RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0074
Articolo sottoposto a peer review

Tutela della salute, sistemi digitali e privacy

Alessandra Pietroletti • Alessandro Nicotra

Le innovazioni e le nuove tecnologie possono contribuire enormemente, nel campo della sanità, a migliorare le cure e la ricerca, ma dovrebbero essere regolamentate sulla base di un processo multistakeholder come quello offerto dall'Internet governance. La trasformazione digitale dei sistemi in campo sanitario richiede una particolare attenzione e sensibilità sotto il profilo della protezione e del trattamento dei dati personali. Occorre costruire un ecosistema digitale funzionale, ma sicuro e rispettoso della dignità e dei diritti delle persone.

Sanità – Privacy – Protezione dati – Nuove tecnologie – Trasformazione digitale

1. Introduzione

Dal WSIS (*World Summit on the Information Society*[1]) del 2005 ad oggi, l'infrastruttura di Internet è cresciuta e si è sviluppata, con i suoi protocolli, trasformandosi in vera e propria spina dorsale non solo della società dell'informazione ma della nostra stessa vita quotidiana. Sarebbe arduo immaginare le nostre vite oggi, senza l'ausilio di tale strumento ed è ormai sotto gli occhi di tutti quanto le questioni legate alla Internet governance[2], che un tempo riguardavano ed appassionavano solo addetti ai lavori o attivisti, non siano più un interesse preminente ed esclusivo delle società di telecomunicazioni, degli innovatori e del mondo accademico. Ecco, quindi, che dal gTLD[3] allo sviluppo dei nomi a dominio, dalle problematiche di accesso all'anonimato, dalle Big tech a *Cambridge Analytica* oggi più che mai l'Internet governance è divenuta anche una questione di privacy, data protection e... salute.

La pandemia di Covid-19 ha reso ancora più evidenti, da un lato, i benefici che possono derivare da una trasformazione digitale dei sistemi anche in campo sanitario, ma dall'altro, ha fatto emergere anche diverse criticità e, con queste, la necessità di adottare nuovi piani e strategie per limitare i danni collaterali che da tale processo di trasformazione possono scaturire. Si pensi, in primo luogo, alla frammentarietà dei database sanitari pubblici (con le Regioni ed il Governo a contendersi le competenze) oppure ancora alle conseguenze dovute a dati mancanti o non esatti.

L'attenzione e la sensibilità verso il funzionamento dei sistemi a tutela della salute devono essere massime. Sono ormai numerosissime, infatti, le innovazioni e le sperimentazioni tecnologiche in ambito sanitario che sfruttano Internet e il digitale, ma che richiedono approfondimenti preliminari e determinate garanzie per i cittadini. Basti pensare alle ricette dematerializzate, alla telemedicina, ai dispositivi in-

A. Pietroletti e A. Nicotra sono avvocati esperti in ICT, privacy e data protection. Sono rispettivamente socio e consulente dello Studio Legale Tributario (EY).

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

dossabili o ai sensori per il monitoraggio remoto dei più svariati parametri di salute dei pazienti. Tutti questi dati, trasposti in digitale, possono essere utilmente inoltrati ai propri medici di riferimento attraverso la rete e possono essere archiviati in un dossier o fascicolo sanitario, ma vanno, in ogni caso, validati e protetti.

Le tecnologie, i sistemi ed i dati attinenti alla Sanità digitale (*eHealth*), per incrementare la loro utilità e protezione, dovrebbero convergere verso la creazione di un ecosistema digitale che, muovendo dalla ricerca (si pensi alla bioinformatica ed al sequenziamento del DNA), possa monitorare e fare arrivare in tempo reale al medico curante i parametri dell'assistito e, magari, curarlo attraverso le terapie digitali (DTx[4]) ovvero interventi terapeutici gestiti da programmi software. Si tenga presente, poi, il parallelo sviluppo di altri programmi decisamente rilevanti sul piano dell'assistenza sanitaria. Ci riferiamo a quelli sviluppati per ottimizzare la logistica e la consegna di farmaci, per lo studio e la produzione dei vaccini, per la gestione dei dispositivi medicali. Ed ancora si pensi alla chirurgia robotica o a quella a distanza, che consentono agli specialisti di operare da remoto e che sono ormai realtà consolidate, ma che necessitano di connessioni stabili e sicure.

Nonostante la sanità sia senz'altro il settore che possa trarre i maggiori benefici dai big data (ad esempio, attraverso la condivisione dei dati scientifici[5]), tutte queste innovazioni, che sono destinate ad una sempre maggiore e migliore tutela della salute, elaborano una quantità enorme di dati sensibili e richiedono, come intuibile, un preciso quadro regolatorio. Non si può che ribadire, quindi, l'importanza che assume il lecito e corretto trattamento di tali dati personali. L'analisi, la valutazione e l'adozione di misure di sicurezza realmente adeguate di dati tanto particolari e sensibili, come sono i dati sanitari, è indispensabile se si vuole evitare che i potenziali benefici offerti dalle tecnologie digitali vengano azzerati da violazioni della dignità e dei diritti delle persone. Fondamentale, in tal senso, si rivela essere il rispetto dei principi della *privacy by default* e della *privacy by design* introdotti dal GDPR ovvero dal Regolamento (UE) 2016/679.

Di fronte al vertiginoso sviluppo delle *big tech companies* e della quantità di dati personali da queste trattati, il GDPR è un prezioso e indispensabile strumento nella ricerca di un punto di equilibrio tra progresso, innovazione, sviluppo economico e rispetto dei diritti delle persone. Per dare un'idea degli interessi che gravitano attorno al settore dell'*eHealth*, si consideri che, in base a una specifica ricerca[6], nel 2016 il mercato dei Big Data nel settore sanitario veniva valutato intorno agli 11 miliardi di dollari, mentre, nel 2020, è stato stimato che tale mercato arriverà a valere 70 miliardi di dollari nel 2025. Non sorprende, dunque, il preoccupante dato che un'altra ricerca ha portato alla luce relativamente al settore sanitario in Italia: nell'ottobre del 2020 l'Italia risultava quarto paese al mondo e primo in Europa per attacchi informatici subiti[7] e il settore più colpito per numero di attacchi davanti, persino, a quello bancario e quello della pubblica amministrazione. Questo dato rende ancora più evidente l'importanza di implementare un piano di governance e data protection sia a livello di reti che di applicativi, cercando di fare tesoro degli incidenti e delle violazioni di dati già occorsi (come, ad esempio, quello subito dalla Regione Lazio nell'agosto 2021 che ne ha bloccato il Ced paralizzando i sistemi digitali regionali e la campagna vaccinale *in primis*) e approntando adeguate procedure di gestione e prevenzione di insidiosi *data breach*.

Al pari di come si sono sviluppati e si sviluppano i protocolli che rendono possibile il funzionamento di Internet, riteniamo che anche per la privacy e la *data protection* siano fondamentali il confronto e la cooperazione tra tutti gli attori coinvolti, secondo un approccio *multistakeholder*. Cercheremo di sintetizzare, qui di seguito, il percorso di alcune delle principali problematiche affrontate in seno agli *Internet Governance Forum* ove sono emersi chiaramente il rapporto e gli intrecci esistenti tra la gestione della rete Internet, l'implementazione di efficaci sistemi di sanità digitale e la necessità di guardare al funzionamento di queste tecnologie anche sotto il profilo della riservatezza e della sicurezza informatiche.

2. L'importanza della Internet governance

Per chi si occupa di Internet da più di vent'anni la tentazione ad indulgere nei ricordi su quale fosse lo spirito e gli ideali dei cd. pionieri della rete e dei suoi primi frequentatori è molto forte. Per comprendere come non sia più l'Internet elitaria, popolata da ricercatori e qualche milione di appassionati, è sufficiente il dato fornito da una ricerca che ha stimato, ad aprile del 2021, in oltre 4,72 miliardi le persone che utilizzano la rete[8]. Come spesso accade con le nuove tecnologie, però, utilizzare non significa conoscere. L'idea di libertà assoluta, di spazio aperto e senza regole, ha ingenerato in molti l'idea che l'Internet sia il *far west*, popolato da hacker cattivi che cospirano nel *dark Web*.

In verità, delle regole di base, per quanto meramente tecniche, sono sempre esistite e si chiamano protocolli. Senza l'accordo e la standardizzazione sui

protocolli[9] la connessione tra reti e dispositivi non sarebbe stata possibile. La realizzazione della *Network neutrality* ha dimostrato, di fatto, quanto siano importanti la trasparenza e l'interoperabilità tra sistemi, soprattutto quando si ha a che fare con l'informatica e le tecnologie digitali. Risulta lapalissianamente disfunzionale, infatti, avere dispositivi che utilizzano "lingue" diverse e non si capiscono fra loro, scambiandosi così documenti o file illeggibili. La neutralità della rete, costantemente messa in discussione da governi autoritari o propensi ad un controllo totale del traffico dati, ha finito in realtà con il favorire lo sviluppo del concetto di neutralità tecnologica al fine di promuovere gli scambi e le comunicazioni transfrontaliere[10].

Reti e dispositivi sono però solo meri mezzi di trasmissione attraverso i quali trasmettere, ricevere o conservare dati ed informazioni. Il problema era ed è "se" e "come" regolare le potenzialità offerte da questi strumenti. Un conto, infatti, è definire uno standard tecnico per la produzione e trasmissioni delle informazioni, altro stabilire limiti, finalità e contenuti dei dati che tali informazioni contengono.

In quest'ottica, dopo il primo boom della new economy nei primi anni del 2000, le Nazioni Unite organizzarono il *World Summit on the Information Society* che produsse una prima dichiarazione di principi[11] che esordiva così: «Noi, rappresentanti dei popoli del mondo, riuniti a Ginevra dal 10 al 12 dicembre 2003 per la prima fase del Vertice mondiale sulla società dell'informazione, dichiariamo il nostro desiderio e impegno comune di costruire una società dell'informazione incentrata sulle persone, inclusiva e orientata allo sviluppo, in cui tutti possono creare, accedere, utilizzare e condividere informazioni e conoscenze, consentendo a individui, comunità e popoli di raggiungere il loro pieno potenziale nel promuovere il loro sviluppo sostenibile e migliorare la loro qualità della vita, sulla base degli scopi e dei principi della Carta delle Nazioni Unite e nel pieno rispetto e sostegno della Dichiarazione Universale dei Diritti Umani. La nostra sfida è sfruttare il potenziale delle tecnologie dell'informazione e della comunicazione per promuovere gli obiettivi di sviluppo della Dichiarazione del Millennio, vale a dire l'eliminazione della povertà estrema e della fame; conseguimento dell'istruzione primaria universale; promozione dell'uguaglianza di genere e dell'emancipazione delle donne; riduzione della mortalità infantile; miglioramento della salute materna; combattere l'HIV/AIDS, la malaria e altre malattie; garantire la sostenibilità ambientale; e lo sviluppo di partenariati globali per lo sviluppo per il raggiungimento di un mondo più pacifico, giusto e prospero...». Nel 2003 poteva far sorridere l'obiettivo di ridurre la mortalità infantile e migliorare la salute materna con le tecnologie dell'informazione e della comunicazione, ma nel 2021 possiamo dire che parte di tali obiettivi è stata effettivamente conseguita[12].

Successivamente, nel WSIS del 2005 a Tunisi, per tentare di dare un seguito concreto a questi principi venne varata la cd. "Agenda di Tunisi per la Società dell'Informazione"[13] che invitava il Segretario Generale delle Nazioni Unite a convocare un forum per il dialogo politico *multistakeholder* denominato *Internet governance Forum* (IGF)[14]. In questi forum, che dal 2006 vengono organizzati ogni anno, si discute sui principali temi correlati alla governance di Internet.

La gestione internazionale di Internet, secondo il mandato originario e la dichiarazione di principi, dovrebbe essere multilaterale, trasparente e democratica, con il pieno coinvolgimento dei governi, del settore privato, della società civile e delle organizzazioni internazionali. Dovrebbe inoltre facilitare l'accesso per tutti e garantire un funzionamento stabile e sicuro di Internet, tenendo conto del multilinguismo. Di fatto, purtroppo, l'attenzione e la partecipazione dei governi a questi forum è divenuta nel tempo in gran parte velleitaria o di facciata. La scarsa promozione di tali eventi si è riflettuta a cascata sulla società civile, ovvero sui comuni cittadini che, non avendone magari notizia non si attivavano per la partecipazione o per farsi rappresentare (salve fortunatamente le presenze da parte di organizzazioni non governative e no profit quali ad esempio l'*Electronic Frontier Foundation*[15], ISOC Italia[16], ISOC.org[17] e molte altre) riducendo le effettive potenzialità ed i molti vantaggi in termini di conoscenza e di proposte che di solito conseguono a questi incontri.

La pandemia scoppiata all'inizio del 2020, però, imponendo tra le priorità politiche dei governi la *digital transformation* e la transizione dei servizi verso il digitale ha avuto l'effetto di ridare all'*Internet Governance Forum* una certa visibilità e di rendergli parte della sua centralità come sede deputata per la discussione ed il confronto sul futuro della rete e lo sviluppo di Internet. A dimostrazione di quanto affermato, il quindicesimo IGF tenutosi interamente online dal 2 al 17 novembre 2020 ha avuto come tema centrale l'*Internet for human resilience and solidarity* e ha registrato una partecipazione straordinaria. Anche l'IGF 2021, tenutosi anche in presenza oltre che online, è stato seguito da numerose persone facendo ben sperare, soprattutto per la forte convergenza che si è avuta tra gli argomenti in discussione nelle varie sezioni tematiche e gli obiettivi fissati con l'*Agenda 2030 per uno sviluppo sostenibile*[18]. Quest'ultima, sottoscritta nel settembre 2015 dai governi dei 193 paesi membri dell'ONU, ci inte-

ressa in particolare, perché tra i 17 obiettivi di sviluppo sostenibile (OSS/SDGs, *Sustainable Development Goals*) ha inserito specificamente quello di "Assicurare la salute ed il benessere per tutti e per tutte le età"[19]. Un obiettivo apparentemente utopistico, ma averlo fissato e sottoscritto formalmente lascia intendere che da più parti si proverà effettivamente a muoversi in tale direzione. Lo stesso Segretario delle Nazioni Unite, Antonio Guterres, ha sottolineato in più occasioni l'importanza di "fare rete", di cooperare, di innovare, ponendo l'attenzione sulla rete come infrastruttura e sulla pandemia come occasione per l'implementazione di piani di *eHealth*.

Lo sviluppo e l'attuazione di strategie e politiche sanitarie è stato un tema centrale e un argomento molto dibattuto nell'IGF del 2020. In quella sede, infatti, è stato rimarcato come ogni paese dovrebbe sfruttare le nuove tecnologie e la rete impegnandosi nell'adozione di una vera e propria strategia digitale nazionale. E tale strategia dovrebbe essere calibrata attentamente sui bisogni delle persone, sulle condizioni esistenti, sulle capacità e risorse disponibili e sugli obiettivi desiderati. Studiosi ed esperti hanno convenuto sul fatto che la definizione di una strategia nazionale facilita, di fatto, l'adozione di progetti ed azioni concrete per migliorare la tutela della salute. In primo luogo, perché tale approccio richiede una preventiva analisi ed indagine sui reali bisogni e, in secondo luogo, perché permette di mettere a fuoco le priorità di intervento. Un siffatto approccio, inoltre, avrebbe come effetto non secondario anche quello di incrementare progressivamente l'affidabilità dei sistemi e dei piani di prevenzione e, con essi, la fiducia e le possibilità delle persone nel fruirli. Chiaramente, l'elaborazione di una strategia per la sanità digitale e le relative azioni richiedono un forte investimento in infrastrutture, nell'alfabetizzazione informatica ed in competenze digitali: problemi da affrontare con partnership pubblico-privato. Del resto, solo connettendo in modo significativo ed efficace le persone, i servizi e gli strumenti sanitari digitali si può pensare di procedere concretamente verso l'ambizioso obiettivo, sopra ricordato, di "Assicurare la salute ed il benessere per tutti e per tutte le età".

Una precondizione è stata però individuata nel guadagnare e mantenere la fiducia degli utenti. In più panel si è rimarcato quanto sia essenziale poter contare su una regolamentazione di Internet che ne garantisca il funzionamento, l'interoperabilità e l'accessibilità. Tali caratteristiche sono indispensabili per l'implementazione di sistemi di sanità digitale che siano realmente efficaci e che abbiano successo. Un successo che non può prescindere da interventi normativi specifici. Da più parti, infatti, è stata segnalata la necessità che la politica ed i legislatori, nel rispetto dei diritti e delle libertà di tutti gli attori, definiscano meglio il quadro delle regole e stabiliscano affidabili meccanismi di convalida e di verifica delle tecnologie destinate alla prevenzione ed alla tutela della salute. Cosa, per esempio, può essere considerato dispositivo medico? Chi lo certifica come tale? Quanto è legittima la raccolta di big data e la profilazione da parte di soggetti privati e commerciali? Quali tutele e protezioni possono considerarsi adeguate?

Il funzionamento stesso di sistemi e applicazioni dovrebbe essere quanto meno trasparente ed occorre renderli accessibili e semplici da usare, in modo da garantire anche un controllo diffuso, non solo da parte di autorità o agenzie all'uopo preposte, ma anche da parte di singoli appassionati ed esperti.

Se si vuole garantire che più persone abbiano accesso a prestazioni e servizi sanitari migliori e più efficienti, la digitalizzazione dei sistemi sanitari deve diventare una priorità in tutto il mondo. E le azioni da intraprendere non riguardano solo gli investimenti e piani strategici... Non vanno infatti ignorate altre precondizioni essenziali quali: il diritto di accesso alla rete, il contrasto al divario digitale, la lotta alla disinformazione sanitaria ed alla disinformazione in generale (le cd. fake news[20]). Occorre, infine, una maggiore sensibilizzazione e responsabilizzazione delle singole persone. Dopo tutto, i social network e la rete sono sempre stati, nel bene e nel male, uno specchio del mondo reale e rimangono degli strumenti da saper utilizzare. Tutte le proposte ed i progetti ideati e portati avanti per creare fonti di informazione e di condivisione affidabili sono, in definitiva, orientati ad aiutare le persone a scegliere, liberamente e con cognizione di causa, in chi aver fiducia ed a filtrare lo tsunami di informazioni cui hanno accesso.

3. Nuove tecnologie e sistemi digitali per la sanità

Occorre alimentare una cultura digitale che, per formarsi, ha comunque bisogno di verifiche empiriche. Oggi assistiamo a persone che per curarsi si affidano indiscriminatamente ai motori di ricerca sul Web o ai social network ed è del tutto evidente quanto sia necessaria un maggior spirito critico circa le fonti e le informazioni consultate o, per esempio, su che fine facciano i propri dati sanitari immessi nelle app dello smartphone o pubblicati in rete.

Guardando alla storia della medicina[21], è possibile constatare come solo negli ultimi due secoli le procedure mediche abbiano iniziato a fondarsi su conoscenze e metodologie in grado di rendere le cure

più sicure ed efficaci per tutti. Negli ultimi vent'anni l'informatica ha accelerato esponenzialmente queste procedure grazie all'aumento della capacità e della velocità di elaborazione dei dati che ha permesso di introdurre e sperimentare nuove metodologie e nuove tecnologie. Parlare di algoritmi, robot ed intelligenza artificiale applicati alla sanità non è più fantascienza, ma una realtà consolidata ed imprescindibile, destinata a espandersi ed a svilupparsi ulteriormente negli anni a venire. Un esempio concreto, a questo riguardo, ci è stato dato durante la pandemia di Covid-19 con l'approntamento di appositi vaccini. Normalmente la produzione e la commercializzazione di un nuovo vaccino richiedono anni[22]. Si consideri che il vaccino sviluppato più velocemente, nel passato, è stato quello contro la parotite, realizzato, negli anni '60, in quattro anni[23] (dal sequenziamento virale all'approvazione finale). Per fronteggiare il Covid-19, invece, in meno di un anno si è assistito allo sviluppo di oltre 200 potenziali vaccini, di cui 5, dopo aver completato le diverse fasi di sperimentazione e controlli, sono risultati pronti per l'uso. Un risultato straordinario reso possibile dalle ingenti risorse economiche messe a disposizione dei ricercatori e dagli interessi in gioco, certo, ma anche e soprattutto grazie ad un processo di sviluppo e di elaborazione dei dati preesistenti e condivisi a livello globale. Con i vaccini anti-Covid, «nessuna tappa del processo è venuta meno, grazie al concorso di diversi fattori:

- ricerche già condotte in passato sulla tecnologia a RNA messaggero (mRNA);
- studi sui coronavirus umani correlati al SARS-CoV-2, per esempio quelli che hanno provocato SARS (Severe acute respiratory syndrome) e MERS (Middle East respiratory syndrome);
- ingenti risorse umane ed economiche messe a disposizione in tempi stretti;
- conduzione parallela delle varie fasi di valutazione e di studio;
- produzione del vaccino parallelamente agli studi e al processo di autorizzazione;
- ottimizzazione della parte burocratica/amministrativa;
- valutazione da parte delle agenzie regolatorie dei risultati ottenuti, man mano che questi venivano prodotti (rolling review) e non, come generalmente si usa fare, solo dopo il completamento di tutti gli studi»[24].

Poter elaborare digitalmente e sinergicamente tutti i dati relativi a ricerche e studi condotti in precedenza e poterli verificare e valutare telematicamente, in tempo reale, rappresenta una dimostrazione lampante dei benefici che possono derivare dalla cd. *digital transformation*. Una vera e propria rivoluzione che avviene modificando le modalità di trattamento del dato biologico e sanitario; modalità che, da analogiche e cartacee, non solo diventano digitali ma vengono elaborate da algoritmi sempre più complessi sino ad arrivare a strabilianti applicazioni di intelligenza artificiale come dimostrato dal progetto *Alphafold*: un software creato dalla Deepmind per la previsione della struttura delle proteine (CASP), usato anche in uno studio per predire le strutture delle proteine di SARS-CoV-2, l'agente eziologico di Covid-19.

Come già accennato, tutto questo è reso possibile sia dalla velocità di elaborazione dei nuovi processori, sia dalla straordinaria quantità di dati disponibili. Attraverso la progressiva ed incrementale trasformazione digitale in corso si assiste ad una accelerazione negli studi e nelle ricerche di nuove terapie e di migliori cure, si possono offrire nuovi servizi ed erogarli telematicamente con notevole risparmio di risorse e dei costi (anche ambientali) legati agli spostamenti. Chiaramente, una simile trasformazione non è immediata e mondo accademico ed esperti sono unanimi nel sottolineare quanto sia indispensabile un'adeguata programmazione: occorre, giova ribadirlo ancora una volta, che i governi si dotino di un piano di sviluppo strategico che consenta di superare problemi culturali, problemi di connessione e di accesso ovvero il già citato *digital divide*. Per restare in ambito salute, poi, serve nello specifico una governance che regolamenti l'uso delle nuove tecnologie e dei dati sanitari digitalizzati per evitare futuri distopici nei quali tali informazioni anziché avvantaggiare le persone le discriminino.

3.1. Lo scenario italiano

L'Italia, grazie ai suoi ricercatori ed imprenditori, può legittimamente annoverarsi tra le prime nazioni ad avere contribuito alla diffusione dell'informatica (si veda la storia di Olivetti) ed allo sviluppo della rete (si veda lo straordinario archivio sull'Internet italiano a cura del compianto Giorgio Giunchi[25]. La politica ed i legislatori hanno, però, dovuto sempre inseguire poiché innovazioni e tecnologie evolvono più velocemente della possibilità e della capacità di regolamentarle. Negli ultimi trenta anni si è assistito ad un susseguirsi di leggi, decreti, circolari in materia di informatica e telecomunicazioni: un dedalo di norme nel quale anche gli esperti a volte faticano a districarsi. Basta guardare all'originaria identificazione obbligatoria per sottoscrivere un abbonamento ad Internet, all'istituzione della Posta Elettronica Certificata e la sua evoluzione con relativi registri pubblici ed assunzione a domicilio digitale, alle firme

e certificati digitali ed alla conservazione sostitutiva, oppure ancora al baluardo rappresentato dal Codice dell'amministrazione digitale, modificato e integrato più volte dal suo varo con il d.lgs. 7 marzo 2005, n. 82, alla fatturazione elettronica, ai provvedimenti per alterare i DNS ed oscurare siti... Anche il percorso degli organismi creati dal nostro Governo per lo sviluppo e la regolamentazione del digitale è stato piuttosto travagliato: quanti si ricordano dell'Autorità per l'informatica nella pubblica amministrazione (AIPA) istituito nel febbraio del 1993 e le cui competenze furono parzialmente ereditate dal Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA)? Da notare che il CNIPA venne istituito dall'art. 176 del d.lgs 30 giugno 2003, n. 196 (il Codice italiano per la protezione dei dati personali) in sostituzione dell'Autorità per l'informatica nella pubblica amministrazione (AIPA), della quale conservava le attribuzioni. Il CNIPA si trasformò in DigitPA per confluire, poi, nell'attuale Agenzia per l'Italia Digitale (AgID).

Paradossalmente, proprio l'emergenza pandemica, ha dato ulteriore impulso allo sviluppo ed alla regolamentazione della sanità digitale. Ai contenuti del *Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022*[26], infatti, si è aggiunto quanto previsto dal *Piano Nazionale di Ripresa e Resilienza*[27]. I punti salienti per quanto riguarda l'attuale Piano Triennale in ambito salute riguardano l'implementazione del FSE (Fascicolo sanitario elettronico), dei CUP (Centri unici di prenotazione) e dei progetti di telemedicina, mentre gli obiettivi fissati dal PNRR Salute[28] sono ancora più ambiziosi: «potenziare la capacità di prevenzione e cura del sistema sanitario nazionale a beneficio di tutti i cittadini, garantendo un accesso equo e capillare alle cure e promuovere l'utilizzo di tecnologie innovative nella medicina».

L'auspicio è che si riesca a passare da progetti sperimentali e scollegati tra loro ad un vero e proprio ecosistema sanitario all'interno del quale poter sfruttare tutti i collegamenti possibili tra le varie banche dati, usando le migliori tecnologie disponibili ed implementando una solida governance che oltre alla salute tuteli anche la sicurezza ed il trattamento dei dati.

3.2. Ecosistema sanitario

La creazione di un ecosistema sanitario vede come attori principali il Ministero della Salute, il Ministero dell'Economia e delle Finanze, il Garante per la protezione dei dati personali, AgID ed ovviamente gli ospedali, i laboratori, le case di cura ed i cittadini. La finalità principale è quella di arrivare all'adozione di soluzioni e di azioni finalizzate a migliorare i servizi sanitari, limitare gli sprechi e le inefficienze, migliorare il rapporto costo-qualità dei servizi sanitari e garantire a tutti i cittadini le medesime possibilità di cura e di accesso ai servizi riducendo le differenze tra i territori[29]. Vanno considerati come parte integrante di questa piattaforma anche i servizi relativi all'identità (CIE, SPID) ed ai pagamenti digitali (PagoPA) che consentono di accedere ai propri dati e di pagare quanto dovuto per le prestazioni fruite.

Senza avventurarci troppo nei dettagli dei singoli progetti, la cui documentazione comunque è facilmente reperibile in rete[30], possiamo affermare che il sistema di base prevede che il cittadino sia dotato della Tessera sanitaria (TS) che abilita all'accesso delle prestazioni sanitarie erogate dal Servizio Sanitario Nazionale. La TS è strutturalmente connessa al codice fiscale ed a questo viene associato per ciascun individuo un fascicolo sanitario elettronico. Quest'ultimo è lo strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria.

La base dati costituita da TS e FSE rende possibili ulteriori implementazioni dell'ecosistema quali l'adozione di un sistema centralizzato informatizzato per la prenotazione unificata delle prestazioni (il CUP) e la dematerializzazione di referti e ricette, che possono essere archiviati e resi direttamente accessibili ai cittadini attraverso diversi canali telematici. Questi dati, tra l'altro, essendo digitalizzati possono essere riutilizzati per diverse finalità e con diverse modalità, purché lecite e conformi alla normativa vigente sulla protezione dei dati personali. Anche per i cittadini la situazione critica della pandemia ha determinato un impulso a dotarsi delle conoscenze e degli strumenti necessari per beneficiare dei servizi sanitari a distanza: non solo sono aumentati esponenzialmente gli accessi telematici ai referti e le ricette dematerializzate, ma si sono avute anche le prime sperimentazioni di tele-visite. L'integrazione e l'interoperabilità di tutte queste piattaforme non è cosa semplice, sia per quanto riguarda gli aspetti tecnici che per quelli legati alla riservatezza, come si è visto in occasione degli applicativi utilizzati per gestire la prenotazione dei vaccini o di quelli creati per il Green Pass e financo per il tracciamento e per avvertire gli utenti che avessero avuto un'esposizione a rischio (app Immuni[31] era stata creata per acquisire e visualizzare la Certificazione verde COVID-19).

3.3. Le applicazioni

In molte strutture ospedaliere si utilizzano già oggi dispositivi certificati che consentono il tele-

monitoraggio ovvero l'osservazione a distanza dello stato di salute dei pazienti assistiti, grazie a dispositivi di misurazione integrati, interfacciati tramite apposite applicazioni con il personale medico. Le evidenze dei benefici dati dalla telemedicina sono evidenti da anni[32], ma lo sviluppo e la diffusione delle sottostanti tecnologie, che la rendono possibile, richiedono un quadro normativo che fatica a delinearsi. Accanto alle sperimentazioni di alcuni ospedali e centri di ricerca od alle iniziative istituzionali di applicazioni per cellulari quali Immuni, quella del Fascicolo Sanitario Elettronico e quella dei servizi pubblici IO, non bisogna dimenticare il fenomeno legato alla diffusione di dispositivi *wearable* e della miriade di applicazioni sviluppate per monitorare la salute o l'attività fisica: la cosiddetta *mobile health* (*mHealth*).

Molti dei più diffusi dispositivi cellulari sono ormai in grado di rilevare battito cardiaco, pressione, quantità e qualità del sonno, ossigenazione, ed i loro applicativi possono essere integrati con altri dati inseriti dagli utenti o acquisiti via Bluetooth da altri dispositivi quali: peso, consumo calorico, glicemia, ciclo mestruale e tutta una serie di altri parametri per monitorare il proprio stato di salute. Per quanto in tutte queste applicazioni in uso sugli smartphone siano presenti precise avvertenze sulla tutela della privacy e su come i parametri rivelati non siano certificati né possano costituire una vera e propria diagnosi, non sfuggirà ai più che le modalità di utilizzo e di controllo di questi dispositivi e di queste app siano totalmente rimesse ai singoli utenti. In assenza di una diffusa cultura digitale e di una maggiore consapevolezza degli utenti è praticamente impossibile determinare il giusto compromesso tra benefici e rischi, fra tutela della salute e corretto trattamento dei propri dati personali[33]. Se da un lato abbiamo app in grado di rivelare aritmie o cadute e di salvare così delle vite, dall'altro abbiamo delle app studiate per facilitare la diagnosi delle malattie che potrebbero indurre a sentirsi tranquillizzati a fronte di una previsione o diagnosi errata. Ritorna qui il tema della fiducia e delle fonti affidabili, emerso anche nel corso di vari panel degli IGF, sia sotto il profilo della certificazione di software e dispositivi, sia sotto il profilo delle garanzie necessarie al loro corretto trattamento ai fini della privacy. Uno spiraglio lo si sta intravedendo grazie al diffondersi del principio della *Evidence Based Medicine* ovvero di un utilizzo verificato e verificabile delle risultanze dei dati raccolti attraverso i diversi dispositivi ed alle discussioni sui modelli predittivi che possono, chiaramente, avere effetti eterogenei su soggetti diversi[34].

4. La tutela dei dati personali in ambito sanitario

Al centro di tutto quanto sinora illustrato vi è il dato personale di carattere sanitario ovvero una particolare categoria di dato considerato molto sensibile in quanto in grado di rivelare lo stato di salute con potenziali conseguenze dirette sulla libertà, sulla dignità e nella vita concreta delle persone. A distanza di quasi vent'anni sono ancora di straordinaria attualità le parole di Stefano Rodotà (di cui consigliamo la lettura integrale al link in nota[35]) nel suo intervento del 2004 alla ventiseiesima Conferenza internazionale sui commissari per la protezione dei dati e la privacy: «Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro. [...] Emerge un legame profondo tra libertà, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo. Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell'eguaglianza. [...] Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo, diventa così evidente che: la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale».

Ogni volta che viene messa in dubbio l'importanza della privacy o la si voglia considerare una cosa astratta e secondaria andrebbero rilette le parole sopra riportate. Ancora oggi, purtroppo, molti vedono la tutela della riservatezza come un farraginoso e fastidioso orpello che ostacola il libero mercato e la stessa azione della pubblica amministrazione. Il periodo pandemico è stato abbastanza eclatante sotto questo aspetto ed ha messo a dura prova il Garante italiano, tutti i *data protection officer* (DPO) e quanti si occupano della materia professionalmente o per motivi di studio e ricerca. La situazione di emergenza ha indotto molti, persino a livello legislativo, a ritenere che, in nome della tutela alla salute, si potesse e si dovesse mettere in secondo piano la tutela dei dati personali.

A questo riguardo, vale la pena ricordare come la normativa dettata del Regolamento UE 2016/679[36] meglio noto come GDPR (*General Data Protection Regulation*) abbia riconosciuto e sancito che la protezione delle persone fisiche con riguardo al trattamen-

to dei dati di carattere personale sia un diritto fondamentale. Ma ha anche precisato come tale diritto non sia assoluto, ma vada considerato alla luce della sua funzione sociale e vada contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (considerando 1 e 4 del GDPR). Più che creare una contrapposizione o invocare una scelta tra la tutela della salute e quella della privacy, occorre cimentarsi in un'operazione di costante bilanciamento tra valori e diritti: diversi, ma ugualmente fondamentali. Vanno lette in quest'ottica alcune delle principali problematiche verificatesi ed affrontate durante il periodo pandemico e riportate brevemente di seguito.

4.1. Pandemia, Garante privacy e nuovo FSE

L'individuazione o la realizzazione, via via, di specifiche piattaforme software per gestire la prenotazione e l'erogazione dei vaccini, per tenere traccia dei contatti, oppure ancora per ricevere ed aggiornare il cd. Green Pass ha sollevato diversi problemi operativi ed infinite discussioni sotto il profilo delle funzionalità, della protezione dei dati e della tutela della riservatezza.

Non si vuole entrare qui nel merito di politiche e scelte legislative, ma solo sottolineare alcune peculiari criticità che si sono verificate. È il caso, per esempio, di soggetti fragili che avrebbero avuto diritto a prenotarsi per la vaccinazione e non hanno potuto farlo in prima battuta a causa di database incompleti e di piattaforme poco flessibili. Vi sono stati poi casi in cui la non esattezza dei dati riguardanti i codici fiscali ha portato a mancate certificazioni o scambio di identità nei referti di positività al virus e a tanti altri disguidi. Mai come in questo caso è diventato evidente quanto il trattamento dei dati personali possa incidere sulle libertà e nella vita quotidiana degli individui e di quanto siano importanti i principi declinati, in particolare, dall'art. 5 del GDPR sulla minimizzazione, esattezza e conservazione dei dati personali.

Altrettanto lungimirante si è rivelato il regolamento europeo laddove ha introdotto con i commi 4 e 5 dell'art. 36 un obbligo di consultazione preventiva delle Autorità garanti da parte dei singoli legislatori europei per tutti gli atti legislativi o regolamentari che incidano sul trattamento di dati personali: «4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento» e «5. ... il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica».

Di fronte all'emergenza medica, al grande impegno del personale sanitario è corrisposto pari impegno, non sempre compreso, da parte del Garante Privacy e dei responsabili per la protezione dei dati personali per salvaguardare diritti e riservatezza degli interessati, ma anche per ridurre i rischi e le responsabilità connesse al trattamento di dati tanto sensibili.

Durante l'emergenza pandemica il Garante della privacy italiano è dovuto intervenire più volte[37] e su più fronti: un'attività poderosa, non sempre compresa o accettata di buon grado.

Uno dei progetti che verrà sostenuto e finanziato dal PNRR Salute è la messa a punto del nuovo Fascicolo Sanitario Elettronico, che sarà basato su un repository centrale HL7 FHIR[38] per la gestione dei dati strutturati oltre che sul protocollo XDS[39] per i documenti. Un progetto molto complesso che richiederebbe una discussione allargata (sul modello IGF) con tutti gli stakeholder ed il coinvolgimento di diverse professionalità, cominciando proprio dai medici, e che dovrà senz'altro coinvolgere il Garante per le implicazioni legate alla sicurezza ed alla protezione dei dati personali[40].

Si deve prendere atto che, se le finalità perseguite con il trattamento dei dati personali sono spesso nobili ed importanti, non si deve mai ignorare, però, il come i dati vengano elaborati. È di fondamentale importanza valutare l'intero ciclo di vita dei dati, dalla raccolta alla cancellazione/distruzione, affinché questo avvenga lecitamente e nel rispetto delle cautele e della normativa dettate in materia di privacy e *data protection*. Il sistema che si vuole adottare prevede la geolocalizzazione? I dati che tratta sono tutti necessari per le finalità che ci si propone? È stata definita la base giuridica che rende legittimo il trattamento? Chi avrà accesso al sistema viene autorizzato, tracciato e (in)formato sui vincoli a tutela della riservatezza degli interessati? Si prevede di comunicare i dati a terzi o che propri fornitori/collaboratori esterni vi abbiano accesso? Il sistema è *on premise* o in cloud e adotta misure di sicurezza adeguate? È previsto trasferimento dati diretto od indiretto all'estero? Per quanto tempo i dati verranno conservati ed è stata messa a disposizione degli interessati un'informativa dettagliata e completa? Queste sono solo alcune delle domande e degli adempimenti che si devono affrontare per una corretta governance ed una reale tutela di tutti i diritti dei cittadini.

4.2. Consenso e registro dei trattamenti

Va ribadito, una volta per tutte, che le finalità di cura non necessitano di consenso e che il consenso informato è cosa diversa dal consenso privacy. Il consenso informato riguarda il trattamento sanitario ed il tipo di cure, il consenso privacy attiene all'autorizzazione a che i propri dati possano essere trattati per le finalità indicate nell'informativa. I dati relativi alla salute, i dati genetici e biometrici, possono del pari essere lecitamente trattati per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria e per finalità sociali quali la gestione dei servizi sociosanitari, nonché per motivi di interesse pubblico nel settore della sanità pubblica. Discorso diverso per tutte le altre finalità che richiedono l'esplicita espressione di apposito e libero consenso.

L'inserimento di dati, ovvero l'alimentazione del Fascicolo Sanitario Elettronico, per esempio, richiedeva il consenso. Nel 2020, poi, al fine di accelerare l'attivazione e l'utilizzo del FSE da parte di tutti gli assistiti, l'articolo 11 del d.l. 19 maggio 2020, n. 34 ha previsto che l'alimentazione del fascicolo avvenga in maniera automatica eliminando la necessità di ottenere il consenso[41]. Sul punto, però, il Garante, che già si era espresso favorevolmente nel 2019 quando aveva fornito dei primi importanti chiarimenti sull'applicazione del GDPR nel trattamento dei dati relativi alla salute in ambito sanitario[42], ha stabilito che, al fine di garantire i diritti degli interessati, venisse effettuata un'adeguata campagna informativa a livello nazionale e regionale e che venisse comunque garantito di poter esercitare il diritto di opposizione all'alimentazione del FSE con i dati sanitari generati da eventi clinici anteriori alla nuova norma, entro un termine prestabilito, non inferiore a 30 giorni.

Non va sottaciuto, però, quanto sia complessa la concreta applicazione del GDPR e l'elaborazione di misure tecnico-organizzative pienamente conformi al Regolamento all'interno delle strutture che caratterizzano il nostro Sistema Sanitario Nazionale (SSN). L'esperienza sul campo ci ha dimostrato quanto siano importanti le competenze, le risorse, la buona volontà e la formazione di tutti i soggetti coinvolti ai quali, spesso, difetta il tempo. Eppure, nonostante l'ostacolo e le urgenze dettate dalla pandemia, abbiamo personalmente constatato un generale e notevole innalzamento della sensibilità e dell'attenzione nella tutela della riservatezza delle persone.

Una vera e propria pietra angolare nel costante percorso di adeguamento alla normativa vigente si è rivelato essere il registro dei trattamenti che, previa adeguato *assessment*, permette di fotografare quali dati vengano raccolti e trattati, da quali unità operative, per quali finalità e con quali misure di sicurezza, censendo anche i fornitori ed i relativi contratti in essere. Un registro organizzato, completo ed aggiornato correttamente rende molto più semplice la messa a punto di adeguate procedure e l'introduzione di un sistema di gestione della privacy sia dal punto di vista documentale (incarichi, nomine, informative, regolamenti interni, etc.), sia dal punto di vista tecnico ed organizzativo (chi fa cosa e con quali strumenti). Per un DPO o responsabile della protezione dei dati la stessa gestione di un *data breach* non sarebbe possibile nella finestra di tempo prevista dall'ordinamento (72 ore) senza i riferimenti contenuti nel registro.

4.3. Nuove tecnologie e valutazioni di impatto

Abbiamo già osservato come la sanità strizzi l'occhio alle nuove tecnologie. Riteniamo opportuno, però, seppur brevemente, mettere in guardia dall'ideazione e dall'avvio di progetti o di sperimentazioni che non tengano in debito e preventivo conto della tutela dei dati personali. Introducendo i principi di *privacy by default* e *privacy by design* il GDPR ha giustamente imposto che nessun trattamento di dati personali avvenga senza che ne sia stato valutato il rischio e senza che siano state adottate adeguate misure di sicurezza.

«Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti – cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato»[43].

Quanto sopra non deve essere visto come un freno all'innovazione o alla possibilità di cambiare il modo di erogare determinati servizi, è invece una doppia tutela sia per gli interessati, i cui dati si intendono trattare, sia per gli stessi titolari dei trattamenti che, in base al principio dell'accountability, devono essere in grado di dimostrare che le misure di sicurezza da loro adottate sono "adeguate", se non vogliono andare incontro a responsabilità e sanzioni.

5. *Cybersecurity* e *data breach*

Merita, da ultimo, un capitolo a parte il tema della sicurezza informatica dei dati personali in grado di

rivelare lo stato di salute trattati da ospedali, centri di cura, laboratori, centri vaccinali, pubbliche amministrazioni, case farmaceutiche e da tutti gli attori del sistema sanitario.

In generale, il principio di accountability introdotto dal GDPR ha correttamente spostato l'attenzione da mere check list di adempimenti (approccio formale) alle indicazioni contenute negli artt. 24-25 e 32 del Regolamento: titolare e responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato ai rischi e, in particolare, a quelli che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (approccio sostanziale). Un adeguato livello di sicurezza non potrà prescindere da una verifica costante delle misure di sicurezza approntate rispetto allo "stato dell'arte", anche in considerazione della rapida evoluzione tecnologica. E nel caso di trattamenti di dati sanitari, il livello di sicurezza dovrà sempre essere il più elevato possibile, specie qualora si trattino dati genetici o dati biometrici.

All'interno del summenzionato art. 32 del GDPR vengono indicate, a titolo esemplificato, alcune misure di sicurezza quali la pseudonimizzazione e la cifratura dei dati personali. Altro strumento indispensabile per la conformità alla normativa vigente in materia di protezione dei dati personali sono le linee guida, le raccomandazioni e le *best practices*[44] pubblicate dallo *European Data Protection Board* (EDPB) Comitato europeo per la protezione dei dati, che è composto da rappresentanti delle autorità nazionali per la protezione dei dati dell'UE e dal Garante europeo della protezione dei dati. Dal punto di vista tecnico, invece, il punto di riferimento e di supporto nella definizione delle misure di sicurezza è dato dall'ENISA[45], l'Agenzia dell'Unione europea per la cybersecurity dedicata al raggiungimento di un livello, comune ed elevato, di sicurezza informatica in tutta Europa. Da segnalare che l'ENISA aveva pubblicato già nel 2017 delle linee guida tecniche per l'attuazione delle misure minime di sicurezza per i fornitori di servizi digitali[46] e messo a disposizione, agli inizi del 2020, un tool per valutare il livello di rischio nei trattamenti dei dati personali[47]. Di ancora maggiore interesse, però, sono le iniziative prese da ENISA nello specifico ambito salute: ha infatti lanciato l'*Health Security Experts Group*[48] per garantire la sicurezza e la resilienza del settore sanitario in Europa, ha pubblicato le linee guida per gli appalti per la sicurezza informatica negli ospedali[49] e uno strumento online per aiutare le organizzazioni sanitarie a identificare rapidamente le linee guida più rilevanti per il loro contesto di approvvigionamento, come i beni acquistati o le relative minacce[50] ed ha pubblicato un rapporto sulla sicurezza cloud per i servizi sanitari nel gennaio 2021. L'ENISA, inoltre, organizza ciclicamente l'*eHealth Security Conference* per discutere temi essenziali di cybersecurity per il settore sanitario[51].

A completare il quadro non si può non citare anche la direttiva (UE) 2016/1148[52], meglio nota come direttiva NIS (*Network and Information Security*) che concerne le misure per garantire un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi in tutta l'Unione europea. Nel recepirla con il d.lgs. 18 maggio 2018, n. 65, sono stati individuati cinque Ministeri (sviluppo economico, infrastrutture e trasporti, economia, salute e ambiente) presso i quali sono state designate le "Autorità competenti NIS". Il Ministero della Salute che è Autorità competente NIS per l'attività di assistenza sanitaria, prestata dagli operatori dipendenti o incaricati dal Ministero o convenzionati con il medesimo, ha poi individuato degli Operatori di Servizi Essenziali (OSE), ovvero soggetti i cui servizi dipendono dalla rete e dai sistemi informativi e per i quali un incidente avrebbe effetti negativi rilevanti sulla fornitura di tali servizi. Questi ultimi sono secretati, hanno degli obblighi particolari in materia di sicurezza e di notifica degli incidenti e devono seguire delle apposite linee guida basate sul Framework nazionale per la cyber security e la data protection.

Purtroppo, i numerosi *data breach* informatici occorsi hanno dimostrato che, pur in presenza di procedure e politiche per la gestione delle informazioni, il fattore umano risulta sempre determinante. Anche per questo continue procedure di *assessment*, formazione ed audit sono indispensabili così come il supporto di team e professionisti esperti in IT, sicurezza informatica e protezione dei dati.

Concludendo, una delle sfide più grandi, in termini di governance, è quella di riuscire a rendere Internet ed i sistemi per la tutela della salute più sicuri ed affidabili, mantenendoli però aperti, interoperabili ed accessibili, tramite una riduzione del divario digitale e l'aumento di fonti *trustable*, ovvero affidabili, senza con ciò sottovalutare la tutela della privacy degli utenti.

Note

[1] World Summit on the Information Society (WSIS), Geneva 10-12 December 2003, and Tunis 16-18 November 2005.

[2] Ministero dello sviluppo economico, *Internet Governance e Attività Internazionali*.

[3]V. L. Abba, A. Nicotra, *Generic Top Level Domain di Internet*, in "Informatica e diritto", 2006, n. 1, pp. 125-147.

[4]Le *Digital Therapeutics*, abbreviato all'americana DTx, sono terapie digitali basate su software ed algoritmi che prendono la forma di videogiochi, sensori o realtà virtuale ed agiscono sia come terapia comportamentale sia come cura specifica per determinate patologie. Si tratta di vere e proprie terapie che necessitano di prescrizione medica e devono essere accompagnate da adeguate istruzioni, esattamente come coi farmaci.

[5]Si veda il progetto per l'hosting e l'elaborazione dei dati della ricerca a sostegno della scienza dell'UE varato con lo *European Open Science Cloud* (EOSC).

[6]*Global healthcare big data market size in 2016 and a forecast for 2025*.

[7]Anitec-Assinform, *Italia quarta al mondo e prima in Europa per attacchi Malware*.

[8]S. Kemp, *Digital 2021 April Global Statshot Report*, 21 April 2021.

[9]*Reti di calcolatori. Protocolli e standard*.

[10]Si veda, ad esempio, il Regolamento (UE) n. 283/2014 del Parlamento Europeo e del Consiglio dell'11 marzo 2014 sugli orientamenti per le reti transeuropee nel settore delle infrastrutture di telecomunicazione.

[11]World Summit on the Information Society, *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium*, 12 December 2003.

[12]Unicef, Mortalità infantile ancora in calo nel mondo, ma il COVID minaccia i progressi, 9 settembre 2020: «Secondo le nuove stime sulla mortalità pubblicate oggi da UNICEF, Organizzazione Mondiale della Sanità (OMS), Divisione per la Popolazione del Dipartimento per gli Affari Economici e Sociali delle Nazioni Unite (UNDESA) e Banca Mondiale, il numero di decessi tra 0 e 5 anni a livello globale nel 2019 è sceso al punto più basso mai registrato nella storia. I decessi sono stati infatti 5,2 milioni, con un calo di quasi il 60% rispetto ai 12,5 milioni del 1990».

[13]World Summit on the Information Society, *Tunis Agenda for the Information Society*, 18 November 2005.

[14]Si veda il sito ufficiale dell'Internet Governance Forum.

[15]L'*Electronic Frontier Foundation* è un'associazione internazionale no profit.

[16]*Società Internet* è l'associazione ed il capitolo italiano di ISOC.

[17]*Internet Society* (ISOC) è l'associazione costituita nel 1992 da Vint Cerf, Bob Kahn e da altri primi pionieri che hanno guidato lo sviluppo tecnico di Internet.

[18]ONU - Assemblea generale, *Trasformare il nostro mondo: l'Agenda 2030 per lo Sviluppo Sostenibile*, 21 ottobre 2015.

[19]Agenzia italiana per la cooperazione allo sviluppo, *Obiettivi di sviluppo sostenibile - SDGs*.

[20]Da elogiare, in tal senso, il nostro Ministero della Salute che, per esempio, ha ritenuto opportuno pubblicare delle FAQ ed una risposta alle fake news circolanti sui vaccini e sul Covid-19.

[21]Si veda per esempio il contributo di Gilberto Corbellini, professore ordinario di Storia della medicina e docente di Bioetica presso la Sapienza Università di Roma, ripreso dalla Encilopedia Treccani, alla voce *Storia della Medicina*.

[22]Istituto Superiore di Sanità, *Come viene sviluppato e commercializzato un vaccino*, aprile 2017.

[23]Ospedale pediatrico Bambin Gesù, *Nuovo Coronavirus: come si è riusciti a produrre rapidamente vaccini sicuri*, agosto 2021.

[24]Istituto Superiore di Sanità, *Sviluppo, valutazione e approvazione dei vaccini contro COVID-19*, gennaio 2021.

[25]Giorgio Giunchi è stato l'ideatore ed il curatore del più completo portale contenente fonti e ricerche sulla storia dell'informazione automatica e dell'Internet in Italia).

[26]AGID, *Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022*, luglio 2020.

[27]Presidenza del Consiglio dei ministri, *PNRR, gli obiettivi e la struttura*, novembre 2021.

[28]Id., *PNRR: salute*, novembre 2021.

[29]AGID, *Sanità digitale*.

[30]Il Ministero della Salute ha reso disponibile il sito *eHealth - Sanità digitale*, con collegamenti e normativa aggiornati.

[31]L'app Immuni

[32]Si veda a questo riguardo la ricerca presentata dalla Dr.ssa Diana Lelli nell'ambito del 63esimo Congresso Nazionale della Società Italiana di Gerontologia e Geriatria (Roma, 28 novembre-1 dicembre 2018).

[33]E. Santoro, *Tutti i problemi delle app mediche: vantaggi dubbi, privacy a rischio*, in "AgendaDigitale.eu", 23 gennaio 2017.

[34]D.M. Kent, E. Steyerberg, D. van Klaveren, *Personalized evidence based medicine: predictive approaches to heterogeneous treatment effects*, 2018.

[35]S. Rodotà - *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, settembre 2004.

[36]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[37]Fra i numerosissimi interventi, si segnala il parere favorevole sullo schema di decreto attuativo, che attiva la Piattaforma nazionale-DGC per il rilascio del *green pass*, prevedendo adeguate garanzie per l'utilizzo delle certificazioni verdi. V. Garante per la protezione dei dati personali, *Certificazioni verdi: via libera del Garante, con adeguate garanzie. Disposto il blocco provvisorio per l'App IO*, 10 giugno 2021.

[38]FHIR è uno standard per lo scambio di dati sanitari, pubblicato da HL7.

[39]Un documento XDS è un qualsiasi tipo di informazione clinica indipendente dal contenuto e rappresentazione con una precisa struttura che si avvale degli standard informatici sanitari.

[40]*Anteprima: ecco come sarà il Fascicolo Sanitario Elettronico 2.0*, 16 novembre 2021.

[41]Ministero della Salute, *L'attivazione e l'alimentazione del FSE*, 4 maggio 2021.

[42]Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019.

[43]Id., *Valutazione d'impatto della protezione dei dati (DPIA)*.

[44]European Data Protection Board, *Guidelines, Recommendations, Best Practices*.

[45]L'*Agenzia dell'Unione europea per la cybersecurity* (ENISA) è incaricata di creare le condizioni per un elevato livello comune di cibersicurezza in tutta Europa.

[46]ENISA, *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*, 16 February 2017.

[47]Id., *Evaluating the level of risk for a personal data processing operation*.

[48]Sul portale dell'ENISA è presente una sezione dedicata alle misure di sicurezza ed infrastrutturale per il settore sanitario.

[49]ENISA, *Procurement Guidelines for Cybersecurity in Hospitals*, 24 February 2020.

[50] Id., *Good practices for the security of healthcare services*.
[51] Id., *Cloud Security for Healthcare Services*, 18 January 2021.
[52] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

* * *

Health protection, digital systems and privacy

Abstract: Innovations and new technologies can greatly contribute to improve care and research, but they should be regulated on the basis of a multistakeholder process such as that offered by Internet Governance. The systems digital transformation in the healthcare requires particular attention and sensitivity in terms of protecting and processing of personal data. It is central to build a functional digital ecosystem, yet safe and respectful of people's dignity and rights.

Keywords: Health – Privacy – Data protection – New technologies – Digital transformation