamente, ogni Piano è caratterizzato da dei principi guida che ne caratterizzano gli scopi: tra questi si trovano il "*principio digital & mobile first*" riferito a tutti quei servizi che richiedono l'accesso tramite l'identità elettronica (spid) come, ad esempio, l'attivazione del Fascicolo Sanitario Elettronico; il "*cloud first (cloud come prima opzione)*" che serve come una garanzia per le pubbliche amministrazioni; la presenza di alcuni servizi inclusivi e accessibili che tengano conto delle diverse necessità degli utenti e che risultino "interoperabili by design" in modo che essi non riscontrano problematiche nelle varie parti del territorio tramite le API;[190]inoltre, la sicurezza e la privacy by design costituiscono elementi essenziali affinchè siano predisposti dei servizi digitali che siano in grado di proteggere i dati ivi contenuti ed eventualmente fronteggiare un *data breach*[191]*;* il "*user-centric, data driven e agile*", ciò che le amministrazioni intendono fare è migliorare costantemente i loro servizi offerti ai clienti; il "*principio once only*" inoltre prevede che le pubbliche amministrazioni richiedano i dati ai propri clienti solo una volta per evitare accumulo di informazioni già rilasciate; i dati pubblici, sono considerati come un bene comune poiché di rilevante importanza ai fini dello sviluppo del Paese; da ultimo si menziona la prassi del "codice aperto", ovvero i software che vengono usati dalle amministrazioni, che deve presentare il codice sorgente[192].

Ovviamente, prima che l'AgiD predisponga il Piano Triennale, è necessaria una preventiva programmazione europea, quella attuale è relativa al periodo 2021-2027, seguita dai principi dell'eGovernment Action Plan 2016-2020 e da quanto previsto dalla eGovernment Declaration

---

[190] "*Le API (acronimo di Application Programming Interface, ovvero Interfaccia di programmazione delle applicazioni) sono set di definizioni e protocolli con i quali vengono realizzati e integrati software applicativi. Consentono ai tuoi prodotti o servizi di comunicare con altri prodotti o servizi senza sapere come vengono implementati, semplificando così lo sviluppo delle app e consentendo un netto risparmio di tempo e denaro. Durante la creazione di nuovi strumenti e prodotti o la gestione di quelli esistenti, le API offrono flessibilità, semplificano la progettazione, l'amministrazione e l'utilizzo, e garantiscono opportunità di innovazione.*
Talvolta vengono concepite come una forma di contratto, con una documentazione che rappresenta un accordo tra le parti: se la parte A invia una richiesta remota strutturata in un determinato modo, il software della parte B risponderà in un altro modo determinato." Definizione di API rinvenibile online: https://www.redhat.com/it/topics/api/what-are-application-programming-interfaces, visto in agosto 2021

[191] Si veda il paragrafo 4 del capitolo 1.

[192] "*Il codice sorgente è il testo di un algoritmo di un programma. Il nome "sorgente" è dovuto al fatto che il codice rappresenta il punto di partenza di tutto il processo di esecuzione del programma. Va detto, per altro, che anche se in teoria il codice sorgente è scritto in un linguaggio di programmazione, ormai nella pratica si parla di codici sorgenti anche per indicare i linguaggi di markup o altri testi scritti non in un linguaggio di programmazione.*
Dal punto di vista strutturale, il codice sorgente è una sorta di algoritmo risolutivo: il programmatore, attraverso un editor di testo che appartiene a un ambiente di sviluppo integrato, scrive il codice tenendo conto della sintassi e del lessico del linguaggio di programmazione a cui fa riferimento. I programmatori più esperti, in verità, non affrontano lo sviluppo e si occupano direttamente della soluzione algoritmica." Definizione di codice sorgente rinvenibile online: https://www.artera.net/it/blog/programmazione/codice-sorgente-software/, del 15 giugno 2016

of Tallinn, che indicano l'effettiva incidenza della tecnologia nell'uso quotidiano sia da parte dei cittadini sia da parte delle imprese e costituiscono gli indicatori dei livelli di digitalizzazione.

Per la stesura di ogni Piano, si vede l'operato del Ministro per l'innovazione tecnologica e la digitalizzazione, un gruppo di lavoro interno all'Agenzia e varie amministrazioni centrali, le regioni e le città metropolitane, così da favorire anche un tipo di attività di cooperazione tra quelli che saranno gli effettivi soggetti coinvolti nell'attività di digitalizzazione, come riportato dagli stessi rapporti redatti dall'AgiD "*Il Piano triennale è elaborato sulla base dei dati e delle informazioni raccolte presso le pubbliche amministrazioni e, a tal fine, annualmente l'Agenzia effettua una rilevazione sulla spesa ICT delle Pubbliche amministrazioni centrali e locali. Nel 2019 è avviata la terza rilevazione: nel tempo, il panel costituito originariamente da 20 amministrazioni centrali (inclusi ACI, Inps, Inail e Agenzie fiscali) si è ampliato, con l'ingresso di Regioni, Città metropolitane e loro Comuni capoluogo. Da ultimo hanno fatto il loro ingresso gli Enti di ricerca e la Corte dei conti: ad oggi il panel è costituito da circa 80 amministrazioni, la cui spesa ICT copre circa l'80% della spesa totale di un perimetro che esclude la spesa ICT del settore sanitario e dell'istruzione scolastica universitaria*."[193]

Per quanto riguarda il settore sanitario, oggetto dell'elaborato, bisogna indicare due interventi dell'AgiD di significativa importanza: la Strategia per la crescita digitale e il Piano Triennale per l'informatica nella Pubblica Amministrazione. Questi due strumenti hanno definito le azioni che sono state predisposte nell'ambito sanitario indicative delle possibili soluzioni per ottimizzare i servizi sanitari offerti, limitare i disguidi che possono accadere e andando a ridurre le differenze in tutto il territorio nazionale per raggiungere una situazione di uniformità di servizi "*Lo sviluppo della strategia deve, infatti, avvenire secondo la logica della co-progettazione, anche valorizzando le best practices sul territorio per definire piani e standard nazionali*."[194] Secondo quanto riferito dalla Strategia per la crescita digitale, la digitalizzazione della sanità, in seguito all'introduzione dello strumento del Fascicolo Sanitario Elettronico da parte del Ministero della Salute nel 2011, ha subìto un forte incremento, grazie all'approvazione e alla previsione dello stesso in diversi strumenti normativi. È stato rilevato però, come visto nel paragrafo precedente, la diversità di attivazione e applicazione dello strumento, e l'Agenzia sostiene che questo è dovuto allo scarso livello di informatizzazione delle aziende sanitarie italiane, riscontrando non pochi problemi per quanto riguarda il rilascio delle ricette dematerializzate e il pagamento di

[193] Rapporto AgiD sulla spesa ICT nella Sanità territoriale italiana, rinvenibile online l'intero documento: https://www.agid.gov.it/sites/default/files/repository_files/rapporto_agid_sulla_spesa_ict_nella_sanita_territoriale_italiana.pdf, visto in agosto 2021

[194] Documento "Strategia per la crescita digitale" pagina 7, rinvenibile online: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf, roma, 3 marzo 2015.

ticket online. Alla base vi è quindi non solo un problema di diffusione, ma anche di accettazione del digitale nelle attività quotidiane, problema a cui l'Agenzia ha cercato di sopperire tramite il Patto per la Sanità Digitale21[195].Il Piano Triennale per l'Informatica nella Pubblica Amministrazione, invece, prevede tre strumenti vincenti per l'attuazione degli obiettivi prefissati: al Fascicolo Sanitario Elettronico (FSE), di cui si è parlato nello scorso paragrafo, è stato attribuito il ruolo di "infrastruttura abilitante", al Centro Unico di Prenotazione (CUP) è stato dato il valore della comunicazione semplice tra i cittadini e le Pubbliche Amministrazioni, e da ultimo la Telemedicina, protagonista del capitolo 1, che è stata funzionale alla descrizione del rapporto con il territorio. Si è già discusso circa l'innovativo strumento del Fse, considerato quindi come un grosso passo in avanti per quanto riguarda la digitalizzazione del rapporto medico-paziente e di cui l'AgiD effettua l'analisi circa la sua applicazione e divulgazione nelle singole regioni italiane.

Oltre a quanto elencato, si prevedono altri strumenti con finalità analoghe.

Il Centro unico di prenotazione (CUP) è un sistema straordinario poiché permette a tutti coloro che sono in possesso della tessera sanitaria italiana di poter effettuare delle prenotazioni di prestazioni sanitarie, avendo quindi un accesso diretto ai servizi e riducendo di molto i tempi di attesa, basti pensare, ad esempio, all'elemento fondamentale della velocità di ottenere una visita e quindi un referto ai fini di una terapia vincente.

La Telemedicina[196], soprattutto come dimostrato in epoca Covid-19, offre un servizio del tutto nuovo: ora infatti è possibile ricevere una consulenza medica da remoto in qualunque momento,

---

[195] "*Il Patto per la Sanità Digitale: è stato stipulato con l'obiettivo di elaborare un Master Plan triennale (2015-2017) per la sanità elettronica, identificando le principali direttive per lo sviluppo digitale nel mondo della salute al fine di sostenere una maggiore continuità assistenziale ospedale-territorio.*
Il fine del Patto per la Sanità Digitale è quello di promuovere su tutto il territorio nazionale l'adozione delle tecnologie digitali, secondo delle priorità strategiche di riferimento, per allineare l'Italia agli standard europei, soprattutto nelle pratiche di presa in carico del paziente.
Più specificatamente il Patto promuove l'adozione del Fascicolo Sanitario Elettronico come strumento fondamentale per la gestione del paziente secondo un Piano Assistenziale Individuale, che integri il contributo in network di tutti gli attori coinvolti e la diffusione di pratiche di telemedicina, teleconsulto e telemonitoraggio, per rendere più facile ed efficiente l'integrazione stessa. Inoltre è fortemente raccomandata la costituzione a livello centrale di banche dati che permettano una conoscenza diffusa e integrata relativa a tutte le attività di servizio sanitario e alla loro spesa, per poter poi implementare una governance "Real World Based". "*Patto per la Sanità Digitale e eHealth*" articolo online: https://www.coinnova.it/contesto/linee-guida/patto-sanita-digitale-ehealth visto in agosto 2021

[196] "*La Telemedicina si può realizzare per le seguenti finalità sanitarie: Prevenzione secondaria Si tratta di servizi dedicati alle categorie di persone già classificate a rischio o persone già affette da patologie (ad esempio diabete o patologie cardiovascolari), le quali, pur conducendo una vita normale devono sottoporsi a costante monitoraggio di alcuni parametri vitali, come ad esempio, tasso di glicemia per il paziente diabetico, al fine di ridurre il rischio di insorgenza di complicazioni. Diagnosi Si tratta di servizi che hanno come obiettivo quello di muovere le informazioni diagnostiche anziché il paziente. Un iter diagnostico completo è difficilmente eseguibile attraverso l'uso esclusivo di strumenti di Telemedicina, ma la Telemedicina può costituire un completamento o consentire approfondimenti utili al processo di diagnosi e cura, ad esempio, attraverso la possibilità di usufruire di esami diagnostici refertati dallo specialista, presso l'ambulatorio del medico di medicina generale, la farmacia, il domicilio del paziente. Cura Si tratta di servizi finalizzati ad operare scelte terapeutiche ed a valutare l'andamento*

servizi di diagnosi e un costante monitoraggio di quelli che sono i parametri vitali della persona sottoposta alle cure, tutto grazie a una rete internet che permette di mantenere in contatto i medici con i propri pazienti, al fine di guidarli nel percorso di guarigione. L'AgiD e il Ministero della Salute, infatti, si impegnano a rilasciare Linee Guida Nazionali al riguardo "*L'innovazione tecnologica può contribuire a una riorganizzazione della assistenza sanitaria, in particolare sostenendo lo spostamento del fulcro dell'assistenza sanitaria dall'ospedale al territorio, attraverso modelli assistenziali innovativi incentrati sul cittadino e facilitando l'accesso alle prestazioni sul territorio nazionale. Le modalità di erogazione delle prestazioni sanitarie e socio-sanitarie abilitate dalla telemedicina sono fondamentali in tal senso, contribuendo ad assicurare equità nell'accesso alle cure nei territori remoti, un supporto alla gestione delle cronicità, un canale di accesso all'alta specializzazione, una migliore continuità della cura attraverso il confronto multidisciplinare e un fondamentale ausilio per i servizi di emergenza-urgenza*."[197]

Ogni persona iscritta al Servizio Sanitario Nazionale (SSN) riceve la propria Tessera Sanitaria (TS)[198], che permette l'accesso della persona alle prestazioni sanitarie che vengono offerte dal sistema nazionale su tutto il territorio italiano. Inoltre, tramite la tessera è possibile ricevere il proprio codice fiscale, essenziale anche ai fini dell'attivazione del proprio Fascicolo Sanitario Elettronico, e la Tessera di assicurazione malattia per quanto riguarda l'attestazione dell'assistenza sanitaria in tutto il territorio europeo.

Anche le ricette digitali svolgono il loro importante contributo all'informatizzazione della sanità: infatti, ora è possibile ottenere le ricette dal proprio medico generale o specialista, e ottenere la prestazione ivi descritta senza neanche servirsi del cartaceo. Modo di ottenere la ricetta abbastanza economico e rapido, se si pensa al fatto che prima era necessario recarsi presso lo

---

prognostico riguardante pazienti per cui la diagnosi è ormai chiara. Si tratta ad esempio, di servizi di Teledialisi o della possibilità di interventi chirurgici a distanza. 11 Riabilitazione Si tratta di servizi erogati presso il domicilio o altre strutture assistenziali a pazienti cui viene prescritto l'intervento riabilitativo come pazienti fragili, bambini, disabili, cronici, anziani. Monitoraggio. Si tratta della gestione, anche nel tempo, dei parametri vitali, definendo lo scambio di dati (parametri vitali) tra il paziente (a casa, in farmacia, in strutture assistenziali dedicate…) in collegamento con una postazione di monitoraggio per l'interpretazione dei dati." Finalità della Telemedicina descritte dalle Linee di indirizzo nazionale a pagina 10-11 del documento in rete: https://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf

[197] Linee di indirizzo nazionale sulla Telemedicina del Ministero della Salute, rinvenibili in rete: https://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf

[198] "*La Tessera Sanitaria è il documento personale che ha sostituito il tesserino plastificato del codice fiscale; viene rilasciata a tutti i cittadini italiani aventi diritto alle prestazioni fornite dal Servizio Sanitario Nazionale (SSN). A partire dal 2011, la Tessera Sanitaria è sostituita dalla Tessera Sanitaria-Carta Nazionale dei Servizi (TS-CNS), dotata di microchip.*

La nuova versione della Tessera Sanitaria rappresenta l'evoluzione tecnologica della Tessera "TS" (senza chip), in quanto, oltre ai servizi sanitari normalmente fruibili con la TS, permette anche l'accesso ai servizi offerti in rete dalla Pubblica Amministrazione, in assoluta sicurezza e nel rispetto della privacy." Definizione offerta da Sistema Tessera Sanitaria, in rete:
https://sistemats1.sanita.finanze.it/portale/tessera-sanitaria

studio del medico. Anche questo strumento finalizzato al miglioramento della medicina poiché rende possibile un intervento tempestivo e una cura immediato nei confronti del paziente, magari dopo aver effettuato una visita da remoto.

Nello scorso capitolo, si è inoltre parlato della dematerializzazione dei referti medici e delle cartelle cliniche, effettuando la distinzione tra queste ultime e la documentazione radiologica ma in generale si può affermare che la loro digitalizzazione è un modo per ottenere vari documenti che, come si è visto, hanno assolutamente valore giuridico di atto pubblico. Pertanto, questi saranno destinati a rivoluzionare la conservazione dei dati personali dei pazienti e le informazioni circa i loro referti, diventando quindi doverosa una tutela giuridica idonea e una regolamentazione di come tenere dette documentazioni in modo legittimo e sicuro, adottando tutte quelle misure necessarie in sede di azienda sanitaria volte a evitare, o meglio, fronteggiare un eventuale *data breach*. Il lavoro effettuato dall'Agenzia vede protagoniste le "Linee guida per la Dematerializzazione del Consenso Informato in Diagnostica per Immagini"[199] redatte grazie anche all'intervento delle Società Italiana di Radiologia Medica e Interventistica (SIRM)[200]. Ponendo come prima definizione quella del "Consenso informato" "*Il consenso informato è un obbligo contrattuale e la violazione del dovere d'informazione dà luogo a precise responsabilità. In particolare la Convenzione di Oviedo (Legge 145, 28 marzo 2001) dedica alla definizione del consenso il capitolo 2, art. da 5 a 9, in cui stabilisce, come regola generale che "un intervento, nel campo della salute, non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato. Questa persona riceve innanzitutto una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle conseguenze e i suoi rischi. La persona interessata può in qualsiasi momento, liberamente ritirare il proprio consenso*.", le Linee Guida si occupano di disciplinare tutta la materia relativa al processo di dematerializzazione, menzionando la normativa di riferimento e tutte le fasi affinché sia instaurato correttamente il trattamento dei dati dei pazienti.

---

[199] Circolare AgID n. 1/2018 del 24/gennaio/2018 "Linee guida per la Dematerializzazione del Consenso Informato in Diagnostica per Immagini", in rete: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/18241028510O__O01+-+AGID+CIRC+n.+01+-+24+gen+2018.pdf

[200] "*lo sviluppo delle linee guida per la dematerializzazione del consenso informato (DCI) contenute in questo documento, affidando la sua realizzazione alla Sezione di studio di Radiologia Informatica con Sezione di studio di Etica e Radiologia Forense e alla Commissione Consenso Informato della società. Le linee guida oggetto della sperimentazione promossa dalla SIRM sono destinate sia all'ambito ospedaliero che all'ambito ambulatoriale, sia Pubblico che Privato in modo indistinto, così come indistinta è la Normativa a cui esse fanno riferimento. Fin dalle prime fasi il gruppo di lavoro ha invitato a far parte del progetto stakeholder industriali del settore IT i quali hanno aderito partecipando alla iniziale fase di sperimentazione clinica e contribuendo alla stesura delle sezioni ad elevato contenuto tecnologico*." Premessa della Circolare AgID n. 1/2018 del 24/gennaio/2018 "Linee guida per la Dematerializzazione del Consenso Informato in Diagnostica per Immagini" pagina 6 , in rete: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/18241028510O__O01+-+AGID+CIRC+n.+01+-+24+gen+2018.pdf

Si noti quindi come i Piani predisposti dall'Agenzia, ma anche la sua attività in generale, comportino indirettamente degli adempimenti a carico delle amministrazioni locali, esercitando quindi una forte influenza. Infatti, principi fondamentali degli ultimi Piani predisposti da AgiD sono quelli relativi all'inclusività, poiché le pubbliche amministrazioni hanno il dovere di predisporre dei servizi che siano resi accessibili a chiunque e che tengano conto delle esigenze di tutta la collettività, e quelli relativi all'interoperabilità, rendendo così l'uniformità dei servizi digitali offerti, l'elemento essenziale per un'integrazione totale, poiché qualora i servizi non lo siano di *default*, implicherebbero ulteriori costi per renderli interoperabili, ad esempio in un'ottica di programmazione o di procedure d'appalto.

3.4 Il Personal Health Record e il Dossier Médical Personnel, l'esperienza americana, inglese e francese.

Come abbiamo visto nel capitolo secondo di questo elaborato, il forte impatto delle nuove tecnologie sulla sanità ha caratterizzato non solo l'esperienza italiana ed europea, ma anche quella americana. È estremamente interessante, quindi, notare come sistemi e Paesi diversi dal nostro, si siano ritrovati a dover fronteggiare la stessa sfida imposta dal progresso digital-sanitario, incontrando non poche difficoltà, ma dando vita a un nuovo modo di fare medicina.

Analizzando la situazione americana, bisogna premettere che, fino agli anni 2000, le tecnologie digitali adoperate all'interno dei sistemi sanitari, come le Health Information Technology, erano pressoché nulle. Secondo le stime[201], infatti, meno del 10% delle strutture sanitarie americane avevano adottato le suddette tecnologie e solo il 16% dei medici di medicina generale americani aveva adottato l'Electronic Health Record, la versione americana del nostro Fascicolo Sanitario Elettronico. Come causa di questo primario scarso sviluppo americano, vi era l'elevato costo di mantenimento di questi tipi di sistemi all'interno delle strutture e la non piena coscienza dei benefici di questi strumenti: infatti, si riteneva che questi sistemi comportassero solo innumerevoli azioni burocratiche in capo al personale dei servizi e gli strumenti idonei a supportarli avrebbero dovuto essere veramente innovativi, cosa non sempre possibile nelle strutture sanitarie. Quindi, inizialmente, riuscirono ad adottare tali strumenti solo quelle strutture che presentavano finanziamenti sufficienti ad adottare nuovi sistemi. Doverosi di menzione, sono stati infatti i sistemi "Kaiser Permanente" e il "Veterans Health Administration (VHA)", essendo stati i primi ad essere adottati.

Il Kaiser Permanente's HealthConnect system si basava sul sistema Epic EHR[202], il software più usato in grado di rintracciare circa otto milioni e seicentomila pazienti in nove diversi Stati e

[201] Dati presenti nel documento online "PAOLO GUARDA FASCICOLO SANITARIO ELETTRONICO E PROTEZIONE DEI DATI PERSONALI", pagina 75, in rete: http://eprints.biblio.unitn.it/2212/1/guarda_fasc_sanit_elettr_94_e-book.pdf, 2011

[202] "*Epic is a cloud-based EHR solution catering to a number of specialties. The software is in use across a broad range of practices, from community hospitals and independent practices to multi-specialty hospital groups and hospice care providers. Epic offers the standard range of 'core' EHR features, and practices can add modules depending on specialty. Epic has a strong focus on patient engagement and facilitating remote care. An extensive patient portal, available as a native app for both Android and iOS operating systems, allows patients more flexibility in managing their healthcare requirements. On top of this Epic offers numerous telehealth options - from supporting video visits and post-surgical follow-ups to patient monitoring features. Epic also emphasizes interoperability and easy integration with third-party systems. More Epic physicians have attested to Meaningful Use Stage 2 than users of any other system, and records can be shared with any EHR that uses these standards. Open.epic - Epic's open API - aims to facilitate integration with third-party software and apps. Epic EHR is cloud-based, so available on*

quattordicimila medici in centinaia di ambulatori e ospedali. Calcolando quindi l'attività straordinaria che è capace di compiere questo tipo di software, possiamo comprendere quanto sia rilevante il beneficio di riuscire a conservare i dati di ogni paziente che ha ricevuto almeno una prestazione sanitaria e che è stato registrato tramite questa piattaforma. I servizi offerti sono molteplici: ad esempio, i medici specialisti sono avvisati in tempo reale, se il paziente in questione non si è sottoposto a una visita di *screening* di prevenzione, oppure è possibile per i pazienti accedere ai loro dati sanitari ed eventualmente ottenere dei consulti tramite un sistema di messagistica con il personale medico. Considerando che circa tre milioni di pazienti sono registrati tramite questo sistema e tenendo conto che circa centomila accessi al giorno vengono effettuati regolarmente, possiamo affermare che sistemi come questo risultino assolutamente validi e idonei a migliorare l'assistenza sanitaria, valorizzando la prevenzione, e quindi gestendo in modo ottimale le terapie delle malattie croniche.

L'altro sistema che è stato adoperato negli USA è stato il Veterans Health Administration (VHA), invece, dotato dell'architettura "VistA", una delle piattaforme più conosciute in ambito sanitario che, servendosi dei sistemi IT, è stata in grado di ridurre la percentuale di errori terapeutici. I due sistemi ora menzionati hanno collaborato con il fine di condividere i dati dei pazienti registrati tramite entrambi, impresa ora circoscritta a solo piccole parti di territorio americano. Da quanto detto nel primo capitolo dell'elaborato, ultimamente grosse aziende stanno investendo sempre di più nel settore della digital health, ad esempio Google ha creato il suo Google Health, un servizio completamente dedicato all'anamnesi remota della persona incentrata sul suo stile di vita, ma anche il colosso Microsoft è sempre più interessato a questo nuovo mercato. Sulla base di tutto questo si può quindi capire come i rischi per i dati dei pazienti si facciano sempre più reali e tangibili e solo lontanamente immaginabili.

Data la situazione iniziale in America, il Presidente Obama ha firmato una legislazione nel 2009, l'American Recovery and Reinvestment Act (ARRA), un accordo con cui si sono previsti ventisette miliardi di dollari destinati a favorire l'adozione delle ultime tecnologie in ambito sanitario. Oltre al precedente atto, necessita di menzione anche l'Health Information Technology for Economic and Clinical Health Act (HITECH), un altro atto che ha dato vita al ruolo del National Coordinator for Health Information Technology che ha il dovere di effettuare delle comparazioni periodiche tra quello che è il Federal Health IT Strategic Plan, ovvero il piano prefissato, e quelli che sono gli obiettivi raggiunti. Scopi principali di questi atti sono: migliorare la qualità delle cure e cercare di ridurre al minimo l'errore medico, creare un rapporto medico-

any device with an internet browser installed. Native apps are available for iOS and Android operating systems." Sito ufficiale di Epic: https://www.ehrinpractice.com/epic-ehr-software-profile-119.html, visto in agosto 2021

paziente più diretto, incentivare economicamente la salute pubblica con il fine di raggiungere standard elevati, garantire un'assistenza adeguata ma soprattutto promuovere e tutelare la privacy dei dati contenuti negli Electronic Health Records[203].

Avendo quindi illustrato quali sono stati i piani predisposti per il raggiungimento di una sanità digitalizzata, è necessario discorrere circa la protezione dei dati sanitari negli Stati Uniti.

In America, il diritto alla riservatezza dei dati sanitari è regolato da una moltitudine di leggi e regolamenti: al centro del sistema vi è il ruolo degli Stati che tramite l'emanazione di vari *statute* regolano la materia, dettando leggi diverse da Stato a Stato. Il 1996 ha rappresentato un anno di svolta per quanto riguarda la disciplina, poiché il Congresso federale decise di emanare un atto di rilevante importanza, l'Health Insurance Portability and Accountability Act (HIPAA), seguito poi da altri regolamenti che ebbero lo scopo di specificare l'applicazione garantendo una disciplina abbastanza uniforme e centrale rispetto a quelle proprie degli Stati. Si può affermare però che la vera prima regolamentazione sulla protezione dei dati a livello federale è la disciplina applicativa dell'atto sopramenzionato, seguita successivamente dai regolamenti del Department of Health and Human Services, volti a rendere la disciplina chiara e di facile attuazione, garantendo però la facoltà degli Stati di porre in essere le loro specifiche leggi, che ovviamente risultano essere più idonee ai loro ordinamenti interni. Negli anni duemila, vi era però la necessità di una normativa onnicomprensiva in materia: vi susseguirono diversi interventi e modifiche normative, presentando come prodotto finale l'entrata in vigora della normativa HIPAA nell'aprile del 2003. Questa, infatti, costituisce la disciplina più completa sulla protezione dei dati poiché presenta determinate misure che devono essere necessariamente impiegate col fine di ottimizzare la sicurezza dei dati. Il percorso normativo americano che ha condotto a questo risultato ha trovato la sua ragione nella volontà di permettere l'accessibilità e la sicurezza dei dati sanitari quando vengono trattati in strutture sanitarie, garantendo le "*protected health information*" (PHI)[204].

---

[203] "*L'Health Information Technology for Economic and Clinical Health (HITECH), emanato come parte dell'American Recovery and Reinvestment Act del 2009, è stato firmato in legge il 17 febbraio 2009, per promuovere l'adozione e l'uso significativo della tecnologia dell'informazione sanitaria. Il sottotitolo D dell'HITECH Act affronta i problemi di privacy e sicurezza associati alla trasmissione elettronica di informazioni sanitarie, in parte, attraverso diverse disposizioni che rafforzano l'applicazione civile e penale delle norme HIPAA*." In rete: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html, 16 giugno 2017

[204] "*Protected health information (PHI), also referred to as personal health information, is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the primary law that oversees the use of, access to and disclosure of PHI in the United States. HIPAA defines PHI as data that relates to the past, present or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. HIPAA regulates how this data is created, collected, transmitted, maintained and stored*

Ovviamente, sarebbe stato impossibile porre degli *standard* specifici in via preventiva essendo un fenomeno del tutto nuovo e in evoluzione, quindi, la normativa stabilì che i livelli di sicurezza da raggiungere sarebbero stati definiti in modo del tutto graduale e in evoluzione con le tecnologie. Il risultato di questo approccio è una normativa straordinaria figlia del presente digitalizzato, "*un modello di information security deve essere in termini di adattabilità e flessibilità*", riconoscendo il ruolo importante delle misure di sicurezza nella gestione dei dati in ambito sanitario. Ma, il modello americano che ha voluto porre la sua flessibilità come il suo punto di forza, in realtà, è stato fortemente criticato, poiché disposizioni estremamente vaghe e generiche potrebbero risultare piuttosto pericolose in merito alla sicurezza dei dati.

La discrezionalità garantita dalla normativa ai titolari dei trattamenti risulta, invece, una strategia apparentemente vincente: infatti questi avranno l'onere di effettuare scelte molto più consapevoli poiché eventuali rischi o danni saranno oggetto della loro responsabilità. Nella prassi americana si parla di due fenomeni diversi, il "*health privacy issue*" e il "*protective model*", elaborati sulla concezione che il momento pericoloso per i dati sanitari è la loro raccolta e la loro divulgazione. Quindi, la legge ha ovviato a questa situazione di rischio ponendo due modelli di sicurezza.

Da un lato, si prevede un modello che vieta qualsiasi trattamento di dati in specifiche circostanze, dall'altro, si adotta un approccio basato alla limitazione della divulgazione degli stessi, vale a dire, permette la consultazione del Personal Health Record solo ed esclusivamente ai medici designati e non anche ad altri soggetti terzi non necessari. Bisogna constatare inoltre, che il common law americano non presenta particolari sistemi di risoluzione in seguito a danni derivanti da minacce digitali e inoltre è espressamente consentito dalla legge ai pazienti di demandare l'intera gestione dei loro dati ad altra persona[205], rendendo quindi la trasferibilità del dato quasi una prassi comune, approccio totalmente opposto a quello europeo esaminato nel

by any HIPAA-covered organization. Healthcare deals with sensitive details about a patient, including birthdate, medical conditions and health insurance claims. Whether in a paper-based record or an electronic health record (EHR) system, PHI explains a patient's medical history, including ailments, various treatments and outcomes." Definizione di Protected Health Information, disponibile *"protected health information (PHI) or personal health information*" articolo scritto da Ben Lutkevich, Technical WriterScott Wallask, Editorial DirectorAlex DelVecchio, Content Development Strategist, in rete: https://searchhealthit.techtarget.com/definition/personal-health-information, visto in agoto 2021

[205] Definita come la "Dottrina della rinuncia" "[…]*We therefore hold that when a patient sues a defendant other than his or her physician, and the information acquired by the physician as a result of the physicianpatient relationship would be legally discoverable by the defendant in that litigation, then the patient will be deemed to have waived any right to proceed against the physician for the physician's disclosure of this information to that defendant or that defendant's attorney.[2] Our recognition *955 of this narrow exception does not, however, encompass a physician's disclosure of information acquired during the physicianpatient relationship to persons other than such a defendant or that defendant's attorney. To hold otherwise and allow public disclosures to unrelated third parties would not only contravene our recognition of the physician's primary duty of non-disclosure in Horne, supra, but also flout the policy considerations protecting the patient's privacy interest in full, confidential disclosure to his or her physician to obtain an accurate diagnosis and treatment.[3]*[…]" Mull v. String 448 So. 2d 952 (1984) Supreme Court of Alabama,March 16, 1984. Caso rinvenibile in rete: https://law.justia.com/cases/alabama/supreme-court/1984/448-so-2d-952-1.html

capitolo secondo di questo elaborato. Quindi, la disciplina Health Insurance Portability and Accountability Act, rappresenta una vera e propria eccezione rispetto all'uso comune americano, essendo però piuttosto debole per apportare un cambio radicale, poiché sono sempre presenti delle clausole di salvaguardia nelle "*Privacy Provision*" riferenti alle legislazioni statali. L'obiettivo della normativa HIPAA rimane quello di assicurare ai pazienti una giusta comunicazione e informazione circa l'informativa in merito al trattamento dei loro dati, così da riuscire a proteggere i loro fascicoli elettronici.

Dopo aver esaminato la disciplina relativa alla sicurezza dei dati sanitari negli Stati Uniti, è opportuno volgere lo sguardo alla sanità inglese, interesse di circa cinquanta milioni di persone. Il "National Health Service Plan (NHS Plan)", è stato il programma governativo volto all'evoluzione digitale in ambito sanitario, prevedendo specifici investimenti nei sistemi IT, elaborato dal Department of Health, e a livello locale, invece, opera l'attività di controllo e di coordinamento delle Strategic Health Authority[206].

Quello introdotto in Inghilterra, ha quindi rappresentato uno dei più grandi investimenti mondiali volti a rendere la sanità pubblica il più digitalizzata possibile, poiché, tramite questi è stato possibile rendere accessibili i dati dei pazienti qualora fosse risultato necessario. Fin dalla sua introduzione nel 2002 ad oggi, il piano si è rivolto non solo a tutti i cittadini e ai medici ma anche a tutte le organizzazioni operanti nel settore. Il National Health Service Plan, però, è costituito a sua volta da altri sottoprogrammi, per raggiungere in modo ottimale tutti gli obiettivi prefissati angli inizi degli anni duemila. Tra questi si ricomprendono innanzitutto il "NHS Care Record Service (NHS CRS)", ovvero un fascicolo sanitario elettronico equivalente al nostro italiano ed equivalenti al Personal Health Record americano, quindi l'insieme degli eventi sanitari della persona, con lo scopo di rendere queste informazioni facilmente trasmissibili tra paziente e medico. Il "Choose and Book", invece, è un servizio attivo in tutto il Paese che permette alla persona di prenotare in modo facile e veloce la visita medica di cui necessita, scegliendo la struttura più vicina a lui e il giorno della prestazione. Infatti, scopo della telemedicina, come osservato nel primo capitolo, è anche quello di rendere il paziente il protagonista e quindi l'unico a poter prendere decisioni circa il suo stato di salute, rendendo allo stesso tempo il processo di

[206] "*Strategic Health Authorities were organisations within the NHS in England that were responsible for developing and improving health services in their local area, ensuring quality, measuring performance and making sure that national priorities were integrated into local plans. Under the changes to the NHS that came into effect in April 2013, the 10 SHAs and the 152 Primary Care Trusts (PCTs), which looked after services at a local level, were replaced by NHS England and more than 200 Clinical Commissioning Groups. Scotland, Wales, and Northern Ireland run their NHS services separately*." Definizione di Strategic Health Authority fornita dall'articolo "Strategic Health Authorities (SHAs)" in rete: https://mstrust.org.uk/a-z/ccg/strategic-health-authorities-shas

prenotazione più rapido ed efficace. L' "Electronic Prescription Service", ovvero il "sistema per la trasmissione elettronica delle prescrizioni mediche" permette un celere scambio di prescrizioni mediche tra il medico (colui che le rilascia), il farmacista (colui che le vende) e l'autorità statale (soggetto che si occupa del pagamento), per garantire una vendita di farmaci più sicura, scongiurando gli episodi di falso ideologico delle ricette. La "N3" ovvero la "NHS National Network" è la rete centrale ad alta velocità che collega tutti gli organismi del Piano, garantendo la comunicazione. Ed infine il programma "Picture Archiving and Communications System" che permette di adattare le immagini diagnostiche ai normali schermi, garantendone un'altissima definizione.

Il Piano inglese ha quindi seguito uno sviluppo costante e graduale, e grazie agli obiettivi raggiunti è stato in grado di mantenere connessi "*più di trentamila medici di medicina generale e duecentosettanta strutture del servizio sanitario*". Inoltre, esso si compone dei dati dettagliati, quindi quelli relativi ai pazienti in determinate porzioni di territorio, e del "Summary Care Record", una banca dati centrale e nazionale. Quindi, il National Health Service è il fascicolo sanitario elettronico individuale del cittadino, il Summary Care Record è invece costituito dalle informazioni di tutti i pazienti: il cittadino ha infatti la libertà di scegliere se essere inserito in quest'ultimo o meno o di limitarne gli accessi, ad esempio oscurando determinate informazioni, come quelle relative a determinate malattie, oppure richiedendo di volta in volta il proprio consenso qualora qualcuno faccia richiesta di accedervi. Quindi il paziente potrà accedere a questo tipo di fascicolo tramite il portale "Heal-thSpace" e dopo che il medico personale del paziente, avrà caricato le informazioni relative alla storia clinica, il Summary Care Record sarà ufficialmente disponibile e visibile sulla piattaforma. In questo modo il paziente potrà tenere traccia non solo della sua anamnesi remota, ma anche di tutti i suoi valori vitali, effettuando delle modifiche e delle comparazioni, risultando il solo e unico gestore della sua salute. Inizialmente, nel giugno del 2007, quando il Piano è stato lanciato, analogamente alle esperienze degli altri Stati, i pazienti che vi avevano aderito risultavano essere circa 615.000 proprio per la mancanza di fiducia in un sistema nuovo di gestione dei dati sanitari. Oggi alla luce anche di più di dieci anni di esperienza e della sempre più presente tecnologia nella nostra vita, il National Health System conta 803 mila accessi solo nel 2020 al suo sito internet, 3000 messaggi al secondo e 21 mila possibili minacce *online* ufficialmente fronteggiate[207] ogni mese, sintomi di un Piano vincente.

[207] Dati forniti dal sito ufficiale del National Health System: https://digital.nhs.uk/, visto in agosto 2021

Il Dossier Médical Personnel (DMP) è la versione francese del Fascicolo Sanitario Elettronico, ma prima di effettuare la sua trattazione, è opportuno illustrare il sistema sanitario in questo Paese.

A partire dagli anni ’80, si è assistito a un forte decentramento dei poteri, rendendo così le regioni sempre più autonome e il sistema sanitario francese può essere definito come “misto” poiché ivi sono presenti sia strutture pubbliche sia strutture private. Quindi, i cittadini francesi, che sono circa sessantadue milioni, sono assolutamente liberi di scegliere il loro medico di base, avendo a disposizione molteplici strutture sanitarie locali e regionali. Come tutti gli altri Paesi, anche la Francia ha adottato a livello nazionale varie iniziative volte alla digitalizzazione sanitaria: primo fra tutti, vi è il sistema “SESAM-Vitale”, introdotto nei primi anni 2000. Questi ha la capacità di connettere tutti i medici e gli operatori sanitari francesi (si parla di 223.000 soggetti), con il fine di rendere il servizio offerto a 48 milioni di assistiti più agevole. Il SESAM-Vitale è costituito a sua volta da altri tre importanti elementi: la “Carte Vitale” ovvero un microprocessore contenente importanti informazioni amministrative, la “Carte de Professionnel de Santé” (CPS), invece, è “*una smart card con microprocessore utilizzata dai medici di medicina generale, creata nel 1993 (potenziata poi attraverso l’Ordonnances Juppé dell’aprile del 1996, «organizzazione di una sicura infrastruttura elettronica per i sistemi informativi sanitari»*” le cui funzioni sono quelle di riuscire a autenticare, identificare l’operatore sanitario e permettergli di poter apporre la sua firma elettronica. Infine, la “Réseau santé social” (RSS), è “*la rete sanitaria atta a gestire i flussi di dati e ad incoraggiare la comunicazione tra operatori sanitari e fondi assicurativi sanitari*”. Inoltre, vi sono numero app e piattaforme a livello regionale interamente dedicate alla telemedicina e un portale ufficiale, creato dal Direttorato Generale della Sanità del Ministero, che permette la diffusione delle ultime ricerche sanitarie rilasciate dalle agenzie pubbliche.

Il Dossier Médical Personnel (DMP), è stato introdotto dalla Loi n. 2004-810 del 13 agosto 2004, sull’Assurance Maladie ed è menzionato nell’art. L. 161-36-1[208] del Code de la Sécurité Sociale.

[208] “*Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même code, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention. Ce dossier médical personnel est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8 du même code. L'adhésion aux conventions nationales régissant les rapports entre les organismes d'assurance maladie et les professionnels de santé, prévues à l'article L. 162-5 du présent code, et son maintien sont subordonnés à la consultation ou à la mise à jour du dossier médical personnel de la personne prise en charge par le médecin. Les dispositions de l'alinéa précédent sont applicables à compter du 1er janvier 2007*.” Testo dell’articolo rinvenibile online: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006741276/2004-08-17

Bisogna ammettere che, analogamente a quanto successo negli altri Paesi, la divulgazione di questo strumento, risulta ancora piuttosto limitata per colpa della non definitiva trasformazione digitale della professione sanitaria. Le finalità del Dossier Mèdical Personnel sono analoghe al nostro Fse, ovvero archiviare i dati sanitari dei pazienti e renderli accessibili a coloro che risultino abilitati. Questi però, essendo interamente controllato e gestito dal paziente, non è proprio del medico, poiché il fascicolo riporta "*i dati che permettono l'identificazione del paziente (nome, cognome, data di nascita, login per l'apertura e il funzionamento del dossier) ed informazioni che ne identificano il medico curante; dati di medicina generale (storia clinica, archivio delle consultazioni specializzate, allergie, intolleranze, vaccinazioni, ecc.); i dati relativi alle cure (risultati degli esami, resoconti degli atti preventivi e terapeutici, patologie in corso, trattamenti in corso, ecc.); i dati utili per la prevenzione (fattori di rischio individuale, resoconti preventivi, ecc.); i dati relativi a reperti clinici (radiografie, scanner)*."[209]Quindi, gli operatori sanitari vi accedono tramite le due *smartcard* CPS e la Vitale, e il paziente vi accede tramite il portale nazionale. Quest'ultimo inoltre deve adottare un sistema denominato "*hèbergeur*" previo contratto di "*hèbergement*", ovvero un contratto con il quale si assicura la sicurezza di dati poiché verranno rispettate le disposizioni di legge. Per incentivare l'utilizzo del Dossier Mèdical Personnel sono stati previsti dei rimborsi economici delle prestazioni mediche, rilasciate automaticamente al momento dell'accesso della persona al suo fascicolo. Quindi, il paziente è l'unico a poter entrare nel proprio fascicolo e ad amministrare le sue informazioni, e ha inoltre la possibilità di contenere tutti i *files* relativi ai referti o alle immagini diagnostiche, e ogni qual volta vi sia un accesso al suo fascicolo da parte di qualcuno, il paziente sarà prontamente avvisato. Vi è però una procedura di emergenza denominata "*bris de glace (rottura del vetro)*", volta a rendere note le informazioni dell'assistito in assenza del suo consenso al medico dell'emergenza proprio per permettere la conoscenza da parte di questi dello stato di salute della persona, ad esempio la presenza di allergie o patologie. È necessario, però, chiarire che, anche se la gestione del fascicolo è demandata al paziente, esso non avrà assolutamente diritto o possibilità di modificare i dati che vengono aggiunti dai medici curanti, bensì potrà solo cambiare i dati non sanitari presso l'*hèbergeur*. Quindi, si avrà il "diritto di *masquage*" ovvero la sua facoltà di nascondere alcune informazioni delicate e di limitarne l'accesso solo al professionista da lui indicato: questo tipo di diritto però ha suscitato non pochi dubbi, infatti, se è vero che il paziente può non rivelare determinate informazioni circa il suo stato di salute, è anche vero che allora si dovrebbe escludere la responsabilità del medico curante qualora adotti

[209] Elenco rinvenibile nel documento "Fascicolo Sanitario Elettronico e Protezione dei Dati Personali" di Paolo Guarda a pagina 68, online: http://eprints.biblio.unitn.it/2212/1/guarda_fasc_sanit_elettr_94_e-book.pdf

una terapia incompatibile con qualche patologia non dichiarata. A questo problema, infatti, il legislatore ha risposto disponendo delle tabelle specifiche in cui sono presenti tutte le tipologie di informazioni ed è indicato quale professionista sanitario risulta abilitato a conoscerle o meno. Quindi, per ogni paziente, vi sarà un solo *dossier* a livello nazionale, al quale ogni professionista, se abilitato, potrà accedervi, effettuando un lavoro concertato con gli altri medici curanti, sempre sotto la cosciente gestione dell'assistito.

CONCLUSIONI

A conclusione di quanto esposto nei tre capitoli è possibile ora comprendere il senso del discorso cominciato.

Scopo di questo elaborato è stato capire come partendo dalla volontà di progresso, caratteristica innata dell'uomo da sempre, si cerchi di raggiungere un'età dell'oro 2.0. Si è assistito a come l'adozione di strumenti tecnologici innovativi in ambito sanitario, abbia destabilizzato, seppur per un attimo, l'inviolabilità di determinati diritti umani.

Il progresso ha quindi costituito il *fil rouge* dell'intero discorso.

Si è discusso inizialmente circa il diritto alla salute, diritto personalissimo e assolutamente irrinunciabile, che pone costantemente dubbi di legittimità costituzionale riguardo molteplici fattispecie. Il rispetto di tale diritto, infatti, comporta non solo la garanzia del benessere fisico e psichico della società, ma, si può affermare che il risultato più importante perseguito sia il rispetto della dignità della persona in quanto tale, dovendo donare la possibilità a tutti gli individui presenti al mondo di poter condurre una vita in modo dignitoso per poter affermare la propria personalità. L'istituzione, quindi, del Servizio Sanitario Nazionale aveva proprio questo fine, garantire un'assistenza piena a chiunque necessiti di cure.

E come quasi tutti gli ambiti, anche quello sanitario ha subìto (*rectius* ha accolto) il progresso tecnologico, affermandosi negli ultimi anni la Digital Health, fenomeno esplicato e discusso nel capitolo primo, sinonimo e simbolo di futuro. Un tipo di sanità che pone ancor di più al centro del suo funzionamento la persona, poiché, tramite le nuove tecnologie, ora è possibile limitare nettamente tutti gli errori possibili in questo sistema, dalla mancata prenotazione di una visita all'errore medico durante una terapia o un intervento. Quello della sanità digitale è diventato uno degli ambiti più interessanti, avendo mosso particolare interesse sia dal punto di vista economico (si ricordino i numerosi investimenti effettuati negli ultimi anni) sia dal punto di vista legale: come visto nel secondo capitolo, questo continuo sviluppo ha obbligato i legislatori di ormai tutto il mondo a dover cercare di disciplinare la materia, e a continuare ad evidenziare l'importanza di determinati diritti che sono lo specchio della incredibile singolarità della persona, aspetto che risulta essere posto in pericolo da una tecnologia formata da *bit*.

Il legislatore europeo e italiano, hanno dovuto fronteggiare l'emergente *quaestio iuris* circa la possibile violazione della segretezza dei dati personali ad opera di un progresso che mai si arresta.

Avendo osservato, però, anche le ulteriori esperienze americane, inglese e francesi, è ormai noto che il presente digitale ha costituito sì un passo in avanti per l'uomo, ma anche una comune preoccupazione. Ed è stato quindi di rilevante interesse notare come anche altri Paesi diversi dall'Italia abbiano impiegato i loro strumenti giuridici per disciplinare fattispecie che anche solo vent'anni fa non sarebbero state neanche immaginabili. Normative, quelle adottate, che cercano di disciplinare fino al singolo aspetto della materia, ma che a volte, ovviamente, possono risultare piuttosto lacunose e incomplete, rendendo quindi necessario e prezioso l'intervento di soggetti di autorevole ruolo come il Garante per la protezione dei dati personali, in grado di far luce sulle questioni sempre nuove. Come accennato, sarebbe impossibile infatti cercare di redigere un Codice specifico per la materia poiché su di esso vi incomberebbe la mutevolezza dettata dal progresso.

È corretto quindi affermare che l'introduzione di strumenti tecnologici nelle attività sanitarie ha posto in serie difficoltà i legislatori di tutto il mondo, poiché a volte non si è stati in grado di criminalizzare determinate condotte e di tutelare situazioni particolarmente gravi e delicate, risultate però funzionali alle normative odierne. E se in determinati Paesi, come negli Stati Uniti d'America, il concetto di dato ha più un valore economico che personale, in Europa, come sempre, l'atteggiamento risulta del tutto diverso, poiché la riservatezza è parte fondamentale della persona, costituendo l'ultimo baluardo caratteristico della nostra tradizione europea, uno dei pilastri fondamentali della civiltà occidentale.

Si è poi osservato più da vicino lo strumento del Fascicolo Sanitario Elettronico, la sua creazione, le sue criticità e i numeri raggiunti fino ad oggi. Fino a pochi anni fa sarebbe stato davvero impossibile concepire un tipo di cartella clinica, contenente dati, analisi e referti completamente dematerializzati: infatti, come osservato nel capitolo terzo, tale strumento ha presentato delle iniziali criticità dovute alla poca familiarità della collettività con l'uso sempre più assiduo della tecnologia. Basti pensare alla mancanza di corsi universitari o lavorativi specifici sull'uso consapevole della tecnologia per il personale medico, causa abbastanza preponderante. I medici, infatti, dovrebbero essere i primi a dover informare i propri assistiti circa le diverse modalità di conservazione della storia clinica e dovrebbero essere i sostenitori di questo radicale cambiamento del tutto positivo, considerando gli enormi benefici.

Tutti questi elementi non sono però riusciti ad arrestare la voglia di progresso: basti pensare che, strumenti come il Fascicolo Sanitario Elettronico, sono stati adottati a maggioranza non solo nel nostro Paese, ma le esperienze estere confermano i risultati italiani, ovvero modalità nuove di

trattamento di dati sanitari che hanno avuto difficoltà iniziali, ma che poi, numeri alla mano, si sono rivelati come ben accetti da parte dell'intera collettività[210].

Quindi, l'obiettivo della trattazione è stato proprio dimostrare l'evoluzione tecnologica, e di conseguenza giurisprudenziale, della normativa relativa al trattamento dei dati personali in ambito sanitario in un periodo che ha posto molteplici esigenze in tale ambito, richiedendo spesso il doveroso intervento di Governi e Autorità. Ed essendo sia il diritto che la tecnologia soggetti in continua evoluzione, tale elaborato si limita a descrivere e ad analizzare una situazione destinata a mutare nuovamente, avendo voluto congelare nel tempo l'odierna materia dei dati, riflesso di una pandemia che forse ha rivoluzionato definitivamente la sanità, auspicandosi normative venture.

[210] Si vedano il paragrafo secondo e quarto del capitolo terzo.

BIBLIOGRAFIA

Ascione R., "Il futuro della salute: come la tecnologia digitale sta rivoluzionando la medicina (e la nostra vita)", Milano: Hoepli, 2018, pp. 182 ss.;

Balduzzi R., "Sistemi costituzionali, diritto alla salute e organizzazione sanitaria: spunti e materiali per l'analisi comparata", Bologna: Il mulino, 2009;

Butti G., Perugini M.R., "GDPR: la privacy nella pratica quotidiana: tutte le domande a cui un DPO deve saper rispondere", Milano: Angeli, 2020;

Carro G., Masato S., Parla M.D., "La privacy nella sanità", Milano: Giuffrè Editore S.p.A., 2018, pp. 19 ss. pp. 75-87;

Cassano G., Previti S., "Il diritto di Internet nell'era digitale", Milano: Giuffrè Francis Lefebvre, 2020;

Ciacci G., "Privacy e sanità: gli adempimenti previsti nel Decreto Legislativo 196/2003 per medici, farmacisti e organismi sanitari", Roma: Il pensiero scientifico, 2005;

Di Federico G., Negri S., "Unione Europea e Salute" di Giacomo di Federico e Stefania Negri, Cedam, 2020, cap. I, II e III;

Finocchiaro G, "La protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n.101", Bologna: Zanichelli Editore, 2019, pp. 244 ss.;

Iaselli M., "La tutela dei dati personali in ambito sanitario", Milano: Giuffrè Francis Lefebvre, 2020, pp. 40 ss.;

Moretti V., "Sociologia del paziente: diseguaglianze sociali, salute digitale e nuove forme di partecipazione in sanità", Milano: Angeli, 2020;

Moruzzi M., "La sanità dematerializzata e il fascicolo sanitario elettronico: Il nuovo welfare a bassa burocrazia", Roma: Il pensiero scientifico, 2014;

Moruzzi M., "Il fascicolo sanitario elettronico in Italia: la sanità ad alta comunicazione", Milano: Il sole 24 ore, 2011;

Rodotà S., "Il diritto di avere diritti", Roma – Bari, Laterza:2013;

Soffientini M., Caccialupi M., "Privacy: protezione e trattamento dei dati", Ipsoa, 2018;

Tosi E., “Privacy Digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy”, Milano: Giuffrè Francis Lefebvre S.p.A., 2019;

SITOGRAFIA

AgiD, definizioni rinvenibili sul sito ufficiale dell'Agenzia: https://www.agid.gov.it/it/agenzia/competenze-funzioni#:~:text=L'Agenzia%20per%20l'Italia,con%20l'Agenda%20digitale%20europea;

AgiD, "Sicurezza informatica: dalla consapevolezza alla gestione del rischio, Il supporto di AgID sul risk management alle PA italiane e l'esperienza del Consorzio dei Comuni Trentini" del 18/10/2019, rinvenibile sul sito ufficiale dell'Agenzia: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/10/18/sicurezza-informatica-consapevolezza-gestione-del-rischio;

AgiD, Dati sul Fascicolo Sanitario Elettronico rinvenibili sul sito ufficiale dell'AgiD, in rete: https://www.fascicolosanitario.gov.it/;

AgiD, "DECRETO-LEGGE 22 giugno 2012, n. 83 Misure urgenti per la crescita del Paese. (12G0109)", atto completo online: https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dl-22-giugno-2012-n.83_0.pdf;

AgiD, "Rapporto AgiD sulla spesa ICT nella Sanità territoriale italiana", rinvenibile online l'intero documento: https://www.agid.gov.it/sites/default/files/repository_files/rapporto_agid_sulla_spesa_ict_nella_sanita_territoriale_italiana.pdf;

AgiD, Documento "Strategia per la crescita digitale", rinvenibile online: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf;

Allegretta Anita, "Il concetto di progresso nel mondo antico: alcune considerazioni": https://www.liceofedericoquercia.edu.it/attachments/article/941/20._A._Allegretta_Progresso.pdf;

Ascione R., imprenditore e opinion leader internazionale in ambito Digital Health, articolo "L'accelerazione della sanità digitale: il futuro è già qui" per Regione Lombardia: www.openinnovation.regione.lombardia.it;

Assiteca Consultive Broker “Privacy: cos’è il diritto alla privacy e perché è bene tutelarlo” del 5/03/2021: https://www.assiteca.it/2019/08/privacy-cose-il-diritto-alla-privacy-e-perche-e-bene-tutelarlo/;

Berkeley University of California, sito ufficiale: www.hr.berkeley.edu;

Bilotta G., CEO di Paginemediche “La medicina digitale e del suo ruolo in questo periodo”: www.paginemediche.it;

C 293/12 e C 594/12, SENTENZA DELLA CORTE (Grande Sezione) del 8 aprile 2014, nelle cause riunite, in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0293&from=IT;

C 131/12 SENTENZA DELLA CORTE (Grande Sezione) del 13 maggio 2014, in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&from=en;

C 92/09 e C 93/09 Volker und Markus Schecke GbR e Hartmut Eifert contro Land Hessen, cause riunite, rinvenibile in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62009CJ0092&from=EN;

Camera dei Deputati, “Speciale Provvedimenti- Sanità e affari sociali COMMISSIONE: XII AFFARI SOCIALI Welfare Consenso informato e disposizioni anticipate di trattamento” informazioni aggiornate a mercoledì, 17 gennaio 2018, in rete: https://www.camera.it/leg17/522?tema=consenso_informato_e_dichiarazioni_anticipate_di_trattamento#disposizioni_anticipate_di_trattamento;

Carli Ballola G., Intervista a Pietro Ferraro, Practice Manager IT Intelligence di Sas su “Ottimizzare i costi IT con il capacity management”: https://www.zerounoweb.it/techtarget/searchdatacenter/ottimizzare-i-costi-it-con-il-capacity-management/;

Carta delle Nazioni Unite: www.difesa.it;

CCTV e IPSecurityForum, Intervista all’ ex Vice Presidente dell’Autorità Garante per la protezione dei dati personali Giuseppe Chiaravalloti, in rete: https://www.youtube.com/watch?v=r0m4vonWSHI;

Celeghin C., Informazioni del webinar “AgiD e l’accessibilità ai servizi pubblici” del 22-23 maggio 2020, (Responsabile Servizio Sviluppo web e communities @ AgID - Agenzia per l'Italia Digitale) durante gli Accessibility Days 2020, in rete: https://www.youtube.com/watch?v=FYalesEbww0;

Cembrani F., articolo “La legge sul consenso informato e sulle disposizioni anticipate di trattamento”(Direttore U.O. di Medicina Legale, Azienda provinciale per i Servizi sanitari di Trento) del 28 Febbraio 2020, in rete: https://www.luoghicura.it/sistema/programmazione-e-governance/2020/02/la-legge-sul-consenso-informato-e-sulle-disposizioni-anticipate-di-trattamento/;

Chiarelli S., “Privacy e sanità nel Provv. Garante n. 55 del 7 marzo 2019 (18 marzo 2019)” rinvenibile in rete: https://www.youtube.com/watch?v=WqmcwaJ6g-8;

Codice di Deontologia medica, rinvenibile in rete: https://www.ordinemedicivenezia.it/codice-deontologico;

Codice della Privacy, rinvenibile in rete: https://www.brocardi.it/codice-della-privacy/parte-ii/titolo-v/capo-i/;

Coinnova, “Patto per la Sanità Digitale e eHealth” articolo online: https://www.coinnova.it/contesto/linee-guida/patto-sanita-digitale-ehealth;

Commissione europea, comunicazione “AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI” “Sanità elettronica – migliorare l’assistenza sanitaria dei cittadini europei: piano d’azione per uno spazio europeo della sanità elettronica” Bruxelles, 30.4.2004 COM (2004) 356: www.eur-lex.europa.eu;

Consiglio Europeo, Convenzione n. 108 sulla “Protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale” adottato il 28 gennaio 1981 a Strasburgo. In rete: https://protezionedatipersonali.it/convenzione-108-consiglio-europa;

Consulenza Privacy, “Articolo 12, capo 3, Diritti dell’Interessato, Sezione 1, Trasparenza e modalità del Regolamento UE”: https://consulenzaprivacyregolamentoue679.it/testo-del-regolamento-ue-2016679/capo-iii-diritti-dellinteressato/#toggle-id-1;

Cort. Cass., Sezione I civile Sentenza del 29 gennaio 2016, n. 1748 Presidente: Di Palma - Estensore: Valitutti, in rete: https://www.eius.it/giurisprudenza/2016/040;

Cort. Cost. sentenza n.88 del 26-07-1979;

Cort. Cost., sentenza n. 455 del 26-9-1990;

Cort. Cost. sentenza n. 307 del 22-7-1990;

Cort. Cost. sentenza 438/2008 (ECLI:IT:COST:2008:438): https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2008&numero=438#:~:text=dichiara%20l'illegittimit%C3%A0%20costituzionale%20dell,Consulta%2C%20il%2015%20dicembre%202008.;

Corte di Giustizia Europea nella sentenza del 29 luglio 2019, nella causa "C-40/17 ECLI:EU:C:2019:629 Nella causa C 40/17, Fashion ID GmbH & Co. KG contro Verbraucherzentrale NRW eV": https://curia.europa.eu/juris/document/document.jsf;jsessionid=1EF0ED4B821E69C93AE9FD65C45A6EA1?text=&docid=216555&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=8326651;

Corte EDU 2002, Calvelli e Ciglio c. Italia [GC], n. 32967/96;

Corte Europea dei Diritti dell'Uomo, Open Door and Dublin Well Woman v Ireland, (14234/88) [1992] ECHR 68 (29 October 1992): http://www.hrcr.org/safrica/life/OpenDoor;

Davi K., Antonello Soro: "Con i suoi dati Google ha più potere delle dittature". Intervista al Garante della Privacy Antonello Soro, "Huffington Post" del 29 agosto 2013: https://www.huffingtonpost.it/news/intervista-ad-antonello-soro/;

D'Ippolito G., articolo "La libertà informatica e il diritto di accesso ad Internet" Pubblicato il 07 Aprile 2014. In rete: https://www.jei.it/approfondimenti-giuridici/409-la-liberta-informatica-e-il-diritto-di-accesso-ad-internet#_ftn2;

D. lgs. Del 30 dicembre 1992, n.502 Riordino della disciplina in materia sanitaria: http://www.handylex.org/stato/d301292.shtml#:~:text=Decreto%20Legislativo%2030%20dicembre%201992,502&text=1.,essenziali%20e%20uniformi%20di%20assistenza.;

D. lgs. 196/03 (Artt. da 33 a 36 del codice) "Trattamenti con strumenti elettronici Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici. Abrogato dal d.lgs. 101/2018", "ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA": https://www.snals.it/archivio_documenti/leggi/Dlgs196-03_all_B.pdf;

Di Giacomo L. Avv. e DPO "Informazioni sul Green Pass", in rete: https://www.instagram.com/tv/CQQsl0xoUAm/;

Di Giacomo L. Avv. e DPO "Privacy by design, cos'è e come attuarla", disponibile in rete: https://www.youtube.com/watch?v=ANPEVkrnP1o;

Di Giacomo L. Avv. e DPO “IL DPO: LA TUA AZIENDA NE HA BISOGNO?”, in rete: https://www.youtube.com/watch?v=olmoWuWrips;

Di Leo D., “AI e salute: Digital Health e Digital Therapeutics, le responsabilità giuridiche”: https://www.ai4business.it/intelligenza-artificiale/ai-e-salute-digital-health-e-digital-therapeutics-le-responsabilita-giuridiche/;

Direttiva 95/46/CE rinvenibile in rete: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31995L0046&from=EL;

Diritto d’autore e industriale, “Sentenza n. 1748 del 2016: la divulgazione dell’immagine altrui senza il consenso dell’interessato”, in rete: https://www.dandi.media/sentenza-n-1748-del-2016/;

DPCM 11/2014 in G.U. 12 gennaio 2015 rinvenibile in rete: https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/dpcm_13_11_2014.pdf;

DPCM del 29 settembre 2015, n. 178: https://www.gazzettaufficiale.it/eli/id/2015/11/11/15G00192/sg;

Filo diritto, “Copyright, hosting e caching provider: il caso Yahoo Italia” del 29 Maggio 2019 in rete: https://www.filodiritto.com/copyright-hosting-e-caching-provider-il-caso-yahoo-italia;

Finocchiaro G., Libro “La giurisprudenza della Corte di Giustizia in materia di dati personali. Da Google Spain a Schrems” pdf rinvenibile in rete: https://romatrepress.uniroma3.it/wp-content/uploads/2019/05/5lagi-gifi.pdf;

Frankelfield J., Definizione disponibile in rete “Cloud Computing” modificato da Julius Mansa del 28 Luglio 2020 https://www.investopedia.com/terms/c/cloud-computing.asp;

Frareg Frafor, articolo “Attacchi informatici in aumento: il Data Breach dell’ospedale di Erba” disponibile in rete: https://www.frareg.com/it/legge-sulla-privacy/attacchi-informatici-in-aumento-il-data-breach-dellospedale-di-erba/;

Frezzato L., Articolo “Image Recognition: cos'è, come funziona e quali sono i vantaggi per le aziende. La consapevolezza del valore dei dati sta portando a una trasformazione dei processi aziendali. L’impiego dell’AI trova così sempre più spazio nei progetti di business, con l’Image Recognition e l’Image Detection tra le declinazioni a maggior tasso di crescita” del 30/09/2020 https://www.internet4things.it/iot-library/image-recognition-cose-come-funziona-e-i-vantaggi-per-le-aziende/;

Garante per la protezione dei dati personali, “Principi fondamentali del trattamento (liceità, minimizzazione…)”: https://www.garanteprivacy.it/home/doveri;

Garante per la protezione dei dati personali, “Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali - 15 giugno 2011”, Pubblicato sulla Gazzetta Ufficiale n. 153 del 4 luglio 2011, Registro dei provvedimenti n. 230 del 15 giugno 2011: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1821257;

Garante per la protezione dei dati personali, “Trattamento di dati personali per finalità di marketing - 15 giugno 2017 [6629169] Registro dei provvedimenti n. 268 del 15 giugno 2017”: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9038386;

Garante per la protezione dei dati personali, “Trattamento dei dati personali attraverso un sistema "Rfid" di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Verifica preliminare richiesta da Azienda Ospedaliera e Sas - 29 novembre 2012 [2276103] Registro dei provvedimenti n. 370 del 29 novembre 2012”: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2276103;

Garante per la protezione dei dati personali, “Trattamento non consentito di dati sanitari raccolti tramite apparecchiature diagnostiche - 10 aprile 2014 [3152119], Registro dei provvedimenti n. 186 del 10 aprile 2014”: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3152119;

Garante per la protezione dei dati personali, [doc. web n. 9269629]” Provvedimento correttivo e sanzionatorio nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona - 23 gennaio 2020 Registro dei provvedimenti n. 18 del 23 gennaio 2020” In rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9269629;

Garante per la protezione dei dati personali, “Provvedimento correttivo e sanzionatorio nei confronti di Azienda Ospedaliero Universitaria Integrata di Verona - 23 gennaio 2020” Registro dei provvedimenti n. 18 del 23 gennaio 2020 In rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9269629;

Garante per la protezione dei dati personali, “Dematerializzazione della documentazione clinica - 26 novembre 2009 [1688961] del 26 novembre del 2009”, in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1688961;

Gazzetta Ufficiale, Legge dell’8 marzo del 2017 n. 24 “Disposizioni in materia di sicurezza delle cure e della persona assistita, nonche' in materia di responsabilita' professionale degli esercenti

le professioni sanitarie. (17G00041) (GU Serie Generale n.64 del 17-03-2017)" testo rinvenibile in rete: https://www.gazzettaufficiale.it/eli/id/2017/03/17/17G00041/sg;

Gazzetta Ufficiale, "Regolamento in materia di fascicolo sanitario elettronico. (15G00192) (GU Serie Generale n.263 del 11-11-2015: https://www.gazzettaufficiale.it/eli/id/2015/11/11/15G00192/sg;

GDPR – "Regolamento generale sulla protezione dei dati (UE/2016/679)" Articolo 9 Trattamento di categorie particolari di dati personali in rete: https://www.altalex.com/documents/news/2018/04/12/articolo-9-gdpr-trattamento-di-categorie-particolari-di-dati;

Governo italiano, Pagina "RIPARTIAMO IN SICUREZZA. La Certificazione verde COVID-19 permette di accedere a eventi, strutture e altri luoghi pubblici in Italia e facilita gli spostamenti in Europa. #EUCOVIDCertificate" in rete: https://www.dgc.gov.it/web/;

Guarda P., "FASCICOLO SANITARIO ELETTRONICO E PROTEZIONE DEI DATI PERSONALI", in rete: http://eprints.biblio.unitn.it/2212/1/guarda_fasc_sanit_elettr_94_e-book.pdf;

Iaselli M., La redazione "Nuovi rapporti fra informatica e diritto": https://www.diritto.it/nuovi-rapporti-fra-informatica-e-diritto/;

Iagnemma C., "Il tempo della comunicazione costituisce tempo di cura: l'approccio narrativo nella Legge 219/2017" del 21 Gennaio 2019in Giurisprudenza Penale Web, 2019, 1-bis – ISSN 2499-846X, in rete: https://www.giurisprudenzapenale.com/2019/01/21/tempo-della-comunicazione-costituisce-tempo-cura-lapproccio-narrativo-nella-legge-219-2017/;

Kleinman Z., "What is Tencent?", BBC News: https://www.bbc.com/news/technology-53696743;

La Redazione "Come la tecnologia ha cambiato le nostre azioni quotidiane": https://www.ilprimatonazionale.it/scienza-e-tecnologia/come-la-tecnologia-ha-cambiato-le-nostre-azioni-quotidiane-126057/;

Lanciano G. Avv., "Cosa è il gruppo di lavoro ex art. 29?", 5 Novembre 2017, aggiornato al 5 Agosto 2018 https://www.miolegale.it/guide/gruppo-lavoro-ex-art-29/;

L. n. 675 del 31 dicembre 1996, rubricata Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335;

Lex Media “Il diritto alla privacy in ambito sanitario”: https://lexmedica.it/il-diritto-alla-privacy-in-ambito-sanitario;

Limone E., su articolo 4 del Regolamento, “Pseudonimizzazione e anonimizzazione dei dati: differenze tecniche e applicative”Cyber Security Expert, rinvenibile in rete: https://www.cybersecurity360.it/legal/privacy-dati-personali/pseudonimizzazione-e-anonimizzazione-dei-dati-differenze-tecniche-e-applicative/;

Locatelli P., Lettieri E., Webinar del 20/05/2020 “Innovazione digitale nella sanità: dalla gestione dell’emergenza a una reale connected care” Politecnico di Milano Graduate School of Business: https://www.youtube.com/watch?v=XMhSK-XNe9w;

Lutkevich B., “Protected health information (PHI) or personal health information” Technical WriterScott Wallask, Editorial DirectorAlex DelVecchio, Content Development Strategist, in rete: https://searchhealthit.techtarget.com/definition/personal-health-information;

Marino F., “Record di investimenti per la Digital Health”: www.digitalic.it;

Marsden P., Chartered psychologist specialising in consumer behaviour, “Wellbeing and technology” University lecturer at UAL and consultant consumer psychologist with Brand Genetics: www.digitalwellbeing.org;

Massella E., (Agid) al minuto 00:05:21 del Webinar “Il Ruolo del Fascicolo Sanitario Elettronico” sul “Fascicolo sanitario elettronico” del 13/12/2018, rinvenibile online: https://www.youtube.com/watch?v=WDGDqYaTVvI;

Medico e Leggi, “Articolo 170 - Inosservanza di provvedimenti del Garante (Decreto legislativo n° 196, 30 giugno 2003)” Testo dell’articolo rinvenibile online: https://www.medicoeleggi.com/argomenti00/italia8/16470.htm;

Ministero della Salute, Circolare del 19 dicembre 1986 n.900 2/AG454/260, in rete: https://www.omceo.me.it/sportello/professione/cartella/archivi.pdf;

Ministero della Salute, “Linee di indirizzo nazionale sulla Telemedicina”, rinvenibili in rete: https://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf;

Mori D., “STANDARD IN SANITA’ PDTA, Percorsi Diagnostico Terapeutici Assistenziali” del 30.11.18: https://www.nurse24.it/studenti/standard/pdta-percorsi-diagnostico-terapeutici-assistenziali.html;

Nefeli M. Avv., “Quanto disposto dalla Cass. civ. Sez. III, Sent., 27-03-2015, n. 6243 Testo della sentenza rinvenibile tramite l’articolo, L'ASL è responsabile per l'errore del medico

convenzionato" martedì 07 aprile 2015: https://www.quotidianogiuridico.it/documents/2015/04/07/l-asl-e-responsabile-per-l-errore-del-medico-convenzionato;

Olivieri L., "Vaccino obbligatorio: cosa dice l'articolo 32": https://www.civicolab.it/vaccino-obbligatorio-cosa-dicono-lart-32-e-la-realta/;

Open Polis, "Quante sono le autorità amministrative indipendenti." Aggiornato a venerdì 19 Giugno 2020 in rete: https://www.openpolis.it/parole/quante-sono-le-autorita-amministrative-indipendenti/;

Osservatori.net, "La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese.":https://www.osservatori.net/it/chi-siamo/conosciamoci/cosa-facciamo;

Pagine Mediche, "Compliance terapeutica: come la tecnologia può migliorarla" del 10/02/2021: https://digitalhealthitalia.com/compliance-terapeutica-tecnologia-aiuta/;

Panda Security, "BYOD: futuro o già passato?" Ottobre 17, 2019: https://www.pandasecurity.com/it/mediacenter/tecnologia/byod-futuro-o-gia-passato/;

Pattaro A. F. "Fascicolo sanitario elettronico: cos'è e come attivarlo" del 23/10/2019: https://www.agendadigitale.eu/sanita/fascicolo-sanitario-elettronico-cose-e-a-che-punto-e-la-guida/;

Perfetti T., "La dematerializzazione dei documenti sanitari" In: Diritto civile e commerciale in rete: file:///C:/Users/Utente/Downloads/la-dematerializzazione-dei-documenti-sanitari.pdf;

Piai S., Spinelli M., Di Giovanni O., Percopo M. per IDC: www.idc.com

Pigliapoco S., Dosio G. "Formazione, gestione e conservazione degli archivi digitali. Il Master FGCAD dell'Università degli Studi di Macerata": https://air.uniud.it/retrieve/handle/11390/1071522/46431/Bonfiglio-Dosio-Pigliapoco%2c%20FGCAD%20%5bcapitolo%20Allegrezza%5d.pdf;

Polizia Postale e delle Comunicazioni Polo Anticrimine della Polizia di Stato "Phishing, cos'è?" In rete: https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html;

Redazione Altalex, Art. 12 GDPR – "Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato-Regolamento UE 2016/679, art. 12":

https://www.altalex.com/documents/news/2018/04/12/articolo-12-gdpr-informazioni-modalita-trasparenti-interessato;

Redazione PMI, "COVID-19: gestione privacy sui dati sanitari"scritto il 11 Maggio 2020 https://www.pmi.it/impresa/normativa/332315/covid-19-gestione-privacy-sui-dati-sanitari.html;

Reg. CE n. 1338/2008, riferimenti agli articoli: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32008R1338&from=IT;

Regolamento UE 2016/679, consultabile presso il sito ufficiale del Regolamento Generale per la Protezione dei Dati Personali. in rete: https://gdpr-info.eu/art-13-gdpr/;

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 Arricchito con riferimenti ai Considerando Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018" in rete: https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018;

Ristretti, "Il diritto alla salute": http://www.ristretti.it/areestudio/salute/inchieste/baccaro/diritto.htm;

Ruocco C. M. "Il diritto alla salute" del 23/07/2020: https://www.diritto.it/la-tutela-della-salute-una-lettura-costituzionalmente-orientata/;

Sabatino C., JD, American Bar Association "Riservatezza e Health Insurance Portability and Accountability Act (HIPAA)": www.msdmanuals.com

Saetta B. "Codice in materia di protezione dei dati personali", pubblicato: Settembre 07, 2018 Ultima modifica: Aprile 13, 2021: https://protezionedatipersonali.it/codice-protezione-dati-personali;

Saetta B. "Direttive europee" Categoria: Normativa, pubblicato il 22 Luglio del 2018 "Direttiva 95/46/CE". In rete: https://protezionedatipersonali.it/direttive-europee;

Saetta B., articolo "Interessato al trattamento" Categoria: Soggetti Pubblicato: Novembre 14, 2018 Ultima modifica: Marzo 01, 2021. In rete: https://protezionedatipersonali.it/interessato-del-trattamento;

Sánchez-Henarejos A., Fernández-Alemán J., Toval A., Hernández-Hernández I., Sánchez-García A.B., Carrillo de Gea J.M. "Guida alle buone pratiche di sicurezza informatica nel

trattamento dei dati sanitari per il personale sanitario nelle cure primarie" del 4/4/2014: https://www.sciencedirect.com/science/article/pii/S0212656714000067;

Sbaraglia G., articolo disponibile su "Guida al ransomware: cos'è, come si prende e come rimuoverlo"Consulente aziendale Cyber Security, membro del Comitato Scientifico CLUSIT, del 20 aprile 2021: https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/;

Scorza G.,"Pericoloso mettere sui social il Qr-Code del green pass, l'allarme del Garante Privacy" Componente del Garante per la protezione dei dati personali (Agenda Digitale, 24 giugno 2021), in rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9673513;

Seocrate, Articolo "GDPR e consenso granulare nell'European Data Protection Board (Edpb)" del 4 maggio 2020, in rete: https://seocrate.it/blog/gdpr-e-consenso-granulare-nell-european-data-protection-board-di-maggio-2020/;

Sinesy, "La comunicazione medico-paziente ai tempi di WhatsApp": https://www.sinesy.it/comunicazione-medico-paziente-whatsapp/;

Sorrentino E, Guaglianone M.T., Cardillo E., Chiaravalloti M.T., Spagnuolo A.F., Cavarretta G."La conservazione dei documenti che alimentano il Fascicolo Sanitario Elettronico" per Rivista italiana di diritto: https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/52/37;

Sorrentino E. "sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico" per Federalismi.it: https://federalismi.it/ApplOpenFilePDF.cfm?artid=44367&dpath=document&dfile=05112020104132.pdf&content=La%2Bsanit%C3%A0%2Bdigitale%2Bin%2Bemergenza%2BCovid%2D19%2E%2BUno%2Bsguardo%2Bal%2Bfascicolo%2Bsanitario%2Belettronico%2B%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B;

Starri M. "Digital 2019: tre italiani su cinque attivi sui sociale per quasi due ore al giorno": https://wearesocial.com/it/blog/2019/01/digital-in-2019;

Stefanini E., Counsel di Portolano Cavallo, Legal Health "Nuove Linee Guida nazionali sulla telemedicina: i nodi critici per la piena attuazione" articolo rinvenibile su <www.agendadigitale.eu;

Stentella M., Content Manager di Forum PA nell'intervista a Claudio Carlo Franzoni, Senior Advisor P4I-Digital360 "La sanità digitale": www.blogsalutedigitale.it;

Studio Cataldi, “Il segreto professionale del medico”: https://www.studiocataldi.it/articoli/33473-il-segreto-professionale-del-medico.asp#ixzz70hHdO968;

Supreme Court of Alabama, Mull v. String 448 So. 2d 952 (1984), March 16, 1984. Caso rinvenibile in rete: https://law.justia.com/cases/alabama/supreme-court/1984/448-so-2d-952-1.html;

Unione Europea, v. Garante Europeo per la protezione dei dati personali: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_it;

Versione consolidata del trattato sul funzionamento dell'Unione europea “PARTE TERZA: POLITICHE DELL'UNIONE E AZIONI INTERNE - TITOLO XIV: SANITÀ PUBBLICA” Articolo 168 (ex articolo 152 del TCE) Gazzetta ufficiale n. 115 del 09/05/2008 pag. 0122 – 0124: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:12008E168&from=EL;