Nel futuro prossimo l'impatto che le nuove tecnologie 5G avranno sulla fruizione e sull'accessibilità dei servizi sanitari per medici e pazienti sarà estremamente rilevante soprattutto grazie alle reti mobili di nuova generazione che si prefiggono di raggiungere obiettivi prestazionali ambiziosi. Se la digitalizzazione delle strutture sanitarie e l'applicazione delle nuove tecnologie 5G garantiscano un importante miglioramento della vita e della salute dei cittadini, dall'altro è, altrettanto, importante non sottovalutare i rischi ed i pregiudizi per la stessa incolumità fisica e psichica delle persone che ne possono derivare, proteggendosi adeguatamente da qualsiasi attacco e/o intrusione.

di Donatella Proto e Caterina Petrigni

IL 5G NEL SETTORE DELL'*E-HEALTH* TRA RISCHI ED OPPORTUNITÀ

Donatella PROTO *è Dirigente della Divisione 1 del MISE "Reti e Servizi di comunicazione elettronica ad uso pubblico della Direzione Generale per i servizi di comunicazione elettronica, di radiodiffusione e postali".*

Caterina Petrigni *è Ingegnere Biomedico. Ha svolto attività di ricerca sui temi della sicurezza, qualità e performance di impianti e tecnologie delle strutture sanitarie e attualmente collabora in qualità di esperto per il raggiungimento degli obiettivi del progetto "Monitoraggio della spesa per la manutenzione degli immobili del SSN" presso l'Agenas e per l'esame e la trattazione delle materie connesse alle questioni energetiche e all'innovazione tecnologica presso il MISE.*

1. Introduzione

Nel futuro prossimo l'impatto che le nuove tecnologie 5G avranno sulla fruizione e sull'accessibilità dei servizi sanitari per medici e pazienti sarà estremamente rilevante soprattutto grazie alle reti mobili di nuova generazione che si prefiggono di raggiungere obiettivi prestazionali ambiziosi, tra cui, in modo particolare, una bassa latenza (<5ms), una elevata densità (fino a 100 dispositivi/m^2) ed una ampia copertura (ubiquità della rete in aree urbane e rurali).

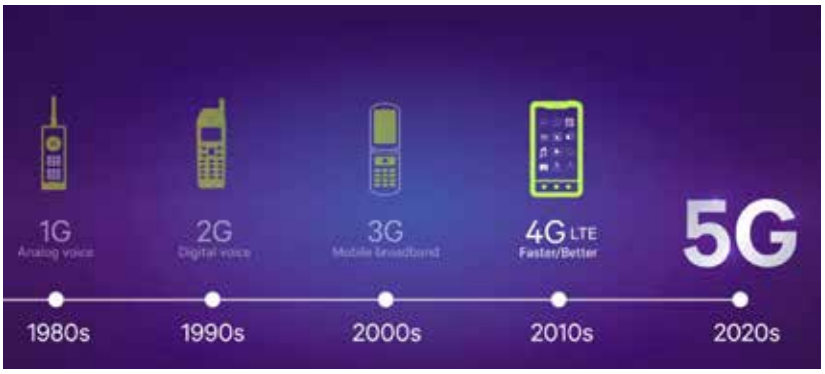
Tali reti diventeranno un veicolo per abilitare applicazioni e servizi nell'ambito della cd *e-Health*, fino ad oggi irrealizzabili a causa dei limiti delle infrastrutture di comunicazione attuali in termini di latenza ed ubiquità. Si pensi, ad esempio, ai limiti della telemedicina a causa del fenomeno del "*cyber sickness*": gli alti tempi di latenza generano un conflitto sensoriale tra quello che si osserva virtualmente e quello che percepiscono gli altri sensi, provocando sintomi quali nausea, vertigini, sudorazione, mal di testa etc. e, quindi, compromettono le capacità operative dei chirurghi.

Le reti di nuova generazione saranno sicuramente il volano attraverso cui abilitare numerose applicazioni, tra cui, ad esempio, proprio l'interazione virtuale medico-paziente, la chirurgia robotica a distanza e, più in generale, tutto ciò che facilita il decentramento dell'assistenza sanitaria dagli ospedali verso le case, a fronte di una forte centralizzazione dei dati. Se da un lato, quindi, la diffusione del 5G sarà un'opportunità di grande innovazione e miglioramento nei processi di *cure* e *care* del paziente con indubbie ricadute positive in termini di sostenibilità del Sistema Sanitario Nazionale, dall'altro, se non ben gestito, tale processo potrebbe diventare causa di una maggiore vulnerabilità agli attacchi hacker dei sistemi informativi sanitari in senso lato e dei dispositivi medici impiantati e non. È, pertanto, indifferibile la necessità di implementare soluzioni che permettano di gestire l'enorme patrimonio di informazioni che arriva da tutti gli apparati che si stano diffondendo, dalla sensoristica IoT ai *wearable*, ma presupposto imprescindibile è che vi sia sufficiente connettività.

2. Attacchi hacker e cybersecurity

L'ultimo attacco contro gli ospedali britannici con computer bloccati ed ambulanze dirottate verso falsi obiettivi, anche se poi si è rilevato essere un attacco globale, ha posto ancora una volta in evidenza la fragilità del sistema sanitario di fronte alla pericolosità di *ransonware* "ricattatori". Il *ransonware* è un termine di recente coniazione con il quale si indica un tipo di *malware* che compromette il funzionamento di un computer, "richiedendo" un riscatto per consentire il riutilizzo del dispositivo e l'accesso ai dati, sul cui furto rispetto all'ultimo attacco hacker non sono pervenute indicazioni.

La crescita esponenziale (non destinata ad arrestarsi alle attuali condizioni) degli attacchi agli ospedali se da un lato è da identificare nel fatto che in campo medico i problemi della sicurezza non sono certamente la priorità e si scontrano con la necessità di intervenire in situazioni di emergenza, in cui è indispensabile un facile e veloce accesso alle informazioni, dall'altro è favorita da sistemi informatici obsoleti e dalla mancanza di una adeguata cultura informatica tra gli operatori del settore, oltre che da un tendenziale ampliamento della superficie d'attacco.



Se la digitalizzazione delle strutture sanitarie e l'applicazione delle nuove tecnologie 5G garantiscano un importante miglioramento della vita e della salute dei cittadini, dall'altro è, altrettanto, importante non sottovalutare i rischi ed i pregiudizi per la stessa incolumità fisica e psichica delle persone che ne possono derivare, proteggendosi adeguatamente da qualsiasi attacco e/o intrusione. I cd *Smart Hospitals*, luoghi in cui pazienti, personale ospedaliero, laboratori e strumenti medici sono tutti interconnessi, sono stati recentemente oggetto di uno specifico studio condotto dall'ENISA (*European Union Agency for Network and Information Security*) che nel proprio report "*Smart Hospitals: Security and Resilience for Smart Health Services and Infrastructures*" ha fornito specifiche raccomandazioni alle organizzazioni sanitarie in materia di sicurezza e "*cyber resilience*", cioè l'abilità di un ospedale di riuscire a garantire la disponibilità e la continuità dei servizi offerti attraverso le tecnologie ICT.

Lo studio dell'ENISA, pubblicato lo scorso 24 novembre 2016, analizza i potenziali scenari di attacco (es. manomissione o furto di equipaggiamento e di dispositivi medici ed attacchi *ransomware*) e propone possibili soluzioni organizzative e tecniche, tra cui l'individuazione precisa dei ruoli e delle responsabilità per la sicurezza, la creazione di norme e procedure per la *cybersecurity*, la formazione e la sensibilizzazione del personale, che nel quadro normativo nazionale, ad oggi, non appaiono sufficientemente valorizzate. C'è, pertanto, da sperare in una immediata operatività ed efficacia del nuovo **Piano nazionale per la protezione cibernetica e la sicurezza informatica**, la cui adozione è stata pubblicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 e la cui visione sistematica è volta ad assicurare la messa in sicurezza degli assetti nazionali secondo una progressione dettata da una scala di criticità:

- 1° livello – sicurezza nazionale dello Stato [Comparto Intelligence, Difesa, Interno, altre amministrazioni CISR];
- 2° livello – infrastrutture critiche nazionali [TLC, utilities, settore finanziario, trasporto] altre amministrazioni pubbliche sensibili [come la Sanità, etc.];
- 3° livello – tessuto produttivo nazionale, cittadinanza.

3. ICT, Big Data e Artificial Intelligence in Sanità

Le tecnologie ICT consentono, dunque, di acquisire – anche da remoto - grandi quantitativi di dati e di elaborarli in tempi brevi, ma è necessario che i processi e le organizzazioni medico-sanitarie siano in grado di recepirli e processarli in modo intelligente, strutturato ed affidabile con altrettanta velocità, evitando pericolose deviazioni e/o indesiderate manipolazioni, per cui il contesto in cui si opera deve essere assolutamente sicuro, considerando anche le sue articolazioni e la marcata interdipendenza settoriale, tra attori pubblici e privati, tra amministrazioni centrali e locali, tra interessi che possono essere o apparire confliggenti, ma che vanno, invece, gestiti attraverso un forte controllo ed il rispetto di stringenti paradigmi tecnici ed amministrativi in una visione utente/paziente centrica, in cui il paziente può (o *rectius* deve) essere fonte di conoscenza ed avere un ruolo attivo e responsabile, attraverso anche l'uso di device consumer in grado di interoperare in maniera efficace con gli apparati medicali tradizionali.

In tal modo si passerebbe da un "welfare di Stato" ad un "welfare di comunità", riducendo la spesa sanitaria complessiva e migliorando lo stato di salute della popolazione, motivata a prendersi in carico il proprio stato di salute e ad adottare uno stile di vita sano. Quanto paradossale possa essere ignorare tale necessità di sicurezza, è reso ancor più evidente se si pensa che i cittadini tendono sempre più spesso, invece, a far uso delle tecnologie per controllare la propria salute e cercare risposte alle proprie esigenze in campo sanitario. Da un recente studio sulla sanità di Ericcson ConsumerLab emerge che il 39% dei pazienti cronici preferisce consultare *on line* i propri medici piuttosto che incontrarli e 2 consumatori su 3 utilizzano i dispositivi indossabili per gestire le patologie.

Per il raggiungimento di tale obiettivo di sicurezza una delle principali criticità è di natura culturale, soprattutto se si considera quanto importante per la sicurezza sia un consapevole e corretto utilizzo dei dispositivi e che solo il 53% dei dispositivi connessi è, invece, protetta adeguatamente. Ma in ambito medicale possono emergere anche problemi di etica, soprattutto se pensiamo a sistemi di intelligenza artificiale ed all'uso della robotica. Il cambiamento rivoluzionario da una "medicina di attesa", di cura delle malattia, laddove si manifesti, ad una "medicina di iniziativa", di prevenzione e orientata al benessere, e di "prossimità" si basa sulla tecnologia o meglio sul'acronimo "NBIC", cioè nanotecnologie, biotecnologie, informatica e cognitive computing.

L'intelligenza artificiale applicata ai *big data*, come nel caso del Fascicolo Sanitario Elettronico, che non dovrebbe essere solo un contenitore di documenti ma una piattaforma informativa a supporto della cura e dell'assistenza del cittadino, può aiutare il medico a migliorare i processi di diagnosi preventiva ed ottimizzare e personalizzare i processi di cura o offrire soluzioni nella logistica dei flussi di lavoro in ambito ospedaliero. Ma non solo: si pensi anche, ad esempio, alla possibilità di sistematizzare ed omogeneizzare sul piano nazionale, avvalendosi di infrastrutture tecnologiche già esistenti (come ad esempio quelle realizzate ai fini dell'implementazione del 112 NUE) la disponibilità in tempo reale di informazioni sui posti letto ospedalieri liberi e sulle prestazioni erogabili, così da ridurre i tempi di ospedalizzazione in condizioni di emergenza ed aumentare significativamente le possibilità di successo dell'intervento, come approfondito di seguito. L'applicazione in sanità dell'intelligenza artificiale e delle tecnologie cognitive e predittive, come dimostrato di recente da una ricerca statunitense, potrà raggiungere i 6,6 miliardi di euro con un tasso annuo di crescita del 40%, migliorando la diagnostica e l'esito delle cure del 40% e riducendo del 50% i costi.

È evidente che tale "*disruptive innovation*" passa attraverso la produzione e l'estrazione di un'enorme quantità di dati sanitari, perciò è essenziale l'operatività in sicurezza dei wearable device e dei *mobile health* (applicazioni di e-health focalizzate sulla fornitura di informazioni attraverso le tecnologie mobili) che costituiscono il serbatoio informativo in grado di abilitare la ricerca e l'innovazione attraverso l'uso delle nuove tecnologie 5G e le sue caratteristiche di bassa latenza, elevata densità e affidabilità, che permetteranno la realizzazione della cd *"Tactile Internet"*, medicazioni intelligenti, gestione e tracciamento degli assets medicali.

Se l'esistenza di una rete con elevate capacità costituisce un presupposto imprescindibile, altrettanto fondamentale è la scelta delle priorità di investimento e le scelte organizzative, che devono valorizzare e rendere accessibili le informazioni in modo sicuro e strutturato per evitare che i *big data* si trasformino in *big error*, come indicato nella Raccomandazione sulla *governance* dei dati relativi alla salute (*Recommendation On Health Data Governance*) adottata dal Consiglio dell'Ocse lo scorso 13 dicembre 2016. In Europa l'Ema (European medicinal agency) nel marzo 2017 ha deciso di dar vita a una Task Force con le autorità competenti regolatorie dello Spazio economico europeo (SEE), per stabilire come utilizzare i *big data* per sostenere la ricerca, l'innovazione e lo sviluppo farmaci a favore della salute umana e animale, al fine di valutare benefici e rischi dei medicinali. I dati potranno essere quelli delle cartelle cliniche elettroniche di milioni di pazienti e quelli provenienti dalla genomica, ma anche dai social media, da studi clinici o rapporti di reazioni avverse spontanee e così via. Collaborazione, conoscenza, sistemi informativi sicuri, fruibilità di informazioni certificate sono alla base di tale cambiamento radicale: si tratta di precondizioni di carattere organizzativo e tecnologico, vincolate naturalmente da considerazioni di carattere economico.

4. Il contesto generale dei Booking Engines e dei CRS (Central Reservation Systems) e la possibile applicazione nel settore ospedaliero

Un qualsiasi sistema di prenotazione "commerciale" di camere di albergo, quali quelli comunemente disponibili su Internet, consiste di due macroelementi (ad eccezione delle componenti legate al pagamento delle camere che non sono pertinenti in questo contesto):

- **un sistema di prenotazione**, che nei casi più semplici rende disponibile all'albergatore una semplice pagina internet per il caricamento delle disponibilità e delle caratteristiche delle camere;
- **un portale di accesso** che, accedendo alle informazioni immesse dagli albergatori attraverso il sistema di prenotazione consente l'effettuazione delle prenotazioni da parte della clientela finale.

Il caso delle prenotazioni alberghiere è molto più complesso di quello ipotizzabile in caso di trasposizione di un modello di questo tipo in ambito sanitario in considerazione dei volumi molto più bassi sia lato offerta (i soli ospedali) che lato domanda (i soli PSAP di primo livello), anche ove si ipotizzasse un sistema centralizzato su base nazionale.
Mentre il tema non presenta alcuna complessità dal punto di vista tecnologico, il principale problema da porsi in uno scenario quale quello qui analizzato è quello organizzativo, se infatti in uno scenario di mercato "competitivo" quale quello degli alberghi l'elemento del costante aggiornamento delle informazioni sulle effettive disponibilità non rappresenta un problema, la trasposizione del modello nel quadro della sanità richiederebbe necessariamente un passaggio normativo che rendesse obbligatorio, da parte degli ospedali, il costante mantenimento ed aggiornamento del dato relativo all'effettiva fruibilità dei posti letto e delle prestazioni erogabili affinché le informazioni siano fruite in modo sicuro e strutturato per evitare i sopracitati "big error".

Per semplificare, nel caso della terapia intensiva neonatale, un ospedale che disponga di 3 postazioni complessive, delle quali due occupate, e che debba "autoprenotare" una postazione in vista di un parto con potenziali complicazioni, dovrebbe assicurare l'immediato aggiornamento del dato sulla disponibilità effettiva per evitare problematiche in caso di contemporanea richiesta esterna per un'emergenza che richieda la stessa postazione.
Sarebbero naturalmente da concordare sugli appositi tavoli deputati alla definizione dei protocolli operativi le migliori modalità per la gestione del sistema, ma anche in questo caso si tratterebbe di un semplice problema di ingegnerizzazione dei processi organizzativi, che una volta definiti dovrebbero solo essere implementati, avendo un'assoluta esigenza della certezza del dato reso disponibile a chi deve gestire l'emergenza.
Naturalmente al crescere delle disponibilità tecnologiche ed infrastrutturali presso Ospedali e 118 il sistema, che è intrinsecamente scalabile dal punto di vista tecnologico, potrà erogare servizi sempre più avanzati, divenendo una sorta di hub delle prestazioni erogabili in emergenza in ambito sanitario.

In conclusione, al di là degli esempi, per il Paese investire congrue risorse finanziarie nell'e-Health può solo aumentare l'efficienza del sistema sanitario, ridurre gli errori medici, aumentare la sicurezza dei pazienti e migliorare la gestione dei malati cronici, purché vi siano, però, specifiche e chiare politiche a garanzia della sicurezza e della privacy. ©